

## **Kebijakan Strategi Anti Fraud PT BPRS Almabrur Klaten (BSA)**

### **Referensi :**

1. Anggaran Dasar PT BPRS Almabrur Klaten No. 4 yang dibuat oleh Tonny Rudhiyanto, SH Notaris di Surakarta tanggal 8 April 2009 dan perubahannya.
2. Undang-Undang Perseroan Terbatas No. 4 tahun 2007.
3. POJK dan SEOJK tentang BPRS, Audit Internal, Manajemen Risiko, Tata kelola dan TKS.
4. SK Direksi No.40/SK/VI/2023 tanggal 8 Juni 2023 tentang Kebijakan Strategi Anti Fraud PT. BPRS Almabrur Klaten.

### **Model Pertahanan Tiga Lini (*The three lines of defense model*)**

Bank menerapkan prinsip *three lines of defense* dalam melakukan mitigasi terjadinya *fraud*, sehingga semua pihak terkait dapat berperan baik dalam mengimplementasikan system pengendalian *fraud*. Penerapan *three lines of defense* dengan membedakan antara fungsi bisnis sebagai fungsi pemilik risiko (*risk owner*), fungsi yang mengawasi risiko (*overseeing risk*), dan fungsi yang menyediakan keyakinan *independen* (*independent assurance*). Semua fungsi tersebut memiliki peran penting dalam membangun kapabilitas kegiatan operasional diseluruh jajaran dan proses bisnis bank sebagai perangkat dalam pengendalian *fraud* yang ditujukan untuk mengurangi potensi terjadinya *fraud*.

#### 1. Pertahanan lini pertama (*first lines Of Defense*)

Pertahanan lini pertama adalah fungsi di level operasional yang merupakan pemilik proses, tanggung jawab dan kewajiban untuk menilai, mengendalikan, serta memitigasi risiko sekaligus memelihara pengendalian internal yang efektif.

#### 2. Pertahanan lini kedua (*second lines Of Defense*)

Pertahanan lini kedua adalah fungsi kontrol, manajemen risiko, kepatuhan dan fungsi lain sejenis, yang memfasilitasi, serta memonitor keefektifan implementasi dari praktik manajemen risiko yang dilakukan oleh fungsi di level operasional sekaligus membantu pemilik risiko untuk melaporkan secara memadai semua informasi yang menyangkut mengenai risiko tersebut.

#### 3. Pertahanan lini ketiga (*third lines Of Defense*)

Pertahanan lini ketiga merupakan fungsi internal audit, yaitu melalui pendekatan berbasis risiko, memberikan keyakinan (*assurance*) atas keefektifan tata kelola, manajemen risiko,

dan pengendalian internal kepada fungsi pengelola dalam organisasi (*senior management/Board Of Director/Board Of Commisioner*) termasuk bagaimana pertahanan lini pertama dan kedua beroperasi.

## Strategi Anti Fraud

Strategi anti *Fraud* yang disusun secara komprehensif integralistik dan diimplementasikan dalam bentuk sistem pengendalian *Fraud* diterapkan dengan menggunakan perangkat yang merupakan penjabaran dari 4 (empat) pilar yang saling berkaitan sebagai berikut :

### 1 Pencegahan

Pilar pencegahan memuat langkah untuk mengurangi potensi risiko terjadinya *Fraud*, yang paling sedikit mencakup:

#### a. Kesadaran Anti *Fraud*

Kesadaran anti *Fraud* yaitu upaya untuk menumbuhkan kesadaran mengenai pentingnya pencegahan *Fraud* bagi seluruh jajaran organisasi Bank dan berbagai pihak yang berhubungan dengan Bank. Melalui kepemimpinan yang baik dan didukung dengan kesadaran anti *Fraud* yang tinggi diharapkan tumbuh kepedulian semua unsur di Bank dan berbagai pihak yang berhubungan dengan Bank terhadap pentingnya pengendalian *Fraud*. Moral dan kesadaran dari pimpinan terhadap anti *Fraud* harus menjiwai setiap kebijakan atau ketentuan yang ditetapkan. Upaya untuk menumbuhkan kesadaran anti *Fraud* dilakukan antara lain melalui :

#### 1) Penyusunan dan Sosialisasi Deklarasi Anti *Fraud*

Sosialisasi kepada pihak intern dan ekstern Bank terkait kebijakan dan komitmen bank untuk tidak memberikan toleransi pada tindakan *Fraud*, misalnya kebijakan dan komitmen untuk :

- a) Menjalankan bisnis secara adil, jujur dan terbuka atau transparan.
- b) Menghindari berbisnis dengan pihak ketiga yang tidak berkomitmen sesuai dengan kebijakan Bank dan/atau
- c) Memberikan konsekuensi pelanggaran terhadap kebijakan dan komitmen.

#### 2) Program Budaya Anti *Fraud* bagi Pegawai

Untuk mendorong penerapan budaya anti *Fraud* bagi pegawai, Bank dapat menyelenggarakan seminar, lokakarya, diskusi, pelatihan yang efektif, pemberian umpan balik, dan diseminasi mengenai pemahaman terkait kebijakan dan prosedur anti *Fraud*, jenis *Fraud*, transparansi hasil investigasi, dan tindak lanjut terhadap *Fraud* yang dilakukan secara berkesinambungan.

#### 3) Program Kepedulian dan Kewaspadaan terhadap *Fraud* bagi Nasabah

Bank perlu meningkatkan kepedulian dan kewaspadaan nasabah terhadap kemungkinan terjadinya *Fraud*, antara lain melalui pembuatan brosur, spanduk,

poster, kartu taktil anti *Fraud*, klausul atau penjelasan tertulis maupun melalui sarana lain.

b. Identifikasi Kerawanan

Identifikasi kerawanan merupakan proses untuk mengidentifikasi, menganalisis, dan menilai potensi risiko terjadinya *Fraud* yang dapat dilakukan secara berkala atau dalam hal terdapat indikasi *Fraud*.

Secara umum, identifikasi kerawanan ditujukan untuk mengidentifikasi risiko terjadinya *Fraud* yang melekat pada setiap aktivitas yang berpotensi merugikan Bank. Bank melakukan identifikasi kerawanan pada setiap aktivitas, baik yang bersumber dari informasi intern maupun ekstern Bank. Hasil identifikasi selain didokumentasikan dan diinformasikan kepada seluruh pihak yang berkepentingan, juga dikinikan secara berkala terutama dalam hal terdapat aktivitas yang dinilai berisiko tinggi untuk terjadinya *Fraud*.

Beberapa faktor intern Bank yang dapat meningkatkan kemungkinan terjadinya *Fraud*, antara lain:

- 1) Kurangnya pelatihan, keterampilan, dan pengetahuan atas pencegahan dan penanganan *Fraud*.
- 2) Budaya pemberian bonus atas pengambilan risiko secara berlebihan.
- 3) Kebijakan dan prosedur yang kurang jelas, antara lain terhadap pengeluaran biaya untuk representasi, hiburan serta sumbangan amal dan politik.
- 4) Pengendalian keuangan yang kurang memadai.
- 5) Kurangnya arahan Direksi dan Dewan Komisaris terkait pencegahan dan penanganan *Fraud*.

c. Kebijakan Mengenal Pegawai

Sebagai upaya pencegahan terjadinya *Fraud*, Bank menerapkan kebijakan mengenal pegawai yang merupakan upaya pengendalian dari aspek SDM. Kebijakan mengenal pegawai secara efektif yang dimiliki Bank paling sedikit mencakup:

- 1) Sistem dan prosedur penerimaan atau rekrutmen yang efektif, yang dapat memberikan gambaran mengenai rekam jejak calon pegawai secara lengkap dan akurat.
- 2) System seleksi yang dilengkapi kualifikasi yang tepat dengan mempertimbangkan risiko, serta ditetapkan secara objektif dan transparan. Sistem tersebut harus menjangkau pelaksanaan promosi maupun mutasi, termasuk penempatan pada posisi yang memiliki risiko tinggi terhadap *Fraud*; dan
- 3) Kebijakan mengenali pegawai antara lain mencakup pengenalan dan pemantauan karakter, integritas, relasi, sikap dan perilaku, serta gaya hidup pegawai.

## 2 Deteksi

Pilar deteksi memuat langkah untuk mengidentifikasi dan menemukan *Fraud* dalam kegiatan usaha Bank, yang paling sedikit mencakup :

### a. Kebijakan dan Mekanisme Penanganan Pengaduan (*Whistleblowing*)

Kebijakan ini ditujukan untuk meningkatkan efektivitas penerapan sistem pengendalian *Fraud* dengan menitikberatkan pada pengungkapan dari pengaduan. Dalam rangka mitigasi dan pencegahan *Fraud* secara efektif, perlu ditingkatkan efektivitas penerapan kebijakan penanganan pengaduan di Bank yang mencakup :

#### 1) Perlindungan Pelapor *Fraud* (*Whistleblower*)

Bank memiliki komitmen untuk meningkatkan saluran komunikasi di Bank dan memberikan dukungan dan perlindungan sepenuhnya kepada setiap pelapor *Fraud*, menjamin kerahasiaan identitas pelapor *Fraud* serta pelaksanaan penyelidikan dan pengungkapan atas laporan yang disampaikan.

Dalam hal ini pelaporan dimungkinkan untuk dilakukan secara anonim maupun melalui pemberian hadiah penghargaan kepada pelapor *Fraud* yang laporannya terbukti benar dan didukung bukti yang memadai.

#### 2) Regulasi yang Terkait dengan Pengaduan *Fraud*

Bank perlu menyusun ketentuan intern terkait pengaduan *Fraud* dengan mengacu pada ketentuan peraturan perundang-undangan.

#### 3) Sistem Pelaporan dan Mekanisme Tindak Lanjut Laporan *Fraud*

Terdapat sejumlah cara untuk menerima pelaporan, antara lain telepon, surat, surat elektronik, dan faksimile. Selain itu, Bank perlu menyusun sistem pelaporan *Fraud* yang efektif yang memuat kejelasan proses pelaporan, antara lain mengenai tata cara pelaporan, sarana, dan pihak yang bertanggung jawab untuk menangani pelaporan. Sistem pelaporan harus didukung dengan adanya kejelasan mekanisme tindak lanjut terhadap *Fraud* yang dilaporkan. Kebijakan tersebut dikomunikasikan secara transparan kepada seluruh jajaran organisasi dan diterapkan secara konsisten agar dapat menimbulkan kepercayaan seluruh pegawai Bank terhadap keandalan dan kerahasiaan mekanisme penanganan pengaduan.

### b. Pemeriksaan Dadakan (*Surprised Audit*)

Kebijakan dan mekanisme pemeriksaan dadakan perlu dilakukan terutama pada unit bisnis dan aktivitas yang berisiko tinggi atau rawan terhadap terjadinya *Fraud*. Pelaksanaan pemeriksaan dadakan dapat meningkatkan kewaspadaan pegawai dalam melaksanakan tugas.

c. Sistem Pengawasan

Sistem Pengawasan merupakan suatu tindakan pengujian atau pemeriksaan yang dilakukan secara rahasia tanpa diketahui atau disadari oleh pihak yang diuji atau diperiksa untuk memantau dan menguji efektivitas kebijakan anti *Fraud*. Sistem Pengawasan dapat dilakukan oleh pihak independen dan/atau pihak intern Bank secara berkala atau sewaktu-waktu apabila diperlukan.

### 3 Investigasi, Pelaporan, dan Sanksi

Pilar investigasi, pelaporan, dan sanksi memuat langkah untuk penyelidikan atau investigasi, sistem pelaporan, dan pengenaan sanksi terhadap kejadian *Fraud*, yang paling sedikit mencakup :

a. Investigasi

Investigasi dilakukan untuk mengumpulkan bukti yang terkait dengan kejadian yang patut diduga merupakan tindakan *Fraud*. Investigasi merupakan bagian penting dalam sistem pengendalian *Fraud* yang memberikan pesan kepada setiap pihak terkait bahwa setiap indikasi tindakan *Fraud* yang terdeteksi selalu diproses sesuai standar investigasi dan pelaku diproses sesuai ketentuan. Standar investigasi yang dimiliki Bank paling sedikit mencakup :

1) Penentuan pihak yang berwenang melaksanakan investigasi dengan memperhatikan independensi dan kompetensi yang dibutuhkan, antara lain kompetensi atau keahlian dalam hal :

a) Analisis dan Investigasi;

b) Akuntansi Forensik;

Akuntansi forensik merupakan teknik dalam melakukan evaluasi dan penyelidikan secara rinci dan menyeluruh terhadap permasalahan keuangan yang diinvestigasi dengan menggunakan standar dan aturan.

c) Komputer Forensik;

Komputer forensik merupakan teknik untuk melakukan investigasi dan analisis melalui pengumpulan dan penyajian bukti data yang ada dalam komputer.

d) Pekerjaan Lapangan dan Wawancara.

Pekerjaan lapangan merupakan proses investigasi untuk mendapatkan keyakinan secara sistematis melalui pengumpulan bukti secara objektif.

2) Mekanisme pelaksanaan investigasi untuk menindaklanjuti hasil deteksi dengan tetap menjaga kerahasiaan informasi yang diperoleh.

b. Pelaporan

Bank menyusun mekanisme pelaporan yang efektif atas pelaksanaan investigasi terhadap kejadian *Fraud* yang ditemukan. Mekanisme pelaporan mencakup pelaporan secara intern Bank maupun kepada Otoritas Jasa Keuangan.

c. Pengenaan Sanksi

Bank menyusun kebijakan pengenaan sanksi secara intern yang efektif untuk menindaklanjuti hasil investigasi agar menimbulkan efek jera bagi pelaku *Fraud*.

Kebijakan ini paling sedikit memuat:

- 1) Jenis sanksi sesuai pelanggaran yang dilakukan.
- 2) Mekanisme pengenaan sanksi.
- 3) Pihak yang berwenang mengenakan sanksi.

Kebijakan pengenaan sanksi harus diterapkan secara adil, transparan, konsisten, dan memberikan efek jera.

4 Pemantauan, Evaluasi, dan Tindak Lanjut

Pilar pemantauan, evaluasi, dan tindak lanjut memuat langkah untuk melakukan pemantauan dan evaluasi serta menindaklanjuti *Fraud*, paling sedikit mencakup:

a. Pemantauan

Salah satu langkah penting dalam mengimplementasikan sistem pengendalian *Fraud* yaitu memantau tindak lanjut yang dilakukan terhadap *Fraud*, baik sesuai ketentuan intern Bank maupun sesuai dengan ketentuan peraturan perundang-undangan.

b. Evaluasi

Untuk mendukung pelaksanaan evaluasi, Bank perlu memelihara data kejadian *Fraud*. Data kejadian dapat digunakan sebagai alat bantu evaluasi. Data kejadian *Fraud* paling sedikit mencakup data dan informasi sebagaimana tercantum pada laporan penerapan strategi anti *Fraud*.

Berdasarkan data kejadian *Fraud* dan hasil evaluasi tersebut dapat diidentifikasi kelemahan dan penyebab terjadinya *Fraud* serta ditentukan langkah penanganan dan perbaikan yang diperlukan, termasuk memperkuat sistem pengendalian intern. Evaluasi menyeluruh terhadap sistem pengendalian *Fraud* perlu dilakukan secara berkala.

c. Tindak lanjut

Bank menyusun mekanisme tindak lanjut berdasarkan hasil evaluasi atas kejadian *Fraud* untuk memperbaiki kelemahan dan memperkuat sistem pengendalian intern agar dapat mencegah terulangnya kembali *Fraud* karena kelemahan yang serupa.