Yth.

1. Direksi Bank Umum Konvensional; dan
2. Direksi Bank Umum Syariah,

di tempat.

SALINAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 35 /SEOJK.03/2017

TENTANG

PEDOMAN STANDAR SISTEM PENGENDALIAN INTERN BAGI BANK UMUM

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 53, Tambahan Lembaran Negara Republik Indonesia Nomor 5861) dan Peraturan Otoritas Jasa Keuangan Nomor 65/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum Syariah dan Unit Usaha Syariah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 298, Tambahan Lembaran Negara Republik Indonesia Nomor 5988), serta sehubungan dengan beralihnya fungsi, tugas, dan wewenang pengaturan dan pengawasan jasa keuangan di sektor perbankan dari Bank Indonesia ke Otoritas Jasa Keuangan, perlu untuk mengatur kembali pelaksanaan mengenai pedoman standar sistem pengendalian intern bagi bank umum dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

1. Pedoman Standar Sistem Pengendalian Intern bagi Bank Umum merupakan acuan standar sistem pengendalian intern yang harus dipenuhi oleh Bank sehingga Bank dapat memperluas dan memperdalam sesuai dengan kebutuhan Bank.
2. Bank yang telah memiliki sistem pengendalian intern namun belum memenuhi acuan Pedoman Standar Sistem Pengendalian Intern bagi Bank Umum, harus menyesuaikan dan menyempurnakan sistem pengendalian intern Bank dengan berpedoman pada Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

3. Dalam penyusunan sistem pengendalian intern, Bank harus mempertimbangkan total aset, produk dan jasa yang ditawarkan, termasuk produk dan jasa baru, kompleksitas operasional, jaringan kantor, profil Risiko dari setiap kegiatan usaha, metode yang digunakan untuk pengolahan data dan pengukuran Risiko, serta ketentuan terkait.
4. Pedoman Standar Sistem Pengendalian Intern bagi Bank Umum paling sedikit meliputi 5 (lima) komponen pokok, yaitu:
   a. pengawasan oleh manajemen dan budaya pengendalian;
   b. identifikasi dan penilaian Risiko;
   c. kegiatan pengendalian dan pemisahan fungsi;
   d. sistem akuntansi, informasi dan komunikasi; dan
   e. kegiatan pemantauan dan tindakan koreksi penyimpangan.

Pada saat Surat Edaran Otoritas Jasa Keuangan ini mulai berlaku, Surat Edaran Bank Indonesia No. 5/22/DPNP perihal Pedoman Standar Sistem Pengendalian Intern bagi Bank Umum dicabut dan dinyatakan tidak berlaku.

Ketentuan dalam Surat Edaran Otoritas Jasa Keuangan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 7 Juli 2017

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,

ttd

NELSON TAMPUBOLON

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana

LAMPIRAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 35 /SEOJK.03/2017

TENTANG

PEDOMAN STANDAR SISTEM PENGENDALIAN INTERN BAGI BANK UMUM

DAFTAR ISI

I. LATAR BELAKANG

1. Sistem Pengendalian Intern (SPI) yang efektif merupakan komponen penting dalam manajemen Bank dan menjadi dasar bagi kegiatan operasional Bank yang sehat dan aman. SPI yang efektif dapat membantu Direksi dan Dewan Komisaris menjaga aset Bank, menjamin tersedianya pelaporan keuangan dan manajerial yang dapat dipercaya, meningkatkan kepatuhan Bank terhadap ketentuan dan peraturan perundang-undangan, serta mengurangi Risiko terjadinya kerugian, penyimpangan, dan pelanggaran aspek kehati-hatian.
2. Terselenggaranya SPI Bank yang andal dan efektif menjadi tanggung jawab dari Direksi, Dewan Komisaris, dan para pejabat Bank. Selain itu, Direksi dan Dewan Komisaris juga berkewajiban untuk meningkatkan budaya Risiko (*risk culture*) yang efektif pada organisasi Bank dan memastikan hal tersebut melekat di setiap jenjang organisasi.
3. SPI perlu mendapat perhatian Bank, mengingat bahwa salah satu faktor penyebab terjadinya kesulitan usaha Bank adalah adanya berbagai kelemahan dalam pelaksanaan SPI Bank, antara lain:
   a. kurangnya mekanisme pengawasan, tidak jelasnya akuntabilitas dari Direksi dan Dewan Komisaris, dan kegagalan dalam mengembangkan budaya pengendalian intern pada seluruh jenjang organisasi;
   b. kurang memadainya pelaksanaan identifikasi dan penilaian atas Risiko dari kegiatan operasional Bank;
   c. tidak ada atau gagalnya suatu pengendalian pokok terhadap kegiatan operasional Bank, seperti pemisahan fungsi, otorisasi, verifikasi, dan kaji ulang atas eksposur Risiko dan kinerja Bank;
   d. kurangnya komunikasi dan informasi antar jenjang dalam organisasi Bank, khususnya informasi di tingkat pengambil keputusan tentang penurunan kualitas eksposur Risiko dan penerapan tindakan perbaikan;
   e. kurang memadai atau kurang efektifnya program audit intern dan kegiatan pemantauan lainnya; dan
   f. kurangnya komitmen manajemen Bank untuk melakukan proses pengendalian intern dan menerapkan sanksi yang tegas

terhadap pelanggaran ketentuan yang berlaku, serta kebijakan dan prosedur yang telah ditetapkan Bank.

II. RUANG LINGKUP SISTEM PENGENDALIAN INTERN BANK

1. Pengertian dan Tujuan Sistem Pengendalian Intern Bank

a. Pengertian

Pengendalian intern merupakan suatu mekanisme pengawasan yang ditetapkan oleh manajemen Bank secara berkesinambungan (*on going basis*), guna:

1) menjaga dan mengamankan harta kekayaan Bank;
2) menjamin tersedianya laporan yang lebih akurat;
3) meningkatkan kepatuhan terhadap ketentuan yang berlaku;
4) mengurangi dampak keuangan atau dampak kerugian, penyimpangan termasuk *fraud,* dan pelanggaran aspek kehati-hatian; dan
5) meningkatkan efektivitas organisasi dan meningkatkan efisiensi biaya.

b. Tujuan

1) Kepatuhan Terhadap Ketentuan dan Peraturan Perundang-undangan atau Tujuan Kepatuhan

Tujuan Kepatuhan dimaksudkan untuk menjamin bahwa semua kegiatan usaha Bank telah dilaksanakan sesuai dengan ketentuan dan peraturan perundang-undangan, baik ketentuan yang dikeluarkan oleh pemerintah, Otoritas Jasa Keuangan maupun kebijakan, ketentuan, dan prosedur intern yang ditetapkan oleh Bank.

2) Tersedianya Informasi Keuangan dan Manajemen yang Lengkap, Akurat, Tepat Guna, dan Tepat Waktu atau Tujuan Informasi

Tujuan Informasi dimaksudkan untuk menjamin tersedianya laporan yang lengkap, akurat, tepat guna, dan tepat waktu yang diperlukan dalam rangka pengambilan keputusan yang tepat dan dapat dipertanggungjawabkan.

3) Efektivitas dan Efisiensi dalam Kegiatan Usaha Bank atau Tujuan Operasional

Tujuan Operasional dimaksudkan untuk meningkatkan efektivitas dan efisiensi terhadap penggunaan aset dan sumber daya lainnya dalam rangka melindungi Bank dari Risiko kerugian.

4) Meningkatkan Efektivitas Budaya Risiko (*Risk Culture*) pada Organisasi Bank Secara Menyeluruh atau Tujuan Budaya Risiko

Tujuan Budaya Risiko dimaksudkan untuk mengidentifikasi kelemahan dan menilai penyimpangan secara dini serta menilai kembali kewajaran kebijakan dan prosedur yang ada di Bank secara berkesinambungan.

2. Pihak-pihak yang Berkepentingan dengan Sistem Pengendalian Intern Bank

Terselenggaranya SPI yang andal dan efektif menjadi tanggung jawab semua pihak yang terlibat dalam organisasi Bank, antara lain sebagai berikut:

a. Direksi

Direksi Bank mempunyai tanggung jawab menciptakan dan memelihara SPI yang efektif serta memastikan bahwa sistem tersebut berjalan secara aman dan andal sesuai dengan tujuan pengendalian intern yang ditetapkan oleh Bank.

Sementara itu direktur yang membawahkan fungsi kepatuhan harus berperan aktif dalam mencegah adanya penyimpangan yang dilakukan oleh manajemen dalam menetapkan kebijakan berkaitan dengan prinsip kehati–hatian.

b. Dewan Komisaris

Dewan Komisaris Bank mempunyai tanggung jawab melakukan pengawasan terhadap pelaksanaan pengendalian intern secara umum, termasuk kebijakan Direksi yang menetapkan pengendalian intern tersebut.

c. Satuan Kerja Audit Intern (SKAI)

SKAI harus mampu mengevaluasi dan berperan aktif dalam meningkatkan efektivitas SPI secara berkesinambungan berkaitan dengan pelaksanaan operasional Bank yang berpotensi menimbulkan kerugian dalam pencapaian sasaran

yang telah ditetapkan oleh manajemen Bank. Di samping itu, Bank perlu memberikan perhatian kepada pelaksanaan audit intern yang independen melalui jalur pelaporan yang memadai, dan keahlian auditor intern khususnya terhadap praktik dan penerapan penilaian Risiko.

d. Pejabat dan pegawai Bank

Setiap pejabat dan pegawai Bank harus memahami dan melaksanakan SPI yang telah ditetapkan oleh manajemen Bank. Pengendalian intern yang efektif akan meningkatkan tanggung jawab pejabat dan pegawai Bank, mendorong budaya Risiko (*risk culture*) yang memadai, dan mempercepat proses identifikasi terhadap praktik perbankan yang tidak sehat dan terhadap organisasi melalui sistem deteksi dini yang efisien.

e. Pihak-pihak ekstern

Pihak-pihak ekstern Bank antara lain Otoritas Jasa Keuangan, auditor ekstern, dan nasabah Bank yang berkepentingan terhadap terlaksananya SPI Bank yang andal dan efektif.

3. Faktor Pertimbangan dalam Penyusunan Sistem Pengendalian Intern Bank

Bank harus memiliki SPI yang dapat diterapkan secara efektif, dengan memperhatikan faktor:

a. total aset;
b. jenis produk dan aktivitas yang ditawarkan, termasuk produk dan aktivitas baru;
c. kompleksitas operasional, termasuk jaringan kantor;
d. profil Risiko dari setiap kegiatan usaha;
e. metode yang digunakan untuk pengolahan data dan teknologi informasi serta metodologi yang diterapkan untuk pengukuran, pemantauan, dan pembatasan (*limit*) Risiko; dan
f. ketentuan dan peraturan perundang-undangan.

4. Lingkungan Pengendalian (*Control Environment*)

Lingkungan pengendalian mencerminkan keseluruhan komitmen, perilaku, kepedulian serta langkah Direksi dan Dewan Komisaris Bank dalam melaksanakan kegiatan pengendalian operasional Bank.

Unsur-unsur lingkungan pengendalian meliputi:

a. struktur organisasi yang memadai;
b. gaya kepemimpinan dan filosofi manajemen Bank;

c. integritas dan nilai-nilai etika serta kompetensi seluruh pegawai;
d. kebijakan dan prosedur sumber daya manusia Bank;
e. atensi dan arahan manajemen Bank dan komite lainnya, seperti Komite Manajemen Risiko; dan
f. faktor-faktor ekstern yang mempengaruhi operasional Bank dan penerapan Manajemen Risiko.

III. KOMPONEN UTAMA SISTEM PENGENDALIAN INTERN BANK

Pengendalian intern Bank terdiri dari lima komponen utama yang satu sama lain saling berkaitan, yaitu Pengawasan oleh Manajemen dan Budaya Pengendalian (*Management Oversight and Control Culture*), Identifikasi dan Penilaian Risiko (*Risk Recognition and Assessment*), Kegiatan Pengendalian dan Pemisahan Fungsi (*Control Activities and Segregation of Duties*), Sistem Akuntansi, Informasi dan Komunikasi (*Accountancy, Information and Communication*), serta Kegiatan Pemantauan dan Tindakan Koreksi Penyimpangan atau Kelemahan (*Monitoring Activities and Correcting Deficiencies*).

Pengendalian Intern paling sedikit mencakup lima komponen utama, yaitu:

1. Pengawasan oleh Manajemen dan Budaya Pengendalian
   a. Direksi

      Direksi mempunyai tanggung jawab:
      1) melaksanakan kebijakan dan strategi yang telah disetujui oleh Dewan Komisaris;
      2) mengembangkan prosedur untuk mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko yang dihadapi Bank;
      3) memelihara suatu struktur organisasi yang mencerminkan kewenangan, tanggung jawab, dan hubungan pelaporan yang jelas;
      4) memastikan bahwa pendelegasian wewenang berjalan secara efektif yang didukung oleh penerapan akuntabilitas yang konsisten;
      5) menetapkan kebijakan dan strategi serta prosedur pengendalian intern; dan
      6) memantau kecukupan dan efektivitas dari SPI.

Dalam rangka melaksanakan tanggung jawab tersebut, Direksi harus melakukan langkah-langkah, antara lain:

i. menugaskan para manajer atau pejabat dan pegawai yang bertanggung jawab dalam kegiatan atau fungsi tertentu untuk menyusun kebijakan dan prosedur pengendalian intern terhadap kegiatan operasional serta kecukupan organisasi;

ii. melakukan pengendalian yang efektif untuk memastikan bahwa para manajer atau pejabat dan pegawai telah mengembangkan dan melaksanakan kebijakan dan prosedur yang telah ditetapkan;

iii. mendokumentasikan dan mensosialisasikan struktur organisasi yang secara jelas menggambarkan jalur kewenangan dan tanggung jawab pelaporan serta menyelenggarakan suatu sistem komunikasi yang efektif kepada seluruh jenjang organisasi Bank;

iv. mengambil langkah-langkah yang tepat untuk memastikan bahwa kegiatan fungsi pengendalian intern telah dilaksanakan oleh manajer atau pejabat dan pegawai yang memiliki pengalaman dan kemampuan yang memadai; dan

v. melaksanakan secara efektif langkah perbaikan atau rekomendasi dari auditor intern dan/atau auditor ekstern, antara lain dengan cara menugaskan pegawai yang bertanggung jawab untuk melaksanakannya.

b. Dewan Komisaris

Dewan Komisaris mempunyai tanggung jawab:

1) mengesahkan dan mengkaji ulang secara berkala terhadap kebijakan dan strategi usaha Bank secara keseluruhan;

2) memahami Risiko utama yang dihadapi Bank, menetapkan tingkat toleransi Risiko, dan memastikan bahwa Direksi telah melakukan langkah-langkah yang diperlukan untuk mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko tersebut;

3) mengesahkan struktur organisasi; dan

4) memastikan bahwa Direksi telah memantau efektivitas pelaksanaan SPI.

Dalam rangka memenuhi tanggung jawab tersebut maka Dewan Komisaris:

i. harus dapat bersikap objektif, memiliki pengetahuan dan kemampuan, serta keingintahuan mengenai kegiatan usaha dan Risiko Bank;

ii. harus berperan secara aktif untuk memastikan adanya perbaikan terhadap permasalahan Bank yang dapat mengurangi efektivitas SPI, seperti adanya hambatan dalam arus informasi dari bawahan kepada pimpinan dan kelemahan dalam pelaksanaan fungsi keuangan, hukum, dan audit intern;

iii. secara berkala mengadakan pertemuan dengan Direksi dan pejabat eksekutif Bank untuk membahas efektivitas SPI;

iv. melakukan kaji ulang terhadap hasil evaluasi pelaksanaan pengendalian intern yang dibuat oleh Direksi, SKAI, dan auditor ekstern;

v. secara berkala melakukan upaya-upaya untuk memastikan bahwa Direksi telah menindaklanjuti dengan tepat atas temuan dan rekomendasi yang disampaikan oleh Otoritas Jasa Keuangan, auditor intern, serta auditor ekstern; dan

vi. secara berkala melakukan kaji ulang terhadap validitas strategi Bank yang telah ditetapkan.

c. Budaya Pengendalian

Direksi dan Dewan Komisaris bertanggung jawab dalam meningkatkan etika kerja dan integritas yang tinggi serta menciptakan suatu budaya organisasi yang menekankan kepada seluruh pegawai Bank mengenai pentingnya pengendalian intern yang berlaku di Bank.

Dalam rangka menciptakan budaya pengendalian tersebut, langkah-langkah yang harus diperhatikan dan dilakukan oleh Bank, antara lain:

1) Direksi dan Dewan Komisaris harus menjadi panutan (*role model*) bagi seluruh pegawai atau memiliki komitmen pribadi yang tinggi terhadap pengembangan Bank yang sehat;

2) Direksi dan Dewan Komisaris harus mampu mengelola sumber daya manusia, termasuk dalam proses penempatan

pegawai yang sesuai dengan keterampilan, pengetahuan, dan perilaku; dan/atau

3) meningkatkan kesadaran bagi seluruh pegawai Bank mengenai pentingnya efektivitas pelaksanaan tugas serta tanggung jawab masing-masing dan selanjutnya pegawai mengomunikasikan kepada pihak manajemen yang terkait mengenai setiap permasalahan yang terjadi dalam kegiatan operasional Bank.

Untuk mendukung budaya pengendalian tersebut maka seluruh kebijakan, standar, dan prosedur operasional harus didokumentasikan secara tertulis dan tersedia bagi setiap pegawai yang terkait.

Dalam rangka memperkuat nilai-nilai etika, Bank harus menghindari kebijakan dan praktik yang dapat mengakibatkan dorongan atau peluang untuk melakukan penyimpangan atau pelanggaran, seperti penekanan pada pencapaian target jangka pendek dengan mengabaikan dampak Risiko yang bersifat jangka panjang, sistem kompensasi yang hanya menitikberatkan pada kinerja jangka pendek, pemisahan fungsi yang tidak efektif, dan pengenaan sanksi yang terlalu ringan atau terlalu berlebihan atas pelanggaran yang dilakukan.

2. Identifikasi dan Penilaian Risiko

a. Penilaian Risiko merupakan serangkaian tindakan yang dilaksanakan oleh Direksi dalam rangka identifikasi, analisis, dan menilai Risiko yang dihadapi oleh Bank dalam rangka pencapaian target yang ditetapkan.

b. Risiko dapat timbul atau berubah sesuai dengan kondisi Bank, antara lain:

1) perubahan kegiatan operasional Bank;
2) perubahan susunan personalia;
3) perubahan sistem informasi;
4) pertumbuhan yang cepat pada kegiatan usaha tertentu;
5) perkembangan teknologi;
6) pengembangan jasa, produk atau aktivitas baru;
7) terjadinya penggabungan usaha, peleburan usaha, pengambilalihan, dan restrukturisasi Bank;
8) perubahan dalam sistem akuntansi;

9) ekspansi usaha;
10) perubahan hukum dan peraturan; dan
11) perubahan perilaku serta ekspektasi nasabah.

c. Suatu SPI yang efektif mengharuskan Bank secara terus menerus mengidentifikasi dan menilai Risiko yang dapat mempengaruhi pencapaian sasaran. Penilaian Risiko harus pula dilakukan oleh auditor intern sehingga cakupan audit yang dilakukan lebih luas dan menyeluruh.

d. Penilaian Risiko ini harus dapat mengidentifikasi jenis Risiko yang dihadapi oleh Bank, penetapan limit Risiko, dan teknik pengendalian Risiko tersebut. Metodologi penilaian Risiko harus menjadi tolok ukur untuk membuat profil Risiko dalam bentuk dokumentasi data, yang dapat diperbarui secara berkala. Penilaian Risiko juga meliputi penilaian terhadap Risiko yang dapat diukur (kuantitatif) dan tidak dapat diukur (kualitatif) maupun terhadap Risiko yang dapat dikendalikan dan tidak dapat dikendalikan, dengan memperhatikan biaya dan manfaatnya. Selanjutnya Bank harus memutuskan untuk mengambil Risiko tersebut atau tidak, dengan cara mengurangi kegiatan usaha tertentu.

e. Penilaian Risiko tersebut harus mencakup semua Risiko yang dihadapi, baik Risiko individual maupun secara keseluruhan (*aggregate*), yang meliputi Risiko Kredit, Risiko Pasar, Risiko Likuiditas, Risiko Operasional, Risiko Hukum, Risiko Reputasi, Risiko Stratejik, dan Risiko Kepatuhan. Khusus untuk Bank Umum Syariah ditambahkan Risiko Imbal Hasil dan Risiko Investasi.

f. Pengendalian intern perlu dikaji ulang secara tepat dalam hal terdapat Risiko yang belum dikendalikan, baik Risiko yang sebelumnya sudah ada maupun Risiko yang baru muncul. Pelaksanaan kaji ulang tersebut antara lain dengan melakukan evaluasi secara terus menerus mengenai pengaruh dari setiap perubahan lingkungan dan kondisi serta dampak dari pencapaian target atau efektivitas pengendalian intern dalam kegiatan operasional dan organisasi Bank.

3. Kegiatan Pengendalian dan Pemisahan Fungsi

Kegiatan pengendalian harus melibatkan seluruh pegawai Bank, termasuk Direksi. Oleh karena itu kegiatan pengendalian akan berjalan efektif apabila direncanakan dan diterapkan guna mengendalikan Risiko yang telah diidentifikasi. Kegiatan pengendalian mencakup pula penetapan kebijakan dan prosedur pengendalian serta proses verifikasi lebih dini untuk memastikan bahwa kebijakan dan prosedur tersebut secara konsisten dipatuhi, serta merupakan kegiatan yang tidak terpisahkan dari setiap fungsi atau kegiatan Bank sehari-hari.

a. Kegiatan Pengendalian

Kegiatan pengendalian meliputi kebijakan, prosedur, dan praktik yang memberikan keyakinan pejabat dan pegawai Bank bahwa arahan Direksi dan Dewan Komisaris Bank telah dilaksanakan secara efektif. Kegiatan pengendalian tersebut akan dapat membantu Direksi dan Dewan Komisaris Bank dalam mengelola dan mengendalikan Risiko yang dapat mempengaruhi kinerja atau mengakibatkan kerugian Bank.

Kegiatan pengendalian diterapkan pada semua tingkatan fungsional sesuai dengan struktur organisasi Bank, yang paling sedikit meliputi:

1) Kaji Ulang Manajemen (*Top Level Reviews*)

Direksi Bank secara berkala meminta penjelasan (informasi) dan laporan kinerja operasional dari pejabat dan pegawai sehingga memungkinkan untuk mengkaji ulang hasil kemajuan (realisasi) dibandingkan dengan target yang akan dicapai, seperti laporan keuangan dibandingkan dengan rencana anggaran yang ditetapkan. Berdasarkan kaji ulang tersebut, Direksi segera mendeteksi permasalahan seperti kelemahan pengendalian, kesalahan laporan keuangan, atau *fraud*.

2) Kaji Ulang Kinerja Operasional (*Functional Review*)

Kaji ulang ini dilaksanakan oleh SKAI dengan frekuensi yang lebih tinggi, baik kaji ulang secara harian, mingguan, maupun bulanan. Dalam kaji ulang kinerja operasional, SKAI:

a) melakukan kaji ulang terhadap penilaian Risiko (laporan profil Risiko) yang dihasilkan oleh satuan kerja Manajemen Risiko;

b) menganalisis data operasional, baik data yang terkait Risiko maupun data keuangan, yaitu melakukan verifikasi rincian dan kegiatan transaksi dibandingkan dengan *output* (laporan) yang dihasilkan oleh satuan kerja Manajemen Risiko; dan

c) melakukan kaji ulang terhadap realisasi pelaksanaan rencana kerja dan anggaran, guna:

(1) mengidentifikasi penyebab penyimpangan yang signifikan; dan

(2) menetapkan persyaratan untuk tindakan perbaikan (*corrective actions*).

3) Pengendalian Sistem Informasi

a) Bank melaksanakan verifikasi terhadap akurasi dan kelengkapan dari transaksi dan melaksanakan prosedur otorisasi, sesuai dengan ketentuan intern.

b) Kegiatan pengendalian sistem informasi dapat digolongkan dalam 2 (dua) kriteria, yaitu:

(1) pengendalian umum, meliputi pengendalian terhadap operasional pusat data, sistem pengadaan dan pemeliharaan perangkat lunak, pengamanan akses, serta pengembangan dan pemeliharaan sistem aplikasi yang ada. Pengendalian umum ini diterapkan terhadap *mainframe, server,* dan *users workstation,* serta jaringan internal-eksternal; dan

(2) pengendalian aplikasi, diterapkan terhadap program yang digunakan Bank dalam mengolah transaksi dan untuk memastikan bahwa semua transaksi adalah benar, akurat, dan telah diotorisasi secara benar. Selain itu, pengendalian aplikasi harus dapat memastikan tersedianya proses audit yang efektif dan untuk mengecek kebenaran proses audit dimaksud.

4) Pengendalian Aset Fisik (*Physical Controls*)
   a) Pengendalian aset fisik dilaksanakan untuk menjamin terselenggaranya pengamanan fisik terhadap aset Bank.
   b) Kegiatan ini meliputi pengamanan aset, catatan, dan akses terbatas terhadap program komputer dan *file* data, serta membandingkan nilai aset dan liabilitas Bank dengan nilai yang tercantum pada catatan pengendali, khususnya pengecekan nilai aset secara berkala.
5) Dokumentasi
   a) Bank paling sedikit harus memformalkan dan mendokumentasikan kebijakan, prosedur, sistem dan standar akuntansi, serta proses audit secara memadai.
   b) Dokumen tersebut harus diperbarui secara berkala guna menggambarkan kegiatan operasional Bank secara aktual, serta harus diinformasikan kepada pejabat dan pegawai Bank.
   c) Atas suatu permintaan, dokumen harus senantiasa tersedia untuk kepentingan auditor intern, akuntan publik, dan pengawasan Bank oleh Otoritas Jasa Keuangan.
   d) Akurasi dan ketersediaan dokumen harus dinilai oleh auditor intern ketika melakukan audit secara rutin maupun non-rutin.

b. Pemisahan Fungsi
   1) Pemisahan fungsi dimaksudkan agar setiap orang dalam jabatannya tidak memiliki peluang untuk melakukan dan menyembunyikan kesalahan atau penyimpangan dalam pelaksanaan tugas pada seluruh jenjang organisasi dan seluruh langkah kegiatan operasional. Bank harus mematuhi prinsip pemisahan fungsi ini, yang dikenal sebagai "*Four-Eyes Principle*".
   2) Dalam hal diperlukan karena perubahan karakteristik kegiatan usaha dan transaksi serta organisasi Bank, Direksi Bank harus menetapkan prosedur (kewenangan)

termasuk penetapan daftar petugas yang dapat mengakses suatu transaksi atau kegiatan usaha yang berisiko tinggi.

3) SPI yang efektif mensyaratkan adanya pemisahan fungsi dan menghindari pemberian wewenang serta tanggung jawab yang dapat menimbulkan berbagai benturan kepentingan (*conflict of interest*). Seluruh aspek yang dapat menimbulkan pertentangan kepentingan tersebut harus diidentifikasi, diminimalisasi, dan dipantau secara hati-hati oleh pihak lain yang independen, seperti akuntan publik.

4) Dalam pelaksanaan pemisahan fungsi tersebut, Bank harus melakukan langkah-langkah, antara lain:

a) menetapkan fungsi atau tugas tertentu pada Bank yang harus dipisahkan atau dialokasikan kepada beberapa orang dalam rangka mengurangi Risiko terjadinya manipulasi data keuangan atau penyalahgunaan aset Bank;

b) pemisahan fungsi tersebut tidak terbatas pada kegiatan *front* dan *back office*, tetapi juga dalam rangka pengendalian terhadap:

(1) persetujuan atas pengeluaran dana dan realisasi pengeluaran;

(2) rekening nasabah dan rekening pemilik Bank;

(3) transaksi dalam pembukuan Bank;

(4) pemberian informasi kepada nasabah Bank;

(5) penilaian terhadap kecukupan dokumentasi perkreditan atau pembiayaan dan pemantauan debitur setelah pencairan kredit atau pembiayaan;

(6) kegiatan usaha lain yang dapat menimbulkan benturan kepentingan yang signifikan; dan

(7) independensi fungsi manajemen Risiko pada Bank.

4. Sistem Akuntansi, Informasi, dan Komunikasi

Sistem akuntansi, informasi, dan komunikasi yang memadai dimaksudkan agar dapat mengidentifikasi masalah yang mungkin timbul dan digunakan sebagai sarana tukar menukar informasi dalam rangka pelaksanaan tugas sesuai dengan tanggung jawab masing-masing.

a. Sistem Akuntansi

1) Sistem akuntansi meliputi metode dan catatan dalam rangka mengidentifikasi, mengelompokkan, menganalisis, mengklasifikasi, mencatat atau membukukan, dan melaporkan transaksi Bank.

2) Untuk menjamin data akuntansi yang akurat dan konsisten dengan data yang tersedia berdasarkan hasil olahan sistem, proses rekonsiliasi antara data akuntansi dan sistem informasi manajemen harus dilaksanakan secara berkala atau paling sedikit setiap bulan. Setiap penyimpangan yang terjadi harus segera diinvestigasi dan diatasi permasalahannya. Proses rekonsiliasi juga harus didokumentasikan sebagai bagian dari persyaratan proses jejak audit secara keseluruhan.

b. Sistem Informasi

1) Sistem informasi harus dapat menghasilkan laporan mengenai kegiatan usaha, kondisi keuangan, penerapan Manajemen Risiko, dan pemenuhan ketentuan yang mendukung pelaksanaan tugas Direksi dan Dewan Komisaris.

2) SPI yang efektif paling sedikit menyediakan data atau informasi internal yang cukup dan menyeluruh mengenai keuangan, kepatuhan Bank terhadap ketentuan dan peraturan perundang-undangan, informasi pasar (kondisi eksternal), dan setiap kejadian serta kondisi yang diperlukan dalam rangka pengambilan keputusan yang tepat dan dapat dipertanggungjawabkan.

3) SPI paling sedikit menyediakan sistem informasi yang dapat dipercaya mengenai seluruh aktivitas fungsional Bank, terutama aktivitas fungsional yang signifikan dan memiliki potensi Risiko tinggi. Sistem informasi tersebut termasuk sistem penyimpanan dan penggunaan data elektronik harus dijamin keamanannya, dipantau oleh pihak yang independen (auditor intern), dan didukung oleh program kontinjensi yang memadai.

4) Bank paling sedikit harus mengorganisasikan suatu rencana pemulihan darurat (*contingency recovery plan*) dan

sistem rekam cadang (*back-up*) untuk mencegah kegagalan usaha yang berisiko tinggi. Untuk memastikan bahwa seluruh rencana dan proses pemulihan darurat (*contingency recovery plan*) serta sistem rekam cadang (*back-up*) telah bekerja secara efektif, pelaksanaan prosedur, proses, dan sistem rekam cadang (*back-up*) harus didokumentasikan dan diuji kembali efektivitasnya secara berkala. Bank harus mendokumentasikan pelaksanaan pengujian secara berkala dan Direksi harus memberikan perhatian yang penuh terhadap temuan kelemahan pada prosedur, proses, dan sistem yang didasarkan atas hasil pengujian serta selanjutnya mengambil langkah perbaikan yang diperlukan.

5) Bank paling sedikit harus memiliki dan memelihara sistem informasi manajemen yang diselenggarakan, baik dalam bentuk elektronik maupun bukan elektronik. Mengingat bahwa sistem informasi elektronik dan penggunaan teknologi informasi tersebut mempunyai dampak Risiko, Bank harus mengendalikan secara efektif guna menghindari adanya gangguan usaha dan kemungkinan timbul kerugian Bank yang signifikan.

6) Dalam rangka pengendalian intern terhadap penyelenggaraan sistem dan teknologi informasi, Bank harus memperhatikan hal-hal sebagai berikut:

   a) Ketersediaan bukti dan dokumen yang memadai dalam rangka mendukung proses jejak audit. Proses jejak audit harus dilaksanakan secara efektif dan didokumentasikan untuk memastikan bahwa proses otomasi telah bekerja secara efektif dan akurat. SKAI harus melakukan penilaian terhadap efektivitas dan akurasi proses jejak audit ketika melakukan evaluasi atas pelaksanaan pengendalian intern Bank.

   b) Pelaksanaan pengendalian terhadap sistem komputer dan pengamanannya (*general controls*) maupun pengendalian terhadap aplikasi perangkat lunak dan prosedur manual lainnya (*application controls*).

c) Antisipasi terjadinya Risiko gangguan atau kerugian yang disebabkan oleh faktor yang berada di luar jangkauan pengendalian rutin Bank sehingga Bank harus menyelenggarakan sistem pemulihan (*recovery*) dan rencana kontinjensi serta pengecekan secara berkala atas kemungkinan terjadinya hal-hal yang sulit diprediksi sebelumnya (*disaster and recovery plan*).

d) Sistem informasi harus menyediakan data dan informasi yang relevan, akurat, tepat waktu, dapat diakses oleh pihak yang berkepentingan, dan disajikan dalam format yang konsisten.

e) Sebagai bagian dari proses pencatatan atau pembukuan, sistem informasi harus didukung oleh sistem akuntansi yang baik termasuk penetapan prosedur dan jadwal retensi pencatatan transaksi.

c. Sistem Komunikasi

1) Sistem komunikasi harus mampu memberikan informasi kepada seluruh pihak, baik intern maupun ekstern seperti Otoritas Jasa Keuangan, auditor ekstern, pemegang saham, dan nasabah Bank.

2) SPI Bank harus memastikan adanya saluran komunikasi yang efektif agar seluruh pejabat dan pegawai Bank sepenuhnya memahami serta mematuhi kebijakan dan prosedur dalam melaksanakan tugas dan tanggung jawab.

3) Direksi Bank harus menyelenggarakan saluran komunikasi yang efektif agar informasi yang diperlukan terjangkau oleh pihak yang berkepentingan. Persyaratan ini berlaku untuk setiap informasi, baik mengenai kebijakan dan prosedur yang telah ditetapkan, eksposur Risiko, dan transaksi aktual maupun mengenai kinerja operasional Bank.

4) Struktur organisasi Bank harus memungkinkan adanya arus informasi yang memadai, yaitu informasi ke atas, ke bawah, dan lintas satuan kerja atau unit kerja, sebagai berikut:

a) Informasi ke atas untuk memastikan bahwa Direksi, Dewan Komisaris, dan pejabat eksekutif Bank mengetahui Risiko dan kinerja operasional Bank.

Saluran informasi harus dapat merespon dengan baik sehingga menghasilkan pelaksanaan langkah-langkah perbaikan dan dapat diketahui oleh jajaran manajemen.

b) Informasi ke bawah untuk memastikan bahwa tujuan, strategi, dan ekspektasi Bank serta kebijakan dan prosedur telah dikomunikasikan kepada para manajer di tingkat bawah dan para pelaksana.

c) Informasi lintas satuan kerja atau unit kerja untuk memastikan bahwa informasi yang diketahui oleh suatu satuan kerja tertentu dapat disampaikan kepada satuan kerja lain yang terkait, khususnya untuk mencegah benturan kepentingan dalam pengambilan keputusan dan untuk menciptakan koordinasi yang memadai.

5. Kegiatan Pemantauan dan Tindakan Koreksi Penyimpangan

a. Kegiatan Pemantauan

1) Bank harus melakukan pemantauan secara terus menerus terhadap efektivitas keseluruhan pelaksanaan pengendalian intern. Pemantauan terhadap Risiko utama Bank harus diprioritaskan dan berfungsi sebagai bagian dari kegiatan Bank sehari-hari termasuk evaluasi secara berkala, baik oleh satuan kerja operasional (*risk taking unit*) maupun oleh SKAI.

2) Bank harus memantau dan mengevaluasi kecukupan SPI secara terus menerus berkaitan dengan adanya perubahan kondisi intern dan ekstern serta harus meningkatkan kapasitas SPI tersebut agar efektivitasnya dapat ditingkatkan.

3) Langkah-langkah yang harus dilakukan oleh Bank dalam rangka terselenggaranya kegiatan pemantauan yang efektif, paling sedikit:

a) memastikan bahwa fungsi pemantauan telah ditetapkan secara jelas dan terstruktur dengan baik dalam organisasi Bank;

b) menetapkan satuan kerja atau pegawai yang ditugaskan untuk memantau efektivitas pengendalian intern;

c) menetapkan frekuensi yang tepat untuk kegiatan pemantauan yang didasarkan pada Risiko yang melekat pada Bank dan sifat atau frekuensi perubahan yang terjadi dalam kegiatan operasional;

d) mengintegrasikan SPI ke dalam kegiatan operasional dan menyediakan laporan rutin seperti jurnal pembukuan, *management review*, dan laporan mengenai persetujuan atas eksepsi atau penyimpangan terhadap kebijakan dan prosedur yang ditetapkan (justifikasi atas *irregularities*) yang selanjutnya dilakukan kaji ulang;

e) melakukan kaji ulang terhadap dokumentasi dan hasil evaluasi dari satuan kerja atau pegawai yang ditugaskan untuk melakukan pemantauan; dan

f) menetapkan informasi atau umpan balik (*feed back*) dalam suatu format dan frekuensi yang tepat.

b. Fungsi SKAI

1) Bank harus menyelenggarakan audit intern yang efektif dan menyeluruh terhadap SPI. Pelaksanaan audit intern yang dilaksanakan oleh SKAI harus didukung oleh tenaga auditor yang independen, kompeten, dan memiliki jumlah yang memadai.

2) Sebagai bagian dari SPI, SKAI harus melaporkan hasil temuan secara langsung kepada Dewan Komisaris atau Komite Audit (apabila ada), direktur utama, dan direktur yang membawahkan fungsi kepatuhan.

3) SKAI harus melakukan penilaian yang independen mengenai kecukupan dari dan kepatuhan Bank terhadap kebijakan dan prosedur yang telah ditetapkan.

4) Dalam menetapkan kedudukan, wewenang, tanggung jawab, profesionalisme, organisasi, dan ruang lingkup tugas SKAI maka Bank harus berpedoman pula pada ketentuan peraturan perundang-undangan mengenai pelaksanaan

fungsi kepatuhan bank umum dan standar pelaksanaan fungsi audit intern.

c. Perbaikan Kelemahan dan Tindakan Koreksi Penyimpangan

1) Kelemahan dalam pengendalian intern, baik yang diidentifikasi oleh satuan kerja operasional (*risk taking unit*), SKAI, maupun pihak lainnya, harus segera dilaporkan kepada dan menjadi perhatian pejabat dan/atau Direksi yang berwenang. Kelemahan pengendalian intern yang material harus dilaporkan kepada Dewan Komisaris.

2) Langkah-langkah perbaikan yang harus dilakukan Bank dalam rangka memperbaiki kelemahan pengendalian intern, antara lain:

a) setiap laporan mengenai kelemahan dalam pengendalian intern atau tidak efektifnya pengendalian Risiko Bank harus segera ditindaklanjuti oleh Direksi, Dewan Komisaris, dan pejabat eksekutif terkait;

b) SKAI harus melakukan kaji ulang atau langkah pemantauan lainnya yang memadai terhadap kelemahan yang terjadi dan segera melaporkan kepada Dewan Komisaris, Komite Audit (apabila ada), dan direktur utama dalam hal masih terdapat kelemahan yang belum diperbaiki atau rekomendasi tindakan korektif yang belum ditindaklanjuti;

c) untuk memastikan bahwa seluruh kelemahan segera ditindaklanjuti maka Direksi harus menciptakan suatu sistem yang dapat menelusuri kelemahan pada pengendalian intern dan mengambil langkah perbaikan; dan

d) Direksi dan Dewan Komisaris harus menerima laporan secara berkala berupa ikhtisar mengenai hasil identifikasi seluruh permasalahan dalam pengendalian intern.

IV. LAIN-LAIN

Dalam penerapan pengendalian intern, Bank harus juga memperhatikan aspek-aspek pengendalian intern yang ditetapkan dalam ketentuan

peraturan perundang-undangan lainnya, antara lain yang mengatur mengenai:

1. kewajiban penyusunan dan pelaksanaan kebijakan perkreditan atau pembiayaan bagi bank umum;
2. penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum;
3. transaksi derivatif;
4. restrukturisasi kredit;
5. Standar Pelaksanaan Fungsi Audit Intern Bank (SPFAIB);
6. penerapan program anti pencucian uang dan pencegahan pendanaan terorisme bagi bank umum;
7. transparansi dan publikasi laporan bank;
8. prinsip kehati-hatian dalam kegiatan penyertaan modal; dan
9. penerapan manajemen risiko bagi bank umum dan penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah.

Ditetapkan di Jakarta
pada tanggal 7 Juli 2017

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,

ttd

NELSON TAMPUBOLON

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana

LAMPIRAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 35 /SEOJK.03/2017

TENTANG

PEDOMAN STANDAR SISTEM PENGENDALIAN INTERN BAGI BANK UMUM

DAFTAR ISI

I. LATAR BELAKANG

1. Sistem Pengendalian Intern (SPI) yang efektif merupakan komponen penting dalam manajemen Bank dan menjadi dasar bagi kegiatan operasional Bank yang sehat dan aman. SPI yang efektif dapat membantu Direksi dan Dewan Komisaris menjaga aset Bank, menjamin tersedianya pelaporan keuangan dan manajerial yang dapat dipercaya, meningkatkan kepatuhan Bank terhadap ketentuan dan peraturan perundang-undangan, serta mengurangi Risiko terjadinya kerugian, penyimpangan, dan pelanggaran aspek kehati-hatian.
2. Terselenggaranya SPI Bank yang andal dan efektif menjadi tanggung jawab dari Direksi, Dewan Komisaris, dan para pejabat Bank. Selain itu, Direksi dan Dewan Komisaris juga berkewajiban untuk meningkatkan budaya Risiko (*risk culture*) yang efektif pada organisasi Bank dan memastikan hal tersebut melekat di setiap jenjang organisasi.
3. SPI perlu mendapat perhatian Bank, mengingat bahwa salah satu faktor penyebab terjadinya kesulitan usaha Bank adalah adanya berbagai kelemahan dalam pelaksanaan SPI Bank, antara lain:
   a. kurangnya mekanisme pengawasan, tidak jelasnya akuntabilitas dari Direksi dan Dewan Komisaris, dan kegagalan dalam mengembangkan budaya pengendalian intern pada seluruh jenjang organisasi;
   b. kurang memadainya pelaksanaan identifikasi dan penilaian atas Risiko dari kegiatan operasional Bank;
   c. tidak ada atau gagalnya suatu pengendalian pokok terhadap kegiatan operasional Bank, seperti pemisahan fungsi, otorisasi, verifikasi, dan kaji ulang atas eksposur Risiko dan kinerja Bank;
   d. kurangnya komunikasi dan informasi antar jenjang dalam organisasi Bank, khususnya informasi di tingkat pengambil keputusan tentang penurunan kualitas eksposur Risiko dan penerapan tindakan perbaikan;
   e. kurang memadai atau kurang efektifnya program audit intern dan kegiatan pemantauan lainnya; dan
   f. kurangnya komitmen manajemen Bank untuk melakukan proses pengendalian intern dan menerapkan sanksi yang tegas

terhadap pelanggaran ketentuan yang berlaku, serta kebijakan dan prosedur yang telah ditetapkan Bank.

II. RUANG LINGKUP SISTEM PENGENDALIAN INTERN BANK

1. Pengertian dan Tujuan Sistem Pengendalian Intern Bank

a. Pengertian

Pengendalian intern merupakan suatu mekanisme pengawasan yang ditetapkan oleh manajemen Bank secara berkesinambungan (*on going basis*), guna:

1) menjaga dan mengamankan harta kekayaan Bank;
2) menjamin tersedianya laporan yang lebih akurat;
3) meningkatkan kepatuhan terhadap ketentuan yang berlaku;
4) mengurangi dampak keuangan atau dampak kerugian, penyimpangan termasuk *fraud,* dan pelanggaran aspek kehati-hatian; dan
5) meningkatkan efektivitas organisasi dan meningkatkan efisiensi biaya.

b. Tujuan

1) Kepatuhan Terhadap Ketentuan dan Peraturan Perundang-undangan atau Tujuan Kepatuhan

Tujuan Kepatuhan dimaksudkan untuk menjamin bahwa semua kegiatan usaha Bank telah dilaksanakan sesuai dengan ketentuan dan peraturan perundang-undangan, baik ketentuan yang dikeluarkan oleh pemerintah, Otoritas Jasa Keuangan maupun kebijakan, ketentuan, dan prosedur intern yang ditetapkan oleh Bank.

2) Tersedianya Informasi Keuangan dan Manajemen yang Lengkap, Akurat, Tepat Guna, dan Tepat Waktu atau Tujuan Informasi

Tujuan Informasi dimaksudkan untuk menjamin tersedianya laporan yang lengkap, akurat, tepat guna, dan tepat waktu yang diperlukan dalam rangka pengambilan keputusan yang tepat dan dapat dipertanggungjawabkan.

3) Efektivitas dan Efisiensi dalam Kegiatan Usaha Bank atau Tujuan Operasional

Tujuan Operasional dimaksudkan untuk meningkatkan efektivitas dan efisiensi terhadap penggunaan aset dan sumber daya lainnya dalam rangka melindungi Bank dari Risiko kerugian.

4) Meningkatkan Efektivitas Budaya Risiko (*Risk Culture*) pada Organisasi Bank Secara Menyeluruh atau Tujuan Budaya Risiko

Tujuan Budaya Risiko dimaksudkan untuk mengidentifikasi kelemahan dan menilai penyimpangan secara dini serta menilai kembali kewajaran kebijakan dan prosedur yang ada di Bank secara berkesinambungan.

2. Pihak-pihak yang Berkepentingan dengan Sistem Pengendalian Intern Bank

Terselenggaranya SPI yang andal dan efektif menjadi tanggung jawab semua pihak yang terlibat dalam organisasi Bank, antara lain sebagai berikut:

a. Direksi

Direksi Bank mempunyai tanggung jawab menciptakan dan memelihara SPI yang efektif serta memastikan bahwa sistem tersebut berjalan secara aman dan andal sesuai dengan tujuan pengendalian intern yang ditetapkan oleh Bank.

Sementara itu direktur yang membawahkan fungsi kepatuhan harus berperan aktif dalam mencegah adanya penyimpangan yang dilakukan oleh manajemen dalam menetapkan kebijakan berkaitan dengan prinsip kehati–hatian.

b. Dewan Komisaris

Dewan Komisaris Bank mempunyai tanggung jawab melakukan pengawasan terhadap pelaksanaan pengendalian intern secara umum, termasuk kebijakan Direksi yang menetapkan pengendalian intern tersebut.

c. Satuan Kerja Audit Intern (SKAI)

SKAI harus mampu mengevaluasi dan berperan aktif dalam meningkatkan efektivitas SPI secara berkesinambungan berkaitan dengan pelaksanaan operasional Bank yang berpotensi menimbulkan kerugian dalam pencapaian sasaran

yang telah ditetapkan oleh manajemen Bank. Di samping itu, Bank perlu memberikan perhatian kepada pelaksanaan audit intern yang independen melalui jalur pelaporan yang memadai, dan keahlian auditor intern khususnya terhadap praktik dan penerapan penilaian Risiko.

d. Pejabat dan pegawai Bank

Setiap pejabat dan pegawai Bank harus memahami dan melaksanakan SPI yang telah ditetapkan oleh manajemen Bank. Pengendalian intern yang efektif akan meningkatkan tanggung jawab pejabat dan pegawai Bank, mendorong budaya Risiko (*risk culture*) yang memadai, dan mempercepat proses identifikasi terhadap praktik perbankan yang tidak sehat dan terhadap organisasi melalui sistem deteksi dini yang efisien.

e. Pihak-pihak ekstern

Pihak-pihak ekstern Bank antara lain Otoritas Jasa Keuangan, auditor ekstern, dan nasabah Bank yang berkepentingan terhadap terlaksananya SPI Bank yang andal dan efektif.

3. Faktor Pertimbangan dalam Penyusunan Sistem Pengendalian Intern Bank

Bank harus memiliki SPI yang dapat diterapkan secara efektif, dengan memperhatikan faktor:

a. total aset;
b. jenis produk dan aktivitas yang ditawarkan, termasuk produk dan aktivitas baru;
c. kompleksitas operasional, termasuk jaringan kantor;
d. profil Risiko dari setiap kegiatan usaha;
e. metode yang digunakan untuk pengolahan data dan teknologi informasi serta metodologi yang diterapkan untuk pengukuran, pemantauan, dan pembatasan (*limit*) Risiko; dan
f. ketentuan dan peraturan perundang-undangan.

4. Lingkungan Pengendalian (*Control Environment*)

Lingkungan pengendalian mencerminkan keseluruhan komitmen, perilaku, kepedulian serta langkah Direksi dan Dewan Komisaris Bank dalam melaksanakan kegiatan pengendalian operasional Bank.

Unsur-unsur lingkungan pengendalian meliputi:

a. struktur organisasi yang memadai;
b. gaya kepemimpinan dan filosofi manajemen Bank;

c. integritas dan nilai-nilai etika serta kompetensi seluruh pegawai;
d. kebijakan dan prosedur sumber daya manusia Bank;
e. atensi dan arahan manajemen Bank dan komite lainnya, seperti Komite Manajemen Risiko; dan
f. faktor-faktor ekstern yang mempengaruhi operasional Bank dan penerapan Manajemen Risiko.

III. KOMPONEN UTAMA SISTEM PENGENDALIAN INTERN BANK

Pengendalian intern Bank terdiri dari lima komponen utama yang satu sama lain saling berkaitan, yaitu Pengawasan oleh Manajemen dan Budaya Pengendalian (*Management Oversight and Control Culture*), Identifikasi dan Penilaian Risiko (*Risk Recognition and Assessment*), Kegiatan Pengendalian dan Pemisahan Fungsi (*Control Activities and Segregation of Duties*), Sistem Akuntansi, Informasi dan Komunikasi (*Accountancy, Information and Communication*), serta Kegiatan Pemantauan dan Tindakan Koreksi Penyimpangan atau Kelemahan (*Monitoring Activities and Correcting Deficiencies*).

Pengendalian Intern paling sedikit mencakup lima komponen utama, yaitu:

1. Pengawasan oleh Manajemen dan Budaya Pengendalian
   a. Direksi

      Direksi mempunyai tanggung jawab:
      1) melaksanakan kebijakan dan strategi yang telah disetujui oleh Dewan Komisaris;
      2) mengembangkan prosedur untuk mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko yang dihadapi Bank;
      3) memelihara suatu struktur organisasi yang mencerminkan kewenangan, tanggung jawab, dan hubungan pelaporan yang jelas;
      4) memastikan bahwa pendelegasian wewenang berjalan secara efektif yang didukung oleh penerapan akuntabilitas yang konsisten;
      5) menetapkan kebijakan dan strategi serta prosedur pengendalian intern; dan
      6) memantau kecukupan dan efektivitas dari SPI.

Dalam rangka melaksanakan tanggung jawab tersebut, Direksi harus melakukan langkah-langkah, antara lain:

i. menugaskan para manajer atau pejabat dan pegawai yang bertanggung jawab dalam kegiatan atau fungsi tertentu untuk menyusun kebijakan dan prosedur pengendalian intern terhadap kegiatan operasional serta kecukupan organisasi;

ii. melakukan pengendalian yang efektif untuk memastikan bahwa para manajer atau pejabat dan pegawai telah mengembangkan dan melaksanakan kebijakan dan prosedur yang telah ditetapkan;

iii. mendokumentasikan dan mensosialisasikan struktur organisasi yang secara jelas menggambarkan jalur kewenangan dan tanggung jawab pelaporan serta menyelenggarakan suatu sistem komunikasi yang efektif kepada seluruh jenjang organisasi Bank;

iv. mengambil langkah-langkah yang tepat untuk memastikan bahwa kegiatan fungsi pengendalian intern telah dilaksanakan oleh manajer atau pejabat dan pegawai yang memiliki pengalaman dan kemampuan yang memadai; dan

v. melaksanakan secara efektif langkah perbaikan atau rekomendasi dari auditor intern dan/atau auditor ekstern, antara lain dengan cara menugaskan pegawai yang bertanggung jawab untuk melaksanakannya.

b. Dewan Komisaris

Dewan Komisaris mempunyai tanggung jawab:

1) mengesahkan dan mengkaji ulang secara berkala terhadap kebijakan dan strategi usaha Bank secara keseluruhan;

2) memahami Risiko utama yang dihadapi Bank, menetapkan tingkat toleransi Risiko, dan memastikan bahwa Direksi telah melakukan langkah-langkah yang diperlukan untuk mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko tersebut;

3) mengesahkan struktur organisasi; dan

4) memastikan bahwa Direksi telah memantau efektivitas pelaksanaan SPI.

Dalam rangka memenuhi tanggung jawab tersebut maka Dewan Komisaris:

i. harus dapat bersikap objektif, memiliki pengetahuan dan kemampuan, serta keingintahuan mengenai kegiatan usaha dan Risiko Bank;

ii. harus berperan secara aktif untuk memastikan adanya perbaikan terhadap permasalahan Bank yang dapat mengurangi efektivitas SPI, seperti adanya hambatan dalam arus informasi dari bawahan kepada pimpinan dan kelemahan dalam pelaksanaan fungsi keuangan, hukum, dan audit intern;

iii. secara berkala mengadakan pertemuan dengan Direksi dan pejabat eksekutif Bank untuk membahas efektivitas SPI;

iv. melakukan kaji ulang terhadap hasil evaluasi pelaksanaan pengendalian intern yang dibuat oleh Direksi, SKAI, dan auditor ekstern;

v. secara berkala melakukan upaya-upaya untuk memastikan bahwa Direksi telah menindaklanjuti dengan tepat atas temuan dan rekomendasi yang disampaikan oleh Otoritas Jasa Keuangan, auditor intern, serta auditor ekstern; dan

vi. secara berkala melakukan kaji ulang terhadap validitas strategi Bank yang telah ditetapkan.

c. Budaya Pengendalian

Direksi dan Dewan Komisaris bertanggung jawab dalam meningkatkan etika kerja dan integritas yang tinggi serta menciptakan suatu budaya organisasi yang menekankan kepada seluruh pegawai Bank mengenai pentingnya pengendalian intern yang berlaku di Bank.

Dalam rangka menciptakan budaya pengendalian tersebut, langkah-langkah yang harus diperhatikan dan dilakukan oleh Bank, antara lain:

1) Direksi dan Dewan Komisaris harus menjadi panutan (*role model*) bagi seluruh pegawai atau memiliki komitmen pribadi yang tinggi terhadap pengembangan Bank yang sehat;

2) Direksi dan Dewan Komisaris harus mampu mengelola sumber daya manusia, termasuk dalam proses penempatan

pegawai yang sesuai dengan keterampilan, pengetahuan, dan perilaku; dan/atau

3) meningkatkan kesadaran bagi seluruh pegawai Bank mengenai pentingnya efektivitas pelaksanaan tugas serta tanggung jawab masing-masing dan selanjutnya pegawai mengomunikasikan kepada pihak manajemen yang terkait mengenai setiap permasalahan yang terjadi dalam kegiatan operasional Bank.

Untuk mendukung budaya pengendalian tersebut maka seluruh kebijakan, standar, dan prosedur operasional harus didokumentasikan secara tertulis dan tersedia bagi setiap pegawai yang terkait.

Dalam rangka memperkuat nilai-nilai etika, Bank harus menghindari kebijakan dan praktik yang dapat mengakibatkan dorongan atau peluang untuk melakukan penyimpangan atau pelanggaran, seperti penekanan pada pencapaian target jangka pendek dengan mengabaikan dampak Risiko yang bersifat jangka panjang, sistem kompensasi yang hanya menitikberatkan pada kinerja jangka pendek, pemisahan fungsi yang tidak efektif, dan pengenaan sanksi yang terlalu ringan atau terlalu berlebihan atas pelanggaran yang dilakukan.

2. Identifikasi dan Penilaian Risiko

a. Penilaian Risiko merupakan serangkaian tindakan yang dilaksanakan oleh Direksi dalam rangka identifikasi, analisis, dan menilai Risiko yang dihadapi oleh Bank dalam rangka pencapaian target yang ditetapkan.

b. Risiko dapat timbul atau berubah sesuai dengan kondisi Bank, antara lain:

1) perubahan kegiatan operasional Bank;
2) perubahan susunan personalia;
3) perubahan sistem informasi;
4) pertumbuhan yang cepat pada kegiatan usaha tertentu;
5) perkembangan teknologi;
6) pengembangan jasa, produk atau aktivitas baru;
7) terjadinya penggabungan usaha, peleburan usaha, pengambilalihan, dan restrukturisasi Bank;
8) perubahan dalam sistem akuntansi;

9) ekspansi usaha;
10) perubahan hukum dan peraturan; dan
11) perubahan perilaku serta ekspektasi nasabah.

c. Suatu SPI yang efektif mengharuskan Bank secara terus menerus mengidentifikasi dan menilai Risiko yang dapat mempengaruhi pencapaian sasaran. Penilaian Risiko harus pula dilakukan oleh auditor intern sehingga cakupan audit yang dilakukan lebih luas dan menyeluruh.

d. Penilaian Risiko ini harus dapat mengidentifikasi jenis Risiko yang dihadapi oleh Bank, penetapan limit Risiko, dan teknik pengendalian Risiko tersebut. Metodologi penilaian Risiko harus menjadi tolok ukur untuk membuat profil Risiko dalam bentuk dokumentasi data, yang dapat diperbarui secara berkala. Penilaian Risiko juga meliputi penilaian terhadap Risiko yang dapat diukur (kuantitatif) dan tidak dapat diukur (kualitatif) maupun terhadap Risiko yang dapat dikendalikan dan tidak dapat dikendalikan, dengan memperhatikan biaya dan manfaatnya. Selanjutnya Bank harus memutuskan untuk mengambil Risiko tersebut atau tidak, dengan cara mengurangi kegiatan usaha tertentu.

e. Penilaian Risiko tersebut harus mencakup semua Risiko yang dihadapi, baik Risiko individual maupun secara keseluruhan (*aggregate*), yang meliputi Risiko Kredit, Risiko Pasar, Risiko Likuiditas, Risiko Operasional, Risiko Hukum, Risiko Reputasi, Risiko Stratejik, dan Risiko Kepatuhan. Khusus untuk Bank Umum Syariah ditambahkan Risiko Imbal Hasil dan Risiko Investasi.

f. Pengendalian intern perlu dikaji ulang secara tepat dalam hal terdapat Risiko yang belum dikendalikan, baik Risiko yang sebelumnya sudah ada maupun Risiko yang baru muncul. Pelaksanaan kaji ulang tersebut antara lain dengan melakukan evaluasi secara terus menerus mengenai pengaruh dari setiap perubahan lingkungan dan kondisi serta dampak dari pencapaian target atau efektivitas pengendalian intern dalam kegiatan operasional dan organisasi Bank.

3. Kegiatan Pengendalian dan Pemisahan Fungsi

Kegiatan pengendalian harus melibatkan seluruh pegawai Bank, termasuk Direksi. Oleh karena itu kegiatan pengendalian akan berjalan efektif apabila direncanakan dan diterapkan guna mengendalikan Risiko yang telah diidentifikasi. Kegiatan pengendalian mencakup pula penetapan kebijakan dan prosedur pengendalian serta proses verifikasi lebih dini untuk memastikan bahwa kebijakan dan prosedur tersebut secara konsisten dipatuhi, serta merupakan kegiatan yang tidak terpisahkan dari setiap fungsi atau kegiatan Bank sehari-hari.

a. Kegiatan Pengendalian

Kegiatan pengendalian meliputi kebijakan, prosedur, dan praktik yang memberikan keyakinan pejabat dan pegawai Bank bahwa arahan Direksi dan Dewan Komisaris Bank telah dilaksanakan secara efektif. Kegiatan pengendalian tersebut akan dapat membantu Direksi dan Dewan Komisaris Bank dalam mengelola dan mengendalikan Risiko yang dapat mempengaruhi kinerja atau mengakibatkan kerugian Bank.

Kegiatan pengendalian diterapkan pada semua tingkatan fungsional sesuai dengan struktur organisasi Bank, yang paling sedikit meliputi:

1) Kaji Ulang Manajemen (*Top Level Reviews*)

Direksi Bank secara berkala meminta penjelasan (informasi) dan laporan kinerja operasional dari pejabat dan pegawai sehingga memungkinkan untuk mengkaji ulang hasil kemajuan (realisasi) dibandingkan dengan target yang akan dicapai, seperti laporan keuangan dibandingkan dengan rencana anggaran yang ditetapkan. Berdasarkan kaji ulang tersebut, Direksi segera mendeteksi permasalahan seperti kelemahan pengendalian, kesalahan laporan keuangan, atau *fraud*.

2) Kaji Ulang Kinerja Operasional (*Functional Review*)

Kaji ulang ini dilaksanakan oleh SKAI dengan frekuensi yang lebih tinggi, baik kaji ulang secara harian, mingguan, maupun bulanan. Dalam kaji ulang kinerja operasional, SKAI:

a) melakukan kaji ulang terhadap penilaian Risiko (laporan profil Risiko) yang dihasilkan oleh satuan kerja Manajemen Risiko;

b) menganalisis data operasional, baik data yang terkait Risiko maupun data keuangan, yaitu melakukan verifikasi rincian dan kegiatan transaksi dibandingkan dengan *output* (laporan) yang dihasilkan oleh satuan kerja Manajemen Risiko; dan

c) melakukan kaji ulang terhadap realisasi pelaksanaan rencana kerja dan anggaran, guna:

(1) mengidentifikasi penyebab penyimpangan yang signifikan; dan

(2) menetapkan persyaratan untuk tindakan perbaikan (*corrective actions*).

3) Pengendalian Sistem Informasi

a) Bank melaksanakan verifikasi terhadap akurasi dan kelengkapan dari transaksi dan melaksanakan prosedur otorisasi, sesuai dengan ketentuan intern.

b) Kegiatan pengendalian sistem informasi dapat digolongkan dalam 2 (dua) kriteria, yaitu:

(1) pengendalian umum, meliputi pengendalian terhadap operasional pusat data, sistem pengadaan dan pemeliharaan perangkat lunak, pengamanan akses, serta pengembangan dan pemeliharaan sistem aplikasi yang ada. Pengendalian umum ini diterapkan terhadap *mainframe, server,* dan *users workstation,* serta jaringan internal-eksternal; dan

(2) pengendalian aplikasi, diterapkan terhadap program yang digunakan Bank dalam mengolah transaksi dan untuk memastikan bahwa semua transaksi adalah benar, akurat, dan telah diotorisasi secara benar. Selain itu, pengendalian aplikasi harus dapat memastikan tersedianya proses audit yang efektif dan untuk mengecek kebenaran proses audit dimaksud.

4) Pengendalian Aset Fisik (*Physical Controls*)
   a) Pengendalian aset fisik dilaksanakan untuk menjamin terselenggaranya pengamanan fisik terhadap aset Bank.
   b) Kegiatan ini meliputi pengamanan aset, catatan, dan akses terbatas terhadap program komputer dan *file* data, serta membandingkan nilai aset dan liabilitas Bank dengan nilai yang tercantum pada catatan pengendali, khususnya pengecekan nilai aset secara berkala.
5) Dokumentasi
   a) Bank paling sedikit harus memformalkan dan mendokumentasikan kebijakan, prosedur, sistem dan standar akuntansi, serta proses audit secara memadai.
   b) Dokumen tersebut harus diperbarui secara berkala guna menggambarkan kegiatan operasional Bank secara aktual, serta harus diinformasikan kepada pejabat dan pegawai Bank.
   c) Atas suatu permintaan, dokumen harus senantiasa tersedia untuk kepentingan auditor intern, akuntan publik, dan pengawasan Bank oleh Otoritas Jasa Keuangan.
   d) Akurasi dan ketersediaan dokumen harus dinilai oleh auditor intern ketika melakukan audit secara rutin maupun non-rutin.

b. Pemisahan Fungsi
   1) Pemisahan fungsi dimaksudkan agar setiap orang dalam jabatannya tidak memiliki peluang untuk melakukan dan menyembunyikan kesalahan atau penyimpangan dalam pelaksanaan tugas pada seluruh jenjang organisasi dan seluruh langkah kegiatan operasional. Bank harus mematuhi prinsip pemisahan fungsi ini, yang dikenal sebagai "*Four-Eyes Principle*".
   2) Dalam hal diperlukan karena perubahan karakteristik kegiatan usaha dan transaksi serta organisasi Bank, Direksi Bank harus menetapkan prosedur (kewenangan)

termasuk penetapan daftar petugas yang dapat mengakses suatu transaksi atau kegiatan usaha yang berisiko tinggi.

3) SPI yang efektif mensyaratkan adanya pemisahan fungsi dan menghindari pemberian wewenang serta tanggung jawab yang dapat menimbulkan berbagai benturan kepentingan (*conflict of interest*). Seluruh aspek yang dapat menimbulkan pertentangan kepentingan tersebut harus diidentifikasi, diminimalisasi, dan dipantau secara hati-hati oleh pihak lain yang independen, seperti akuntan publik.

4) Dalam pelaksanaan pemisahan fungsi tersebut, Bank harus melakukan langkah-langkah, antara lain:

a) menetapkan fungsi atau tugas tertentu pada Bank yang harus dipisahkan atau dialokasikan kepada beberapa orang dalam rangka mengurangi Risiko terjadinya manipulasi data keuangan atau penyalahgunaan aset Bank;

b) pemisahan fungsi tersebut tidak terbatas pada kegiatan *front* dan *back office*, tetapi juga dalam rangka pengendalian terhadap:

(1) persetujuan atas pengeluaran dana dan realisasi pengeluaran;

(2) rekening nasabah dan rekening pemilik Bank;

(3) transaksi dalam pembukuan Bank;

(4) pemberian informasi kepada nasabah Bank;

(5) penilaian terhadap kecukupan dokumentasi perkreditan atau pembiayaan dan pemantauan debitur setelah pencairan kredit atau pembiayaan;

(6) kegiatan usaha lain yang dapat menimbulkan benturan kepentingan yang signifikan; dan

(7) independensi fungsi manajemen Risiko pada Bank.

4. Sistem Akuntansi, Informasi, dan Komunikasi

Sistem akuntansi, informasi, dan komunikasi yang memadai dimaksudkan agar dapat mengidentifikasi masalah yang mungkin timbul dan digunakan sebagai sarana tukar menukar informasi dalam rangka pelaksanaan tugas sesuai dengan tanggung jawab masing-masing.

a. Sistem Akuntansi

1) Sistem akuntansi meliputi metode dan catatan dalam rangka mengidentifikasi, mengelompokkan, menganalisis, mengklasifikasi, mencatat atau membukukan, dan melaporkan transaksi Bank.

2) Untuk menjamin data akuntansi yang akurat dan konsisten dengan data yang tersedia berdasarkan hasil olahan sistem, proses rekonsiliasi antara data akuntansi dan sistem informasi manajemen harus dilaksanakan secara berkala atau paling sedikit setiap bulan. Setiap penyimpangan yang terjadi harus segera diinvestigasi dan diatasi permasalahannya. Proses rekonsiliasi juga harus didokumentasikan sebagai bagian dari persyaratan proses jejak audit secara keseluruhan.

b. Sistem Informasi

1) Sistem informasi harus dapat menghasilkan laporan mengenai kegiatan usaha, kondisi keuangan, penerapan Manajemen Risiko, dan pemenuhan ketentuan yang mendukung pelaksanaan tugas Direksi dan Dewan Komisaris.

2) SPI yang efektif paling sedikit menyediakan data atau informasi internal yang cukup dan menyeluruh mengenai keuangan, kepatuhan Bank terhadap ketentuan dan peraturan perundang-undangan, informasi pasar (kondisi eksternal), dan setiap kejadian serta kondisi yang diperlukan dalam rangka pengambilan keputusan yang tepat dan dapat dipertanggungjawabkan.

3) SPI paling sedikit menyediakan sistem informasi yang dapat dipercaya mengenai seluruh aktivitas fungsional Bank, terutama aktivitas fungsional yang signifikan dan memiliki potensi Risiko tinggi. Sistem informasi tersebut termasuk sistem penyimpanan dan penggunaan data elektronik harus dijamin keamanannya, dipantau oleh pihak yang independen (auditor intern), dan didukung oleh program kontinjensi yang memadai.

4) Bank paling sedikit harus mengorganisasikan suatu rencana pemulihan darurat (*contingency recovery plan*) dan

sistem rekam cadang (*back-up*) untuk mencegah kegagalan usaha yang berisiko tinggi. Untuk memastikan bahwa seluruh rencana dan proses pemulihan darurat (*contingency recovery plan*) serta sistem rekam cadang (*back-up*) telah bekerja secara efektif, pelaksanaan prosedur, proses, dan sistem rekam cadang (*back-up*) harus didokumentasikan dan diuji kembali efektivitasnya secara berkala. Bank harus mendokumentasikan pelaksanaan pengujian secara berkala dan Direksi harus memberikan perhatian yang penuh terhadap temuan kelemahan pada prosedur, proses, dan sistem yang didasarkan atas hasil pengujian serta selanjutnya mengambil langkah perbaikan yang diperlukan.

5) Bank paling sedikit harus memiliki dan memelihara sistem informasi manajemen yang diselenggarakan, baik dalam bentuk elektronik maupun bukan elektronik. Mengingat bahwa sistem informasi elektronik dan penggunaan teknologi informasi tersebut mempunyai dampak Risiko, Bank harus mengendalikan secara efektif guna menghindari adanya gangguan usaha dan kemungkinan timbul kerugian Bank yang signifikan.

6) Dalam rangka pengendalian intern terhadap penyelenggaraan sistem dan teknologi informasi, Bank harus memperhatikan hal-hal sebagai berikut:

   a) Ketersediaan bukti dan dokumen yang memadai dalam rangka mendukung proses jejak audit. Proses jejak audit harus dilaksanakan secara efektif dan didokumentasikan untuk memastikan bahwa proses otomasi telah bekerja secara efektif dan akurat. SKAI harus melakukan penilaian terhadap efektivitas dan akurasi proses jejak audit ketika melakukan evaluasi atas pelaksanaan pengendalian intern Bank.

   b) Pelaksanaan pengendalian terhadap sistem komputer dan pengamanannya (*general controls*) maupun pengendalian terhadap aplikasi perangkat lunak dan prosedur manual lainnya (*application controls*).

c) Antisipasi terjadinya Risiko gangguan atau kerugian yang disebabkan oleh faktor yang berada di luar jangkauan pengendalian rutin Bank sehingga Bank harus menyelenggarakan sistem pemulihan (*recovery*) dan rencana kontinjensi serta pengecekan secara berkala atas kemungkinan terjadinya hal-hal yang sulit diprediksi sebelumnya (*disaster and recovery plan*).

d) Sistem informasi harus menyediakan data dan informasi yang relevan, akurat, tepat waktu, dapat diakses oleh pihak yang berkepentingan, dan disajikan dalam format yang konsisten.

e) Sebagai bagian dari proses pencatatan atau pembukuan, sistem informasi harus didukung oleh sistem akuntansi yang baik termasuk penetapan prosedur dan jadwal retensi pencatatan transaksi.

c. Sistem Komunikasi

1) Sistem komunikasi harus mampu memberikan informasi kepada seluruh pihak, baik intern maupun ekstern seperti Otoritas Jasa Keuangan, auditor ekstern, pemegang saham, dan nasabah Bank.

2) SPI Bank harus memastikan adanya saluran komunikasi yang efektif agar seluruh pejabat dan pegawai Bank sepenuhnya memahami serta mematuhi kebijakan dan prosedur dalam melaksanakan tugas dan tanggung jawab.

3) Direksi Bank harus menyelenggarakan saluran komunikasi yang efektif agar informasi yang diperlukan terjangkau oleh pihak yang berkepentingan. Persyaratan ini berlaku untuk setiap informasi, baik mengenai kebijakan dan prosedur yang telah ditetapkan, eksposur Risiko, dan transaksi aktual maupun mengenai kinerja operasional Bank.

4) Struktur organisasi Bank harus memungkinkan adanya arus informasi yang memadai, yaitu informasi ke atas, ke bawah, dan lintas satuan kerja atau unit kerja, sebagai berikut:

a) Informasi ke atas untuk memastikan bahwa Direksi, Dewan Komisaris, dan pejabat eksekutif Bank mengetahui Risiko dan kinerja operasional Bank.

Saluran informasi harus dapat merespon dengan baik sehingga menghasilkan pelaksanaan langkah-langkah perbaikan dan dapat diketahui oleh jajaran manajemen.

b) Informasi ke bawah untuk memastikan bahwa tujuan, strategi, dan ekspektasi Bank serta kebijakan dan prosedur telah dikomunikasikan kepada para manajer di tingkat bawah dan para pelaksana.

c) Informasi lintas satuan kerja atau unit kerja untuk memastikan bahwa informasi yang diketahui oleh suatu satuan kerja tertentu dapat disampaikan kepada satuan kerja lain yang terkait, khususnya untuk mencegah benturan kepentingan dalam pengambilan keputusan dan untuk menciptakan koordinasi yang memadai.

5. Kegiatan Pemantauan dan Tindakan Koreksi Penyimpangan

a. Kegiatan Pemantauan

1) Bank harus melakukan pemantauan secara terus menerus terhadap efektivitas keseluruhan pelaksanaan pengendalian intern. Pemantauan terhadap Risiko utama Bank harus diprioritaskan dan berfungsi sebagai bagian dari kegiatan Bank sehari-hari termasuk evaluasi secara berkala, baik oleh satuan kerja operasional (*risk taking unit*) maupun oleh SKAI.

2) Bank harus memantau dan mengevaluasi kecukupan SPI secara terus menerus berkaitan dengan adanya perubahan kondisi intern dan ekstern serta harus meningkatkan kapasitas SPI tersebut agar efektivitasnya dapat ditingkatkan.

3) Langkah-langkah yang harus dilakukan oleh Bank dalam rangka terselenggaranya kegiatan pemantauan yang efektif, paling sedikit:

a) memastikan bahwa fungsi pemantauan telah ditetapkan secara jelas dan terstruktur dengan baik dalam organisasi Bank;

b) menetapkan satuan kerja atau pegawai yang ditugaskan untuk memantau efektivitas pengendalian intern;

c) menetapkan frekuensi yang tepat untuk kegiatan pemantauan yang didasarkan pada Risiko yang melekat pada Bank dan sifat atau frekuensi perubahan yang terjadi dalam kegiatan operasional;

d) mengintegrasikan SPI ke dalam kegiatan operasional dan menyediakan laporan rutin seperti jurnal pembukuan, *management review*, dan laporan mengenai persetujuan atas eksepsi atau penyimpangan terhadap kebijakan dan prosedur yang ditetapkan (justifikasi atas *irregularities*) yang selanjutnya dilakukan kaji ulang;

e) melakukan kaji ulang terhadap dokumentasi dan hasil evaluasi dari satuan kerja atau pegawai yang ditugaskan untuk melakukan pemantauan; dan

f) menetapkan informasi atau umpan balik (*feed back*) dalam suatu format dan frekuensi yang tepat.

b. Fungsi SKAI

1) Bank harus menyelenggarakan audit intern yang efektif dan menyeluruh terhadap SPI. Pelaksanaan audit intern yang dilaksanakan oleh SKAI harus didukung oleh tenaga auditor yang independen, kompeten, dan memiliki jumlah yang memadai.

2) Sebagai bagian dari SPI, SKAI harus melaporkan hasil temuan secara langsung kepada Dewan Komisaris atau Komite Audit (apabila ada), direktur utama, dan direktur yang membawahkan fungsi kepatuhan.

3) SKAI harus melakukan penilaian yang independen mengenai kecukupan dari dan kepatuhan Bank terhadap kebijakan dan prosedur yang telah ditetapkan.

4) Dalam menetapkan kedudukan, wewenang, tanggung jawab, profesionalisme, organisasi, dan ruang lingkup tugas SKAI maka Bank harus berpedoman pula pada ketentuan peraturan perundang-undangan mengenai pelaksanaan

fungsi kepatuhan bank umum dan standar pelaksanaan fungsi audit intern.

c. Perbaikan Kelemahan dan Tindakan Koreksi Penyimpangan

1) Kelemahan dalam pengendalian intern, baik yang diidentifikasi oleh satuan kerja operasional (*risk taking unit*), SKAI, maupun pihak lainnya, harus segera dilaporkan kepada dan menjadi perhatian pejabat dan/atau Direksi yang berwenang. Kelemahan pengendalian intern yang material harus dilaporkan kepada Dewan Komisaris.

2) Langkah-langkah perbaikan yang harus dilakukan Bank dalam rangka memperbaiki kelemahan pengendalian intern, antara lain:

a) setiap laporan mengenai kelemahan dalam pengendalian intern atau tidak efektifnya pengendalian Risiko Bank harus segera ditindaklanjuti oleh Direksi, Dewan Komisaris, dan pejabat eksekutif terkait;

b) SKAI harus melakukan kaji ulang atau langkah pemantauan lainnya yang memadai terhadap kelemahan yang terjadi dan segera melaporkan kepada Dewan Komisaris, Komite Audit (apabila ada), dan direktur utama dalam hal masih terdapat kelemahan yang belum diperbaiki atau rekomendasi tindakan korektif yang belum ditindaklanjuti;

c) untuk memastikan bahwa seluruh kelemahan segera ditindaklanjuti maka Direksi harus menciptakan suatu sistem yang dapat menelusuri kelemahan pada pengendalian intern dan mengambil langkah perbaikan; dan

d) Direksi dan Dewan Komisaris harus menerima laporan secara berkala berupa ikhtisar mengenai hasil identifikasi seluruh permasalahan dalam pengendalian intern.

IV. LAIN-LAIN

Dalam penerapan pengendalian intern, Bank harus juga memperhatikan aspek-aspek pengendalian intern yang ditetapkan dalam ketentuan

peraturan perundang-undangan lainnya, antara lain yang mengatur mengenai:

1. kewajiban penyusunan dan pelaksanaan kebijakan perkreditan atau pembiayaan bagi bank umum;
2. penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum;
3. transaksi derivatif;
4. restrukturisasi kredit;
5. Standar Pelaksanaan Fungsi Audit Intern Bank (SPFAIB);
6. penerapan program anti pencucian uang dan pencegahan pendanaan terorisme bagi bank umum;
7. transparansi dan publikasi laporan bank;
8. prinsip kehati-hatian dalam kegiatan penyertaan modal; dan
9. penerapan manajemen risiko bagi bank umum dan penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah.

Ditetapkan di Jakarta
pada tanggal 7 Juli 2017

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,

ttd

NELSON TAMPUBOLON

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana