**Penilaian Risiko *(Risk Assessment)***

Oleh:

Muhyiddin, S.Ak., M.Ak.

Universitas Esa Unggul

muhyiddin@esaunggul.ac.id

**Pendahuluan**

Manajemen Risiko *(Risk Management)* menjadi dasar dalam pengelolaan bank-bank sejak akhir tahun 90-an dan semakin populer penggunaannya sejak awal milenium baru ini terutama sejak diperkenalkannya konsep Basel II oleh Komite Basel dari Bank for International Settlement (BIS). Dalam konsep baru tersebut identifikasi dan penghitungan risiko untuk keperluan penetapan kebutuhan modal minimum bank dirubah dari ketentuan yang sudah diberlakukan sejak 1988 (accord 1988) dimana risiko untuk penghitungan kebutuhan modal minimum bank sudah harus memperhitungkan risiko pasar serta risiko operasional, selain risiko kredit. Dasar semuanya adalah identifikasi Risiko, kalkulasi Risiko, pemantauan Risiko dan Pengendalian Risiko yang lebih lanjut dikenal sebagai Manajemen Risiko dalam perbankan.

Bank Indonesia (2003), menjelaskan tentang pengertian Manajemen Risiko yaitu serangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, memantau dan mengendalikan risiko yang timbul dari kegiatan usaha bank. Sedangkan yang dimaksud dengan “Risiko” adalah potensi terjadinya suatu peristiwa (event) yang dapat menimbulkan kerugian bank.

Menurut Bank Indonesia (2003), sesungguhnya risiko saat ini merupakan potensi kerugian di waktu mendatang. Karena itu sangat perlu diperhatikan dan diperhitungkan. Menurut Arens (2003), materialitas dan risiko merupakan konsep- 2 konsep fundamental yang sifatnya penting dalam perencanaan audit dan dalam perancangan atas pendekatan audit yang akan dipergunakan.

Walaupun tidak senyata sebagaimana penetapan biaya dan hasil (tangible cost & revenue), penghitungan risiko dalam kegiatan perbankan akan semakin diperlukan dan akan semakin luas penggunaannya.

Bank Indonesia (2003), menjelaskan bahwa penerapan manajemen risiko akan memberikan manfaat, baik kepada perbankan maupun kepada otoritas pengawasan bank. Bagi perbankan, penerapan manajemen risiko dapat meningkatkan shareholder value, memberikan gambaran kepada pengelola bank mengenai kemungkinan kerugian bank di masa datang, meningkatkan metode dan proses pengambilan keputusan yang sistimatis, yang didasarkan pada ketersediaan informasi, digunakan sebagai dasar pengukuran yang lebih akurat mengenai kinerja bank, digunakan untuk menilai risiko yang melekat pada instrumen atau kegiatan usaha bank yang relatif komplek serta menciptakan infrastruktur manajemen risiko yang kokoh dalam rangka meningkatkan daya saing bank. Bagi otoritas pengawasan bank, penerapan manajemen risiko akan mempermudah penilaian terhadap kemungkinan kerugian yang dihadapi bank yang dapat mempengaruhi permodalan bank dan sebagai salah satu dasar penilaian dalam menetapkan strategi dan fokus pengawasan bank.

Esensi dari penerapan manajemen risiko adalah kecukupan prosedur dan metodologi pengelolaan risiko sehingga kegiatan usaha bank tetap dapat terkendali (manageable) pada batas/limit yang dapat diterima serta menguntungkan bank. Namun demikian mengingat perbedaan kondisi pasar dan struktur, ukuran serta kompleksitas usaha bank, maka tidak terdapat satu sistem manajemen risiko yang 3 universal untuk seluruh bank, sehingga setiap bank harus membangun sistem manajemen risiko sesuai dengan fungsi dan organisasi manajemen risiko pada bank.

Risiko dalam konteks perbankan merupakan suatu kejadian potensial, baik yang dapat diperkirakan (anticipated) maupun yang tidak diperkirakan (unanticipated) yang berdampak negatif terhadap pendapatan dan permodalan bank. Untuk dapat menerapkan proses manajemen risiko, maka pada tahap awal bank harus secara tepat mengidentifikasi risiko dengan cara mengenal dan memahami seluruh risiko yang sudah ada (inherent) maupun yang mungkin timbul dari bisnis baru bank, termasuk risiko yang bersumber dari perusahaan terkait dan afiliasi lainnya. Menurut Arens (2003), cara utama yang dipergunakan oleh Auditor untuk mempertimbangkan risiko yang ada dalam perencanaan audit adalah melalui penerapan model risiko audit yang terdiri dari 4 komponen yaitu risiko deteksi terencana (planned detection risk), risiko akseptibilitas audit (acceptable audit risk), risiko inheren (inherent risk) dan risiko pengendalian (control risk).

Menurut Taswan (2006), bisnis adalah berbagi risiko bukan hanya berbagi keuntungan. Tidak menyadari bahwa risiko berhubungan positif dengan return. Artinya dalam bisnis perbankan ketika ingin mencapai return yang tinggi maka berhadapan dengan risiko yang tinggi. Hal lain yang kurang diperhatikan adalah bahwa risiko bisa berakibat berantai dalam bisnis perbankan. Contoh kesalahan dalam analisis kredit akan berakibat bank menghadapi risiko kredit yang tinggi, risiko kredit yang tinggi akan menjadi potensi atau sumber kerugian bank. Kerugian bank akan mengurangi posisi modal. Posisi modal yang turun akan menurunkan rasio kecukupan modal. Penurunan rasio ini bisa berhadapan dengan regulasi bank yang pada gilirannya menurunkan kesehatan bank, penurunan kesehatan bank akan 4 menurunkan kepercayaan masyarakat, menaikkan premi penjaminan simpanan, cost of fund menjadi tinggi, profit turun dan seterusnya berakibat buruk bagi bank. Kondisi eksternal juga sering menjadi penyebab risiko, misalnya pasar, inflasi dan politik yang bergejolak fluktuatif akan mengakibatkan risiko perbankan menjadi semakin besar. Dengan memperhatikan hal-hal tersebut dan belajar dari krisis perbankan di Indonesia pada tahun 1997, maka memasuki tahun 2003 (yang ditandai dengan kewajiban penerapan manajemen risiko perbankan), manajemen risiko menjadi perhatian sangat serius di Indonesia, walaupun sebelumnya hal ini telah mewabah ke seluruh dunia.

Bank Indonesia telah mewajibkan bank komersial untuk menerapkan manajemen risiko sebagai bagian dari penilaian kinerja bank. Para komisaris dan direktur bank diwajibkan memiliki sertifikat manajemen risiko yang dikeluarkan oleh Badan Sertifikasi Manajemen Risiko. Sertifikat ini menunjukkan bahwa hanya orang-orang yang memahami manajemen risiko saja yang pantas menduduki komite manajemen risiko. Di satu sisi, bank komersial juga berkepentingan untuk mengelola risiko yang lebih baik. Penyadaran akan pengelolaan risiko untuk mencapai tujuan bisnis perbankan sangat tinggi saat ini. Praktisi perbankan menyadari bahwa pencapaian return tertentu pada risiko minimal atau pencapaian return maksimal pada risiko tertentu bisa dilakukan bila risiko dikelola dengan baik. Dengan penilaian risiko yang jelas, akan memudahkan justifikasi manajemen, apakah bank yang bersangkutan dalam kondisi risiko tinggi, sedang atau rendah. Disamping itu pihak bank dapat mengendalikan tingkat risiko yang wajar, terarah, terintegrasi dan berkesinambungan melalui sistem manajemen risiko yang dapat memberikan peringatan dini (early warning system).

Kegiatan audit intern dalam suatu badan usaha seperti bank merupakan tuntutan atau kebutuhan bagi semua pihak guna melahirkan usaha yang sehat. Kegiatan ini pada hakikatnya mendorong terciptanya efisiensi usaha, sehingga bank mampu bersaing secara sehat dalam pasar yang makin kompetitif, mengacu penciptaan laba yang baik. Dalam hal ini tentunya bank diharapkan terjaga kelangsungan hidupnya serta mampu memberikan kontribusi bagi masyarakat banyak dan pemerintah.

Keberhasilan kegiatan audit intern bank banyak bergantung kepada ketepatan dan kesesuaian perencanaan audit dalam mengantisipasi dan mempertimbangkan kebutuhan perusahaan untuk menentukan pemilihan objek audit, jenis, cakupan, dan tujuan audit yang dilakukan, perkiraan kebutuhan sumber daya audit dan pengalokasian sumber daya audit yang tersedia. Perencanaan audit tersebut harus konsisten dengan Piagam Internal Audit, tujuan bank dan disetujui oleh Direktur Utama dan dilaporkan kepada Dewan Audit.

Penyusunan rencana kegiatan audit dapat efektif apabila mempertimbangkan faktor risiko (salah satunya), yang tujuannya adalah untuk mengindentifikasikan bagian yang material atau signifikan dari kegiatan yang akan diaudit, sehingga dapat diatur skala prioritas pelaksanaan audit dengan mengetahui unit mana yang memerlukan segera dan unit mana yang bisa ditempatkan pada urutan terakhir, sehingga pelaksanaan kegiatan audit dapat memudahkan dalam membagi pekerjaan sesuai dengan tenaga auditor yang tersedia, dan menciptakan efisiensi biaya audit.

Selain itu penilaian risiko dalam menentukan objek audit adalah sangat penting, karena sesuai dengan fungsi dan peran audit intern saat ini telah memasuki orientasi baru (paradigma baru) dari peran tradisionalnya sebagai polisi atau pihak yang cenderung mencari-cari kesalahan pihak lain dalam organisasi tanpa mampu memberikan solusi, kearah fungsi dan peran yang baru sebagai mitra dan atau konsultan dan atau katalis.

**Penilaian Risiko *(Risk Assessment)***

***Risk Assessment*** atau dapat diartikan ke dalam bahasa Indonesia sebagai penilaian risiko merupakan suatu aktivitas yang dilaksanakan untuk memperkirakan suatu risiko dari situasi yang bisa didefinisikan dengan jelas ataupun potensi dari suatu ancaman atau bahaya baik secara kuantitatif atau kualitatif. Penilaian risiko juga bisa diartikan sebagai suatu proses pemeriksaan keamanan dengan suatu struktur tertentu, pembuatan suatu rekomendasi khusus, dan rekomendasi pengambilan keputusan dalam suatu proyek dengan menggunakan analisis risiko, perkiraan risiko, dan informasi lain yang memiliki potensi untuk mempengaruhi keputusan.

**Tinjauan Penilaian Risiko**

Penilaian risiko berbeda dengan analisis risiko atau dengan manajemen risiko, akan tetapi antara ketiga hal tersebut terdapat hubungan yang saling berkaitan satu dengan yang lain. Analisis risiko sendiri kegiatan menganalisa untuk menentukan besar kecilnya suatu risiko dengan mempertimbangkan kemungkinan terjadinya dan besarnya akibat yang ditimbulkan. (Andani EN, 2015).

Setelah menganalisis risiko yang ada dan sebelumnya mengidentifikasi terlebih dahulu risiko sepert apa yang akan terjadi dan bagaimana suatu bisa terjadi maka tahapan selanjutnya memberikan penilaian tentang besarnya tingkatan terkait risiko tersebut. Hal itulah menjadi bagian dari penilaian risiko itu sendiri dimana memberikan makna terhadap suatau bahaya yang teridentifikasi untuk memberikan gambaran seberapa besar risiko tersebut. Sehingga dapat diambil tindakan lanjutan terhadap bahaya yang teridentifikasi, apakah bahaya itu dapat diterima atau tidak.

Dalam menilai suatu risiko terdapat standard yang bisa dipakai acuan, salah satunya ialah standard AS/NZS 4360 yang membuat peringkat risiko sebagai berikut:

1. L : Low Risk (Risiko rendah masih ditoleransi)
2. M : Moderat Risk (Risiko sedang, diibutuhkan sebuah tinggakan agar risiko berkurang)
3. H : High Risk (Risiko yang besar dibutuhkan perhatian dari manajer puncak)
4. E : Extreme Risk (Sangat berisiko segera secepatnya dibutuhkan tindakan)

Penilaian risiko sendiri bisa didefinisikan sebagai keseluruhan proses dari identifikasi risiko, analisis risiko dan evaluasi risiko.Terdapat 6 fokus dan tipe penialaian risiko yaitu:

1. Risiko Keselamatan
2. Risiko Kesehatan
3. Risiko Lingkungan
4. Risiko Kesejahteraan
5. Risiko Keuangan

Pertanyaan yang mendasar yang bisa dijawab dari penilaian risiko diantaranya yaitu:

1. Apa yang akan terjadi dan bagaimana bisa terjadi (Dapat dijawab ketika memasuki tahap identifikasi)?
2. Apa kemungkinan yang terjadi di masa depan?
3. Apa saja dampaknya? dan
4. Apakah ada faktor-faktor yang mengurangi kemungkinan dari risiko itu atau mengurangi dampak yang ditimbulkan akan risiko yang ada?

Secara khusus untuk memulai Penilaian risiko terdapat hal-hal yang harus dipahami dan jelas yaitu:

1. Konteks dan objek dari organisasi
2. Risiko-risko apa saja yang bisa ditoleransi, dan bagaimana resiko yang tidak diterima akan diperlakukan
3. Bagaiaman penilaian risiko dapat diintegrasikan ke dalam proses organisasi
4. Metode dan teknik yang digunakan untuk penilaian risiko terhadapproses manajemen risiko secara kesuluruhan
5. Akuntabilitas, tanggung jawab dan kewenangan dalam melaksanakan penialaian risiko
6. Sumberdaya yang memadai untuk melaksanakan penialaian risiko dan
7. Bagaimana penilaian risiko akan ditinjau dan dilaporkan

Hasil dari tahapan-tahapan ketika fase analisis resiko dan khususnya penilaian risiko ditindaklanjuti dengan proses manajemen risiko. Manajmeen risiko menurut Clough and Sears (1994 dikutip dalam Anonim 2009), Manajemen risiko didefinisikan sebagai suatu pendekatan yang komprehensif untuk menangani semua kejadian yang menimbulkan kerugian.

Menurut AS/NZS 4360 manajemen risiko adalah “*the culture, process, and structures that are directed towards the effective management of potential opportunities and adserve effects*”. Panduan untuk manajemen risiko terdapat dalam ISO 31000 yang terdiri dari 5 aktivitas kunci:

1. Komunikasi dan konsultasi
2. Menentukan konteks
3. Penilaian risiko
4. Pengendalian risiko
5. Monitor dan review

**Penggunaan Penilaian Risiko**

1. **Bidang Kesehatan**

HRA atau penilaian risiko kesehatan merupakan suatu prosedur yang tersistematis untuk mengidentifikasi potensi dari bahaya kesehatan, mengevaluasi dari paparan secara subjective & atau objective, serta bertujuan untuk menentukan dan menilai efektivitas dari pengendalian yang dibutuhkannya.

“Peniliaian Risiko juga dibutuhkan tidak hanya untuk seseorang yang memenuhi syarat untuk mammografi tetapi juga dibutuhkan untuk seseorang yang menginginkan screening MRI atau test DNA” kata Jennifer Plichta, MD, 2016 annual meeting of the American Society of Breast Surgeons (ASBS).

1. **Bidang Audit**

Auditor internal menggunakan teknik penilaian risiko dalam mengembangkan perencanaan aktivitas audit internal dan pada penentuan prioritas untuk mengalokasikan sumberdaya. Penilaian risiko ini juga digunakan untuk pengujian unit dan pemilihan area yang akan dimasukkan dalam rencana kegiatan internal yang memiliki tingkat kerentanan terhadap risiko yang tinggi.

1. **Bidang Teknologi Informasi**

Penilaian risiko adalah alat yang tersedia yang bisa digunakan oleh organisasi modern untuk membantu mengidentifikasi serta memberikan tingkatan terhadap resiko yang berhubungan dengan penggunaan sistem informasi dan secara tepat mengambil tindakan untuk melindungi sistem informasi. Terdapat dua metodologi terkait penilaian resiko yakni Operationally Critical Threat, Asset, Vulnerability Evaluation (OCTAVE) Risk Assessment dan Central Computer and Telecommunicationd Agency (CCTA’s) Risk Assessment.

Dalam tahapan penilaian risiko, dilakukan proses membandingkan tingkat risiko dengan kriteria risiko pada basis yang sama. Hasil penilaian risiko adalah berupa daftar prioritas risiko dimana area yang dinilai berisiko tinggi ditindaklanjuti dan yang berisiko rendah dipantau.

Definisi penilaian risiko (risk assesment) dalam buku pegangan bagi anggota IIA sebagai berikut: “Risk assesment is a systematic process for assesing and integrating professional judgment about probable adverse condition and/or events”. Maksudnya penilaian risiko (risk assesment) adalah suatu proses yang sistematik untuk menilai dan mengintegrasikan pertimbangan profesional mengenai kemungkinan kondisi yang jelek. Proses penilaian risiko seharusnya dapat memberikan suatu cara untuk mengorganisir dan mengintegrasikan pertimbangan profesional dalam pengembangan jadwal pelaksanaan audit.

Dari definisi tersebut, bahwa audit internal harus melaksanakan perencanaan audit dengan seksama yang mempertimbangkan faktor-faktor risiko pada suatu unit yang akan diperiksa berdasarkan pertimbangan profesional, sebagaimana diatur dalam Standard Professional Internal Auditor point 280, yaitu dalam setiap penugasan audit, baik yang dilandasi dengan pengetahuannya yang diperoleh dari proses pendidikan yang terus menerus maupun berdasarkan pengalaman audit pada masa-masa yang lalu.

Sebagai konsekuensi adanya pendekatan risk-based maka auditor akan sering berkecimpung dengan risiko dan penilaian risiko. Salah satu alasannya adalah paradigma baru seperti yang dikemukakan oleh David McNamee and Georges Selim (1998): Risk Management; Changing the Internal Auditor's Paradigm.

**Metode Penilaian Risiko**

Penilaian risiko merupakan perangkat utama dan sangat penting artinya bagi tata kelola organisasi. Ada 3 (tiga) pendekatan yang dapat digunakan dan masing masing dengan kelebihan dan kekurangannya, yaitu:

* 1. **Pendekatan Database (database approach)**

Pendekatan database dikenal juga sebagai pendekatan Risk Profiling. Setiap unit kerja diwawancara dan dibuat katalog untuk produk dan proses utama disertai dengan risiko-risiko speisifik yang terkait dengan masing-masing unit. Selanjutnya hasil akhir dapat diekstrak dari database untuk melihat risiko-risiko umum dalam setiap unit atau untuk melihat semua risiko yang dihadapi oleh sebuah unit kerja. Sebagai contoh, perusahaan asuransi mencoba merekam data individu, aset keuangan, risiko umum dan risiko keuangan atas aset yang bersangkutan. Terdapat sejumlah perangkat lunak yang dapat digunakan untuk mengikhtisarkan data dan menampilkan risiko keuangan per jenis risiko, jenis aset dan lain sebagainya.

Pendekatan database menggunakan data secara intensif dan memerlukan banyak waktu untuk membuatnya. Database juga banyak menyita waktu untuk memelihara dan cepat out-dated di lingkungan yang cepat sekali berubah. Terlalu banyaknya jumlah data juga mengakibatkan tidak mudahnya pengendalian dalam pengambilan keputusan.

* 1. **Pendekatan Algoritma (algorithm approach)**

Pendekatan algoritma menggunakan urutan tahapan-tahapan logik untuk memecahkan masalah dan sekumpulan masalah dengan menggunakan perhitungan matematis yang diterapkan untuk masing-masing unit kerja guna menghitung risiko yang dihadapi. Apabila menggunakan metode ini maka auditor harus menentukan faktor risiko (risk factor) untuk menilai risiko. Faktor risiko merupakan indikator risiko yang dapat diamati dan diukur, misalnya periode terakhir dimana dilakukan audit mencerminkan penurunan sistem pengendalian karena tidak secara berkala diaudit. Sekumpulan faktor risiko dan hasil pengukuran pada setiap unit kerja akan 43 menghasilkan model faktor risiko yang seringkali menggunakan spreadsheets untuk merekam dan memanipulasi data.

* 1. **Pendekatan Matriks (matrix approach)**

Pendekatan matriks dilakukan dengan menyusun unit-unit bisnis organisasi dan risiko ke dalam baris horisontal dan vertikal. Selanjutnya dilakukan penilaian risiko terhadap setiap jenis risiko bagi setiap unit bisnis dan hasilnya akan tertuang dalam cell, misalnya warna hijau untuk risiko rendah, kuning untuk risiko menengah dan merah untuk risiko tinggi serta putih (kosong) untuk jenis risiko yang tidak dapat diaplikasikan bagi unit bisnis tertentu.

Sebagai alternatif, setiap unit bisnis membuat matriks tersendiri menggunakan model risiko yang sama dan selanjutnya digabung untuk membentuk matriks risiko organisasi.

Kelebihan pendekatan matriks adalah fleksibilitas dan cepat diimplementasikan namun memerlukan kredibilitas pemahaman bisnis yang memadai

Sebagai pedoman dalam menentukan pendekatan yang akan digunakan dalam menilai risiko, dapat digambarkan dalam tabel sebagai berikut:

|  |  |  |  |
| --- | --- | --- | --- |
| **Jenis Pedekatan** | **Kemudahan Implementasi** | **Kemudahan Pemeliharaan** | **Paling Baik Digunakan** |
| Database | Sullit | Sulit | Pedoman Rinci |
| Algoritma | Sedang | Mudah | Manajemen Operasi |
| Matriks | Mudah | Sedang | Rencana Strategis |

**Tujuan penggunaan penilaian Risiko dalam Penentuan Objek Audit**

Tujuan dilakukannya penilaian risiko dalam penentuan objek audit, adalah untuk mengidentifikasikan bagian yang material atau signifikan dari kegiatan yang akan diaudit, sehingga dapat diatur skala prioritas pelaksanaan audit dengan mengetahui unit mana yang memerlukan segera dan unit mana yang bisa ditempatkan pada urutan terakhir.

Hal tersebut dimaksudkan bahwa penilaian risiko digunakan untuk memilih objek audit tertentu berdasarkan tingkat kerawanannya (menekankan audit pada kegiatan yang mempunyai risiko, tanpa harus memeriksa seluruh kegiatan secara ekstensif), sehingga dapat memudahkan dalam membagi pekerjaan sesuai dengan tenaga auditor yang tersedia.

Penilaian risiko dalam penentuan objek audit didasari dari adanya perubahan fungsi dan peran audit intern pada saat ini, yang telah memasuki orientasi baru (paradigma baru) dari peran tradisionalnya sebagai polisi atau pihak yang cenderung mencari-cari kesalahan pihak lain dalam organisasi tanpa mampu memberikan solusi, kearah fungsi dan peran yang baru sebagai mitra dan atau konsultan dan atau katalis. Sehingga dengan keberadaannya dapat memberikan nilai tambah yang signifikan, efisien, efektif dan ekonomis.

**Tujuan penggunaan penilaian Risiko dalam Perencanaan Audit**

Rencana audit disusun untuk dapat memenuhi tujuan audit sebagaimana tercermin dari definisinya. Tujuan audit adalah untuk mengetahui kondisi perusahaan yang sedang berjalan dan yang akan datang, serta risiko yang melekat di dalamnya untuk kemudian mengembangkan rencana audit secara efektif. Hal ini dilakukan agar pemeriksa dapat mengarahkan pemeriksaannya atas risiko yang perlu mendapat perhatian. Untuk dapat memenuhi tujuan dimaksud diperlukan dua tahap dalam proses penyusunan rencana audit, yaitu:

1. Menemukan risiko apa saja yang ada. Dalam perusahaan yang telah memiliki satuan kerja manajemen risiko, maka audit intern dapat menggunakan profil risiko yang telah dibuat oleh satuan kerja dimaksud. Tetapi ada kalanya audit intern melakukan sendiri pendataan dan penaksiran risiko dimaksud, apalagi dalam perusahaan yang belum memiliki satuan kerja khusus manajemen risiko.

Hal-hal yang dilakukan dalam tahap ini yaitu:

1. Melakukan review pendahuluan, mulai dari corporate plan, rencana kerja dan anggaran perusahaan (RKAP), rencana kerja dan anggaran cabang (RKAC), laporan keuangan, ketentuan hukum dan regulasi yang berlaku, sistem informasi manajemen, kertas kerja audit yang lalu, dan lainnya.
2. Menetapkan Audit Unviverse
3. Melakukan risk assessment termasuk melakukan wawancara dengan manajemen dari satuan kerja operasional.
4. Membahas hasil risk assessment dengan manajemen terkait untuk mendapatkan validasi.
5. Menyusun rencana audit.
6. Menjalankan tugas audit dalam rangka meyakinkan manajemen bahwa semua risiko yang dapat diidentifikasi telah dimitigasi ke tingkat yang dapat diterima.

Tahap kedua ini memiliki tiga bagian yang ada kaitannya dengan tahap terdahulu yaitu:

1. Memecah-mecah sebuah satuan kerja menjadi satuan-satuan yang lebih kecil untuk dapat dikelola. Satuan ini disebut juga sebagai satuan layak audit (auditable unit),
2. Menentukan auditable unit mana yang perlu diaudit, yang dapat mewakili dalam hal mendapatkan keyakinan bahwa risiko-risiko utama telah dimitigasi secara memadai. Penentuan ini yang akan menghasilkan rencana audit,
3. Melaksanakan tugas audit sesuai rencana yang telah disusun dan harus terlebih dahulu mendapat persetujuan dari dewan komisaris dan direksi.

**Prinsip Penyusunan Perencanaan Audit**

Menurut Robert T. (2005), ada beberapa prinsip yang perlu diperhatikan dalam penyusunan rencana audit, yaitu sebagai berikut:

1. Mempertimbangkan peran dan tanggung jawab auditor yang unik serta kebutuhan untuk mengintegrasikan faktor risiko ke dalam setiap audit mulai dari yang memiliki score risiko lebih tinggi.
2. Karena sumber daya untuk melaksanakan audit (tenaga, waktu dan dana) terbatas, tidak mungkin untuk melakukan audit dengan coverage 100%. Keterbatasan ini tercermin dari pemakaian risk assessment guna menetapkan skala prioritas audit.
3. Kriteria dalam risk assessment yang digunakan untuk menetapkan ranking dari audit universe, memberi penekanan akan pentingnya pemahaman mengenai sistem pengendalian intern dari auditee yang sebenarnya, yang mungkin saja berbeda dari yang lain.
4. Apabila pada konsep lama seorang atau beberapa auditor mendapat tugas audit untuk satu subyek pada satu saat tertentu, maka dengan konsep baru ini seorang atau lebih auditor akan mendapat beberapa tugas audit untuk satu saat tertentu.
5. Adanya inherent risk dan keterbatasan metode atau sistem penetapan prioritas audit, mengharuskan internal audit untuk secara berkala mengkaji semua faktor risiko serta proses scoring yang ada dalam rangka menyempurnakan rencana audit.

Berdasarkan prinsip-prinsip di atas, kegiatan penyusunan rencana audit harus didasarkan pada sebuah penilaian atas risiko dan eksposur yang punya dampak negatif terhadap upaya pencapaian tujuan perusahaan. Informasi mengenai program memitigasi risiko yang memiliki dampak pada tujuan perusahaan haruslah menjadi tujuan akhir dari audit.

 Proses penyusunan rencana audit yang didasarkan pada penilaian risiko ini, selanjutnya akan melibatkan kegiatan penetapan:

1. Tujuan audit, tujuan ini harus mampu dipenuhi dalam jangka waktu dan anggaran yang telah ditentukan dan juga harus dapat diukur. Harus ada kriteria pengukuran dan batas waktu pemenuhan tujuan audit.
2. Jadwal audit, jadwal audit ini sekurangnya harus mencakup kegiatan atau fungsi yang akan diaudit, kapan audit dilakukan dan berapa lama. Jadwal audit harus mempertimbangkan prioritas risiko yang diperoleh dari hasil risk assessment, baik yang dilakukan oleh Manajemen atau pun yang dilakukan sendiri oleh Audit Intern. Apabila risk assessment juga dilakukan oleh audit intern, sebaiknya model yang digunakan merupakan pelengkap dari model yang digunakan oleh Manajemen. Model yang umum dipergunakan untuk menetapkan prioritas risiko yaitu model yang mempertimbangkan faktor-faktor seperti antara lain: kompleksitas usaha, besarnya aset, volume transaksi dan materialitas nilai rupiahnya, likuiditas dari aset yang ada, jumlah dan kualitas pegawai, system security, dan hubungan dengan masyarakat/aparat pemerintah.
3. Perencanaan sumber daya manusia, waktu dan anggaran biaya audit. Perencanaan SDM, waktu dan anggaran biaya ini merupakan konsekuensi dari jadwal audit di atas, dengan terlebih dahulu mempertimbangkan waktu cuti, pendidikan dan kemungkinan ijin untuk kepentingan pribadi para auditornya. Untuk mengatur penggunaan sumber daya yang efisien dan efektif, metode dan teknik pengujian dan validasi risiko harus mengarah kepada materialitas serta tingkat kemungkinan terjadinya risiko.
4. Kegiatan pelaporan dan pemantauan. Bagian akhir dari tugas audit adalah menyajikan informasi mengenai pengelolaan dan pengendalian risiko ke manajemen. Laporan ke manajemen harus mengungkapkan konklusi mengenai manajemen risiko dan rekomendasi untuk mengendalikan atau mengurangi risiko. Agar memberikan informasi mengenai risiko secara tepat, laporan tersebut harus menggambarkan seberapa kritis dampak risiko terhadap penca- paian tujuan perusahaan. Sekurangnya setahun sekali, kepala DAI wajib menyusun laporan mengenai kecukupan kontrol intern untuk memitigasi risiko. Termasuk dalam laporan ini, risiko yang tidak dimitigasi, dampaknya, dan alasan mengapa Manajemen tetap menerima risiko dimaksud. Dalam kelompok pelaporan ini, perlu diperhitungkan waktu para auditor untuk menyusun laporan. Semua rekomendasi yang telah disetujui dan ditindaklanjuti oleh manajemen harus terus dipantau.

**Contoh Hasil dari Penilaian Risiko (Risk Assessmet)**

Hasil dari penilaian risiko dapat digambarkan dalam mentuk Risk Heatmap seperti dibawah ini:

**Contoh 1**



**Contoh 2**



**Contoh 3**



**Contoh 4**



**Appendix B**

**CORPORATE RISK ASSESSMENT**

**Impact**

|  |  |
| --- | --- |
| **Score** |  **What's the worst that could happen?** |
| 1 | * Insignificant disruption with no loss of service to citizens
* No harm to life or limb
* No reputation damage
* No or insignificant environmental damage
* Low financial loss
 |
| 2 | * Some disruption to non-critical citizen service
* LCC liable for disruption to key partner but no loss of service
* Minor injury to third parties (requiring first aid treatment)
* Minimal reputation damage (minimal adverse coverage in local press)
* LCC responsible for minor damage to local environment
* Medium financial loss
 |
| 3 | * Noticeable disruption to critical service not exceeding 48 hours
* LCC responsible for disruption to key partner resulting in loss of their service not exceeding 48 hours
* Violence or threat of serious injury (medical treatment required)
* Adverse coverage in national tabloid press and/or extensive front page coverage in local press or TV
* LCC liable for moderate damage to local environment
* High financial loss
 |
| 4 | * Serious disruption LCC's ability to provide a critical service to citizens (loss of service between 2 and 7 days)
* LCC responsible for major disruption to key partner resulting in a loss of their service lasting between 2 and 7 days
* Adverse coverage in national broadsheet press and/or low level national TV reporting
* Extensive and multiple injuries
* LCC liable for major damage to local environment
* Major financial loss
 |
| 5 | * Central Government intervention in running of LCC / Directorate
* Loss of critical citizen service for more than 7 days
* Business failure of partner or loss of service delivery of over 7 days
* Multiple injuries including loss of life
* Extensive coverage in national press and broadsheet editorial and/or national TV item
* Significant local, national or international environment damage
* Enormous financial loss
 |

**Likelihood**

|  |  |
| --- | --- |
| **Score** | **Descriptors** |
| 5 | Almost Certain. Expected to occur in most circumstances or more than a 75% chance of occurrence. |
| 4 | Likely. Potential of occurring several times in 10 years or has occurred recently. Between 50% and 75% chance of occurrence. |
| 3 | Moderate. Could occur more than once in 10 years. History of occurrence or near miss. Less than a 50% chance of occurrence. |
| 2 | Unlikely. May occur over a 10 year period. Less than 10% chance of occurrence. |
| 1 | Rare. Has not occurred. May occur in exceptional circumstances. Less than 2% chance of occurrence. |

**Impact / Likelihood matrix**

|  |  |  |
| --- | --- | --- |
|  |  | Impact |
|  |  | 1 | 2 | 3 | 4 | 5 |
| Likelihood | 5 | **1/5** | **2/5** | **3/5** | **4/5** | **5/5** |
| 4 | **1/4** | **2/4** | **3/4** | **4/4** | **5/4** |
| 3 | **1/3** | **2/3** | **3/3** | **4/3** | **5/3** |
| 2 | **1/2** | **2/2** | **3/2** | **4/2** | **5/2** |
| 1 | **1/1** | **2/1** | **3/1** | **4/1** | **5/1** |

|  |  |
| --- | --- |
| **Level of Concern** | **Action Required** |
| Very concerned | Urgent attention required at senior level to ensure risk is reduced to an acceptable level. Action planning should start without delay. Progress on actions should be reported to ELT. |
| Concerned | Minimum of robust contingency plan plus early warning indicators. Some control measures likely to be necessary. Progress on actions should be reported on at directorate senior management team. |
| Uneasy | Acceptable with some mitigation and contingency planning. Routine reviews should be carried out to ensure there has been no change which will make them more severe. |
| Content | Acceptable, but keep under review. No further action required unless risk becomes more severe. |

**Referensi:**

Adriansah, A, 2000, Kebijakan dan Manajemen Risiko-risiko Bank Komersial, Unit 1. Bahan Pembelajaran pada program Pengembangan Profesional Perbankan, Institut Bankir Indonesia

Audittindo Education, 2006, An Introductory Course for Implementing Risk-Based Auditing, PT Audittindo Arin Prima, Jakarta

Bank Indonesia, 1997, Surat Edaran Bank Indonesia No 30/11/KEP/DIR, perihal Tata Cara Penilaian Tingkat Kesehatan Bank Umum, Bank Indonesia, Jakarta

Bank Indonesia, 2001, Surat Edaran Bank Indonesia No 3/30/DPNP, Bank Indonesia, Jakarta

Holton, Lisa, 1999, New Risks Redefine Risk management.. Knowledge Space Contributing Writer. http://knowledgespace.com

Namee, David MC, Assesing Risk Assessment., page.2000 http//:www.mc2consulting.com.

The Institute of Internal Auditors, 1991, Statement on Internal Auditing Standards (SIAS) no.9: Risk Assessment,. 249 Maitland Avenue, Altamonte Springs, Florida.