LEMBARAN NEGARA REPUBLIK INDONESIA

No.246, 2019 KEUANGAN OJK. Strategi Anti *Fraud.* Bank Umum. (Pejelasan dalam Tambahan Lembaran Negara Republik Indonesia Nomor 6439)

PERATURAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 39 /POJK.03/2019

TENTANG

PENERAPAN STRATEGI ANTI *FRAUD*

BAGI BANK UMUM

DENGAN RAHMAT TUHAN YANG MAHA ESA

DEWAN KOMISIONER OTORITAS JASA KEUANGAN,

Menimbang : a. bahwa kegiatan usaha bank dapat terpapar risiko operasional yang salah satunya berasal dari *Fraud*;

b. bahwa untuk meminimalisasi terjadinya *Fraud* diperlukan penguatan sistem pengendalian intern berupa penerapan strategi anti *Fraud* oleh bank;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Otoritas Jasa Keuangan tentang Penerapan Strategi Anti *Fraud* Bagi Bank Umum;

Mengingat : 1. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1992 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 3472) sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor

7 Tahun 1992 tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790);

2. Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 94, Tambahan Lembaran Negara Republik Indonesia Nomor 4867);
3. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 5253);

MEMUTUSKAN:

Menetapkan : PERATURAN OTORITAS JASA KEUANGAN TENTANG PENERAPAN STRATEGI ANTI *FRAUD* BAGI BANK UMUM.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Otoritas Jasa Keuangan ini yang dimaksud dengan:

1. Bank Umum yang selanjutnya disebut Bank adalah Bank yang melaksanakan kegiatan usaha secara konvensional atau berdasarkan prinsip syariah yang dalam kegiatannya memberikan jasa dalam lalu lintas pembayaran, termasuk kantor cabang dari bank yang berkedudukan di luar negeri.
2. *Fraud* adalah tindakan penyimpangan atau pembiaran yang sengaja dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain, yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah, atau pihak lain menderita kerugian dan/atau pelaku *Fraud* memperoleh keuntungan

keuangan baik secara langsung maupun tidak langsung.

3. Direksi adalah organ Bank yang berwenang dan bertanggung jawab penuh atas pengurusan untuk kepentingan Bank, sesuai dengan maksud dan tujuan Bank serta mewakili Bank, baik di dalam maupun di luar pengadilan sesuai dengan ketentuan anggaran dasar Bank, atau pemimpin kantor cabang dan pejabat satu tingkat di bawah pemimpin kantor cabang bagi kantor cabang dari bank yang berkedudukan di luar negeri.
4. Dewan Komisaris adalah organ Bank yang bertugas melakukan pengawasan secara umum dan/atau khusus sesuai dengan anggaran dasar serta memberi nasihat kepada Direksi, atau pihak yang ditunjuk untuk melaksanakan fungsi pengawasan bagi kantor cabang dari bank yang berkedudukan di luar negeri.

Pasal 2

(1) Jenis perbuatan yang tergolong *Fraud* terdiri atas:
   a. kecurangan;
   b. penipuan;
   c. penggelapan aset;
   d. pembocoran informasi;
   e. tindak pidana perbankan; dan
   f. tindakan lain.

(2) Tindakan lain sebagaimana dimaksud pada ayat (1) huruf f merupakan tindakan lain yang dapat dipersamakan dengan *Fraud* sesuai dengan ketentuan peraturan perundang-undangan.

BAB II

PENERAPAN STRATEGI ANTI *FRAUD*

Pasal 3

(1) Bank wajib menyusun dan menerapkan strategi anti *Fraud* secara efektif.

(2) Penyusunan dan penerapan strategi anti *Fraud* yang efektif sebagaimana dimaksud pada ayat (1) paling sedikit memenuhi pedoman penerapan strategi anti *Fraud* yang tercantum pada Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Otoritas Jasa Keuangan ini.

(3) Dalam menyusun dan menerapkan strategi anti *Fraud* yang efektif, Bank wajib memperhatikan paling sedikit:
   a. kondisi lingkungan intern dan ekstern;
   b. kompleksitas kegiatan usaha;
   c. jenis, potensi, dan risiko *Fraud*; dan
   d. kecukupan sumber daya yang dibutuhkan.

Pasal 4

(1) Penyusunan dan penerapan strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 3 ayat (1) paling sedikit memuat 4 (empat) pilar.

(2) 4 (empat) pilar sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. pencegahan;
   b. deteksi;
   c. investigasi, pelaporan, dan sanksi; dan
   d. pemantauan, evaluasi, dan tindak lanjut.

Pasal 5

(1) Untuk mengendalikan risiko terjadinya *Fraud*, Bank wajib menerapkan manajemen risiko sesuai dengan ketentuan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum dan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah.

(2) Penerapan manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit memuat penguatan terhadap aspek:
   a. pengawasan aktif Direksi dan Dewan Komisaris;
   b. kebijakan dan prosedur;

c. struktur organisasi dan pertanggungjawaban; dan
d. pengendalian dan pemantauan,

sebagaimana tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Otoritas Jasa Keuangan ini.

Pasal 6

Direksi dan Dewan Komisaris Bank wajib menerapkan strategi anti *Fraud* di Bank.

Pasal 7

(1) Bank wajib membentuk unit kerja atau fungsi yang bertugas menangani penerapan strategi anti *Fraud* dalam organisasi Bank.
(2) Unit kerja atau fungsi yang bertugas menangani penerapan strategi anti *Fraud* dalam organisasi Bank sebagaimana dimaksud pada ayat (1):
    a. bertanggung jawab kepada direktur utama; dan
    b. memiliki hubungan komunikasi dan pelaporan secara langsung kepada Dewan Komisaris.
(3) Pimpinan unit kerja atau pejabat yang membawahkan fungsi yang bertugas menangani penerapan strategi anti *Fraud* sebagaimana dimaksud pada ayat (1) harus memiliki:
    a. sertifikat keahlian di bidang anti *Fraud*; dan/atau
    b. pengalaman yang memadai di bidang perbankan atau perbankan syariah.

Pasal 8

(1) Bank, Direksi, dan/atau anggota Dewan Komisaris yang tidak memenuhi ketentuan sebagaimana dimaksud dalam Pasal 3 ayat (1), Pasal 3 ayat (3), Pasal 6, dan/atau Pasal 7 ayat (1) dikenai sanksi administratif berupa teguran tertulis.
(2) Dalam hal Bank, Direksi dan/atau anggota Dewan Komisaris tidak memenuhi ketentuan dan telah dikenai sanksi administratif sebagaimana dimaksud

pada ayat (1), Bank dapat dikenai sanksi administratif berupa:

a. penurunan tingkat kesehatan Bank;
b. larangan untuk menerbitkan produk atau melaksanakan aktivitas baru;
c. pembekuan kegiatan usaha tertentu; dan/atau
d. larangan sebagai pihak utama lembaga jasa keuangan yang dilaksanakan sesuai dengan ketentuan Peraturan Otoritas Jasa Keuangan mengenai penilaian kembali bagi pihak utama lembaga jasa keuangan.

(3) Bank yang tidak memenuhi ketentuan sebagaimana dimaksud dalam Pasal 5 ayat (1) dikenai sanksi administratif sesuai dengan ketentuan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum dan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah.

BAB III
PELAPORAN

Pasal 9

(1) Untuk pemantauan penerapan strategi anti *Fraud*, Bank wajib menyampaikan kepada Otoritas Jasa Keuangan:
   a. strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 3; dan
   b. laporan dan/atau koreksi laporan penerapan strategi anti *Fraud*.

(2) Dalam hal terdapat kejadian *Fraud* berdampak signifikan, Bank wajib menyampaikan laporan dan/atau koreksi laporan *Fraud* berdampak signifikan.

(3) Laporan dan/atau koreksi laporan penerapan strategi anti *Fraud* sebagaimana dimaksud pada ayat (1) huruf b disusun dengan format yang tercantum dalam

Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Otoritas Jasa Keuangan ini.

(4) Laporan dan/atau koreksi laporan *Fraud* berdampak siginifikan sebagaimana dimaksud pada ayat (2) disusun dengan format yang tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Otoritas Jasa Keuangan ini.

Pasal 10

(1) Bank wajib menyesuaikan strategi anti *Fraud* yang telah dimiliki dengan pedoman penerapan strategi anti *Fraud* sebagaimana tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Otoritas Jasa Keuangan ini.

(2) Bank wajib menyampaikan strategi anti *Fraud* yang telah disesuaikan sebagaimana dimaksud pada ayat (1) kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan sejak berlakunya Peraturan Otoritas Jasa Keuangan ini.

Pasal 11

Dalam hal terdapat perubahan terhadap strategi anti *Fraud* yang telah disampaikan kepada Otoritas Jasa Keuangan sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, Bank wajib menyampaikan perubahan strategi anti *Fraud* paling lambat 7 (tujuh) hari kerja sejak perubahan dilakukan.

Pasal 12

Bank wajib menyampaikan:

a. laporan penerapan strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf b setiap semester untuk posisi akhir bulan Juni dan akhir bulan Desember, paling lambat pada tanggal 15 bulan berikutnya setelah akhir bulan laporan; dan

b. laporan *Fraud* berdampak signifikan sebagaimana dimaksud dalam Pasal 9 ayat (2) paling lambat 3 (tiga) hari kerja setelah Bank mengetahui terjadinya *Fraud* yang berdampak signifikan.

Pasal 13

(1) Bank wajib melakukan koreksi atas kesalahan data dan/atau informasi dalam laporan penerapan strategi anti *Fraud* dan laporan *Fraud* berdampak signifikan yang telah disampaikan kepada Otoritas Jasa Keuangan.

(2) Koreksi atas kesalahan data dan/atau informasi sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan temuan Bank dan/atau temuan Otoritas Jasa Keuangan.

Pasal 14

Bank wajib menyampaikan strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 10 ayat (2) dan Pasal 11 secara luring kepada Otoritas Jasa Keuangan melalui:

a. Departemen Pengawasan Bank terkait atau Kantor Regional Otoritas Jasa Keuangan di Jakarta, bagi Bank yang berkantor pusat atau kantor cabang dari bank yang berkedudukan di luar negeri yang berada di wilayah Provinsi Daerah Khusus Ibukota Jakarta dan Provinsi Banten; atau

b. Kantor Regional Otoritas Jasa Keuangan atau Kantor Otoritas Jasa Keuangan setempat sesuai dengan wilayah tempat kedudukan kantor pusat Bank, bagi Bank yang berkantor pusat di luar wilayah Provinsi Daerah Khusus Ibukota Jakarta dan Provinsi Banten.

Pasal 15

(1) Bank wajib menyampaikan laporan dan/atau koreksi laporan penerapan strategi anti *Fraud* serta laporan dan/atau koreksi laporan *Fraud* berdampak signifikan sebagaimana dimaksud dalam Pasal 12 dan Pasal 13

secara daring melalui sistem pelaporan Otoritas Jasa Keuangan.

(2) Dalam hal penyampaian laporan dan/atau koreksi laporan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan sebagaimana dimaksud pada ayat (1) belum dapat dilakukan, Bank wajib menyampaikan laporan dan/atau koreksi laporan secara luring.

(3) Bank wajib menyampaikan laporan dan/atau koreksi laporan secara luring sebagaimana dimaksud pada ayat (2) kepada Otoritas Jasa Keuangan melalui:

a. Departemen Pengawasan Bank terkait atau Kantor Regional Otoritas Jasa Keuangan di Jakarta, bagi Bank yang berkantor pusat atau kantor cabang dari bank yang berkedudukan di luar negeri yang berada di wilayah Provinsi Daerah Khusus Ibukota Jakarta dan Provinsi Banten; atau

b. Kantor Regional Otoritas Jasa Keuangan atau Kantor Otoritas Jasa Keuangan setempat sesuai dengan wilayah tempat kedudukan kantor pusat Bank, bagi Bank yang berkantor pusat di luar wilayah Provinsi Daerah Khusus Ibukota Jakarta dan Provinsi Banten.

Pasal 16

Apabila batas waktu penyampaian strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 10 ayat (2) dan batas waktu penyampaian laporan penerapan strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 12 huruf a jatuh pada hari Sabtu, hari Minggu, dan/atau hari libur lain maka strategi anti *Fraud* dan/atau laporan penerapan strategi anti *Fraud* disampaikan pada hari kerja berikutnya.

Pasal 17

Dalam hal Bank mengalami keadaan kahar sehingga tidak dapat menyampaikan:

a. strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 10 ayat (2);
b. perubahan terhadap strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 11; dan/atau
c. laporan penerapan strategi anti *Fraud* dan laporan *Fraud* berdampak signifikan sebagaimana dimaksud dalam Pasal 12,

sampai dengan batas waktu penyampaian dokumen dan/atau laporan, Bank wajib segera memberitahukan secara tertulis kepada Otoritas Jasa Keuangan untuk memperoleh penundaan batas waktu penyampaian.

Pasal 18

(1) Bank yang tidak memenuhi ketentuan sebagaimana dimaksud dalam Pasal 9 ayat (1), Pasal 9 ayat (2), Pasal 10 ayat (1), Pasal 13 ayat (1), Pasal 14, dan/atau Pasal 15, dikenai sanksi administratif berupa teguran tertulis.
(2) Bank yang tidak menyampaikan strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 10 ayat (2), perubahan terhadap strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 11, dan/atau laporan penerapan strategi anti *Fraud* dan laporan *Fraud* berdampak signifikan sebagaimana dimaksud dalam Pasal 12 dikenai sanksi administratif berupa teguran tertulis dan denda sebesar Rp1.000.000,00 (satu juta rupiah) per hari kerja dan paling banyak sebesar Rp30.000.000,00 (tiga puluh juta rupiah) per jenis dokumen atau laporan.
(3) Bank yang tidak menyampaikan strategi anti *Fraud* dan laporan sampai dengan 30 (tiga puluh) hari kerja setelah batas akhir waktu penyampaian strategi anti *Fraud* sebagaimana dimaksud dalam Pasal 10 ayat (2), perubahan terhadap strategi anti *Fraud* sebagaimana

dimaksud dalam Pasal 11, dan/atau laporan penerapan strategi anti *Fraud* dan laporan *Fraud* berdampak signifikan sebagaimana dimaksud dalam Pasal 12 dan telah dikenai sanksi administratif berupa denda sebesar Rp30.000.000,00 (tiga puluh juta rupiah) sebagaimana dimaksud pada ayat (2), tetap wajib menyampaikan strategi anti *Fraud*, perubahan terhadap strategi anti *Fraud*, laporan penerapan strategi anti *Fraud*, dan/atau laporan *Fraud* berdampak signifikan.

(4) Dalam hal Bank tidak memenuhi ketentuan dan telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1), ayat (2), dan/atau ayat (3), Bank dapat dikenai sanksi administratif berupa:

a. penurunan tingkat kesehatan bank;
b. larangan untuk menerbitkan produk atau melaksanakan aktivitas baru;
c. pembekuan kegiatan usaha tertentu; dan/atau
d. larangan sebagai pihak utama lembaga jasa keuangan yang dilaksanakan sesuai dengan ketentuan Peraturan Otoritas Jasa Keuangan mengenai penilaian kembali bagi pihak utama lembaga jasa keuangan.

Pasal 19

(1) Kesalahan data dan/atau informasi yang disampaikan dalam laporan penerapan strategi anti *Fraud* dan laporan *Fraud* berdampak signifikan sebagaimana dimaksud dalam Pasal 13 ayat (1) dikenai sanksi administratif berupa teguran tertulis dan denda sebesar Rp100.000,00 (seratus ribu rupiah) per kesalahan isian dan paling banyak Rp10.000.000,00 (sepuluh juta rupiah) per laporan.

(2) Sanksi administratif berupa teguran tertulis dan denda sebagaimana dimaksud pada ayat (1) dikecualikan terhadap:

a. koreksi yang merupakan pengkinian atas data dan/atau informasi yang disampaikan pada laporan sebelumnya; dan/atau
b. koreksi atas laporan yang sama dan/atau laporan lain yang diakibatkan oleh adanya koreksi atas kesalahan data dan/atau informasi pada laporan sebelumnya yang telah dikenai sanksi administratif.

BAB IV
LAIN-LAIN

Pasal 20

Pertanggungjawaban Bank atas kerugian nasabah atau pihak lain yang timbul akibat kesalahan dan/atau kelalaian Direksi, Dewan Komisaris, pegawai, dan/atau pihak ketiga yang bekerja untuk kepentingan Bank dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
KETENTUAN PENUTUP

Pasal 21

Pada saat Peraturan Otoritas Jasa Keuangan ini mulai berlaku, Surat Edaran Bank Indonesia Nomor 13/28/DPNP tanggal 9 Desember 2011 perihal Penerapan Strategi Anti *Fraud* Bagi Bank Umum dicabut dan dinyatakan tidak berlaku.

Pasal 22

Peraturan Otoritas Jasa Keuangan ini mulai berlaku pada tanggal 1 Januari 2020.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Otoritas Jasa Keuangan ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 19 Desember 2019

KETUA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

WIMBOH SANTOSO

Diundangkan di Jakarta
pada tanggal 19 Desember 2019

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

YASONNA H LAOLY

LAMPIRAN I

PERATURAN OTORITAS JASA KEUANGAN
NOMOR 39 /POJK.03/2019
TENTANG PENERAPAN STRATEGI ANTI *FRAUD* BAGI BANK UMUM

PEDOMAN PENERAPAN STRATEGI ANTI *FRAUD* BAGI BANK

I. LATAR BELAKANG

1. Untuk mencegah terjadinya kasus penyimpangan operasional pada perbankan dan pelanggaran terhadap ketentuan peraturan perundang-undangan, khususnya *Fraud*, yang dapat menyebabkan kerugian baik secara langsung maupun tidak langsung bagi Bank, nasabah, dan/atau pihak lain, diperlukan peningkatan efektivitas pengendalian intern, sebagai upaya meminimalisasi risiko *Fraud* dengan cara menerapkan strategi anti *Fraud*.
2. Dalam Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, antara lain diatur bahwa Direksi, Dewan Komisaris, atau pegawai Bank yang dengan sengaja meminta atau menerima, mengizinkan atau menyetujui untuk menerima suatu imbalan, komisi, uang tambahan, pelayanan, uang atau barang berharga, untuk keuntungan pribadinya atau untuk keuntungan keluarganya, untuk mendapatkan atau berusaha mendapatkan bagi orang lain dalam memperoleh uang muka, bank garansi, atau fasilitas kredit dari Bank, atau untuk pembelian atau pendiskontoan oleh Bank atas surat wesel, surat promes, cek, dan kertas dagang atau bukti kewajiban lain, atau untuk memberikan persetujuan bagi orang lain untuk melaksanakan penarikan dana yang melebihi batas kredit pada Bank diancam dengan pidana. Dalam hal ini termasuk juga tindakan lain berupa pemberian atau penerimaan suap yang merupakan jenis perbuatan yang tergolong *Fraud*.

3. Selama ini, baik secara langsung maupun tidak langsung, pelaksanaan pencegahan *Fraud* telah dilaksanakan Bank, antara lain melalui penerapan manajemen risiko, khususnya sistem pengendalian intern, dan pelaksanaan tata kelola yang baik. Namun demikian, agar penerapan strategi anti *Fraud* menjadi lebih efektif masih diperlukan upaya peningkatan budaya sadar risiko agar pencegahan *Fraud* menjadi fokus perhatian dan kepedulian bagi seluruh jajaran organisasi Bank, baik oleh Direksi, Dewan Komisaris, maupun pegawai Bank, yang antara lain diwujudkan dengan kesediaan penandatanganan pakta integritas oleh Direksi, Dewan Komisaris, dan pegawai Bank.
4. Efektivitas pengendalian *Fraud* dalam proses bisnis merupakan tanggung jawab Direksi dan Dewan Komisaris, sehingga diperlukan pemahaman yang tepat dan menyeluruh tentang *Fraud* oleh Direksi dan Dewan Komisaris agar dapat memberikan arahan dan menumbuhkan kesadaran untuk pengendalian risiko *Fraud* pada Bank.
5. Strategi anti *Fraud* merupakan wujud komitmen Direksi dan Dewan Komisaris Bank dalam mengendalikan *Fraud* yang diterapkan dalam bentuk sistem pengendalian *Fraud*. Strategi ini menuntut Direksi dan Dewan Komisaris untuk mengoptimalkan sumber daya yang ada agar sistem pengendalian *Fraud* dapat diimplementasikan secara efektif dan berkesinambungan.
6. Pedoman penerapan strategi anti *Fraud* dalam ketentuan ini mengarahkan Bank dalam melakukan pengendalian *Fraud* melalui upaya yang tidak hanya ditujukan untuk mencegah namun juga untuk mendeteksi dan melakukan investigasi serta memperbaiki sistem sebagai bagian dari strategi yang bersifat integral dalam mengendalikan *Fraud*.

II. PEDOMAN UMUM PENERAPAN STRATEGI ANTI *FRAUD*

1. Dalam pedoman ini yang dimaksud dengan *Fraud* adalah tindakan penyimpangan atau pembiaran yang sengaja dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain, yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah, atau pihak lain menderita kerugian dan/atau pelaku *Fraud* memperoleh keuntungan

keuangan baik secara langsung maupun tidak langsung. Jenis-jenis perbuatan yang tergolong *Fraud* yaitu kecurangan, penipuan, penggelapan aset, pembocoran informasi, tindak pidana perbankan, dan tindakan lain yang dapat dipersamakan dengan *Fraud*.

2. Berdasarkan pendekatan kegiatan usaha Bank, pengelompokan aktivitas terjadinya *Fraud* dibedakan sebagai berikut: pendanaan, perkreditan atau pembiayaan, penggunaan identitas dan data orang/pihak lain/nasabah, pengelolaan aset, penggunaan siber, penyajian laporan keuangan, dan aktivitas lain. Yang dimaksud dengan aktivitas lain yaitu kegiatan usaha Bank di luar pendanaan, perkreditan atau pembiayaan, penggunaan identitas dan data orang/pihak lain/nasabah, pengelolaan aset, penggunaan siber, dan penyajian laporan keuangan.
3. Strategi anti *Fraud* merupakan strategi Bank dalam mengendalikan *Fraud* yang dirancang untuk mengembangkan, menerapkan dan meningkatkan program kepatuhan anti *Fraud* di Bank, dengan mengacu pada proses terjadinya *Fraud* dan memperhatikan karakteristik serta jangkauan dari potensi terjadinya *Fraud* yang tersusun secara komprehensif integralistik dan diimplementasikan dalam bentuk sistem pengendalian *Fraud*. Penerapan strategi anti *Fraud* merupakan bagian dari penerapan manajemen risiko, khususnya yang terkait dengan aspek sistem pengendalian intern.
4. Keberhasilan strategi anti *Fraud* dipengaruhi oleh lingkungan intern dan ekstern yang mendukung terciptanya kondisi yang kondusif sehingga semua pihak yang terkait dapat berperan dengan optimal dalam mengimplementasikan sistem pengendalian *Fraud* di Bank.
5. Struktur strategi anti *Fraud* secara utuh menggabungkan prinsip dasar dari manajemen risiko khususnya sistem pengendalian intern dan tata kelola yang baik. Implementasi strategi anti *Fraud* dalam bentuk sistem pengendalian *Fraud* dijabarkan melalui 4 (empat) pilar strategi pengendalian *Fraud* yang saling berkaitan yaitu: (i) pencegahan; (ii) deteksi; (iii) investigasi, pelaporan, dan sanksi; serta (iv) pemantauan, evaluasi, dan tindak lanjut.

III. PENERAPAN MANAJEMEN RISIKO

Penerapan strategi anti *Fraud* sebagai bagian dari pelaksanaan penerapan manajemen risiko tidak dapat dipisahkan dari cakupan penerapan manajemen risiko secara umum. Oleh karena itu efektivitas penerapan strategi anti *Fraud* paling sedikit perlu didukung dengan penguatan pada aspek manajemen risiko yang fokus pada pengendalian *Fraud*. Aspek tersebut paling sedikit meliputi pengawasan aktif Direksi dan Dewan Komisaris, kebijakan dan prosedur, struktur organisasi dan pertanggungjawaban, serta pengendalian dan pemantauan.

Cakupan minimum untuk setiap aspek pendukung tersebut adalah sebagai berikut:

1. Pengawasan Aktif Direksi dan Dewan Komisaris

   Pengawasan aktif Direksi dan Dewan Komisaris terhadap *Fraud* mencakup hal-hal yang menjadi kewenangan dan tanggung jawab Direksi dan Dewan Komisaris dalam penerapan strategi anti *Fraud* di Bank. Kewenangan dan tanggung jawab tersebut paling sedikit sebagai berikut:

   a. pengembangan kepedulian dan budaya anti *Fraud* pada seluruh jajaran organisasi, antara lain meliputi deklarasi anti *Fraud* dan komunikasi yang memadai tentang perilaku yang termasuk *Fraud*;

   b. penandatanganan pakta integritas oleh seluruh jajaran organisasi Bank, baik Direksi, Dewan Komisaris, maupun setiap pegawai Bank, dengan cakupan pakta integritas paling sedikit:

      1) senantiasa mematuhi hukum dan ketentuan peraturan perundang-undangan;

      2) bertindak objektif dan berpegang teguh pada nilai etika dan moral, adil, transparan, konsisten serta menjunjung tinggi kejujuran dan komitmen;

      3) berperan aktif dalam upaya pencegahan dan pemberantasan *Fraud* serta bersedia melakukan pelaporan dalam hal terjadi tindakan *Fraud* di lingkungan Bank; dan

      4) menciptakan lingkungan kerja yang bebas dari korupsi, kolusi, dan nepotisme (KKN);

   c. penyusunan dan pengawasan penerapan kode etik terkait dengan pencegahan *Fraud* bagi seluruh jajaran organisasi;

d. penyusunan dan pengawasan penerapan strategi anti *Fraud* secara menyeluruh;
e. pengembangan kualitas sumber daya manusia (SDM), khususnya yang terkait dengan peningkatan kesadaran dan pengendalian *Fraud*;
f. pemantauan dan evaluasi atas kejadian *Fraud* serta penetapan tindak lanjut; dan
g. pengembangan saluran komunikasi yang efektif di intern dan bagi ekstern Bank agar seluruh pejabat dan pegawai Bank memahami dan mematuhi kebijakan dan prosedur yang berlaku, termasuk kebijakan dan prosedur untuk pengendalian *Fraud*.

2. Kebijakan dan Prosedur

Kebijakan dan prosedur yang disusun oleh Bank untuk penerapan pengendalian *Fraud* perlu mempertimbangkan ukuran Bank dan kompleksitas kegiatan usaha Bank. Agar pelaksanaan kebijakan dan prosedur dapat berjalan dengan efektif, maka kebijakan dan prosedur tersebut perlu dikomunikasikan dengan baik kepada seluruh jajaran organisasi Bank dan berbagai pihak yang berhubungan dengan Bank. Kebijakan dan prosedur dimaksud harus dirancang untuk mengurangi risiko yang teridentifikasi dan dapat mencegah perilaku yang mengarah pada tindakan *Fraud*.

Hal yang perlu diperhatikan dalam penyusunan dan penerapan kebijakan dan prosedur pencegahan *Fraud*, paling sedikit mencakup:

a. komitmen Direksi dan Dewan Komisaris;
b. penetapan sistem pengendalian intern yang menyeluruh dan prosedur penilaian risiko;
c. uji tuntas terhadap pihak ketiga yang berhubungan dengan Bank;
d. penetapan remunerasi sesuai tugas dan tanggung jawab;
e. penerapan tata kelola yang baik dalam kegiatan usaha Bank;
f. pengendalian keuangan dan penerapan akuntansi sesuai dengan standar akuntansi keuangan yang berlaku;
g. penghindaran konflik kepentingan dalam pengambilan keputusan, pendelegasian wewenang, dan pemisahan fungsi;
h. mekanisme pelaporan *Fraud*, termasuk prosedur *whistleblowing system*;
i. penegakan disiplin dan sanksi atas pelanggaran terhadap aturan anti *Fraud*;

j. komunikasi dan pelatihan atas kebijakan dan prosedur pencegahan *Fraud*;

k. pemantauan dan evaluasi secara berkala terhadap kebijakan dan prosedur pencegahan *Fraud*; dan

l. hal lain yang dipandang perlu.

3. Struktur Organisasi dan Pertanggungjawaban

Untuk mendukung efektivitas penerapan strategi anti *Fraud*, Bank memiliki unit kerja atau fungsi yang bertugas menangani penerapan strategi anti *Fraud*.

Hal-hal yang perlu diperhatikan dalam pembentukan unit kerja atau fungsi tersebut paling sedikit sebagai berikut:

a. pembentukan unit kerja atau fungsi dalam struktur organisasi disesuaikan dengan ukuran dan kompleksitas kegiatan usaha Bank;

b. penetapan uraian tugas dan tanggung jawab yang jelas;

c. pertanggungjawaban unit kerja atau fungsi tersebut kepada direktur utama;

d. penjaminan terselenggaranya hubungan komunikasi dan pelaporan secara langsung kepada Dewan Komisaris; dan

e. pelaksanaan tugas pada unit kerja atau fungsi tersebut harus dilakukan oleh SDM yang memiliki kompetensi, integritas, dan independensi, serta didukung dengan pertanggungjawaban yang jelas.

4. Pengendalian dan Pemantauan

Dalam melakukan pengendalian dan pemantauan, Bank melakukan langkah untuk meningkatkan efektivitas penerapan strategi anti *Fraud* paling sedikit sebagai berikut:

a. pengendalian melalui kaji ulang baik oleh Direksi dan Dewan Komisaris maupun kaji ulang operasional oleh satuan kerja audit intern atas penerapan strategi anti *Fraud*;

b. pengendalian di bidang SDM yang ditujukan untuk meningkatkan efektivitas pelaksanaan tugas dan pengendalian *Fraud*, misalnya kebijakan rotasi, kebijakan mutasi, cuti wajib, dan aktivitas sosial atau kebersamaan;

c. penetapan pemisahan fungsi dalam pelaksanaan aktivitas Bank pada seluruh jajaran organisasi, misalnya penerapan *four eyes principle* dalam aktivitas perkreditan atau pembiayaan dengan

tujuan agar setiap pihak yang terkait dalam aktivitas tersebut tidak memiliki peluang untuk melakukan dan menyembunyikan *Fraud* dalam pelaksanaan tugasnya;

d. pengendalian sistem informasi yang mendukung pengolahan, penyimpanan, dan pengamanan data secara elektronik untuk mencegah potensi terjadinya *Fraud*. Bank memiliki program kontinjensi yang memadai, termasuk untuk pengamanan data. Pengendalian sistem informasi ini perlu disertai dengan tersedianya sistem akuntansi untuk menjamin penggunaan data yang akurat dan konsisten dalam pencatatan dan pelaporan keuangan Bank, antara lain melalui rekonsiliasi atau verifikasi data secara berkala; dan

e. pengendalian dan pemantauan lain untuk meningkatkan efektivitas penerapan strategi anti *Fraud* seperti pengendalian, pemantauan, dan dokumentasi terhadap fisik aset.

IV. 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; dan
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) sistem 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.

Kebijakan penanganan pengaduan harus dirumuskan secara jelas, mudah dimengerti, dan dapat diimplementasikan secara efektif agar memberikan dorongan serta kesadaran kepada pegawai dan pejabat Bank untuk melaporkan *Fraud* yang terjadi di Bank. Dalam rangka mitigasi dan pencegahan *Fraud* secara efektif, perlu ditingkatkan efektivitas penerapan kebijakan penanganan pengaduan di Bank yang paling sedikit mencakup:

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

Bank harus 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; dan
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* (Lampiran II Peraturan Otoritas Jasa Keuangan ini) dan laporan *Fraud* berdampak signifikan (Lampiran III Peraturan Otoritas Jasa Keuangan ini).

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.

Ditetapkan di Jakarta
pada tanggal 19 Desember 2019

KETUA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

WIMBOH SANTOSO

LAMPIRAN II

PERATURAN OTORITAS JASA KEUANGAN
NOMOR 39 /POJK.03/2019
TENTANG PENERAPAN STRATEGI ANTI *FRAUD* BAGI BANK UMUM

LAPORAN PENERAPAN STRATEGI ANTI *FRAUD*

PT BANK .....

LAPORAN PENERAPAN STRATEGI ANTI *FRAUD*

SEMESTER ... TAHUN ...

I. Perkembangan Pelaksanaan Penerapan Strategi Anti *Fraud*

(Diisi penjelasan secara singkat mengenai hasil evaluasi dan tindak lanjut penerapan strategi anti *Fraud* pada periode laporan)

II. Laporan Penerapan Strategi Anti *Fraud*

A. Tabel Kejadian *Fraud*

Kejadian *Fraud* Menurut Pelaku (I)	ID Kejadian *Fraud* (II)	Jenis *Fraud* (III)		Aktivitas Terkait *Fraud* (IV)	Deskripsi *Fraud*/ Modus Operandi (V)	Lokasi *Fraud* (VI)		Divisi/Unit Kerja Terjadinya *Fraud* (VII)	Pihak yang Dirugikan (VIII)	Waktu (IX)			Jumlah Kerugian (X)									Kelemahan Pengelolaan *Fraud* (XI)		Tindakan untuk Penanganan *Fraud* (XII)		Tindakan Perbaikan untuk Pencegahan *Fraud* (XIII)			
										Fraud Terjadi		*Fraud* Diketahui	Bank			Nasabah			Pihak Lain									
		Jenis *Fraud*	Keterangan Jenis *Fraud*			Lokasi *Fraud*	Keterangan Lokasi *Fraud*			Awal	Akhir		Rkl (Incurred)	Potensial (Potential)	Setelah Pengembalian (Recovery)	Rkl (Incurred)	Potensial (Potential)	Setelah Pengembalian (Recovery)	Rkl (Incurred)	Potensial (Potential)	Setelah Pengembalian (Recovery)	Kelemahan Penyebab *Fraud*	Keterangan	Tindakan untuk Penanganan *Fraud*	Keterangan	Tindakan Perbaikan untuk Pencegahan *Fraud*	Keterangan	Target Waktu Pelaksanaan	Realisasi Pelaksanaan
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

B. Tabel Pelaku *Fraud*

ID Kejadian *Fraud* (I)	Intern/ Ekstern (II)	Identitas Pelaku (III)								Status Pelaku (IV)	Jabatan Pelaku (V)				Keterangan Pelaku (VI)	Pengenaan Sanksi (VII)
		Nama	Jenis Identitas	Nomor Identitas	Jenis Kelamin	Alamat Identitas	Alamat Domisili	Tempat Lahir	Tanggal Lahir		Pada Saat *Fraud* Terjadi	Keterangan Jabatan	Pada Saat *Fraud* Diketahui	Keterangan Jabatan		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

PEDOMAN PENGISIAN LAPORAN PENERAPAN STRATEGI ANTI *FRAUD*

A. Tabel Kejadian *Fraud*

I. Kejadian *Fraud* Menurut Pelaku (Harus Diisi)

Diisi karakter sebanyak 1 (satu) digit berupa huruf kapital sesuai dengan sandi sebagai berikut:

Kejadian *Fraud* Menurut Pelaku	Sandi
Kejadian *Fraud* dengan pelaku intern	A
Kejadian *Fraud* dengan pelaku ekstern	B
Kejadian *Fraud* dengan pelaku intern dan ekstern	C

II. ID Kejadian *Fraud* (Harus Diisi)

Diisi karakter sebanyak 6 (enam) digit sesuai urutan kejadian *Fraud* dengan digit pertama diawali sandi kejadian *Fraud* menurut pelaku yang mencerminkan bahwa kejadian tersebut merupakan kejadian *Fraud* dengan melibatkan pelaku intern, pelaku ekstern, atau pelaku intern dan ekstern. Selanjutnya digit ke-2 sampai dengan digit ke-6 diisi dengan angka sesuai urutan kejadian *Fraud*.

Contoh:

Kejadian *Fraud* dengan pelaku intern untuk nomor urut 1 dituliskan A00001.

III. Jenis *Fraud* (Harus Diisi)

1. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Jenis *Fraud*	Sandi
Kecurangan	201
Penipuan	202
Penggelapan aset	203
Pembocoran informasi	204
Tindak pidana perbankan	205
Tindakan lain	209

2. Keterangan Jenis *Fraud*:
   Harus diisi jika memilih "Tindakan lain yang dapat dipersamakan dengan *Fraud*" pada kolom "Jenis *Fraud*" (menggunakan format bebas).

IV. Aktivitas Terkait *Fraud* (Harus Diisi)
Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Aktivitas Terkait *Fraud*	Sandi
Pendanaan	301
Perkreditan/pembiayaan	302
Penggunaan identitas dan dan data orang, pihak lain, atau nasabah	303
Pengelolaan aset	304
Penggunaan siber	305
Penyajian laporan keuangan	306
Aktivitas lain	309

Penjelasan aktivitas terkait *Fraud* berdasarkan jenis kegiatan usaha Bank yaitu sebagai berikut:

1. Pendanaan
   Fraud yang terjadi pada aktivitas penghimpunan Dana Pihak Ketiga (DPK) yang dilakukan Bank.
   Contoh:
   a. Penghimpunan DPK yang tidak dicatat dalam pembukuan Bank atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu Bank.
      Penjelasan:
      Ketidaksesuaian atau rekayasa pencatatan dana masuk dari nasabah yang berupa tabungan, giro, deposito, dan bentuk simpanan lain yang dipersamakan dengan tabungan, giro, deposito, yang dilakukan oleh pegawai atau pejabat Bank sehingga menimbulkan selisih pencatatan dalam pembukuan Bank.
   b. Penarikan atau pencairan DPK yang dilakukan bukan oleh pemilik atau kuasanya atau oleh pegawai Bank yang tidak

dicatat dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu Bank.

Penjelasan:

Penarikan atau pencairan DPK nasabah untuk kepentingan pribadi Direksi, Dewan Komisaris, pegawai, dan/atau pihak lain tanpa seizin dan sepengetahuan nasabah. Penarikan atau pencairan DPK dapat menggunakan antara lain bilyet deposito palsu, bilyet giro palsu, dan surat kuasa palsu.

c. Penyetoran atau pemindahbukuan tabungan, giro, atau deposito yang tidak dicatat dengan benar dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu Bank.

d. Penyetoran atau pemindahbukuan tabungan, giro, atau deposito yang dicatat dalam pembukuan Bank tanpa disertai aliran dana.

e. Pemberian pelayanan terhadap nasabah prima di luar prosedur atau ketentuan yang telah ditetapkan oleh Bank yang menimbulkan kerugian bagi Bank.

2. Perkreditan/Pembiayaan

Fraud yang terjadi pada aktivitas pemberian kredit/pembiayaan yang dilakukan oleh Bank, dimulai dari pengajuan kredit/pembiayaan hingga pelunasan kredit/pembiayaan oleh debitur.

Contoh:

a. Debitur fiktif

Penjelasan:

Pemberian kredit/pembiayaan kepada satu atau lebih debitur dengan menggunakan identitas palsu atau identitas pihak lain.

b. Debitur topengan

Penjelasan:

Pemberian kredit/pembiayaan kepada debitur dengan menggunakan identitas asli dari debitur yang bersangkutan namun dana digunakan oleh pihak lain.

c. Rekayasa atau manipulasi dokumen atau informasi kredit/pembiayaan

Penjelasan:

Rekayasa dokumen atau infomasi oleh debitur dan/atau pihak Bank untuk memenuhi persyaratan dan kelayakan pemberian kredit/pembiayaan atau restrukturisasi kredit/pembiayaan antara lain:

1) rekayasa kemampuan dan prospek usaha debitur;
2) rekayasa laporan keuangan debitur;
3) *overvalued/undervalued* penilaian agunan atau penggunaan agunan fiktif;
4) rekayasa analisa kredit/pembiayaan oleh pihak Bank;
5) ketiadaan dokumen permohonan, analisis, keputusan, dan/atau perjanjian kredit/pembiayaan; dan
6) dokumen persyaratan kredit/pembiayaan yang tidak benar.

d. Rekayasa atau ketidaksesuaian pencatatan angsuran kredit/pembiayaan dalam pembukuan Bank

Penjelasan:

Tidak mencatat angsuran kredit/pembiayaan, ketidaksesuaian pencatatan nominal angsuran kredit/pembiayaan dengan dana yang diterima, atau pencatatan angsuran kredit/pembiayaan yang tidak disertai dengan aliran dana.

e. Ketidaksesuaian penggunaan kredit/pembiayaan dengan tujuan atau kebutuhan

Penjelasan:

Penggunaan dana kredit/pembiayaan yang dicairkan tidak sesuai dengan tujuan awal pengajuan kredit/pembiayaan atau kebutuhan kredit/pembiayaan yang sesungguhnya.

f. Pembebanan biaya Bank untuk menjaga kolektibilitas kredit/pembiayaan

Penjelasan:

Direksi, Dewan Komisaris, dan/atau pegawai Bank melakukan pembebanan biaya untuk suatu kegiatan fiktif yang sebenarnya digunakan sebagai setoran angsuran

kredit/pembiayaan untuk menjaga kolektibilitas kredit/pembiayaan.

g. Penghindaran pelanggaran Batas Maksimum Pemberian Kredit (BMPK) atau Batas Maksimum Penyaluran Dana (BMPD)

Penjelasan:

Pemecahan satu fasilitas kredit/pembiayaan menjadi beberapa fasilitas kredit/pembiayaan dan pemberian fasilitas kredit/pembiayaan melalui kelompok usaha atau pihak lain untuk menghindari pelanggaran BMPK/BMPD.

h. Pelampauan dan/atau penyalahgunaan wewenang

Penjelasan:

Pelampauan wewenang berupa pemutusan pemberian kredit/pembiayaan dalam jumlah yang melampaui batas kewenangan pejabat/komite kredit/pembiayaan.

Penyalahgunaan wewenang berupa pemutusan pemberian kredit yang tidak didasarkan pada prinsip kehati-hatian.

i. Gratifikasi, skema *cash back*, atau penyuapan

Penjelasan:

Direksi, Dewan Komisaris, dan/atau pegawai Bank menerima atau meminta fasilitas tambahan dari debitur sebagai imbal jasa pencairan kredit/pembiayaan.

j. Pemberian kredit/pembiayaan yang melanggar prinsip kehati-hatian

Penjelasan:

Pemberian kredit/pembiayaan oleh Bank yang melanggar prinsip kehati-hatian sebagaimana diatur dalam ketentuan peraturan perundang-undangan atau Standar Prosedur Operasional (SPO) Bank, antara lain:

1) pemberian kredit/pembiayaan yang tidak sesuai dengan prosedur tahapan pemberian kredit/pembiayaan;
2) pencairan kredit/pembiayaan yang dilakukan sebelum memenuhi persyaratan pencairan kredit/pembiayaan; dan
3) pengikatan agunan kredit/pembiayaan yang tidak sesuai dengan ketentuan peraturan perundang-undangan.

k. Pelunasan kredit/pembiayaan dari dana hasil pencairan kredit/pembiayaan baru yang ditujukan untuk memperbaiki atau menjaga kolektibilitas kredit/pembiayaan
l. Rekayasa kolektibilitas kredit/pembiayaan

3. Penggunaan Identitas dan Data Orang, Pihak Lain, atau Nasabah

Fraud yang terjadi dengan cara menggunakan identitas dan data orang, pihak lain, atau nasabah untuk melakukan transaksi perbankan tanpa sepengetahuan dan/atau persetujuan dari orang, pihak lain, atau nasabah.

Contoh:

a. Penyalahgunaan kartu Anjungan Tunai Mandiri (ATM) nasabah.
b. Penjualan atau pertukaran data nasabah secara tidak sah antar Bank atau pihak ketiga yang dipekerjakan Bank.

4. Pengelolaan Aset

Fraud yang terjadi pada aktivitas pengelolaan aset Bank, termasuk kas.

Contoh:

a. Penggunaan kas yang ada pada brankas oleh Direksi, Dewan Komisaris, dan/atau pegawai Bank untuk kepentingan pribadi serta tidak dicatat dalam pembukuan Bank.
b. Pencurian kas yang dilakukan dengan memanfaatkan kelemahan perangkat lunak dan/atau perangkat keras pada mesin ATM dan/atau kartu ATM Bank.
c. Penyalahgunaan kendaraan Bank untuk kepentingan pribadi Direksi, Dewan Komisaris, dan/atau pegawai Bank.
d. Penjualan Agunan Yang Diambil Alih (AYDA) oleh pegawai Bank kepada debitur dengan harga yang tidak wajar untuk memperoleh keuntungan pribadi pegawai.
e. Pegawai tidak melakukan pencatatan atas pembelian atau penjualan aset milik Bank.
f. Penggelembungan (*mark up*) biaya sewa gedung kantor untuk keuntungan pribadi, Direksi, Dewan Komisaris, dan/atau pegawai Bank.

g. Rekayasa setoran dan penarikan rekening penempatan pada bank lain oleh Direksi Bank.

h. Penempatan, investasi, atau penyertaan dana Bank tidak sesuai dengan SPO Bank yang dilakukan pegawai berkolusi dengan pihak lain.

i. Penarikan uang kas tanpa transaksi yang mendasari dan tidak dicatat pada pos yang seharusnya.

5. Penggunaan Siber

Fraud yang terjadi dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik untuk mengelabui Bank, nasabah, orang, atau pihak lain agar memperoleh informasi dan data pribadi nasabah.

Contoh:

a. Peretasan (*Hacking*) atau Pembobolan (*Cracking*)

Penjelasan:

Penggunaan atau pencarian akses secara tidak sah ke dalam data Bank atau nasabah dalam sistem perbankan diantaranya melalui perbankan elektronik.

b. Pengelabuan (*Phising*)

Penjelasan:

Tindakan memperoleh informasi pribadi nasabah dengan menyamar sebagai pihak yang berwenang melalui surel untuk mengarahkan nasabah agar mengakses tautan tertentu dalam surel tersebut.

c. Penyalinan Informasi (*Skimming*)

Penjelasan:

Penggunaan mesin atau kamera yang dipasang pada mesin ATM dengan tujuan untuk mencuri informasi kartu dan nomor *Personal Identification Number* (PIN) nasabah ketika nasabah menggunakan mesin ATM.

d. Rekayasa Sosial (*Social Engineering*)

Penjelasan:

Tindakan memperoleh informasi nasabah seperti PIN, nomor kartu, dan/atau informasi lain dengan cara menghubungi nasabah melalui telepon, *short message service* (sms), atau media lain untuk menginformasikan pemberian hadiah dan

meminta nasabah untuk menghubungi nomor telepon atau membuka situs web tertentu.

e. Virus, *malware, ransomware*

Penjelasan:

Merupakan suatu program yang dirancang dengan tujuan untuk merusak, menyusup, dan/atau mencuri informasi atau data rahasia Bank dan/atau nasabah dalam sistem elektronik Bank.

6. Penyajian Laporan Keuangan

Fraud yang terjadi dalam penyajian laporan keuangan Bank antara lain laporan keuangan tidak disajikan sesuai dengan prinsip akuntansi yang berlaku umum dan/atau tidak sesuai dengan kondisi keuangan yang sebenarnya, termasuk pencatatan yang tidak benar, antara lain penggelembungan (*mark up*) biaya dan biaya fiktif dalam pembukuan atau dalam laporan Bank.

Contoh:

Rekayasa atau manipulasi laporan keuangan Bank (*window dressing*).

Penjelasan:

Rekayasa laporan keuangan agar kinerja Bank terlihat lebih baik dari kondisi keuangan yang sebenarnya atau berhasil mencapai target yang telah ditetapkan.

7. Aktivitas Lain

Fraud yang terjadi pada setiap aspek aktivitas Bank selain kategori yang telah dikelompokkan di atas (angka 1 sampai dengan angka 6).

V. Deskripsi *Fraud* atau Modus Operandi (Harus Diisi)

Diisi dengan deskripsi mengenai *Fraud* yang terjadi paling banyak 4000 karakter (menggunakan format bebas), serta dilengkapi dengan mengunggah *file* PDF yang memuat rincian deskripsi. Dalam hal tidak terdapat rincian deskripsi, *file* PDF tetap harus diunggah.

VI. Lokasi *Fraud* (Harus Diisi)

1. Diisi karakter sebanyak 2 (dua) digit sesuai dengan sandi lokasi *Fraud* berdasarkan jenis kantor bank umum konvensional dan bank umum syariah sebagai berikut:

Lokasi	Sandi
Kantor Pusat Operasional	01
Kantor Pusat Non Operasional	02
Kantor Cabang dari bank yang berkedudukan di Luar Negeri	03
Unit Usaha Syariah Bank Umum	04
Kantor Wilayah Bank Umum	05
Kantor Cabang (Dalam Negeri)	06
Kantor Cabang (Luar Negeri)	07
Kantor Cabang Pembantu dari bank yang berkedudukan di Luar Negeri	08
Kantor Cabang Pembantu (Dalam Negeri)	09
Kantor Cabang Pembantu (Luar Negeri)	10
Kantor Kas	11
Kantor Fungsional	12
Payment Point	13
Kas Keliling/Kas Mobil/Kas Terapung	14
Kantor di bawah KCP dari bank yang berkedudukan di Luar Negeri yang Tidak Termasuk 11,12,13,14	15
Kantor Perwakilan Bank Umum di Luar Negeri	16
ATM/CDM/CRM	17
Kantor Pusat Operasional Bank Umum Syariah	51
Kantor Pusat Non Operasional Bank Umum Syariah	52
Kantor Wilayah Bank Umum Syariah	53
Kantor Cabang (Dalam Negeri) Bank Umum Syariah	54
Kantor Cabang (Luar Negeri) Bank Umum Syariah	55
Kantor Cabang Pembantu (Dalam Negeri) Bank Umum Syariah	56
Kantor Cabang Pembantu (Luar Negeri) Bank Umum Syariah	57
Kantor Kas Bank Umum Syariah	58
Kantor Fungsional Bank Umum Syariah	59

Payment Point Bank Umum Syariah	60
Kas Keliling/Kas Mobil/Kas Terapung Bank Umum Syariah	61
Kantor Perwakilan Bank Umum Syariah di Luar Negeri	62
ATM/CDM/CRM Bank Umum Syariah	63
Layanan Syariah Bank Umum	64

Bank umum konvensional yang memiliki unit usaha syariah harus mengisi Unit Usaha Syariah Bank Umum (sandi 04) untuk kejadian *Fraud* yang terjadi di kantor yang melaksanakan fungsi unit usaha syariah tersebut.

2. Keterangan Lokasi *Fraud*

Diisi karakter sebanyak 4 (empat) digit sesuai dengan sandi kota/kabupaten yang tercantum dalam pedoman Sistem Layanan Informasi Keuangan (SLIK) sebagaimana dimaksud dalam ketentuan Otoritas Jasa Keuangan mengenai pelaporan dan permintaan informasi debitur melalui SLIK.

VII. Divisi atau Unit Kerja Terjadinya *Fraud* (Harus Diisi)

Diisi nama divisi atau unit kerja terjadinya *Fraud* atau yang terkena dampak *Fraud* secara langsung (menggunakan format bebas).

VIII. Pihak yang Dirugikan (Harus Diisi)

Pihak yang dirugikan yaitu Bank, nasabah, dan/atau pihak lain. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Pihak yang Dirugikan	Sandi
Bank	001
Nasabah	002
Pihak Lain	003

Dalam hal pihak yang dirugikan lebih dari satu, maka diisi pada baris berikutnya dengan ID kejadian *Fraud* yang sama.

IX. Waktu (Harus Diisi)

1. *Fraud* Terjadi
   a. Awal
      Diisi dengan tanggal mulai terjadinya *Fraud* (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD.
   b. Akhir
      Diisi dengan tanggal selesai terjadinya *Fraud* (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD.
2. *Fraud* Diketahui
   Diisi dengan tanggal *Fraud* diketahui Bank (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD.

X. Jumlah Kerugian (Harus Diisi)

Diisi dengan digit angka jumlah kerugian yang terjadi dalam satuan penuh dengan mata uang Rupiah baik kerugian yang dialami oleh Bank, nasabah dan/atau pihak lain.

1. Riil (*incurred*)
   Diisi dengan jumlah kerugian yang telah terjadi.
2. Potensial (*potential*)
   Diisi dengan jumlah kerugian yang mungkin timbul (*potential loss*).
3. Setelah Pengembalian (*recovery*)
   Diisi dengan jumlah kerugian setelah ada pengembalian atau diganti.

XI. Kelemahan Penyebab *Fraud* (Harus Diisi)

1. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Kelemahan Penyebab *Fraud*	Sandi
Sumber Daya Manusia – Integritas	101
Sumber Daya Manusia – Kompetensi	102
Sistem Pengendalian Intern – Pengendalian Intern Pimpinan	201

Sistem Pengendalian Intern - pada Kebijakan Intern Bank	202
Sistem Pengendalian Intern - Ketidaksesuaian atas Tingkat dan Toleransi Risiko	203
Sistem Pengendalian Intern - Pelanggaran Standar dan Prosedur Bank	204
Sistem Pengendalian Intern - Tidak Berjalannya Pemisahan Fungsi (*Four Eyes Principle*)	205
Sistem Pengendalian Intern - Pelaporan Keuangan dan Kegiatan Operasional yang Tidak Akurat dan Tidak Tepat Waktu	206
Sistem Pengendalian Intern - Struktur Organisasi yang Belum Berjalan Efektif	207
Teknologi Informasi	301
Penerapan Strategi Anti *Fraud* Belum Berjalan Efektif	401
Kelemahan Lain	901

Dalam hal terdapat lebih dari satu kelemahan penyebab *Fraud*, maka diisi pada baris berikutnya dengan ID kejadian *Fraud* yang sama.

2. Keterangan Kelemahan Penyebab *Fraud*:
   Harus diisi jika memilih "Kelemahan Lain" pada kolom "Kelemahan Penyebab *Fraud*" (menggunakan format bebas).

XII. Tindakan Untuk Penanganan *Fraud* (Harus Diisi)

Tindakan untuk penanganan *Fraud* merupakan respon Bank atas kejadian *Fraud* baik berupa tindakan kepada pelaku, pihak yang dirugikan, atau tindakan lain.

1. Diisi karakter sebanyak 2 (dua) digit sesuai dengan sandi sebagai berikut:

Tindakan Untuk Penanganan *Fraud*	Sandi
Pemberian Surat Peringatan	01
Rotasi atau Mutasi	02
Penurunan Jabatan	03

Pengunduran Diri	04
Pemutusan Hubungan Kerja	05
Pemblokiran Kartu Debit/Kartu Kredit	06
Pemblokiran Rekening	07
Penggantian Kartu Debit/Kartu Kredit	08
Pelaporan Kepolisian atau Tindakan Hukum	09
Ganti Rugi	10
Tindakan Lain	19

Dalam hal terdapat lebih dari satu tindakan untuk penanganan *Fraud*, maka diisi pada baris berikutnya dengan ID kejadian *Fraud* yang sama.

2. Keterangan Tindakan Untuk Penanganan *Fraud*:
Harus diisi jika memilih "Tindakan Lain" pada kolom "Tindakan Untuk Penanganan *Fraud*" (menggunakan format bebas).

XIII. Tindakan Perbaikan Untuk Pencegahan *Fraud* (harus diisi)

1. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Tindakan Perbaikan Untuk Pencegahan *Fraud*	Sandi
Sumber Daya Manusia	100
Sistem Pengendalian Intern	200
Teknologi Informasi	300
Penerapan Strategi Anti *Fraud*	400
Tindakan Lain	900

Dalam hal terdapat lebih dari satu tindakan perbaikan untuk pencegahan *Fraud*, maka diisi pada baris berikutnya dengan ID kejadian *Fraud* yang sama.

2. Keterangan Tindakan Perbaikan Untuk Pencegahan *Fraud*
Diisi dengan deskripsi tindakan perbaikan yang dilakukan oleh Bank untuk pencegahan kejadian *Fraud* serupa di masa mendatang (menggunakan format bebas).

3. Target Waktu Pelaksanaan

Diisi dengan target waktu pelaksanaan dari tindakan perbaikan yang dilakukan oleh Bank (menggunakan format bebas).

4. Realisasi Pelaksanaan

Diisi dengan realisasi atas target waktu pelaksanaan dari tindakan perbaikan yang dilakukan oleh Bank (menggunakan format bebas).

B. Tabel Pelaku *Fraud*

Pelaku *Fraud* merupakan pihak yang terlibat dalam kejadian *Fraud*.

I. ID Kejadian *Fraud* (Harus Diisi)

Diisi karakter sebanyak 6 (enam) digit sesuai dengan ID kejadian *Fraud* yang melibatkan pelaku tersebut. ID kejadian *Fraud* pada Tabel Pelaku *Fraud* harus sesuai dengan ID kejadian *Fraud* pada Tabel Kejadian *Fraud*.

Dalam hal terdapat kejadian *Fraud* yang pelakunya belum diketahui, maka ID kejadian *Fraud* tetap wajib diisi dalam Tabel Pelaku *Fraud*.

II. Intern/Ekstern (Harus Diisi)

Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi pelaku *Fraud*.

Pelaku *Fraud*	Sandi
Intern	001
Ekstern	002

III. Identitas Pelaku

Untuk pelaku *Fraud* ekstern, dalam hal pelaku *Fraud* atas nama perusahaan maka kolom Jenis Kelamin, Tempat Lahir, dan Tanggal Lahir tidak perlu diisi.

Untuk pelaku *Fraud* ekstern, dalam hal pelaku *Fraud* tidak diketahui maka kolom Jenis Kelamin, Alamat Identitas, Alamat Domisili, Tempat Lahir, dan Tanggal Lahir tidak perlu diisi.

1. Nama (Harus Diisi)

Diisi dengan nama pelaku *Fraud* tanpa gelar sesuai dengan yang tercantum dalam dokumen identitas.

Untuk pelaku *Fraud* ekstern, dalam hal nama pelaku *Fraud* tidak diketahui maka kolom tersebut tetap harus diisi (tidak boleh dikosongkan) dan Bank mendefinisikan nama pelaku yang tidak diketahui tersebut. Contoh: *unknown client*.

2. Jenis Identitas (Harus Diisi)

   Diisi dengan karakter sebanyak 3 digit sesuai dengan jenis identitas.

Jenis Identitas	Sandi	Keterangan
KTP (Nomor Induk Kependudukan)	001	Pelaku *Fraud* WNI
Paspor (Nomor Paspor)	002	Pelaku *Fraud* WNA
NPWP	003	Pelaku *Fraud* atas nama perusahaan
Tidak Diketahui	009	

3. Nomor Identitas (Harus Diisi)

   Diisi dengan nomor identitas sesuai dengan jenis identitas yang dipilih.

   Nomor identitas untuk jenis identitas yang tidak diketahui menggunakan kode unik yang dibuat oleh Bank.

   Dalam hal nomor identitas mengandung karakter selain huruf dan angka maka karakter tersebut tidak perlu disertakan.

   Contoh:

   Pelaku *Fraud* memiliki nomor NPWP 49.810.734.1-035.000, maka diisi pada kolom Nomor Identitas yaitu 498107341035000.

4. Jenis Kelamin

   Diisi karakter sebanyak 1 (satu) digit sesuai dengan sandi jenis kelamin pelaku *Fraud* sebagai berikut:

Jenis Kelamin	Sandi
Laki-laki	L
Perempuan	P

   Dalam hal pelaku *Fraud* atas nama perusahaan atau tidak diketahui maka kolom Jenis Kelamin tidak perlu diisi.

5. Alamat Identitas

   Diisi dengan alamat identitas sesuai dengan yang tertera pada dokumen identitas pelaku *Fraud*.

6. Alamat Domisili

   Diisi alamat domisili dengan informasi (menggunakan format bebas, kecuali untuk kota atau kabupaten, provinsi, negara mengacu pada pedoman SLIK sebagaimana dimaksud dalam ketentuan Otoritas Jasa Keuangan mengenai pelaporan dan permintaan informasi debitur melalui SLIK):

   a. Jalan/blok;
   b. Nomor rumah;
   c. RT/RW;
   d. Kelurahan;
   e. Kecamatan;
   f. Kota/Kabupaten;
   g. Provinsi;
   h. Negara; dan
   i. Kode Pos.

7. Tempat Lahir

   Diisi dengan tempat kelahiran pelaku *Fraud* sesuai yang tercantum dalam dokumen identitas.

8. Tanggal Lahir

   Tanggal lahir diisi (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD sesuai dengan tanggal yang tercantum pada dokumen identitas.

   Contoh:

   Tanggal lahir 15 Desember 1975, ditulis 19751215.

IV. Status Pelaku (Harus Diisi jika Pelaku *Fraud* Intern dan jika Pelaku *Fraud* Ekstern Diketahui)

Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Status	Sandi	Keterangan
Pelaku Utama	001	Pelaku Utama adalah: a. Orang yang memerintahkan, menyuruh melakukan, atau mengusulkan terjadinya tindakan atau perbuatan;

		b. Orang yang menyetujui, turut serta menyetujui, atau menandatangani; c. Orang yang melakukan atau turut serta melakukan suatu perbuatan berdasarkan perintah dari pihak lain, baik dengan atau tanpa tekanan, dan yang bersangkutan patut mengetahui atau patut menduga bahwa perbuatan atau perintah yang dilakukan tersebut bertentangan dengan ketentuan yang berlaku serta tidak berusaha untuk menolak melakukan perbuatan atau perintah tersebut; atau d. Orang yang melakukan suatu perbuatan karena adanya janji atau imbalan tertentu.
Pihak Terlibat	002	Pihak Terlibat adalah orang yang karena melaksanakan tugas, jabatan, dan/atau adanya suatu perintah dari pihak lain, baik dengan atau tanpa tekanan, melakukan atau turut serta melakukan suatu perbuatan, dan yang bersangkutan patut mengetahui atau patut menduga bahwa perbuatan atau perintah yang dilakukan tersebut bertentangan dengan ketentuan yang berlaku, namun yang bersangkutan telah berusaha

		untuk menolak melakukan perbuatan atau perintah tersebut.

V. Jabatan Pelaku (Harus Diisi jika Pelaku *Fraud* Intern)

1. Pada saat *Fraud* terjadi

a. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi jabatan

Jabatan	Sandi	Keterangan
Direktur Utama	001	
Direktur	002	
Direktur Kepatuhan	003	Direktur yang membawahkan fungsi kepatuhan.
Komisaris Utama	004	
Komisaris	005	
Dewan Pengawas Syariah	006	
Pejabat Eksekutif	007	Pejabat yang bertanggungjawab langsung kepada anggota Direksi atau mempunyai pengaruh yang signifikan terhadap kebijakan dan/atau operasional Bank.
Pejabat non Pejabat Eksekutif	018	Semua pejabat selain Pejabat Eksekutif.
Pegawai non Pejabat	019	Semua pegawai selain Pejabat Eksekutif dan Pejabat non Pejabat Eksekutif.
Tenaga Ahli dan Konsultan	010	

b. Keterangan Jabatan

Diisi nama jabatan pelaku *Fraud* di Bank (menggunakan format bebas).

Contoh: *Account Officer* (AO) Kredit, *Group Head* Kredit.

2. Pada saat *Fraud* diketahui

a. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi jabatan

Jabatan	Sandi	Keterangan
Direktur Utama	001	
Direktur	002	
Direktur Kepatuhan	003	Direktur yang membawahkan fungsi kepatuhan.
Komisaris Utama	004	
Komisaris	005	
Dewan Pengawas Syariah	006	
Pejabat Eksekutif	007	Pejabat yang bertanggungjawab langsung kepada anggota Direksi atau mempunyai pengaruh yang signifikan terhadap kebijakan dan/atau operasional Bank.
Pejabat non Pejabat Eksekutif	018	Semua pejabat selain Pejabat Eksekutif.
Pegawai non Pejabat	019	Semua pegawai selain Pejabat Eksekutif dan Pejabat non Pejabat Eksekutif.
Tenaga Ahli dan Konsultan	010	
Sudah tidak bekerja di Bank:		
Pensiun Karir	041	
Pensiun Dini	042	

Diberhentikan	043	
Berhenti atas Keinginan Sendiri	044	
Berakhir Masa Kontrak/Penugasan	045	
Meninggal Dunia	046	

b. Keterangan Jabatan

Diisi nama jabatan pelaku *Fraud* di Bank (menggunakan format bebas).

Contoh: AO Kredit, *Group Head* Kredit.

VI. Keterangan Pelaku (Harus Diisi jika Pelaku *Fraud* Ekstern Diketahui)

Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Jabatan	Sandi
Nasabah	001
Pihak yang berhubungan langsung dengan Bank (antara lain vendor, investor, *supplier*, pejabat negara, atau rekanan)	002
Pihak yang tidak berhubungan langsung dengan Bank	003

VII. Pengenaan Sanksi (Harus Diisi)

Diisi sesuai dengan tindakan untuk penanganan *Fraud* pada Tabel Kejadian *Fraud* (menggunakan format bebas) sesuai dengan ID kejadian *Fraud* yang melibatkan pelaku tersebut.

Ditetapkan di Jakarta
pada tanggal 19 Desember 2019

KETUA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

WIMBOH SANTOSO

LAMPIRAN III

PERATURAN OTORITAS JASA KEUANGAN
NOMOR 39 /POJK.03/2019
TENTANG PENERAPAN STRATEGI ANTI *FRAUD* BAGI BANK UMUM

LAPORAN *FRAUD* BERDAMPAK SIGNIFIKAN

Fraud yang dilaporkan melalui laporan ini merupakan kejadian *Fraud* yang berdampak signifikan berdasarkan kriteria signifikan dalam pedoman penerapan strategi anti *Fraud* Bank.

A. Tabel Kejadian *Fraud*

Kejadian *Fraud* Menurut Pelaku (I)	ID Kejadian *Fraud* (II)	Jenis *Fraud* (III)		Aktivitas Terkait *Fraud* (IV)	Deskripsi *Fraud* /Modus Operandi (V)	Lokasi *Fraud* (VI)		Divisi/Unit Kerja Terjadinya *Fraud* (VII)	Waktu (VIII)			Jumlah Kerugian Potensial (IX)	Tindak Lanjut Bank (X)
									Fraud Terjadi		*Fraud* Diketahui		
		Jenis *Fraud*	Keterangan Jenis *Fraud*			Lokasi *Fraud*	Keterangan Lokasi *Fraud*		Awal	Akhir			
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*

B. Tabel Pelaku *Fraud*

ID Kejadian Fraud (I)	Intern/ Ekstern (II)	Identitas Pelaku (III)								Jabatan Pelaku (IV)				Keterangan Pelaku (V)
		Nama	Jenis Identitas	Nomor Identitas	Jenis Kelamin	Alamat Identitas	Alamat Domisili	Tempat Lahir	Tanggal Lahir	Pada Saat *Fraud* Terjadi	Keterangan Jabatan	Pada Saat *Fraud* Diketahui	Keterangan Jabatan	
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*

PEDOMAN PENGISIAN LAPORAN *FRAUD* BERDAMPAK SIGNIFIKAN

A. Tabel Kejadian *Fraud*

I. Kejadian *Fraud* Menurut Pelaku (Harus Diisi)

Diisi karakter sebanyak 2 (dua) digit berupa huruf kapital sesuai dengan sandi sebagai berikut:

Kejadian *Fraud* Menurut Pelaku	Sandi
Kejadian *Fraud* dengan pelaku intern	AS
Kejadian *Fraud* dengan pelaku ekstern	BS
Kejadian *Fraud* dengan pelaku intern dan ekstern	CS

II. ID Kejadian *Fraud* (Harus Diisi)

Diisi karakter sebanyak 6 (enam) digit sesuai dengan urutan kejadian *Fraud* dengan 2 (dua) digit pertama diawali sandi kejadian *Fraud* menurut pelaku yang mencerminkan bahwa kejadian tersebut merupakan kejadian *Fraud* berdampak signifikan dengan melibatkan pelaku intern, pelaku ekstern, atau pelaku intern dan ekstern. Selanjutnya digit ke-3 sampai dengan digit ke-6 diisi dengan angka sesuai urutan kejadian *Fraud*.

Contoh:

Kejadian *Fraud* berdampak signifikan dengan pelaku intern untuk nomor urut 1 dituliskan AS0001.

III. Jenis *Fraud* (Harus Diisi)

1. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Jenis *Fraud*	Sandi
Kecurangan	201
Penipuan	202
Penggelapan aset	203
Pembocoran informasi	204
Tindak pidana perbankan	205
Tindakan lain	209

2. Keterangan Jenis *Fraud*:
   Harus diisi jika memilih "Tindakan lain yang dapat dipersamakan dengan *Fraud*" pada kolom "Jenis *Fraud*" (menggunakan format bebas).

IV. Aktivitas Terkait *Fraud* (Harus Diisi)
Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Aktivitas Terkait *Fraud*	Sandi
Pendanaan	301
Perkreditan/pembiayaan	302
Penggunaan identitas dan data orang, pihak lain, atau nasabah	303
Pengelolaan aset	304
Penggunaan siber	305
Penyajian laporan keuangan	306
Aktivitas lain	309

Penjelasan aktivitas terkait *Fraud* berdasarkan kegiatan operasional Bank yaitu sebagai berikut:

1. Pendanaan
   Fraud yang terjadi pada aktivitas penghimpunan Dana Pihak Ketiga (DPK) yang dilakukan Bank.
   Contoh:
   a. Penghimpunan DPK yang tidak dicatat dalam pembukuan Bank atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu Bank.
      Penjelasan:
      Ketidaksesuaian atau rekayasa pencatatan dana masuk dari nasabah yang berupa tabungan, giro, deposito, dan bentuk simpanan lain yang dipersamakan dengan tabungan, giro, atau deposito, yang dilakukan oleh pegawai atau pejabat Bank sehingga menimbulkan selisih pencatatan dalam pembukuan Bank.
   b. Penarikan atau pencairan DPK yang dilakukan bukan oleh pemilik atau kuasanya atau oleh pegawai Bank yang tidak

dicatat dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu Bank.

Penjelasan:

Penarikan atau pencairan DPK nasabah untuk kepentingan pribadi Direksi, Dewan Komisaris, pegawai, dan/atau pihak lain tanpa seizin dan sepengetahuan nasabah. Penarikan atau pencairan DPK dapat menggunakan antara lain bilyet deposito palsu, bilyet giro palsu, dan surat kuasa palsu.

c. Penyetoran atau pemindahbukuan tabungan, giro, atau deposito yang tidak dicatat dengan benar dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu Bank.

d. Penyetoran atau pemindahbukuan tabungan, giro, atau deposito yang dicatat dalam pembukuan Bank tanpa disertai aliran dana.

e. Pemberian pelayanan terhadap nasabah prima di luar prosedur atau ketentuan yang telah ditetapkan oleh Bank yang menimbulkan kerugian bagi Bank.

2. Perkreditan/Pembiayaan

Fraud yang terjadi pada aktivitas pemberian kredit/pembiayaan yang dilakukan oleh Bank, dimulai dari pengajuan kredit/pembiayaan hingga pelunasan kredit/pembiayaan oleh debitur.

Contoh:

a. Debitur fiktif

Penjelasan:

Pemberian kredit/pembiayaan kepada satu atau lebih debitur dengan menggunakan identitas palsu atau identitas pihak lain.

b. Debitur topengan

Penjelasan:

Pemberian kredit/pembiayaan kepada debitur dengan menggunakan identitas asli dari debitur yang bersangkutan namun dananya digunakan oleh pihak lain.

c. Rekayasa atau manipulasi dokumen atau informasi kredit/pembiayaan

Penjelasan:

Rekayasa dokumen atau infomasi oleh debitur dan/atau pihak Bank untuk memenuhi persyaratan dan kelayakan pemberian kredit/pembiayaan atau restrukturisasi kredit/pembiayaan antara lain:

1) rekayasa kemampuan dan prospek usaha debitur;
2) rekayasa laporan keuangan debitur;
3) *overvalued/undervalued* penilaian agunan atau penggunaan agunan fiktif;
4) rekayasa analisa kredit/pembiayaan oleh pihak Bank;
5) ketiadaan dokumen permohonan, analisis, keputusan, dan/atau perjanjian kredit/pembiayaan; dan
6) dokumen persyaratan kredit/pembiayaan yang tidak benar.

d. Rekayasa atau ketidaksesuaian pencatatan angsuran kredit/pembiayaan dalam pembukuan Bank

Penjelasan:

Tidak mencatat angsuran kredit/pembiayaan, ketidaksesuaian pencatatan nominal angsuran kredit/pembiayaan dengan dana yang diterima, atau pencatatan angsuran kredit/pembiayaan yang tidak disertai dengan aliran dana.

e. Ketidaksesuaian penggunaan kredit/pembiayaan dengan tujuan atau kebutuhan

Penjelasan:

Penggunaan dana kredit/pembiayaan yang dicairkan tidak sesuai dengan tujuan awal pengajuan kredit/pembiayaan atau kebutuhan kredit/pembiayaan yang sesungguhnya.

f. Pembebanan biaya Bank untuk menjaga kolektibilitas kredit/pembiayaan

Penjelasan:

Direksi, Dewan Komisaris, dan/atau pegawai Bank melakukan pembebanan biaya untuk suatu kegiatan fiktif yang sebenarnya digunakan sebagai setoran angsuran

kredit/pembiayaan untuk menjaga kolektibilitas kredit/pembiayaan.

g. Penghindaran pelanggaran Batas Maksimum Pemberian Kredit (BMPK) atau Batas Maksimum Penyaluran Dana (BMPD)

Penjelasan:

Pemecahan satu fasilitas kredit/pembiayaan menjadi beberapa fasilitas kredit/pembiayaan dan pemberian fasilitas kredit/pembiayaan melalui kelompok usaha atau pihak lain untuk menghindari pelanggaran BMPK/BMPD.

h. Pelampauan dan/atau penyalahgunaan wewenang

Penjelasan:

Pelampauan wewenang berupa pemutusan pemberian kredit dalam jumlah yang melampaui batas kewenangan pejabat/komite kredit/pembiayaan.

Penyalahgunaan wewenang berupa pemutusan pemberian kredit/pembiayaan yang tidak didasarkan pada prinsip kehati-hatian.

i. Gratifikasi, skema *cash back*, atau penyuapan

Penjelasan:

Direksi, Dewan Komisaris, dan/atau pegawai Bank menerima atau meminta fasilitas tambahan dari debitur sebagai imbal jasa pencairan kredit/pembiayaan.

j. Pemberian kredit/pembiayaan yang melanggar prinsip kehati-hatian

Penjelasan:

Pemberian kredit/pembiayaan oleh Bank yang melanggar prinsip kehati-hatian sebagaimana diatur dalam ketentuan peraturan perundang-undangan atau SPO Bank, antara lain:

1) pemberian kredit/pembiayaan yang tidak sesuai dengan prosedur tahapan pemberian kredit/pembiayaan;
2) pencairan kredit/pembiayaan yang dilakukan sebelum memenuhi persyaratan pencairan kredit/pembiayaan; dan
3) pengikatan agunan kredit/pembiayaan yang tidak sesuai dengan ketentuan peraturan perundang-undangan.

k. Pelunasan kredit/pembiayaan dari hasil pencairan kredit/pembiayaan baru yang ditujukan untuk memperbaiki atau menjaga kolektibilitas kredit/pembiayaan.
l. Rekayasa kolektibilitas kredit/pembiayaan;

3. Penggunaan Identitas dan Data Orang, Pihak Lain, atau Nasabah

Fraud yang terjadi dengan cara menggunakan identitas dan data orang, pihak lain, atau nasabah untuk melakukan transaksi perbankan tanpa sepengetahuan dan/atau persetujuan dari orang, pihak lain, atau nasabah.

Contoh:

a. Penyalahgunaan kartu ATM nasabah.
b. Penjualan atau pertukaran data nasabah secara tidak sah antar Bank atau pihak ketiga yang dipekerjakan oleh Bank.

4. Pengelolaan Aset

Fraud yang terjadi pada aktivitas pengelolaan aset Bank, termasuk kas.

Contoh:

a. Penggunaan kas yang ada pada brankas oleh Direksi, Dewan Komisaris, dan/atau pegawai Bank untuk kepentingan pribadi serta tidak dicatat dalam pembukuan Bank.
b. Pencurian kas yang dilakukan dengan memanfaatkan kelemahan perangkat lunak dan/atau perangkat keras pada mesin ATM dan/atau kartu ATM Bank.
c. Penyalahgunaan kendaraan Bank untuk kepentingan pribadi Direksi, Dewan Komisaris, pejabat, dan/atau pegawai Bank.
d. Penjualan AYDA oleh pegawai Bank kepada debitur dengan harga yang tidak wajar untuk memperoleh keuntungan pribadi pegawai.
e. Pegawai tidak melakukan pencatatan atas pembelian atau penjualan aset milik Bank.
f. Penggelembungan (*mark up*) biaya sewa gedung kantor untuk keuntungan pribadi, Direksi, Dewan Komisaris, dan/atau pegawai Bank.

g. Rekayasa setoran dan penarikan rekening penempatan pada bank lain oleh Direksi Bank.

h. Penempatan/Investasi/Penyertaan Dana Bank tidak sesuai dengan SPO Bank yang dilakukan pegawai berkolusi dengan pihak lain.

i. Penarikan uang kas tanpa transaksi yang mendasari dan tidak dicatat pada pos yang seharusnya.

5. Penggunaan Siber

Fraud yang terjadi dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik untuk mengelabui Bank, nasabah, orang, atau pihak lain agar memperoleh informasi dan data pribadi nasabah.

Contoh:

a. Peretasan (*Hacking*) atau Pembobolan (*Cracking*)

Penjelasan:

Penggunaan atau pencarian akses secara tidak sah ke dalam data Bank atau nasabah dalam sistem perbankan diantaranya melalui perbankan elektronik.

b. Pengelabuan (*Phising*)

Penjelasan:

Tindakan memperoleh informasi pribadi nasabah dengan menyamar sebagai pihak yang berwenang melalui surel untuk mengarahkan nasabah agar mengakses tautan tertentu dalam surel tersebut.

c. Penyalinan Informasi (*Skimming*)

Penjelasan:

Penggunaan mesin atau kamera yang dipasang pada mesin ATM dengan tujuan untuk mencuri informasi kartu dan nomor PIN nasabah ketika nasabah menggunakan mesin ATM.

d. Rekayasa Sosial (*Social Engineering*)

Penjelasan:

Tindakan memperoleh informasi nasabah seperti PIN, nomor kartu, dan/atau informasi lain dengan cara menghubungi nasabah melalui telepon, sms, atau media lain untuk menginformasikan pemberian hadiah dan meminta nasabah

untuk menghubungi nomor telepon atau membuka situs web tertentu.

e. Virus, *malware*, atau *ransomwar*

Penjelasan:

Merupakan suatu program yang dirancang dengan tujuan untuk merusak, menyusup, dan/atau mencuri informasi atau data rahasia Bank dan/atau nasabah dalam sistem elektronik Bank.

6. Penyajian Laporan Keuangan

Fraud yang terjadi dalam penyajian laporan keuangan Bank antara lain laporan keuangan tidak disajikan sesuai dengan prinsip akuntansi yang berlaku umum dan/atau tidak sesuai dengan kondisi keuangan yang sebenarnya, termasuk pencatatan yang tidak benar antara lain penggelembungan (*mark up*) biaya dan biaya fiktif dalam pembukuan atau dalam laporan Bank.

Contoh:

Rekayasa atau manipulasi laporan keuangan Bank (*window dressing*).

Penjelasan:

Rekayasa laporan keuangan agar kinerja Bank terlihat lebih baik dari kondisi keuangan yang sebenarnya atau berhasil mencapai target yang telah ditetapkan.

7. Aktivitas Lain

Fraud yang terjadi pada setiap aspek aktivitas Bank selain kategori yang telah dikelompokkan di atas (angka 1 sampai dengan angka 6).

V. Deskripsi *Fraud* atau Modus Operandi (Harus Diisi)

Diisi dengan deskripsi mengenai *Fraud* yang terjadi paling banyak 4000 karakter (menggunakan format bebas), serta dilengkapi dengan mengunggah *file* PDF yang memuat rincian deskripsi. Dalam hal tidak terdapat rincian deskripsi, *file* PDF tetap harus diunggah.

VI. Lokasi *Fraud* (Harus Diisi)

1. Diisi karakter sebanyak 2 (dua) digit sesuai dengan sandi lokasi *Fraud* berdasarkan jenis kantor bank umum konvensional dan bank umum syariah sebagai berikut:

Lokasi	Sandi
Kantor Pusat Operasional	01
Kantor Pusat Non Operasional	02
Kantor Cabang dari bank yang berkedudukan di Luar Negeri	03
Unit Usaha Syariah Bank Umum	04
Kantor Wilayah Bank Umum	05
Kantor Cabang (Dalam Negeri)	06
Kantor Cabang (Luar Negeri)	07
Kantor Cabang Pembantu dari bank yang berkedudukan di Luar Negeri	08
Kantor Cabang Pembantu (Dalam Negeri)	09
Kantor Cabang Pembantu (Luar Negeri)	10
Kantor Kas	11
Kantor Fungsional	12
Payment Point	13
Kas Keliling/Kas Mobil/Kas Terapung	14
Kantor di bawah KCP dari bank yang berkedudukan di Luar Negeri yang Tidak Termasuk 11,12,13,14	15
Kantor Perwakilan Bank Umum di Luar Negeri	16
ATM/CDM/CRM	17
Kantor Pusat Operasional Bank Umum Syariah	51
Kantor Pusat Non Operasional Bank Umum Syariah	52
Kantor Wilayah Bank Umum Syariah	53
Kantor Cabang (Dalam Negeri) Bank Umum Syariah	54
Kantor Cabang (Luar Negeri) Bank Umum Syariah	55
Kantor Cabang Pembantu (Dalam Negeri) Bank Umum Syariah	56

Kantor Cabang Pembantu (Luar Negeri) Bank Umum Syariah	57
Kantor Kas Bank Umum Syariah	58
Kantor Fungsional Bank Umum Syariah	59
Payment Point Bank Umum Syariah	60
Kas Keliling/Kas Mobil/Kas Terapung Bank Umum Syariah	61
Kantor Perwakilan Bank Umum Syariah di Luar Negeri	62
ATM/CDM/CRM Bank Umum Syariah	63
Layanan Syariah Bank Umum	64

Bank umum konvensional yang memiliki unit usaha syariah harus mengisi Unit Usaha Syariah Bank Umum (sandi 04) untuk kejadian *Fraud* yang terjadi di kantor yang melaksanakan fungsi unit usaha syariah tersebut.

2. Keterangan Lokasi *Fraud*

Diisi karakter sebanyak 4 (empat) digit sesuai dengan sandi kota/kabupaten yang tercantum dalam pedoman Sistem Layanan Informasi Keuangan (SLIK) sebagaimana dimaksud dalam ketentuan Otoritas Jasa Keuangan mengenai pelaporan dan permintaan informasi debitur melalui SLIK.

VII. Divisi atau Unit Kerja Terjadinya *Fraud* (Harus Diisi)

Diisi nama divisi atau unit kerja terjadinya *Fraud* atau terkena dampak *Fraud* secara langsung (menggunakan format bebas).

VIII. Waktu (Harus Diisi)

1. *Fraud* Terjadi

a. Awal

Diisi dengan tanggal mulai terjadinya *Fraud* (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD.

b. Akhir

Diisi dengan tanggal selesai terjadinya *Fraud* (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD.

2. *Fraud* Diketahui

Diisi dengan tanggal *Fraud* diketahui Bank (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD.

IX. Jumlah Kerugian Potensial (Harus Diisi)

Diisi dengan digit angka jumlah kerugian yang terjadi dalam satuan penuh dengan mata uang Rupiah.

X. Tindak Lanjut Bank

Diisi dengan penjelasan mengenai tindak lanjut yang telah dilakukan oleh Bank terkait dengan temuan *Fraud* (menggunakan format bebas maksimal 4000 karakter).

B. Tabel Pelaku *Fraud*

Pelaku *Fraud* merupakan pihak yang terlibat dalam kejadian *Fraud*.

I. ID Kejadian *Fraud* (Harus Diisi)

Diisi karakter sebanyak 6 (enam) digit sesuai dengan ID kejadian *Fraud* yang melibatkan pelaku tersebut. ID kejadian *Fraud* pada Tabel Pelaku *Fraud* harus sesuai dengan ID kejadian *Fraud* pada Tabel Kejadian *Fraud*.

Dalam hal terdapat kejadian *Fraud* yang pelakunya belum diketahui, maka ID kejadian *Fraud* tetap wajib diisi dalam Tabel Pelaku *Fraud*.

II. Intern atau Ekstern (Harus Diisi)

Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi pelaku *Fraud*.

Pelaku *Fraud*	Sandi
Intern	001
Ekstern	002

III. Identitas Pelaku (Harus Diisi)

Untuk pelaku *Fraud* ekstern, dalam hal pelaku *Fraud* atas nama perusahaan maka kolom Jenis Kelamin, Tempat Lahir, dan Tanggal lahir tidak perlu diisi.

Untuk pelaku *Fraud* ekstern, dalam hal pelaku *Fraud* tidak diketahui maka kolom Jenis Kelamin, Alamat Identitas, Alamat Domisili, Tempat Lahir, dan Tanggal lahir tidak perlu diisi.

1. Nama (Harus Diisi)

   Diisi dengan nama pelaku *Fraud* tanpa gelar sesuai dengan yang tercantum dalam dokumen identitas.

   Untuk pelaku *Fraud* ekstern, dalam hal nama pelaku *Fraud* tidak diketahui maka kolom tersebut tetap harus diisi (tidak boleh dikosongkan) dan Bank mendefinisikan nama pelaku yang tidak diketahui tersebut. Contoh: *unknown client*.

2. Jenis Identitas (Harus Diisi)

   Diisi dengan karakter sebanyak 3 (tiga) digit sesuai dengan jenis identitas.

Jenis Identitas	Sandi	Keterangan
KTP (Nomor Induk Kependudukan)	001	Pelaku *Fraud* WNI
Paspor (Nomor Paspor)	002	Pelaku *Fraud* WNA
NPWP	003	Pelaku *Fraud* atas nama perusahaan
Tidak Diketahui	009	

3. Nomor Identitas (Harus Diisi)

   Diisi dengan nomor identitas sesuai dengan jenis identitas yang dipilih.

   Nomor identitas untuk jenis identitas yang tidak diketahui menggunakan kode unik yang dibuat oleh Bank.

   Dalam hal nomor identitas mengandung karakter selain huruf dan angka maka karakter tersebut tidak perlu disertakan.

   Contoh:

   Pelaku *Fraud* memiliki nomor NPWP 49.810.734.1-035.000, maka diisi pada kolom Nomor Identitas yaitu 498107341035000.

4. Jenis Kelamin

Diisi karakter sebanyak 1 (satu) digit sesuai dengan sandi jenis kelamin pelaku *Fraud* sebagai berikut:

Jenis Kelamin	Sandi
Laki-laki	L
Perempuan	P

Dalam hal pelaku *Fraud* atas nama perusahaan atau tidak diketahui maka kolom Jenis Kelamin tidak perlu diisi.

5. Alamat Identitas (Harus Diisi jika Pelaku *Fraud* Intern)

Diisi dengan alamat identitas sesuai dengan yang tertera pada dokumen identitas pelaku *Fraud*.

6. Alamat Domisili (Harus Diisi jika Pelaku *Fraud* Intern)

Diisi alamat domisili dengan informasi (menggunakan format bebas, kecuali untuk kota atau kabupaten, provinsi, dan negara mengacu pada lampiran SLIK sebagaimana dimaksud dalam ketentuan Otoritas Jasa Keuangan mengenai pelaporan dan permintaan informasi debitur melalui SLIK):

a. Jalan/blok;
b. Nomor rumah;
c. RT/RW;
d. Kelurahan;
e. Kecamatan;
f. Kota/Kabupaten;
g. Provinsi;
h. Negara; dan
i. Kode Pos.

7. Tempat Lahir (Harus Diisi jika Pelaku *Fraud* Intern)

Diisi dengan tempat kelahiran pelaku *Fraud* sesuai yang tercantum dalam dokumen identitas.

8. Tanggal Lahir (Harus Diisi jika Pelaku *Fraud* Intern)

Tanggal lahir diisi (tahun/bulan/tanggal) dengan format pengisian YYYYMMDD sesuai dengan tanggal yang tercantum pada dokumen identitas.

Contoh:

Tanggal lahir 15 Desember 1975, ditulis 19751215.

IV. Jabatan Pelaku (Harus Diisi jika Pelaku *Fraud* Intern)

1. Pada saat *Fraud* terjadi

a. Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi jabatan

Jabatan	Sandi	Keterangan
Direktur Utama	001	
Direktur	002	
Direktur Kepatuhan	003	Direktur yang membawahkan fungsi kepatuhan.
Komisaris Utama	004	
Komisaris	005	
Dewan Pengawas Syariah	006	
Pejabat Eksekutif	007	Pejabat yang bertanggungjawab langsung kepada anggota Direksi atau mempunyai pengaruh yang signifikan terhadap kebijakan dan/atau operasional Bank.
Pejabat non Pejabat Eksekutif	018	Semua pejabat selain Pejabat Eksekutif.
Pegawai non Pejabat	019	Semua pegawai selain Pejabat Eksekutif dan Pejabat non Pejabat Eksekutif.
Tenaga Ahli dan Konsultan	010	

b. Keterangan Jabatan

Diisi nama jabatan pelaku *Fraud* di Bank (menggunakan format bebas).

Contoh: AO Kredit, *Group Head* Kredit.

2. Pada saat *Fraud* diketahui

a. Diisi karakter sebanyak 3 digit (tiga) sesuai dengan sandi jabatan

Jabatan	Sandi	Keterangan
Direktur Utama	001	
Direktur	002	
Direktur Kepatuhan	003	Direktur yang membawahkan fungsi kepatuhan.
Komisaris Utama	004	
Komisaris	005	
Dewan Pengawas Syariah	006	
Pejabat Eksekutif	007	Pejabat yang bertanggungjawab langsung kepada anggota Direksi atau mempunyai pengaruh yang signifikan terhadap kebijakan dan/atau operasional Bank.
Pejabat non Pejabat Eksekutif	018	Semua pejabat selain Pejabat Eksekutif.
Pegawai non Pejabat	019	Semua pegawai selain Pejabat Eksekutif dan Pejabat non Pejabat Eksekutif.
Tenaga Ahli dan Konsultan	010	
Sudah tidak bekerja di Bank:		

Pensiun Karir	041	
Pensiun Dini	042	
Diberhentikan	043	
Berhenti atas Keinginan Sendiri	044	
Berakhir Masa Kontrak/Penugasan	045	
Meninggal Dunia	046	

b. Keterangan Jabatan (Harus Diisi jika Pelaku *Fraud* Intern)
Diisi nama jabatan pelaku *Fraud* di Bank (menggunakan format bebas).
Contoh: AO Kredit, *Group Head* Kredit.

V. Keterangan Pelaku (Harus Diisi jika Pelaku *Fraud* Ekstern Diketahui)
Diisi karakter sebanyak 3 (tiga) digit sesuai dengan sandi sebagai berikut:

Jabatan	Sandi
Nasabah	001
Pihak yang berhubungan langsung dengan Bank (antara lain vendor, investor, *supplier*, pejabat negara, atau rekanan)	002
Pihak yang tidak berhubungan langsung dengan Bank	003

Ditetapkan di Jakarta
pada tanggal 19 Desember 2019

KETUA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

WIMBOH SANTOSO