Jelaskan dimana peran Risk Management pada proses IT Audit? (perorangan)

Nama : Miftahul Fallah

Nim : 182420132

Kelas : MTI 20A

Jawaban :

Peran Risk Management pada proses IT Audit adalah Dalam manajemen risiko melibatkan seluruh bagian dari organisasi. Keterlibatan organisasi secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, *missing link*, atau inefisiensi pada kegiatan manajemen risiko.

Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko adalah fungsi manajemen risiko dan internal audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

Peran Internal Audit terkait Manajemen Risiko
Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.

Kolaborasi Fungsi Manajemen Risiko dan Internal Audit
Terdapat beberapa alasan yang mendasari paradigma bahwa fungsi manajemen risiko sebaiknya berkolaborasi dengan fungsi internal audit. Berdasarkan *case study* yang dilakukan oleh RIMS dan IIA, alasan-alasan tersebut adalah

- Untuk menghubungkan rencana audit dan penilaian risiko perusahaan, serta berbagi produk kerja lainnya. Hal ini dibutuhkan untuk meningkatkan koordinasi dalam usaha menjamin bahwa risiko-risiko utama dapat ditangani dengan efektif.
- Berbagi sumber daya-sumber daya tertentu untuk mendukung efisiensi. Sumber daya yang dimaksud termasuk sumber daya keuangan, manusia, dan waktu.
- Saling meningkatkan kompetensi, peran, dan tanggung jawab setiap fungsi. Menyediakan infrastruktur komunikasi yang konsisten.
- Menilai dan memantau risiko strategis. Dapat membentuk pemahaman yang lebih mendalam dan treatment yang fokus untuk mengatasi risiko strategis. Berdasarkan pengalamannya, *Irene Corbe (Whirlpool Corp.)* menyatakan bahwa pengadaan pertemuan dengan divisi manajemen risiko dapat meningkatkan pemahaman fungsi audit internal terhadap profil risiko perusahaan.

Nama : Moh Fajri Al Amin

Nim : 182420121

Kelas : MTI 20A

Jawaban :

Fungsi manajemen risiko merupakan bagian dari manajemen organisasi. Tanggung jawab dari fungsi manajemen risiko antara lain:

- Menyediakan kerangka manajemen risiko bagi organisasi.
- Mengidentifikasi isu-isu baru atau perubahan-2 yang signifikan.
- Mengkoordinasi dan membantu manajemen dalam mendesain proses dan pengendalian untuk mengelola risiko dan isu-isu, dengan cara antara lain fasilitasi, memberikan panduan, dan pelatihan.
- Memfasilitasi, mengkoordinasi, dan memonitor implementasi praktik manajemen risiko yang efektif terhadap para manajer dan personil, termasuk koordinasi pelaporan dan tindakan koreksi yang diperlukan.

Peran Internal Audit terkait Manajemen Risiko
Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.

Kolaborasi Fungsi Manajemen Risiko dan Internal Audit
Terdapat beberapa alasan yang mendasari paradigma bahwa fungsi manajemen risiko sebaiknya berkolaborasi dengan fungsi internal audit. Berdasarkan *case study* yang dilakukan oleh RIMS dan IIA, alasan-alasan tersebut adalah

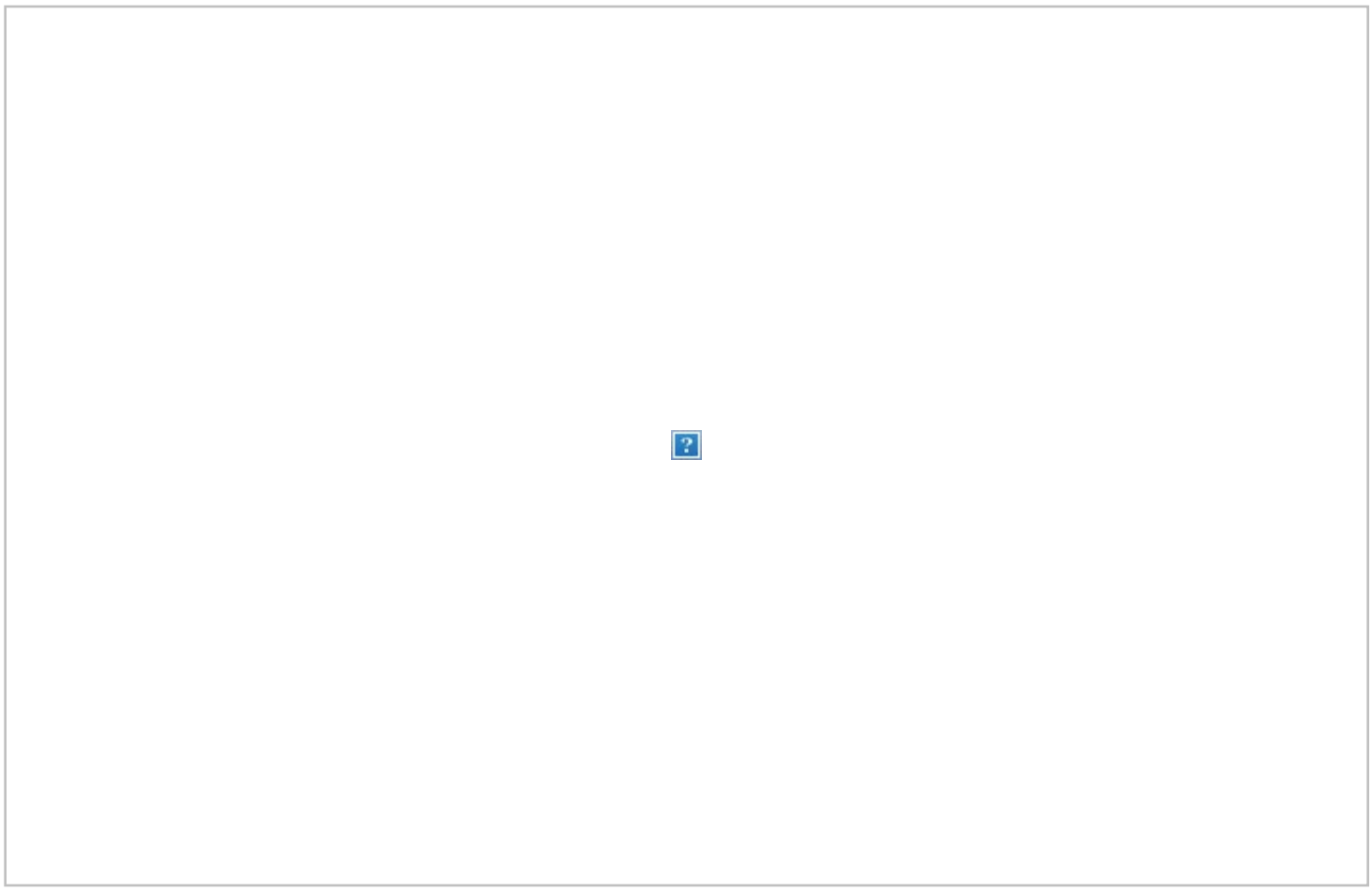
- Untuk menghubungkan rencana audit dan penilaian risiko perusahaan, serta berbagi produk kerja lainnya. Hal ini dibutuhkan untuk meningkatkan koordinasi dalam usaha menjamin bahwa risiko-risiko utama dapat ditangani dengan efektif.
- Berbagi sumber daya-sumber daya tertentu untuk mendukung efisiensi. Sumber daya yang dimaksud termasuk sumber daya keuangan, manusia, dan waktu.
- Saling meningkatkan kompetensi, peran, dan tanggung jawab setiap fungsi. Menyediakan infrastruktur komunikasi yang konsisten.
- Menilai dan memantau risiko strategis. Dapat membentuk pemahaman yang lebih mendalam dan treatment yang fokus untuk mengatasi risiko strategis. Berdasarkan pengalamannya, *Irene Corbe (Whirlpool Corp.)* menyatakan bahwa pengadaan pertemuan dengan divisi manajemen risiko dapat meningkatkan pemahaman fungsi audit internal terhadap profil risiko perusahaan.

FUNGSI MANAJEMEN RISIKO DAN INTERNAL AUDIT

Berdasarkan ISO31000: 2009 *Risk Management – Principles and Guidelines*, praktik terbaik manajemen risiko melibatkan seluruh bagian dari organisasi. Keterlibatan organisasi secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, *missing link*, atau inefisiensi pada kegiatan manajemen risiko.

Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko adalah fungsi manajemen risiko dan internal audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

Gambar 1 Perubahan Sasaran dan Aktivitas Kunci dari Fungsi Manajemen Risiko



Sumber: The Risk Perspective, Executive Summary (2012).

Gambar 1 mendeskripsikan perkembangan fungsi manajemen risiko yang dijelaskan oleh *Risk and Insurance Management Society* (RIMS). Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi. *Integrated risk management* menerapkan kegiatan pencegahan dan pengurangan dampak negatif dari risiko. Seiring berjalannya waktu, manajemen risiko yang tadinya berperan untuk melindungi kegagalan organisasi, berubah menjadi komponen *competitive advantage* bagi organisasi. Selain menciptakan kerangka kerja dan proses manajemen

risiko dalam menghadapi risiko, fungsi manajemen risiko juga meningkatkan kapabilitas organisasi dalam mengejar peluang. Fungsi ini juga meningkatkan kemampuan pengambilan keputusan strategis organisasi melalui penyediaan informasi yang relevan dan komprehensif. Dalam menciptakan manajemen risiko yang efektif bagi organisasi, fungsi manajemen risiko berkolaborasi dengan fungsi internal audit.

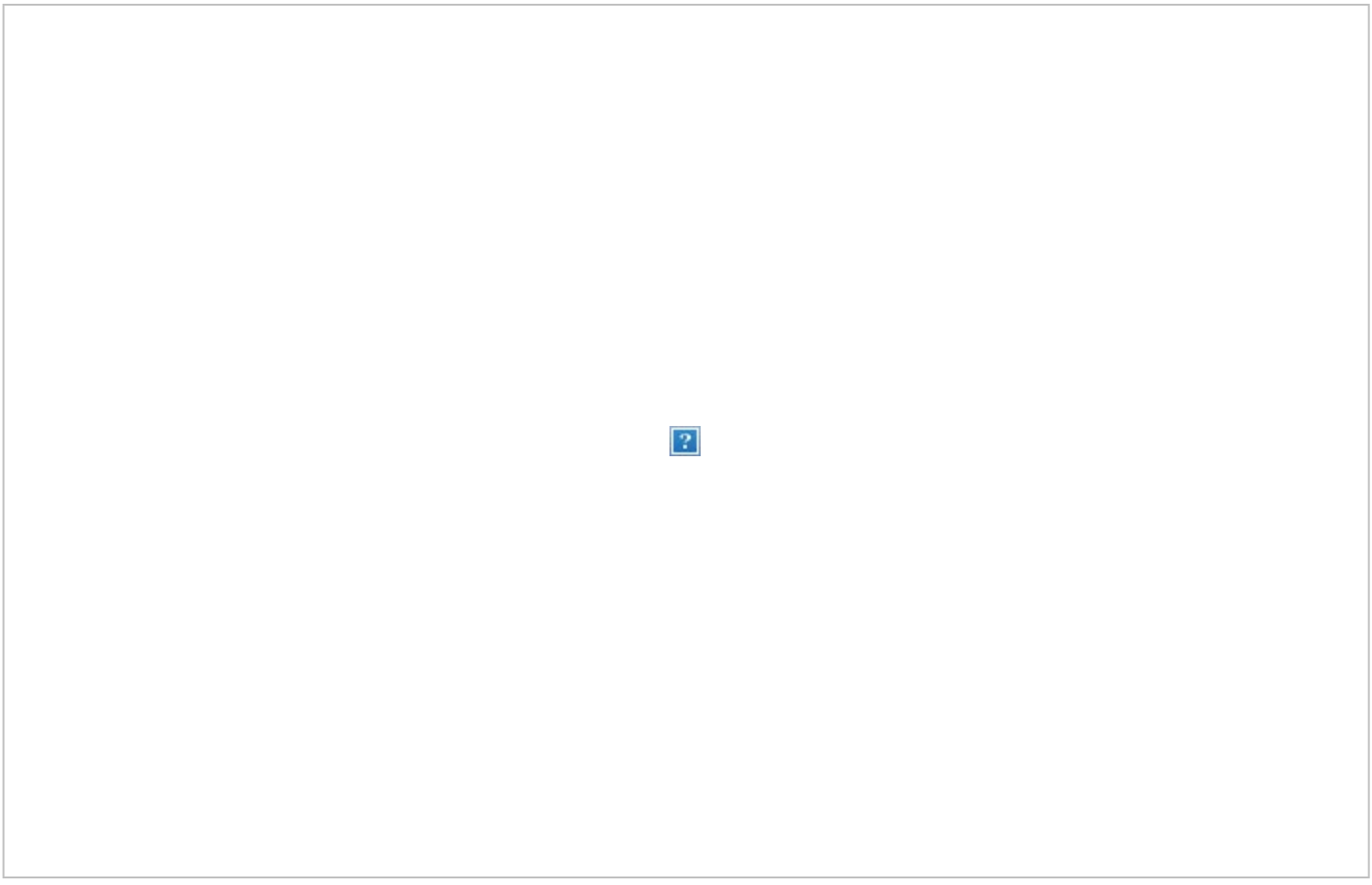
Peran Internal Audit terkait Manajemen Risiko

Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.

Gambar 2 Tanggung Jawab Internal Audit Terkait Manajemen Risiko



Sumber: *The Role of Internal Auditing In E nterprise-Wide Risk Management.* (2009).

Hal yang perlu disoroti dari Gambar 2 adalah “tanggung jawab kegiatan manajemen risiko yang tidak boleh didelegasikan kepada internal audit”. Untuk menjaga efektivitas kegiatan audit internal, tanggung jawab yang diberikan terhadap auditor internal terkait kegiatan manajemen risiko harus didesain agar tidak mengganggu independensinya. Hal

ini dikarenakan internal audit memiliki peran penting dalam melakukan pengawasan, pemantauan, dan penilaian terhadap efektivitas pengendalian internal dan kegiatan manajemen risiko organisasi. Pemberian tanggung jawab kepada auditor internal untuk menentukan risk appetite, membentuk *risk management process,* dan sebagainya dapat menimbulkan *clash of interest* yang berpotensi untuk mengganggu penilaian mereka pada efektivitas manajemen risiko.

Kolaborasi Fungsi Manajemen Risiko dan Internal Audit
Terdapat beberapa alasan yang mendasari paradigma bahwa fungsi manajemen risiko sebaiknya berkolaborasi dengan fungsi internal audit. Berdasarkan *case study* yang dilakukan oleh RIMS dan IIA, alasan-alasan tersebut adalah

- Untuk menghubungkan rencana audit dan penilaian risiko perusahaan, serta berbagi produk kerja lainnya. Hal ini dibutuhkan untuk meningkatkan koordinasi dalam usaha menjamin bahwa risiko-risiko utama dapat ditangani dengan efektif.
- Berbagi sumber daya-sumber daya tertentu untuk mendukung efisiensi. Sumber daya yang dimaksud termasuk sumber daya keuangan, manusia, dan waktu.
- Saling meningkatkan kompetensi, peran, dan tanggung jawab setiap fungsi. Menyediakan infrastruktur komunikasi yang konsisten.
- Menilai dan memantau risiko strategis. Dapat membentuk pemahaman yang lebih mendalam dan treatment yang fokus untuk mengatasi risiko strategis. Berdasarkan pengalamannya, *Irene Corbe (Whirlpool Corp.)* menyatakan bahwa pengadaan pertemuan dengan divisi manajemen risiko dapat meningkatkan pemahaman fungsi audit internal terhadap profil risiko perusahaan.

Berikut adalah contoh yang menggambarkan kolaborasi fungsi manajemen risiko dan internal audit pada beberapa perusahaan internasional:

- Cisco Systems

- Hospital Corporation of America

- Whirlpool Corporation

Sumber : ***https://crmsindonesia.org/publications/fungsi-manajemen-risiko-dan-internal-audit/***

Peran Risk Management pada proses IT Audit adalah bertugas untuk mengarahkan praktik enterprise risk management pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi. Integrated risk management menerapkan kegiatan pencegahan dan pengurangan dampak negatif dari risiko. Seiring berjalannya waktu, manajemen risiko yang tadinya berperan untuk melindungi kegagalan organisasi, berubah menjadi komponen competitive advantage bagi organisasi. Selain menciptakan kerangka kerja dan proses manajemen risiko dalam menghadapi risiko, fungsi manajemen risiko juga meningkatkan kapabilitas organisasi dalam mengejar peluang. Fungsi ini juga meningkatkan kemampuan pengambilan keputusan strategis organisasi melalui penyediaan informasi yang relevan dan komprehensif. Dalam menciptakan manajemen risiko yang efektif bagi organisasi, fungsi manajemen risiko berkolaborasi dengan fungsi internal audit.

Terima kasih, salam.

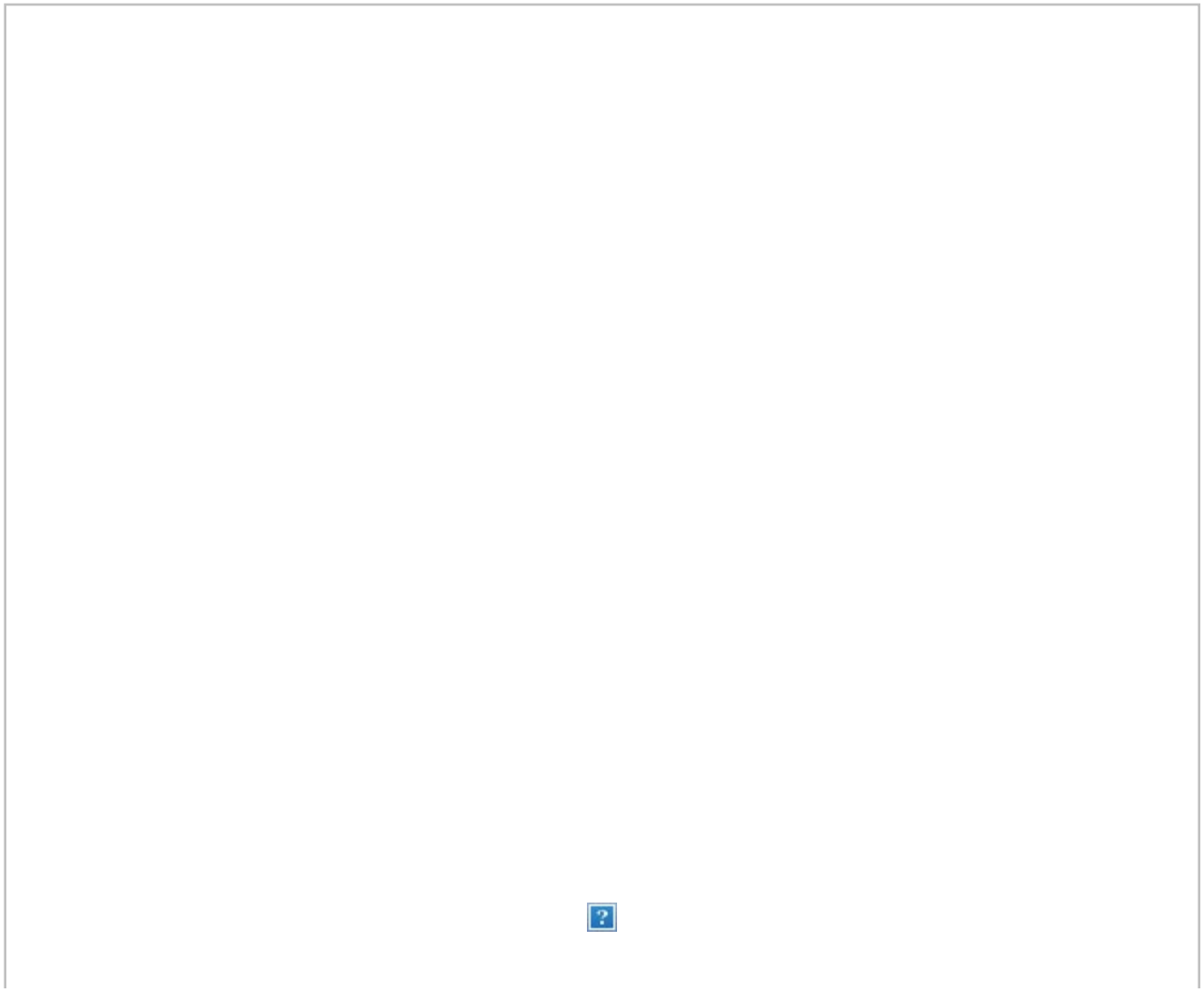
IT risk management (manajemen resiko teknologi informasi) adalah proses yang dilakukan oleh para manajer IT untuk menyeimbangkan kegiatan operasional dan pengeluaran *cost* dalam mencapai keuntungan dengan melindungi sistem IT dan data yang medukung misi organisasinya. Menurut G. Stoneburner 2002, *IT risk management* meliputi tiga proses:

1. *Risk Assessment*
2. *Risk Mitigation*
3. *Evaluation and assessment*

1. *Risk Assessment*

Penilaian resiko *(risk assessment)* merupakan proses awal di dalam metodologi manajemen resiko. Secara lebih spesifik sejak dikeluarkannya COSO *Internal Control Integrated Framework*, *risk assessment* dengan tegas dianggap sebagai salah satu komponen dari sistem *internal control* (Woods; 2007).

Organisasi menggunakan *risk assessment* untuk menentukan tingkat ancaman yang potensial dan resiko yang berhubungan dengan suatu sistem IT seluruh *System Development Life Cycle* (SDLC). Output hasil dari proses ini membantu kearah mengidentifikasi kendali yang sesuai untuk mengurangi atau menghapuskan resiko sepanjang/ketika proses peringanan resiko *(risk mitigation).* Untuk menentukan kemungkinan suatu peristiwa/kejadian masa depan yang kurang baik, ancaman pada suatu sistem IT harus dianalisis bersama dengan *vulnerability* yang potensial dan pengendalian pada tempatnya untuk sistem IT. Menurut G. Stoneburner (2002) metodologi penilaian resiko meliputi sembilan langkah, sebagai berikut:



2. *Risk Mitigation*

Risk mitigation adalah satu langkah yang melibatkan usaha-usaha untuk memprioritaskan, mengevaluasi dan menjalankan kontrol atau pengendalian yang dapat mengurangi resiko yang tepat yang direkomendasikan dari proses *risk assessment* (Stoneburner; 2002). *Risk mitigation* biasanya dilakukan dengan memenuhi pendekatan biaya terendah *(least-cost approach)* dan melaksanakan kontrol atau pengendalian yang paling tepat *(the most appropriate controls)* sehingga dapat mengurangi resiko ke dalam tingkat yang dapat diterima dengan resiko yang paling minim *(minimal adverse impact)* terhadap sumber daya dan tujuan organisasi.

3. *Evaluation and Assessment*

Pada umumnya, di dalam suatu organisasi, jaringan secara terus menerus akan diperluas dan diperbaharui, komponen diubah dan aplikasi software-nya diganti atau diperbaharui dengan versi yang lebih baru. Perubahan ini berarti bahwa, resiko baru akan timbul dan resiko yang sebelumnya dikurangi, akan menjadi suatu perhatian. Demikian seterusnya, sehingga manajemen resiko akan berkembang.

Manajemen resiko seharusnya diselenggarakan dan terintergrasi dengan SDLC untuk sistem IT, bukan dikarenakan untuk kepentingan hukum atau regulasi, melainkan suatu *"good practice"* dan dukungan bisnis organisasi secara objektif atau berdasarkan misi.

https://itgid.org/3-proses-it-risk-management/

Peran RRisk Management pada proses IT Audit adalah bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi.

Gambar perubahan Sasaran dan Aktivitas Kunci dari Fungsi Manajemen Risiko mendeskripsikan perkembangan fungsi manajemen risiko yang dijelaskan oleh *Risk and Insurance Management Society* (RIMS).

Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi. *Integrated risk management* menerapkan kegiatan pencegahan dan pengurangan dampak negatif dari risiko. Seiring berjalannya waktu, manajemen risiko yang tadinya berperan untuk melindungi kegagalan organisasi, berubah menjadi komponen *competitive advantage* bagi organisasi. Selain menciptakan kerangka kerja dan proses manajemen risiko dalam menghadapi risiko, fungsi manajemen risiko juga meningkatkan kapabilitas organisasi dalam mengejar peluang. Fungsi ini juga meningkatkan kemampuan pengambilan keputusan strategis organisasi melalui penyediaan informasi yang relevan dan komprehensif. Dalam menciptakan manajemen risiko yang efektif bagi organisasi, fungsi manajemen risiko berkolaborasi dengan fungsi internal audit.

Berdasarkan ISO31000: 2009 Risk Management – Principles and Guidelines, praktik terbaik manajemen risiko melibatkan seluruh bagian dari organisasi. Keterlibatan organisasi secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, missing link, atau inefisiensi pada kegiatan manajemen risiko. Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko adalah fungsi manajemen risiko dan internal audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko bertugas untuk mengarahkan praktik enterprise risk management pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko. Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi. Integrated risk management menerapkan kegiatan pencegahan dan pengurangan dampak negatif dari risiko. Seiring berjalannya waktu, manajemen risiko yang tadinya berperan untuk melindungi kegagalan organisasi, berubah menjadi komponen competitive advantage bagi organisasi. Selain menciptakan kerangka kerja dan proses manajemen risiko dalam menghadapi risiko, fungsi manajemen risiko juga meningkatkan kapabilitas organisasi dalam mengejar peluang. Fungsi ini juga meningkatkan kemampuan pengambilan keputusan strategis organisasi melalui penyediaan informasi yang relevan dan komprehensif. Dalam menciptakan manajemen risiko yang efektif bagi organisasi, fungsi manajemen risiko berkolaborasi dengan fungsi internal audit. Peran Internal Audit terkait Manajemen Risiko Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses governance. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan: memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif. Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.Untuk menjaga efektivitas kegiatan audit internal, tanggung jawab yang diberikan terhadap auditor internal terkait kegiatan manajemen risiko harus didesain agar tidak mengganggu independensinya. Hal ini dikarenakan internal audit memiliki peran penting dalam melakukan pengawasan, pemantauan, dan penilaian terhadap efektivitas pengendalian internal dan kegiatan manajemen risiko organisasi. Pemberian tanggung jawab kepada auditor internal untuk menentukan risk appetite, membentuk risk management process, dan sebagainya dapat menimbulkan clash of interest yang berpotensi untuk mengganggu penilaian mereka pada efektivitas manajemen risiko.

--> manajemen risiko melibatkan seluruh bagian dari organisasi/Perusahaan IT. Keterlibatan organisasi/Perusahaan IT secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, *missing link*, atau inefisiensi pada kegiatan manajemen risiko.

-->Peran manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada proses IT Audit, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi/perusahaan IT. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

-->Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi.

IT Risk Management- (manajemen resiko teknologi informasi) adalah proses yang dilakukan oleh para manajer IT untuk menyeimbangkan kegiatan operasional dan pengeluaran *cost* dalam mencapai keuntungan dengan melindungi sistem IT dan data yang medukung misi organisasinya.

1. Risk Assesment - Penilaian resiko *(risk assessment)* merupakan proses awal di dalam metodologi manajemen resiko. Secara lebih spesifik sejak dikeluarkannya COSO *Internal Control Integrated Framework*, *risk assessment* dengan tegas dianggap sebagai salah satu komponen dari sistem *internal control.* Organisasi menggunakan *risk assessment* untuk menentukan tingkat ancaman yang potensial dan resiko yang berhubungan dengan suatu sistem IT seluruh *System Development Life Cycle* (SDLC). Output hasil dari proses ini membantu kearah mengidentifikasi kendali yang sesuai untuk mengurangi atau menghapuskan resiko sepanjang/ketika proses peringanan resiko *(risk mitigation).* Untuk menentukan kemungkinan suatu peristiwa/kejadian masa depan yang kurang baik, ancaman pada suatu sistem IT harus dianalisis bersama dengan *vulnerability* yang potensial dan pengendalian pada tempatnya untuk sistem IT.

2. *Risk Mitigation* - adalah satu langkah yang melibatkan usaha-usaha untuk memprioritaskan, mengevaluasi dan menjalankan kontrol atau pengendalian yang dapat mengurangi resiko yang tepat yang direkomendasikan dari proses *risk assessment*. *Risk mitigation* biasanya dilakukan dengan memenuhi pendekatan biaya terendah *(least-cost approach)* dan melaksanakan kontrol atau pengendalian yang paling tepat *(the most appropriate controls)* sehingga dapat mengurangi resiko ke dalam tingkat yang dapat diterima dengan resiko yang paling minim *(minimal adverse impact)* terhadap sumber daya dan tujuan organisasi.

3. Evalution dan Assessment - Pada umumnya, di dalam suatu organisasi, jaringan secara terus menerus akan diperluas dan diperbaharui, komponen diubah dan aplikasi software-nya diganti atau diperbaharui dengan versi yang lebih baru. Perubahan ini berarti bahwa, resiko baru akan timbul dan resiko yang sebelumnya dikurangi, akan menjadi suatu perhatian. Demikian seterusnya, sehingga manajemen resiko akan berkembang. Manajemen resiko seharusnya diselenggarakan dan terintergrasi dengan SDLC untuk sistem IT, bukan dikarenakan untuk kepentingan hukum atau regulasi, melainkan suatu *"good practice"* dan dukungan bisnis organisasi secara objektif atau berdasarkan misi.

Berdasarkan dari penjelasan 3 proses Risk Management di atas, peran Risk management pada IT Audit terletak pada bagia **Evaluation dan Assessment** karena IT Audit senidii adalah sebuah bentuk pengawasan dan pengendalian infrastruktur IT secara menyeluruh yang dapat berjalan bersama-sama dengan audit finania dan audit internal, atau dengan kegiatan pengawaan dan evaluasi lain yang sejenisnya

Nama : Rio Permata

NIM : 182420108

Kelas : MTI B

Manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

tugas Risk Management

Fungsi manajemen risiko merupakan bagian dari manajemen organisasi. Tanggung jawab dari fungsi manajemen risiko antara lain:

- Menyediakan kerangka manajemen risiko bagi organisasi.
- Mengidentifikasi isu-isu baru atau perubahan-2 yang signifikan.
- Mengkoordinasi dan membantu manajemen dalam mendesain proses dan pengendalian untuk mengelola risiko dan isu-isu, dengan cara antara lain fasilitasi, memberikan panduan, dan pelatihan.
- Memfasilitasi, mengkoordinasi, dan memonitor implementasi praktik manajemen risiko yang efektif terhadap para manajer dan personil, termasuk koordinasi pelaporan dan tindakan koreksi yang diperlukan.

Kami perlu menekankan bahwa identifikasi dan analisis risiko, serta pengembangan dan implementasi pengendalian merupakan tanggung jawab pemilik risiko, yaitu unit kerja dan para personil, bukan unit manajemen risiko.

IT risk management (manajemen resiko teknologi informasi) adalah proses yang dilakukan oleh para manajer IT untuk menyeimbangkan kegiatan operasional dan pengeluaran *cost* dalam mencapai keuntungan dengan melindungi sistem IT dan data yang medukung misi organisasinya. Menurut G. Stoneburner 2002, *IT risk management* meliputi tiga proses:

1. Risk Assessment

2. Risk Mitigation

3. Evaluation and assessment

1. *Risk Assessment*

Penilaian resiko *(risk assessment)* merupakan proses awal di dalam metodologi manajemen resiko. Secara lebih spesifik sejak dikeluarkannya COSO *Internal Control Integrated Framework*, *risk assessment* dengan tegas dianggap sebagai salah satu komponen dari sistem *internal control* (Woods; 2007).

2. *Risk Mitigation*

Risk mitigation adalah satu langkah yang melibatkan usaha-usaha untuk memprioritaskan, mengevaluasi dan menjalankan kontrol atau pengendalian yang dapat mengurangi resiko yang tepat yang direkomendasikan dari proses *risk assessment* (Stoneburner; 2002). *Risk mitigation* biasanya dilakukan dengan memenuhi pendekatan biaya terendah *(least-cost approach)* dan melaksanakan kontrol atau pengendalian yang paling tepat *(the most appropriate controls)* sehingga dapat mengurangi resiko ke dalam tingkat yang dapat diterima dengan resiko yang paling minim *(minimal adverse impact)* terhadap sumber daya dan tujuan organisasi.

3. *Evaluation and Assessment*

Pada umumnya, di dalam suatu organisasi, jaringan secara terus menerus akan diperluas dan diperbaharui, komponen diubah dan aplikasi software-nya diganti atau diperbaharui dengan versi yang lebih baru. Perubahan ini berarti bahwa, resiko baru akan timbul dan resiko yang sebelumnya dikurangi, akan menjadi suatu perhatian. Demikian seterusnya, sehingga manajemen resiko akan berkembang.

Peran Internal Audit terkait Manajemen Risiko

Institute of Internal Auditors (IIA), Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses governance. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi.

Menurut Pendapat

Setiap proses bisnis memiliki risiko, demikian halnya dengan proses TI. Risiko yang terkait dengan TI yakni IT Risk(risiko TI) adalah risiko bisnis yang terkait dengan penggunaan, kepemilikan, pengoperasian, keterlibatan, pengaruh dan penerapan TI dalam suatu organisasi. Risiko TI menjadi bahan pertimbangan prioritas proses TI yang akan diaudit. Oleh karena itu, digunakan audit berbasis risiko yakni audit yang dilakukan berdasarkan proses-proses yang memiliki potensi risiko yang tinggi atau pada proses kritikal yang berdampak negatif jika terjadi masalah. Dalam melakukan analisis risiko didukung oleh Risk IT Framework yang menyediakan framework untuk mengidentifikasi, mengendalikan, dan mengelola risiko TI. Domain yang digunakan adalah domain Risk Evaluation. Kombinasi dari COBIT Versi 4.1 dan Risk IT sangat cocok digunakan dalam audit penerapan TI di Perguruan Tinggi XYZ karena audit akan lebih terfokus pada proses kritikal dan tidak terjebak pada proses yang kurang berisiko. Untuk itu, rumusan masalah dalam penelitian ini adalah bagaimana tingkat kematangan TI di Perguruan Tinggi XYZ dari hasil audit TI berbasis risiko dengan framework COBIT Versi 4.1 dan bagaimana rekomendasi dari hasil audit TI untuk meningkatkan performansi TIdi Perguruan Tinggi XYZ.Manfaat yang akan diperoleh dari penelitian ini adalah memperoleh hasil evaluasi yang dapat digunakan untuk menyelaraskan TI dengan tujuan Perguruan Tinggi XYZ, membangun kesadaran dan tanggung jawab atas risiko TI, meningkatkan performansi IT untuk menuju World Class University, dan persiapan menghadapi audit eksternal.

Internal audit seharusnya menghindari aktifitas berikut yang dapat mengganggu independensi dan objektifitas, yaitu:

1. Menentukan risk appetite.
2. Memiliki atau mengelola risiko (lini pertama).
3. Memegang tanggung jawab untuk akuntansi, pengembangan bisnis, dan fungsi lini pertama lainnya.
4. Menetapkan keputusan respon terhadap risiko, dengan mengatasnamakan manajemen.
5. Menerapkan atau memegang pertanggung jawaban untuk proses manajemen risiko atau tata kelola.
6. Melaksanakan penugasan asurans terhadap aktifitas lini kedua yang dilaksanakan oleh internal audit.

Peran Risk Management pada proses IT Audit

Risk Management mengelola risiko bisnis menggunakan kerangka manajemen risiko teknologi informasi sehingga tata kelola dan proses kepastian audit dapat dilakukan secara menyeluruh

Peran teknologi informasi (TI) bagi kita semua sudah sedemikian penting baik untuk kebutuhan pribadi, personal, maupun bisnis. Oleh karena itu, insiden atau peristiwa penting dalam industri ini tentunya akan mempengaruhi aset maupun bisnis perusahaan, termasuk kehilangan penerimaan dan berakibat buruk bagi nama baik perusahaan. Agar tercapai tata kelola teknologi (*Technology Governance*) dan program kepastian (*Assurance Program*) maka perlu dirancang melalui kerangka manajemen resiko (*IT risk management*) untuk memastikan manajemen pengendalian dan resiko berjalan efektif.

Berdasarkan ISO31000: 2009 *Risk Management – Principles and Guidelines*, praktik terbaik manajemen risiko melibatkan seluruh bagian dari organisasi. Keterlibatan organisasi secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, *missing link*, atau inefisiensi pada kegiatan manajemen risiko.

Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko adalah fungsi manajemen risiko dan internal audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

Gambar 1 mendeskripsikan perkembangan fungsi manajemen risiko yang dijelaskan oleh *Risk and Insurance Management Society* (RIMS). Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi. *Integrated risk management* menerapkan kegiatan pencegahan dan pengurangan dampak negatif dari risiko. Seiring berjalannya waktu, manajemen risiko yang tadinya berperan untuk melindungi kegagalan organisasi, berubah menjadi komponen *competitive advantage* bagi organisasi. Selain menciptakan kerangka kerja dan proses manajemen risiko dalam menghadapi risiko, fungsi manajemen risiko juga meningkatkan kapabilitas organisasi dalam mengejar peluang. Fungsi ini juga meningkatkan kemampuan pengambilan keputusan strategis organisasi melalui penyediaan informasi yang relevan dan komprehensif. Dalam menciptakan manajemen risiko yang efektif bagi organisasi, fungsi manajemen risiko berkolaborasi dengan fungsi internal audit.

Peran Internal Audit terkait Manajemen Risiko

Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.

Kolaborasi Fungsi Manajemen Risiko dan Internal Audit

Terdapat beberapa alasan yang mendasari paradigma bahwa fungsi manajemen risiko sebaiknya berkolaborasi dengan fungsi internal audit. Berdasarkan *case study* yang dilakukan oleh RIMS dan IIA, alasan-alasan tersebut adalah

- Untuk menghubungkan rencana audit dan penilaian risiko perusahaan, serta berbagi produk kerja lainnya. Hal ini dibutuhkan untuk meningkatkan koordinasi dalam usaha menjamin bahwa risiko-risiko utama dapat ditangani dengan efektif.
- Berbagi sumber daya-sumber daya tertentu untuk mendukung efisiensi. Sumber daya yang dimaksud termasuk sumber daya keuangan, manusia, dan waktu.
- Saling meningkatkan kompetensi, peran, dan tanggung jawab setiap fungsi. Menyediakan infrastruktur komunikasi yang konsisten.
- Menilai dan memantau risiko strategis. Dapat membentuk pemahaman yang lebih mendalam dan treatment yang fokus untuk mengatasi risiko strategis. Berdasarkan pengalamannya, *Irene Corbe (Whirlpool Corp.)* menyatakan bahwa pengadaan pertemuan dengan divisi manajemen risiko dapat meningkatkan pemahaman fungsi audit

internal terhadap profil risiko perusahaan.

Peran Risk Management pada proses IT Audit

Nama : Arie Ansyah
NIM : 182420117
Kelas : MTI 20A
Mata Kuliah : IT Audit

IT Risk Management

Merupakan proses yang digunakan untuk mengurangi dan mengelola risiko yang mungkin terjadi dalam infrastruktur IT yang ada atau sistem yang diterapkan dalam organisasi. Manajemen risiko memegang peranan penting sebagai tindakan perlindungan asset sistem dan teknologi informasi.

Manajemen risiko meliputi 3 proses besar yaitu:

1. Risk Assessment : adalah proses awal dalam manajemen risiko untuk memetakan tingkat ancaman yang potensial dan risiko yang ada dalam SDLC IT.
2. Risk Mitigation : adalah langkah yang melibatkan usaha untuk memprioritaskan, mengevaluasi dan menjalankan control atau pengendalian yang dapat mengurangi risiko yang tepat yang diinisiasi dari proses risk assessment.
3. Evaluation dan Assessment : evaluasi dan penilaian ulang terhadap risiko yang ada dan yang telah terjadi.

IT Audit

Merupakan bentuk pengawasan dan pengandalian dari infrastruktur teknologi informasi secara menyeluruh. Tujuan dari IT Audit adalah untuk meninjau dan mengevaluasi factor-faktor ketersediaan, kerahasiaan dan keutuhan (confidentiality, availability, integrity) dari sistem informasi organisasi.

Jenis-jenis IT Audit :

1. Sistem dan aplikasi, yaitu audit yang berfungsi untuk memeriksa apakah system dan aplikasi sesuai dengan kebutuhan organisasi, dan memiliki control yang cukup baik untuk menjamin keabsahan, kehandalan, tepat waktu dan keamanan pada input, proses dan output pada semua kegiatan sistem.
2. Fasilitas pemrosesan informasi, yaitu jenis audit yang berfungsi untuk memeriksa apakah fasilitas pemrosesan terkendali untuk menjamin ketepatan

waktu, ketelitian dan pemrosesan aplikasi yang efisien dalam keadaan normal dan buruk.

3. Pengembangan Sistem, yaitu jenis audit yang berfungsi untuk memeriksa apakah sistem yang dikembangkan mencakup kebutuhan obyektif organisasi.
4. Arsitektur perusahaan dan manajemen TI. Audit yang berfungsi untuk memeriksa apakah manajemen TI dapat mengembangkan struktur organisasi dan prosedur yang menjamin kontrol dan lingkungan yang berdaya guna untuk pemrosesan informasi.
5. Client/Server, Telekomunikasi, Intranet dan Internet. Suatu audit yang berfungsi untuk memeriksa apakah kontrol-kontrol berfungsi pada client, server, dan jaringan yang menghubungkan client dan server.

Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko adalah fungsi manajemen risiko dan internal audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

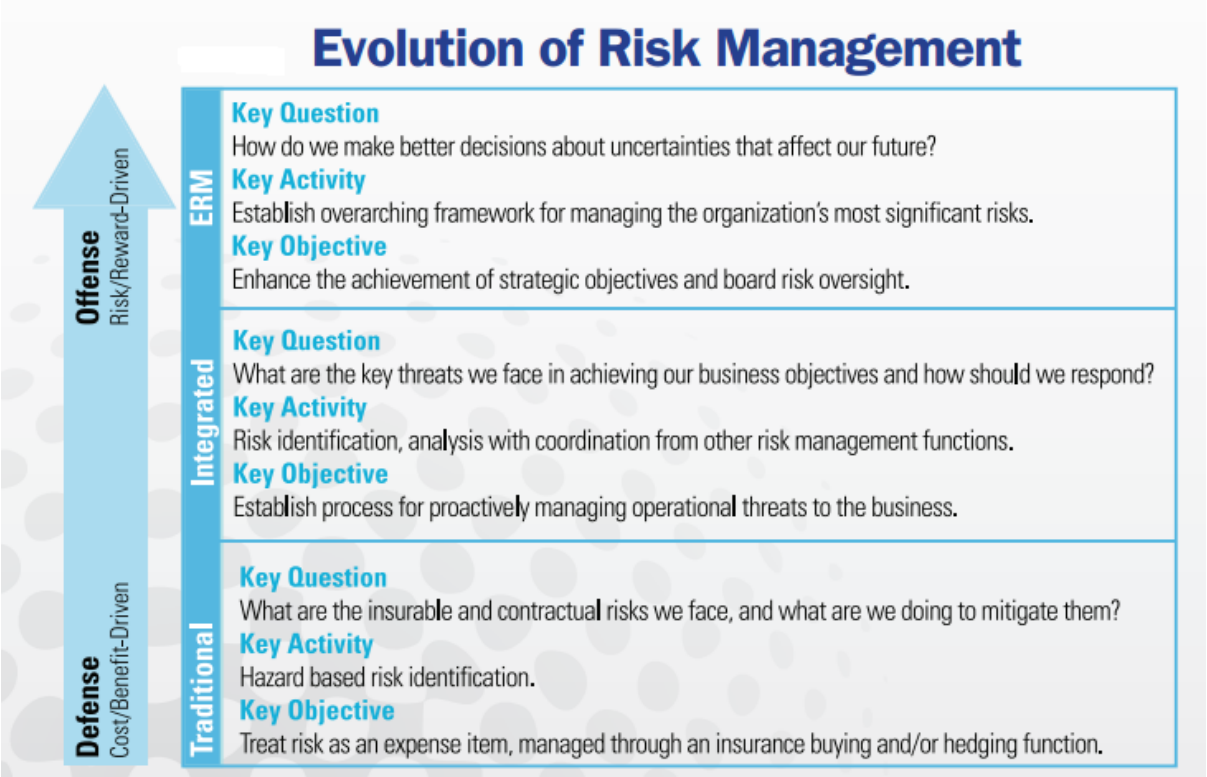
FUNGSI MANAJEMEN RISIKO DAN INTERNAL AUDIT

Berdasarkan ISO31000: 2009 *Risk Management – Principles and Guidelines*, praktik terbaik manajemen risiko melibatkan seluruh bagian dari organisasi. Keterlibatan organisasi secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, *missing link*, atau inefisiensi pada kegiatan manajemen risiko.

Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko adalah fungsi manajemen risiko dan internal audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan

fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

Gambar 1 Perubahan Sasaran dan Aktivitas Kunci dari Fungsi Manajemen Risiko



Sumber: The Risk Perspective, Executive Summary (2012).

Gambar 1 mendeskripsikan perkembangan fungsi manajemen risiko yang dijelaskan oleh *Risk and Insurance Management Society* (RIMS). Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi. *Integrated risk management* menerapkan kegiatan pencegahan dan pengurangan dampak negatif dari risiko. Seiring berjalannya waktu, manajemen risiko yang tadinya berperan untuk melindungi kegagalan organisasi, berubah menjadi komponen *competitive advantage* bagi organisasi. Selain menciptakan kerangka kerja dan proses manajemen risiko dalam menghadapi risiko, fungsi manajemen risiko juga meningkatkan kapabilitas organisasi dalam mengejar peluang.

Fungsi ini juga meningkatkan kemampuan pengambilan keputusan strategis organisasi melalui penyediaan informasi yang relevan dan komprehensif. Dalam menciptakan manajemen risiko yang efektif bagi organisasi, fungsi manajemen risiko berkolaborasi dengan fungsi internal audit.

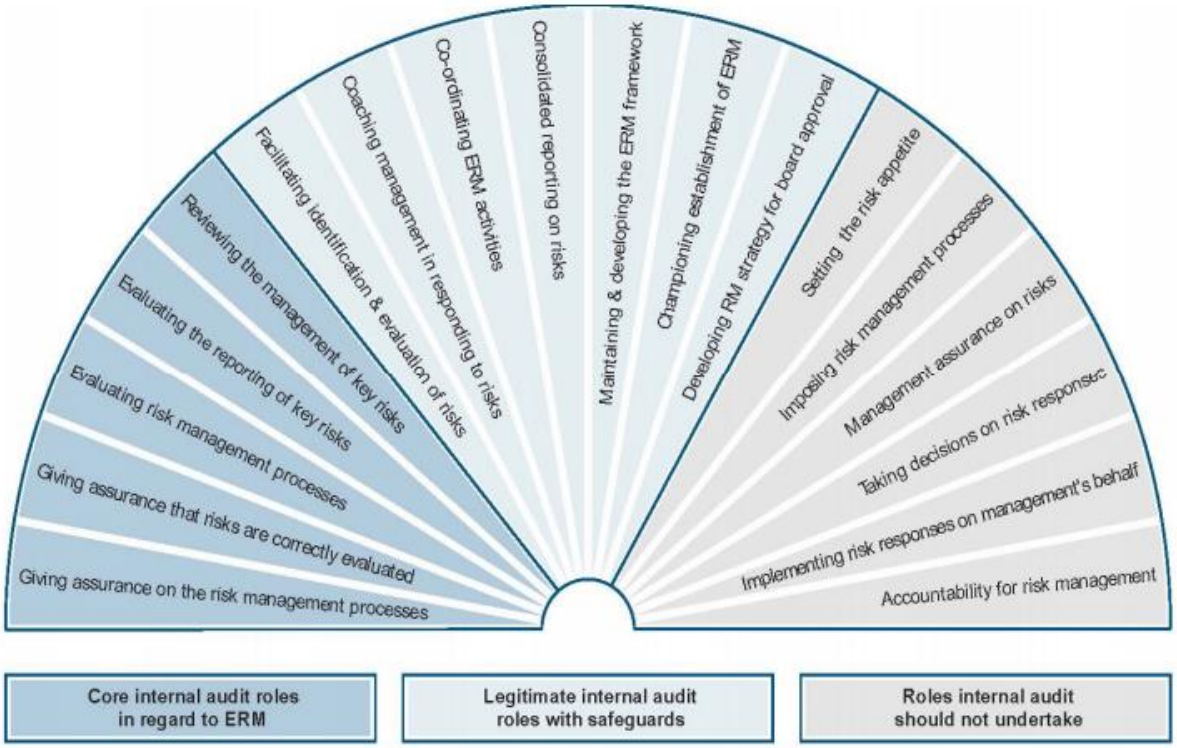
Peran Internal Audit terkait Manajemen Risiko

Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.

Gambar 2 Tanggung Jawab Internal Audit Terkait Manajemen Risiko



Sumber: *The Role of Internal Auditing In E nterprise-Wide Risk Management.* (2009).

Hal yang perlu disoroti dari Gambar 2 adalah "tanggung jawab kegiatan manajemen risiko yang tidak boleh didelegasikan kepada internal audit". Untuk menjaga efektivitas kegiatan audit internal, tanggung jawab yang diberikan terhadap auditor internal terkait kegiatan manajemen risiko harus didesain agar tidak mengganggu independensinya. Hal ini dikarenakan internal audit memiliki peran penting dalam melakukan pengawasan, pemantauan, dan penilaian terhadap efektivitas pengendalian internal dan kegiatan manajemen risiko organisasi. Pemberian tanggung jawab kepada auditor internal untuk menentukan risk appetite, membentuk *risk management process,* dan sebagainya dapat menimbulkan *clash of interest* yang berpotensi untuk mengganggu penilaian mereka pada efektivitas manajemen risiko.

Kolaborasi Fungsi Manajemen Risiko dan Internal Audit

Terdapat beberapa alasan yang mendasari paradigma bahwa fungsi manajemen risiko sebaiknya berkolaborasi dengan fungsi internal audit. Berdasarkan *case study* yang dilakukan oleh RIMS dan IIA, alasan-alasan tersebut adalah

- Untuk menghubungkan rencana audit dan penilaian risiko perusahaan, serta berbagi produk kerja lainnya. Hal ini dibutuhkan untuk meningkatkan koordinasi dalam usaha menjamin bahwa risiko-risiko utama dapat ditangani dengan efektif.
- Berbagi sumber daya-sumber daya tertentu untuk mendukung efisiensi. Sumber daya yang dimaksud termasuk sumber daya keuangan, manusia, dan waktu.
- Saling meningkatkan kompetensi, peran, dan tanggung jawab setiap fungsi. Menyediakan infrastruktur komunikasi yang konsisten.
- Menilai dan memantau risiko strategis. Dapat membentuk pemahaman yang lebih mendalam dan treatment yang fokus untuk mengatasi risiko strategis. Berdasarkan pengalamannya, *Irene Corbe (Whirlpool Corp.)* menyatakan bahwa pengadaan pertemuan dengan divisi manajemen risiko dapat meningkatkan pemahaman fungsi audit internal terhadap profil risiko perusahaan.

Kolaborasi antara fungsi manajemen risiko dan internal audit merupakan sebuah inisiasi yang dapat mendatangkan manfaat pada berbagai jenis perusahaan. Menurut RIMS dan IIA, manfaat-manfaat yang dapat diperoleh dari kolaborasi tersebut berupa:

1. Memastikan bahwa risiko-risiko kritikal telah diidentifikasi secara efektif;
2. Penggunaan sumber daya langka dengan efisien;
3. Komunikasi yang dalam dan konsisten, terutama pada level Board dan manajemen;
4. Pengertian yang lebih dalam dan penanganan yang terfokus pada risiko yang paling signifikan terhadap pencapaian tujuan organisasi.

Komunikasi secara terbuka dan konsisten merupakan metode utama yang dapat diterapkan dalam kolaborasi kedua fungsi ini. Komunikasi dapat membangun pendalaman pandangan terhadap risiko-risiko yang melekat pada organisasi dan meningkatkan kapabilatas tiap divisi untuk mengelola risiko-risiko tersebut. Namun kolaborasi tersebut harus memiliki batasan yang jelas mengenai tanggung jawab dan peran setiap fungsinya. Kolaborasi yang dilakukan juga harus disesuaikan dengan karakteristik dan tujuan perusahaan.

Peran Internal Audit terkait Manajemen Risiko

Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses governance. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi.

IT risk management adalah usaha untuk mengelola risiko bisnis menggunakan kerangka manajemen risiko teknologi informasi sehingga tata kelola dan proses kepastian audit dapat dilakukan secara menyeluruh atau biasa dikenal dengan IT *enterprise risk management (ERM) framework*.

Peran teknologi informasi (TI) bagi kita semua sudah sedemikian penting baik untuk kebutuhan pribadi, personal, maupun bisnis. Oleh karena itu, insiden atau peristiwa penting dalam industri ini tentunya akan mempengaruhi aset maupun bisnis perusahaan, termasuk kehilangan penerimaan dan berakibat buruk bagi nama baik perusahaan. Agar tercapai tata kelola teknologi (*Technology Governance*) dan program kepastian (*Assurance Program*) maka perlu dirancang melalui kerangka manajemen resiko (*IT risk management*) untuk memastikan manajemen pengendalian dan resiko berjalan efektif.

Sebagai catatan tambahan, kerangka di atas akan membuat departemen TI lebih memahami risiko operasional apa saja yang paling penting dan pengaruhnya terhadap kepentingan perusahaan secara umum.

IT Risk Management adalah usaha untuk mengelola risiko bisnis menggunakan kerangka IT Risk Management sehingga tata kelola dan proses kepastian audit dapat dilakukan secara menyeluruh atau biasa dikenal dengan IT enterprise risk management (ERM) framework. Tugas auditor berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

IT risk management (manajemen resiko teknologi informasi) adalah proses yang dilakukan oleh para manajer IT untuk menyeimbangkan kegiatan operasional dan pengeluaran cost dalam mencapai keuntungan dengan melindungi sistem IT dan data yang medukung misi organisasinya. Menurut G. Stoneburner 2002, IT risk management meliputi tiga proses:

1. Risk Assessment

Penilaian resiko (risk assessment) merupakan proses awal di dalam metodologi manajemen resiko. Secara lebih spesifik sejak dikeluarkannya COSO Internal Control Integrated Framework, risk assessment dengan tegas dianggap sebagai salah satu komponen dari sistem internal control (Woods; 2007). Organisasi menggunakan risk assessment untuk menentukan tingkat ancaman yang potensial dan resiko yang berhubungan dengan suatu sistem IT seluruh System Development Life Cycle (SDLC). Output hasil dari proses ini membantu kearah mengidentifikasi kendali yang sesuai untuk mengurangi atau menghapuskan resiko sepanjang/ketika proses peringanan resiko (risk mitigation). Untuk menentukan kemungkinan suatu peristiwa/kejadian masa depan yang kurang baik, ancaman pada suatu sistem IT harus dianalisis bersama dengan vulnerability yang potensial dan pengendalian pada tempatnya untuk sistem IT.

1. Risk Mitigation

Risk mitigation adalah satu langkah yang melibatkan usaha-usaha untuk memprioritaskan, mengevaluasi dan menjalankan kontrol atau pengendalian yang dapat mengurangi resiko yang tepat yang direkomendasikan dari proses risk assessment (Stoneburner; 2002). Risk mitigation biasanya dilakukan dengan memenuhi pendekatan biaya terendah (least-cost approach) dan melaksanakan kontrol atau pengendalian yang paling tepat (the most appropriate controls) sehingga dapat mengurangi resiko ke dalam tingkat yang dapat diterima dengan resiko yang paling minim (minimal adverse impact) terhadap sumber daya dan tujuan organisasi.

1. Evaluation and Assessment

Pada umumnya, di dalam suatu organisasi, jaringan secara terus menerus akan diperluas dan diperbaharui, komponen diubah dan aplikasi software-nya diganti atau diperbaharui dengan versi yang lebih baru. Perubahan ini berarti bahwa, resiko baru akan timbul dan resiko yang sebelumnya dikurangi, akan menjadi suatu perhatian. Demikian seterusnya, sehingga manajemen resiko akan berkembang.

nama: Dini Rahmadia

nim : 182420134

peranan it Risk Management pada proses IT Audit

Pemanfaatan Teknologi Informasi sebagai pendukung pencapaian tujuan dan sasaran organisasi harus diimbangi dengan keefektifan dan efisiensi pengelolaannya. Maka dari itu, audit TI haruslah dilakukan untuk menjaga keamanan sistem informasi sebagai asset organisasi, untuk mempertahankan integritas informasi yang disimpan dan diolah dan tentu saja untuk meningkatkan keefektifan penggunaan teknologi informasi serta mendukung efisiensi dalam organisasi.

IT risk management adalah usaha untuk mengelola risiko bisnis menggunakan kerangka manajemen risiko teknologi informasi sehingga tata kelola dan proses kepastian audit dapat dilakukan secara menyeluruh atau biasa dikenal dengan IT *enterprise risk management (ERM) framework*.

Peran auditor internal bervariasi dalam proses ERM bergantung pada kematangan proses ERM dalam organisasi. Sebelum auditor internal melaksanakan apapun peran yang terkait dengan ERM, harus dipastikan terlebih dahulu bahwa seluruh organisasi sepenuhnya memahami bahwa tanggung jawab manajemen risiko terutama berada pada manajemen. Makalah Posisi (*Position Paper*) *Institute of Internal Audit* (IIA) dalam **Kurt F. Reding, et.all (2013)** memberikan pedoman peran audit internal mana yang harus, boleh, dan tidak boleh dilaksanakan di dalam proses ERM organisasi.

Peran inti audit internal dalam ERM adalah kegiatan yang berhubungan dengan layanan pemastian yang meliputi:

Memberikan keyakinan pada desain dan efektivitas proses manajemen risiko;

Memberikan keyakinan bahwa risiko dievaluasi dengan benar;

Mengevaluasi proses manajemen risiko;

Mengevaluasi pelaporan mengenai status dari risiko-risiko kunci dan pengendaliannya;

Meninjau pengelolaan risiko-risiko kunci, termasuk efektivitas dari pengendalian dan respons lain terhadap risiko-risiko tersebut.

Peran tambahan lain yang boleh dilaksanakan dalam layanan konsultasi dengan dibarengi pengamanan independensi dan objektivitas yang cukup, antara lain:

Memulai pembentukan ERM dalam organisasi;

Mengembangkan strategi manajemen risiko bagi persetujuan Dewan;

Memfasilitasi identifikasi dan evaluasi risiko;

Pelatihan manajemen tentang merespons risiko;

Mengoordinasikan kegiatan ERM;

Mengonsolidasi laporan mengenai risiko;

Memelihara dan mengembangkan kerangka ERM.

Peran dalam ERM yang tidak boleh dilakukan auditor internal adalah:

Mengatur minat risiko (*risk appetite*);

Menerapkan proses manajemen risiko;

Menjamin manajemen risiko;

Membuat keputusan pada respons risiko;

Menerapkan respons dan manajemen risiko atas nama manajemen;

Akuntabilitas manajemen risiko.

IT risk management adalah usaha untuk mengelola risiko bisnis menggunakan kerangka manajemen risiko teknologi informasi sehingga tata kelola dan proses kepastian audit dapat dilakukan secara menyeluruh atau biasa dikenal dengan IT *enterprise risk management (ERM) framework*.

“*Opportunity creates risk*” artinya kesempatan akan melahirkan resiko. Keduanya seperti 2 sisi mata uang yang tak terpisahkan. Begitupun dalam bisnis dan dunia IT. Pencurian informasi kustomer, email dan password yang terungkap, *human error* karyawan sendiri yang dapat membahayakan sistem, sistem IT yang sudah usang, informasi kartu kredit yang terungkap, dan masih banyak lagi jenis-jenis resiko yang bisa muncul dan sulit untuk dikendalikan. Bahayanya bila terjadi kegagalan penanganan resiko antara lain: seluruh bagian dari organisasi dapat terkena imbasnya, bisnis menjadi terganggu, terjadi pelanggaran ranah privasi, bisnis mengalami krisis finansial, rusaknya reputasi, dan lain sebagainya.

Lalu bagaimana menanganinya? Tidak ada solusi yang benar-benar 100% mampu menangani resiko yang muncul, ditambah dengan ketidakmungkinan semua masalah dapat teratasi sekaligus, paling tidak resiko mampu dikurangi sampai pada tingkatan minimum yang dapat diterima saja. Salah satu cara mengendalikan resiko adalah dengan praktek terbaik (*best practice*) yakni audit. Metode audit salah satunya adalah menggunakan *framework*. Ada banyak sekali *framework* yang tersedia dan sudah teruji mampu menekan hingga minim resiko, satu diantaranya adalah COBIT.

Dalam COBIT, dan mungkin juga pada beberapa *framework* lainnya, manajemen resiko ditempatkan pada tahapan *plan & organise*, artinya alur *framework* menandainya sebagai wujud penting yang harus dipetakan terlebih dahulu, sebelum dilakukan implementasi, serta monitoring & evaluasi.

Dalam tahapan manajemen resiko, bentuk-bentuk resiko yang bisa muncul dipetakan terlebih dahulu. Kemudian resiko-resiko yang muncul dan menjadi temuan audit dinilai tingkatannya, apakah masuk kedalam bentuk minim, sedang, atau resiko tinggi yang akan sangat mempengaruhi obyek audit dan dapat mempengaruhi proses/obyek lainnya yang terhubung dalam sistem, bila sumber resiko tersebut terus terjadi dan tidak segera ditindaklanjuti. Proses ini disebut dengan *Risk Assessment*. Kemudian setelah itu diberikan *Risk Response*, untuk mengatasi, mensubstitusi, maupun sebatas meminimalisir resiko yang ada. Setelah dilakukan *Risk Response*, perlu dilakukan *control* berkala untuk menilai kinerja *Risk Management* yang telah dilakukan, maupun mendeteksi adanya resiko-resiko baru yang bisa muncul.

Nama : **Hari Febriadi**
NIM : **182420127**
Kelas : **MTI.20A**

Sebelum saya menjelaskan peran **IT RISK MANAGEMENT pada IT AUDIT** ! saya akan menjelaskan IT RISK secara umum ;

- **IT RISK SECARA UMUM**

IT risk management (manajemen resiko teknologi informasi) adalah proses yang dilakukan oleh para manajer IT untuk menyeimbangkan kegiatan operasional dan pengeluaran cost dalam mencapai keuntungan dengan melindungi sistem IT dan data yang medukung misi organisasinya. Menurut **G. Stoneburner 2002**, IT risk management meliputi tiga proses:

1. ***RISK ASSESSMENT***
2. ***RISK MITIGATION***
3. ***EVALUATION AND ASSESSMENT***

Risk Management (Manajemen Resiko) merupakan suatu proses mengidentifikasi resiko, menilai resiko, dan mengambil langkah meminimalisir resiko untuk mengontrol dan menjamin resiko tetap pada level yang dapat diterima. IT Risk Management mencoba untuk melindungi confidentiality, integrity, dan availability (CIA). Yaitu dengan meminimalisir dampak yang mungkin muncul yang dapat berefek pada confidentiality dari informasi, integrity dari data pada sistem, dan availability dari infrastruktur sistem.

- **PERAN IT RISK MANAGEMENT**

Peran utaman IT Risk Management untuk mendukung misi organisasi dan melindungi aset dari organisasi tersebut. Pada IT Risk Management, erat kaitannya dengan bagaimana implementasi security pada suatu organisasi sehingga diperlukan pemahaman tentang proses bisnis organisasi dan kemungkinan resiko yang berdampak pada proses bisnis tersebut. Risk Management akan sangat membantu manajemen organisasi untuk menyeimbangkan antara dampak dari *risk* dan *cost* yang dibutuhkan untuk meminimalisir resiko tersebut.

- **PROSES MENERAPAN IT Risk Management**

Berikut beberapa proses yang dilakukan ketika menerapkan IT Risk Manajemen:

1. **Threat Assessment and Analysis**
2. **Asset Identifitiction and Valuation**
3. **Vulnerability Analysis**
4. **Risk Evaluation**
5. **Interim Report**

Dalam tata kelola dan manajemen COBIT 5, terdapat dimensi proses tata kelola IT. dimensi Evaluate, Direct and Monitor (EDM) dimana proses tata kelola berhubungan dengan tata kelola tujuan stakeholder (pengantaran nilai, optimasi resiko dan optimasi sumber daya) serta termasuk didalamnya praktik dan aktivitas yang bertujuan untuk mengevaluasi pilihan strategis, pengerahan menuju IT dan monitoring outcome (pengawasan terhadap hasil). Proses ini bertujuan untuk memastikan resiko organisasi yang berkaitan dengan penggunaan TI tidak melampaui toleransi resiko, dampak dari resiko penggunaan IT dapat diidentifikasi dan potensi kegagalan dapat diminimalisasi. Optimasi resiko TI berada dalam domain tata kelola yaitu EDM03 yang terdiri dari 3 sub proses yaitu EDM03.01 (evaluate risk management), EDM03.03 (direct risk management) dan EDM03.03 (monitor risk management). Optimasi resiko TI di organisasi harus dinilai untuk mengetahui tingkat kapabilitas proses yang dilaksanakan dan membantu organisasi dalam menyusun langkah-langkah perbaikan untuk peningkatan level kapabilitas. Model penilaian kapabilitas proses dirancang untuk mengetahui tingkat kapabilitas optimasi resiko TI yang terdiri dari lima level kapabilitas yang dimulai dari level 1 sampai dengan level 5.

Peran Risk Management pada proses IT Audit adalah bertugas untuk mengarahkan praktik enterprise risk management pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Fungsi manajemen risiko bertanggung jawab untuk membentuk kerangka kerja dan proses manajemen risiko dalam menghadapi risiko-risiko signifikan yang dapat mempengaruhi pencapaian tujuan organisasi. Integrated risk management menerapkan kegiatan pencegahan dan pengurangan dampak negatif dari risiko. Seiring berjalannya waktu, manajemen risiko yang tadinya berperan untuk melindungi kegagalan organisasi, berubah menjadi komponen competitive advantage bagi organisasi. Selain menciptakan kerangka kerja dan proses manajemen risiko dalam menghadapi risiko, fungsi manajemen risiko juga meningkatkan kapabilitas organisasi dalam mengejar peluang. Fungsi ini juga meningkatkan kemampuan pengambilan keputusan strategis organisasi melalui penyediaan informasi yang relevan dan komprehensif. Dalam menciptakan manajemen risiko yang efektif bagi organisasi, fungsi manajemen risiko berkolaborasi dengan fungsi internal audit.

Terima kasih, salam.

Berdasarkan ISO31000: 2009 *Risk Management – Principles and Guidelines*, praktik terbaik manajemen risiko melibatkan seluruh bagian dari organisasi. Keterlibatan organisasi secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, *missing link*, atau inefisiensi pada kegiatan manajemen risiko.

Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko IT adalah fungsi manajemen risiko dan internal audit dalam IT audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko IT bertugas untuk mengarahkan praktik *enterprise risk IT management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

*K*egiatan internal audit dalam IT audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko IT, pengendalian, dan proses *governance*. Tugas inti auditor internal dalam IT audit berkaitan dengan manajemen risiko IT adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko IT telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi.

IT Risk Management adalah penerapan dari prinsip-prinisip manajemen risiko terhadap perusahaan yang memanfaatkan teknologi informasi dengan tujuan untuk dapat mengelola risiko-risiko yang berhubungan dengan perusahaan tersebut. Risiko-risiko yang dikelola meliputi kepemilikan, operasional, keterkaitan, dampak, dan penggunaan dari teknologi informasi pada sebuah perusahaan.

Hambatan umum terhadap data dan sistem teknologi informasi meliputi:

- Kerusakan perangkat keras dan perangkat lunak
- *Malware*
- Virus komputer
- *Spam, scams, and phishing*
- *Human error*

Selain hambatan umum, dalam IT Risk Management juga mengelola hambatan criminal terhadap teknologi informasi suatu perusahaan, antara lain:

- *Hackers*, yaitu orang-orang yang secara tidak sah menerobos ke dalam sistem computer
- *Fraud*, yaitu penggunaan computer untuk memanipulasi data untuk kepentingan yang melanggar hukum
- *Denial-of-service*, yaitu serangan *online* yang membuat pengguna tidak dapat mengakses situs tertentu
- *Staff dishonesty*, yaitu pencurian data atau informasi penting oleh karyawan internal.

IT Risk Management tidak hanya berfokus tentang penanganan terhadap risiko dan dampak negative dari hambatan-hambatan di atas terhadap operasional perusahaan dalam hal value sebuah perusahaan, tetapi juga dapat memberikan keuntungan potensial. Berikut adalah langkah-langkah yang dilakukan untuk mengelola risiko teknologi informasi dalam sebuah perusahaan:

1. *Assessment*, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.
2. *Mitigation*, yaitu penanggulanan yang dilakukan untuk mengurangi dampat risiko.
3. *Evaluation and Assessment*, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

Hubungan nya dengan IT Audit adalah Penerapan ini berguna untuk mengetahui profil resiko IT, analisa terhadap resiko, kemudian melakukan respon terhadap resiko tersebut sehingga tidak terjadi dampak - dampak yang ditimbulkan oleh resiko tersebut. Sehingga perusahaan dapat meminimalisir resiko resiko yang telah teridentifikasi pada it risk management ini.

Peran Risk Management pada proses IT Audit adalah Dalam manajemen risiko melibatkan seluruh bagian dari organisasi. Keterlibatan organisasi secara keseluruhan pada kegiatan manajemen risiko menuntut adanya pembagian peran dan tanggung jawab yang jelas, dengan turut mempertimbangkan kompetensi dan peran lain dari tiap unit tersebut. Hal ini diperlukan agar tidak terjadi tumpang tindih, *missing link*, atau inefisiensi pada kegiatan manajemen risiko.

Dua fungsi esensial yang memiliki keterkaitan erat pada kegiatan manajemen risiko adalah fungsi manajemen risiko dan internal audit. Kedua fungsi ini memiliki peran dalam menjamin efektivitas penerapan manajemen risiko organisasi. Perbedaan fundamental dari kedua fungsi tersebut terletak pada delegasi tanggung jawab. Fungsi manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

Peran Internal Audit terkait Manajemen Risiko
Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.

Kolaborasi Fungsi Manajemen Risiko dan Internal Audit
Terdapat beberapa alasan yang mendasari paradigma bahwa fungsi manajemen risiko sebaiknya berkolaborasi dengan fungsi internal audit. Berdasarkan *case study* yang dilakukan oleh RIMS dan IIA, alasan-alasan tersebut adalah

- Untuk menghubungkan rencana audit dan penilaian risiko perusahaan, serta berbagi produk kerja lainnya. Hal ini dibutuhkan untuk meningkatkan koordinasi dalam usaha menjamin bahwa risiko-risiko utama dapat ditangani dengan efektif.
- Berbagi sumber daya-sumber daya tertentu untuk mendukung efisiensi. Sumber daya yang dimaksud termasuk sumber daya keuangan, manusia, dan waktu.
- Saling meningkatkan kompetensi, peran, dan tanggung jawab setiap fungsi. Menyediakan infrastruktur komunikasi yang konsisten.

Menilai dan memantau risiko strategis. Dapat membentuk pemahaman yang lebih mendalam dan treatment yang fokus untuk mengatasi risiko strategis. Berdasarkan pengalamannya, *Irene Corbe (Whirlpool Corp.)* menyatakan bahwa pengadaan pertemuan dengan divisi manajemen risiko dapat meningkatkan pemahaman fungsi audit internal terhadap profil risiko perusahaan.

Peran Internal Audit terkait Manajemen Risiko

kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Berikut adalah gambaran mengenai hal-hal yang menjadi, peran dan tanggung jawab auditor internal terkait dengan manajemen risiko, yang dapat menjadi bagian dari tanggung jawab auditor internal, serta yang seharusnya tidak menjadi tanggung jawabnya.

Setiap proses bisnis memiliki risiko, demikian halnya dengan proses TI. Risiko yang terkait dengan TI yakni IT Risk(risiko TI) adalah risiko bisnis yang terkait dengan penggunaan, kepemilikan, pengoperasian, keterlibatan, pengaruh dan penerapan TI dalam suatu organisasi. Risiko TI menjadi bahan pertimbangan prioritas proses TI yang akan diaudit. Oleh karena itu, digunakan audit berbasis risiko yakni audit yang dilakukan berdasarkan proses-proses yang memiliki potensi risiko yang tinggi atau pada proses kritikal yang berdampak negatif jika terjadi masalah. Dalam melakukan analisis risiko didukung oleh Risk IT Framework yang menyediakan framework untuk mengidentifikasi, mengendalikan, dan mengelola risiko TI. Domain yang digunakan adalah domain Risk Evaluation. Kombinasi dari COBIT Versi 4.1 dan Risk IT sangat cocok digunakan dalam audit penerapan TI di Perguruan Tinggi XYZ karena audit akan lebih terfokus pada proses kritikal dan tidak terjebak pada proses yang kurang berisiko. Untuk itu, rumusan masalah dalam penelitian ini adalah bagaimana tingkat kematangan TI di Perguruan Tinggi XYZ dari hasil audit TI berbasis risiko dengan framework COBIT Versi 4.1 dan bagaimana rekomendasi dari hasil audit TI untuk meningkatkan performansi TIdi Perguruan Tinggi XYZ.Manfaat yang akan diperoleh dari penelitian ini adalah memperoleh hasil evaluasi yang dapat digunakan untuk menyelaraskan TI dengan tujuan Perguruan Tinggi XYZ, membangun kesadaran dan tanggung jawab atas risiko TI, meningkatkan performansi IT untuk menuju World Class University, dan persiapan menghadapi audit eksternal.

Internal audit seharusnya menghindari aktifitas berikut yang dapat mengganggu independensi dan objektifitas, yaitu:

1. Menentukan risk appetite.
2. Memiliki atau mengelola risiko (lini pertama).
3. Memegang tanggung jawab untuk akuntansi, pengembangan bisnis, dan fungsi lini pertama lainnya.
4. Menetapkan keputusan respon terhadap risiko, dengan mengatasnamakan manajemen.
5. Menerapkan atau memegang pertanggung jawaban untuk proses manajemen risiko atau tata kelola.
6. Melaksanakan penugasan asurans terhadap aktifitas lini kedua yang dilaksanakan oleh internal audit.