FRAUD, MENDETEKSI DAN MENGATASINYA (PENDEKATAN AKUNTANSI FORENSIK & AUDIT INVESTIGATIF)

Johan Arifin, SE, M.Si, Ph.D, CfrA

Penerbit EKONISIA
Fakultas Bisnis dan Ekonomika
Universitas Islam Indonesia
Yogyakarta

Fraud, Mendeteksi dan Mengatasinya (Pendekatan Akuntansi Forensik & Audit Investigatif)

Oleh:
Johan Arifin, SE, M.Si, Ph.D, CfrA

Edisi Pertama
Cetakan Pertama, Oktober 2020

Penerbit EKONISIA
Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia
Condongcatur, Depok, Sleman, Yogyakarta 55283
Telp (0274) 886478, 881546 Fax. (0274) 882589

ISBN: 978-602-6617-56-9

KATA PENGANTAR

Dalam kesempatan ini, penulis menyampaikan puji syukur atas selesainya penulisan buku ini. Allah SWT merupakan satu-satunya Dzat yang menjadi luapan ungkapan syukur atas selesainya buku ini, karena berkat Dia-lah yang telah memberi kesehatan, kesempatan, dan motivasi penulis untuk menyelesaikan buku ini.

Fraud dan audit investigatif saat ini sedang menjadi salah satu bidang kajian yang marak dibicarakan orang khususnya di Indonesia. Hal ini karena perkembangan teknologi informasi yang begitu pesat membuat kejahatan fraud di bidang teknologi informasi juga berkembang dengan pesat baik jenis maupun metodenya. Buku ini adalah buku pengantar yang berisi berbagai konsep dasar terkait dengan fraud yang antara lain mencakup pengertian, pencegahan, pendeteksian serta penanggulangannya, dan juga dibahas sekilas tentang akuntansi forensik serta audit investigasi dalam upaya pencegahan dan pendeteksian fraud. Penulis berharap, terbitnya buku ini dapat membantu para mahasiswa maupun para pembaca dari berbagai lapisan masyarakat yang ingin mempelajari dan memperluas pengetahuannya dalam bidang akuntansi forensik. Untuk mencapai keinginan tersebut, penulis mencoba melakukan perpaduan dan kajian pemikiran para ahli yang terdiri dari berbagai kalangan akademisi maupun praktisi dalam bidang ukuntansi dan auditing forensik.

Buku ini terdiri atas 9 Bab yang mencakup pembahasan materi utama yang berisi kajian tentang fraud, jenis-jenis fraud, pencegahan, pendeteksian, serta antisipasinya. Selain itu, pada bagian akhir dipaparkan juga tentang akuntansi forensik dan auditing investigasi sebagai alternatif untuk mendeteksi dan mengatasi terjadinya fraud baik di lembaga sektor publik maupun sektor bisnis. Penulis mengucapkan terimakasih kepada Tri Enastutu (istri), serta anak-anak yaitu Fahrian Ahwaz Safa Muhammad, dan Farah Muna Safa Taqiya yang telah memberikan dukungan penuh guna terselesainya buku ini. Tak lupa, dalam kesempatan ini penulis juga mengucapkan banyak terimakasih kepada semua pihak yang telah memberikan bantuan dan motivasi kepada penulis untuk menyelesaikan buku ini terutama Fakultas Bisnis dan Ekonomika yang telah menyelenggarakan Hibah Program Produktivitas Dosen, Program Studi Akuntansi, dan Program Magister Akuntansi Universitas Islam Indonesia serta semua pihak yang tidak bisa kami sebut satu persatu.

Akhirnya kami sangat menunggu masukan, saran, tanggapan, dan kritik dari para pembaca. Buku ini tidak terlepas dari kekurangan, namun kami tetap berharap buku ini bermanfaat untuk pengembangan bidang akuntansi forensik khususnya di Indonesia.

Yogyakarta, 2020
Penulis,

Johan Arifin, SE, M.Si, Ph.D, CFrA

Fraud, Mendeteksi dan Mengatasinya (Pendekatan Akuntansi Forensik & Audit Investigatif)

DAFTAR ISI

BAB 1 FRAUD

Pendahuluan

Dalam suatu organisasi/perusahaan pasti terdapat bagian atau departemen, setiap bagian atau depertemen ini kemungkinan dibagi lagi dalam banyak devisi dan seterusnya hingga unit terkecil. Semakin banyak pembagian level dan variasi unit, maka semakin besar potensi terdapat kecurangan dalam bentuk penyalahgunaan wewenang, penyelewengan prosedur, manipulasi, dan lainnya. Semua jenis kecurangan tersebut sering dikenal dengan istilah *fraud*. Banyak orang mengartikan *fraud* dengan "kecurangan". Hal ini tidak keliru asalkan kecurangan yang dimaksudkan adalah segala tindakan yang terkait dengan aspek pelanggaran hukum atau aturan. Fraud dalam laporan keuangan biasanya berbentuk salah saji atau kelalaian yang disengaja baik dalam jumlah maupun pengungkapan pos-pos dalam pelaporan keuangan untuk menyesatkan pemakai informasi laporan keuangan tersebut. Fraud dapat terungkap, bila ada kerja sama antara beberapa pihak yang terkait dengan entitas, seperti dewan direksi, pihak manajemen, akuntan publik serta internal auditor. Dalam bab ini, akan dilakukan kajian terkait dengan istilah fraud. Hal ini penting supaya kita mengenal lebih jauh makna kata *"fraud"* yang benar serta segala sesuatu yang terkait dengannya. Pada umumnya, kecurangan yang terjadi pada berbagai organisasi atau perusahaan disebabkan oleh lingkungan internal dan lingkungan eksternal. Pengaruh lingkungan internal biasanya berhubungan dengan lemahnya pengendalian internal, lemahnya perilaku etika manajemen atau faktor likuiditas, serta profitabilitas entitas yang bersangkutan. Sedangkan pengaruh lingkungan eksternal biasanya terkait dengan kondisi entitas secara umum, lingkungan bisnis secara umum, maupun pertimbangan hukum dan perundang-undangan.

Pengertian Fraud

Fraud merupakan tindakan ilegal yang dilakukan satu orang atau sekelompok orang secara sengaja atau terencana yang menyebabkan orang atau kelompok tersebut mendapat keuntungan, dan merugikan orang atau kelompok lain. *Fraud* meliputi berbagai tindakan melawan hukum, dan audit investigatif biasanya melakukan pemetaan terhadap *occupational fraud* (*fraud* dalam hubungan kerja) dalam proses investigasinya. Ada juga istilah lain yang sering kali digunakan untuk menggambarkan suatu jenis *fraud* yakni kejahatan kerah putih atau *white-collar crime*. Menurut Burnes *et al.* (2017) *fraud* dapat bedakan ke dalam beberapa perspektif meliputi keterkaitan dengan konflik kepentingan, keterkaitan dengan *asset misappropriation* (pengambilan aset secara ilegal) serta keterkaitan dengan penerimaan dan persediaan.

Dari sisi konfik kepentingan, kita mengenal beberapa jenis *fraud* yang sangat sering kita lihat dalam praktik organisasi pemerintahan maupun bisnis, seperti:

1. *Bribery* atau penyuapan merupakan tindakan pemberian atau penerimaan sesuatu yang bernilai dengan tujuan untuk mempengaruhi tindakan orang yang menerima.
2. *Kickback* merupakan salah satu bentuk penyuapan dimana penjual dengan ikhlas memberikan sebagain hasil penjualanya kembali ke pembeli.
3. *Bid rigging* merupakan skema dimana karyawan membantu sebuah vendor untuk memenangkan suatu kontrak dengan perusahaan.
4. *Illegal gratuities* merupakan pemberian atau hadiah yang merupakan bentuk terselubung dari penyuapan.

Selanjutnya, terkait dengan tindakan asset *misappropriation* atau pengambilan aset secara ilegal terdapat 3 bentuk skema. Dalam klasifikasi ini, pelaku *fraud* memang seorang yang sudah cukup berpengalaman dan sangat lihai. Pada umumnya kecurangan jenis ini dilakukan secara kelompok dengan peralatan dan fasilitas yang sangat lengkap dan dilakukan dengan cara-cara yang rapi. Ketiga jenis skema *fraud* ini meliputi:

1. *Skimming*, yaitu pencurian atau penjarahan uang sebelum uang tersebut secara fisik masuk ke perusahaan atau dicatat didalam pembukuan.
2. *Larceny*, yaitu pencurian atau penjarahan uang dimana uang tersebut secara fisik telah masuk ke perusahaan, hal ini berkaitan erat dengan lemahnya pengendalian internal suatu perusahaan.
3. *Fraudulent disbursement*, yaitu pencurian melalui pengeluaran yang tidak sah.

Lebih lanjut, Albrecht (2012) mengungkapkan jenis-jenis *fraud* yang terkait dengan penerimaan dan persediaan. Jenis *fraud* ini sangat erat kaitannya dengan kegiatan *procurement* atau pengadaan barang dan jasa. Perlu kita ketahui bahwa kecurangan terkait dengan kegiatan *procurement* atau pengadaan barang dan jasa menjadi salah satu jenis *fraud* yang paling populer dan sangat tinggi kejadiannya, khususnya di Indonesia. Hal ini berdasarkan data penanganan perkara yang ditangani oleh Komisi Pemberantasan Korupsi (KPK) sesuai dengan tingkat jabatannya. Jenis-jenis *fraud* ini diantaranya meliputi:

1. *Related–party transaction*, yaitu perjanjian bisnis yang dilakukan oleh kedua belah pihak yang telah memiliki hubungan sebelumnya, sehingga timbul konflik kepentingan.
2. *Sham sales*, yaitu berbagai jenis penjualan palsu.
3. *Bill and hold sales*, yaitu pemesanan atas barang yang masih disimpan oleh pemasok, kecurangan ini terjadi karena pembeli belum siap membeli barang tersebut.
4. *Side agreements*, adalah syarat dan perjanjian penjualan yang dibuat diluar dari ketentuan yang biasanya, hal ini menjadi kecurangan, ketika perjanjian tersebut merusak syarat dan ketentuan atas kontrak yang berjalan sehingga melanggar kriteria pengakuan pendapatan.
5. *Consignment sales*, transaksi dimana salah satu perusahaan menahan dan menjual barang yang dimiliki oleh perusahaan lain.

Lebih jauh lagi, berkaitan dengan praktik-praktik *fraud* dalam aktivitas pengadaan barang dan jasa khususnya terkait dengan permasalahan hutang *(liabilities)*, Allen (2018) mengungkapkan berbagai macam cara yang umum dilakukan oleh pelaku *fraud* untuk memanipulasi hutang, sebagai berikut:

1. *Understating account payable*, yang dapat dilakukan dengan kombinasi dari tidak mencatat pembelian atau mencatat pembelian setelah akhir tahun, melebihkan retur pembelian atau diskon pembelian, dan membuat *liabities* seolah-olah telah dibayar atau dihapus.
2. *Understating accrued liabilities*, tidak melakukan pencatatan atas accrued *liabities* yang seharusnya dilakukan di akhir tahun.
3. *Recognizing unearned revenue (liability) as earned revenue*, perusahaan yang menerima pembayaran dimuka akan melakukan pencatatan atas penerimaan dan mengakui pendapatan daripada mengakui sebagai kewajiban.
4. *Underrecording future obligation*, tindakan menurunkan pencatatan kewajiban berupa garansi atau *service*.
5. *Not recording or underrecording various type of debt*, dapat berupa tindakan tidak mencatat atau merendahkan hutang kepada pihak ketiga, melakukan peminjaman tapi tidak dilakukan pengungkapan, tidak mencatat pinjaman yang terjadi, dan mengakui bahwa hutang yang ada telah dilupakan dan dihapus oleh kreditor.

Selanjutnya, perlu kita ketahui bahwa kata *"fraud"* tidak hanya diartikan secara sempit sebagai kecurangan, sehubungan dengan hal itu, maka ada banyak sinonim yang bisa digunakan untuk mendefinisikan kecurangan. Berikut ini beberapa pengertian *fraud* dari beberapa sumber terutama terkait dengan peraturan hukum di Indonesia, diantaranya meliputi:

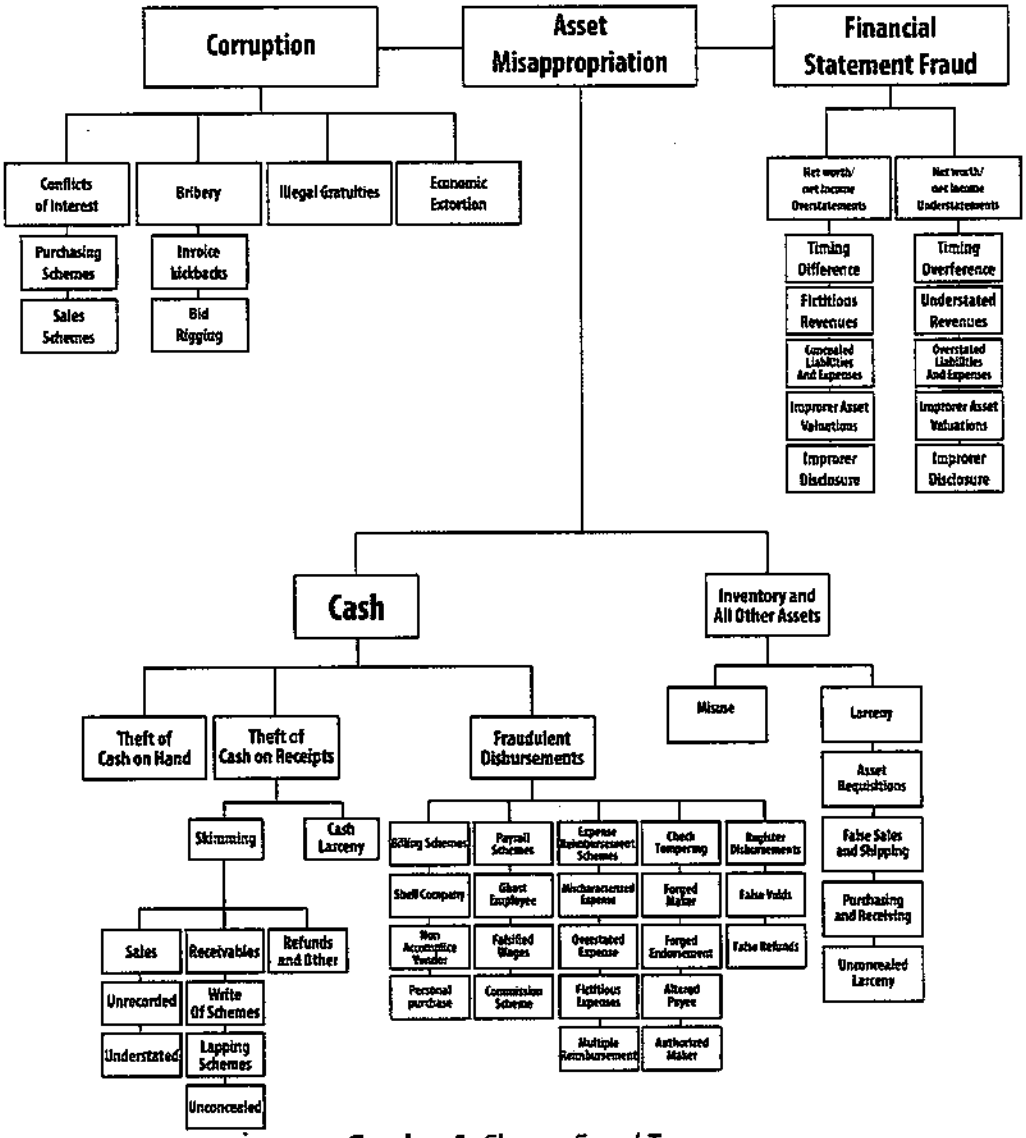
1. Mengutip pernyataan *"Fraud Examiners Manual"* yang mendefinisikan kecurangan sebagai keuntungan yang diperoleh dari seseorang dengan cara menghadirkan sesuatu yang palsu.
2. Menurut Kitab Undang-undang Hukum Pidana (KUHP) ada empat pasal yang mendefinisikan kecurangan dalam dunia keuangan , yaitu:
   a. Pasal 362 Pencurian (definisi KUHP: "mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum").
   b. Pasal 368: Pemerasan dan pengancaman definisi KUHP: "dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seseorang dengan kekerasan atau ancaman kekerasan untuk memberikan sesuatu barang, seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya membuat utang maupun menghapuskan piutang".
   c. Pasal 372: Penggelapan (definisi KUHP: "dengan sengaja melawan hukum memiliki sesuatu barang seluruhnya atau sebagian yang adalah kepunyaan orang lain, tetapi yang ada dalam kekuasaannya bukan karena kejahatan").
   d. Pasal 378: Perbuatan curang (definisi KUHP: "dengan maksud sengaja untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakan orang lain untuk menyerahkan sesuatu barang kepadanya, atau supaya memberi hutang atau maupun menghapuskan piutang").

The *Association of Certified Fraud Examiners* (ACFE) atau Asosiasi Pemeriksa Kecurangan Bersertifikat, merupakan organisasi profesional yang bergerak dibidang pemeriksaan atas kecurangan yang berkedudukan di Amerika Serikat dan mempunyai tujuan untuk memberantas kecurangan. Organisasi ini mengklasifikasikan fraud dalam

beberapa klasifikasi, dan dikenal dengan istilah *"Fraud Tree"* yaitu sistem klasifikasi mengenai hal-hal yang ditimbulkan oleh kecurangan.

1. Penyimpangan atas asset *(Asset Misappropriation)*
   Asset misappropriation meliputi penyalahgunaan/pencurian aset atau harta benda milik perusahaan atau pihak lain. Ini merupakan bentuk *fraud* yang paling mudah dideteksi karena sifatnya *tangible* atau dapat diukur/dihitung. *Fraud* jenis ini telah kita jelaskan pada bagian terdahulu dari bab ini.
2. Pernyataan palsu atau salah pernyataan *(Fraudulent Statement)*
   Fraudulent statement meliputi tindakan yang dilakukan oleh pejabat atau eksekutif suatu perusahaan atau instansi pemerintah untuk menutupi kondisi keuangan yang sebenarnya dengan melakukan rekayasa keuangan *(financial engineering)* dalam penyajian laporan keuangannya untuk memperoleh keuntungan atau mungkin dapat dianalogikan dengan istilah *window dressing.*
3. Korupsi *(Corruption)*
   Jenis fraud ini yang paling sulit dideteksi karena menyangkut kerja sama dengan pihak lain seperti suap dan korupsi, di mana hal ini merupakan jenis yang terbanyak terjadi di negara-negara berkembang yang penegakan hukumnya lemah dan masih kurang kesadaran akan tata kelola yang baik sehingga faktor integritasnya masih dipertanyakan. Fraud jenis ini sering kali tidak dapat dideteksi karena para pihak yang bekerja sama menikmati keuntungan *(simbiosis mutualisme)*. Termasuk didalamnya adalah penyalahgunaan wewenang/konflik kepentingan *(conflict of interest)*, penyuapan *(bribery)*, penerimaan yang tidak sah/illegal *(illegal gratuities)*, dan pemerasan secara ekonomi *(economic extortion)* (Albrecht *et al.*, 2009).

Secara skematis *The Association of Certified Fraud Examiners* (ACFE) menggambarkan *occupational fraud* dalam bentuk fraud tree. Pohon ini menggambarkan cabang-cabang dari fraud dalam hubungan kerja, beserta ranting dan anak rantingnya. Berikut ini adalah gambar *fraud tree*:



Gambar 1. Skema *Fraud Tree*

Fraud Triangle

Penelitian tradisional tentang kecurangan dilakukan pertama kali oleh Donald Cressey pada tahun 1950. Penelitian ini sangat monumental karena setelah itu sering muncul berbagai pertanyaan mengapa kecurangan dapat terjadi. Hasil dari penelitian itu memunculkan faktor-faktor pemicu kecurangan yang saat ini dikenal dengan istilah *"Fraud Triangle"*.

Gambar 2. *Fraud Triangle*

Fraud Triangle tersebut menunjukkan bahwa seseorang melakukan kecurangan didasarkan atas 3 faktor, meliputi:

1. *Pressure* (Tekanan).
   Cressey mempercayai bahwa pelaku kecurangan bermula dari suatu tekanan yang menghimpitnya kehidupannya. Dalam hal ini pelaku mempunyai kebutuhan keuangan yang mendesak, yang tidak diceritakan kepada orang lain, baik pihak keluarga, kolega, maupun orang terdekatnya. Konsep yang penting di sini adalah tekanan yang menghimpit hidupnya dimana pada umumnya terkait dengan kebutuhan akan uang, padahal ia tidak bisa berbagi dengan orang lain. Tekanan *(pressure)* yang dirasakan oleh pelaku kecurangan, yang dipandangnya sebagai kebutuhan keuangan yang tidak dapat diceritakannya kepada orang lain. Berikut ini merupakan faktor-faktor yang dapat mengakibatkan terjadinya tekanan tersebut:
   a. Tingkat persaingan yang kuat atau kejenuhan pasar yang diiringi dengan menurunnya margin keuntungan.
   b. Kerawanan yang tinggi karena perubahan yang cepat misalnya dalam teknologi, keusangan produk atau perubahan tingkat bunga.
   c. Kerugian operasional yang mengancam kebangkrutan.
   d. Arus kas negatif atau ketidakmampuan menghasilkan arus kas dari kegiatan usaha meskipun entitas itu melaporkan laba secara normal maupun pertumbuhan laba.

   Faktor-faktor tersebut secara potensial menjadi pemicu seseorang melakukan tindakan *fraud*. Dan jika kita telaah dengan seksama, kesemua faktor tersebut menjadi penyebab seseorang mengalami kondisi kekurangan finansial. Kondisi inilah yang menjadi pemicu munculnya "tekanan" seseorang untuk melakukan tindakan fraud.

2. *Opportunity* (Kesempatan).
   Peluang *(opportunity)* merupakan suatu peluang untuk melakukan kecurangan seperti yang dipersepsikan pelaku kecurangan. Sifat industry atau kegiatan entitas yang berpeluang melakukan pelaporan keuangan curang dapat melalui:

a. Transaksi dengan pihak terkait yang signifikan yang tidak merupakan bagian normal bisnis entitas yang bersangkutan atau dengan entitas terkait yang tidak diaudit atau yang diaudit KAP lain.
b. Posisi keuangan yang begitu kuat atau kemampuan mendominasi industri atau sektor tertentu yang memungkinkan entitas memaksakan syarat atau kondisi tertentu kepada pemasok atau pelanggan.

Pelaku kecurangan memiliki persepsi bahwa ada peluang baginya untuk melakukan kejahatan tanpa diketahui orang lain. Cressey berpendapat bahwa ada dua komponen dari persepsi tentang peluang. Yang pertama, *general information*, yang merupakan pengetahuan bahwa kedudukan yang mengandung *trust* atau kepercayaan, dapat dilanggar tanpa konsekuensi. Pengetahuan ini dapat diperoleh dari apa yang ia dengar atau yang ia lihat. Kedua adalah *technical skill* atau keahlian/keterampilan yang dibutuhkan untuk melaksanakan kecurangan tersebut.

3. *Razionalization (Pembenaran)*

Rationalization (rasionalisasi) merupakan sikap, karakter, atau sistem nilai yang dipakai (digunakan) oleh pelaku *fraud* dengan cara mencari pembenaran atas segala perbuatan curang yang telah dilakukannya. Ada dua aspek pembenaran dalam *fraud* yang dilakukan oleh pelaku kecurangan, meliputi:

a. Pelaku merasa bahwa kemungkinan untuk mendapatkan keuntungan dari kecurangan lebih besar dari kemungkinan terdeteksinya kecurangan contohnya perusahaan telah mendapatkan keuntungan yang sangat besar dan tidak mengapa jika pelaku mengambil bagian sedikit dari keuntungan tersebut.
b. Pelaku memiliki alasan pembenaran atas perbuatannya, misalnya: pendapatan gaji yang rendah jika dibandingkan dengan beban kerjanya, dan masa kerja pelaku sudah cukup lama dan dia merasa seharusnya berhak mendapatkan lebih dari yang telah dia dapatkan pada saat ini (posisi, gaji, promosi, dan lain-lain).

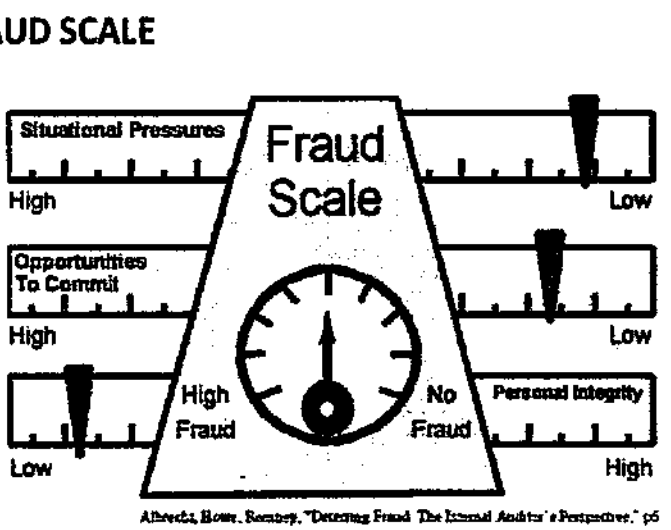
Pembenaran *(Rationalization)* merupakan tindakan pembenaran yang disampaikan untuk melawan hati nurani si pelaku kecurangan. Faktor–faktor yang dapat mengakibatkan terjadinya pembenaran tersebut antara lain berupa:

a. Komunikasi, implementasi atau penerapan nilai–nilai entitas dan standar entika oleh manajemen yang tidak efektif.
b. Keinginan manajemen yang berlebihan untuk meningkatkan harga saham yang tinggi atau mempertahankan tren laba.
c. Adanya kepentingan manajemen untuk menggunakan cara-cara yang tidak benar untuk menekan angka laba bagi kepentingan perpajakan.

Pada umumnya, *fraud triangle* ini dikaitkan dengan pihak internal dan eksternal. Pihak internal merupakan orang dalam perusahaan yang berbuat curang dengan memanfaatkan kekayaan perusahaan untuk kepentingan diri sendiri atau kelompoknya secara ilegal. Sementara itu, faktor eksternal merupakan pihak-pihak vendor/supplier terkait yang menyediakan layanan dan jasa untuk mendukung kegiatan operasional perusahaan. Selain itu pula adanya kolusi bersama antara pihak internal dan pihak eksternal yang sama-sama memiliki kepentingan di dalamnya. Pihak vendor berambisi untuk memenangkan tender, sementara pihak internal (oknum) memanfaatkan vendor dengan cara meloloskannya dalam proses tender. Selanjutnya oknum tersebut mendapatkan imbalan cek palsu yang tidak sesuai dengan yang diterima vendor, atau meminta *kickback* kepada vendor karena sudah lolos dalam proses tender.

Fraud Scale

Menurut teori Fraud Scale, asal muasal penyebab terjadinya *fraud* sama dengan teori Fraud Triangle. Teori Fraud Scale ini merupakan teori lanjutan dari teori sebelumnya yaitu teori Fraud Triangle yang merupakan pengukuran dari teori tersebut. Dalam teori Fraud Scale dikemukakan bahwa kemungkinan tindakan penipuan dapat dinilai dengan mengevaluasi kekuatan tekanan, kesempatan dan integritas pribadi. Pada tekanan yang tinggi, kesempatan besar serta integritas pribadi yang rendah dapat mengakibatkan resiko terjadinya *fraud* tinggi. Sebaliknya tekanan yang rendah, kesempatan kecil, dan integritas pribadi tinggi menyebabkan resiko terjadinya *fraud* yang rendah.



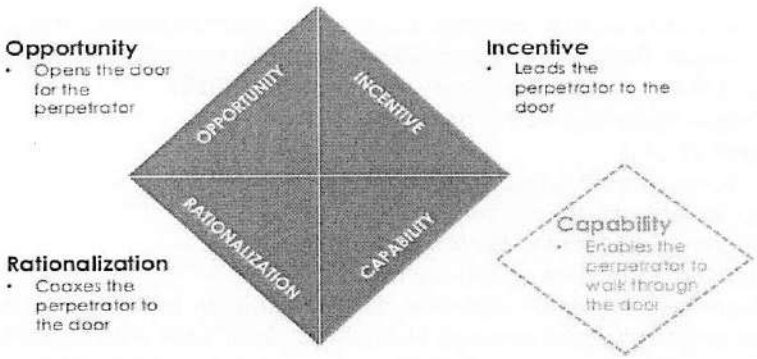
Gambar 3. Fraud Scale

Teori ini mempunyai tujuan untuk mengukur kemungkinan terjadinya pelanggaran etika, kepercayaan dan tanggung jawab. Teori ini berlaku untuk berbagai jenis pelanggaran, salah satunya pelanggaran yang mengarah kepada penipuan laporan keuangan. Sumber tekanan menurut teori ini adalah perkiraan penjualan dan laba manajemen.

Fraud Diamond

Fraud diamond merupakan sebuah pandangan baru tentang fenomena *fraud* yang dikemukakan oleh Wolfe dan Hermanson (2004). *Fraud Diamond* merupakan suatu bentuk penyempurnaan dari teori *Fraud Triangle* oleh Cressey (1953). Dalam teori *Fraud Diamond* ditambahkan satu elemen kualitatif yang diyakini memiliki pengaruh signifikan terhadap *fraud* yaitu *"capability"*.

Pada awalnya Cressey melakukan penelitian terhadap 113 orang yang melakukan pelanggaran hukum terkait dengan penggelapan uang di perusahaan. Berdasarkan hasil penelitian tersebut bahwa alasan yang mendorong seseorang melakukan *fraud* ada tiga macam yang tergabung dalam *Fraud Triangle* yang sudah dijelaskan pada bagian sebelumnya dalam bab ini. Akan tetapi, seiring dengan perkembangan zaman, ditemukanlah satu faktor potensial lagi yang merupakan alasan seseorang melakukan aktivitas kecurangan.



Gambar 4. Fraud Diamond

Insentif atau Tekanan (Pressure)

Seperti telah dijelaskan pada bagian sebelumnya. Bahwa insentif *(pressure)* merupakan sesuatu yang mendorong orang melakukan kecurangan dapat disebabkan oleh tuntutan gaya hidup, ketidakberdayaan dalam soal keuangan, perilaku gambling, mencoba-coba untuk mengalahkan sistem, dan ketidakpuasan kerja. Pada dasarnya motif (tekanan) ini sesungguhnya mempunyai dua bentuk meliputi:

a. Bentuk nyata *(direct)* ini adalah kondisi kehidupan nyata yang dihadapi oleh pelaku seperti kebiasaan sering berjudi, *party/clubbing*, atau persoalan keuangan.
b. Berikutnya adalah bentuk Persepsi *(indirect)* yang merupakan opini yang dibangun oleh pelaku yang mendorong untuk melakukan kecurangan seperti *executive need.*

Dalam SAS No. 99, terdapat empat jenis kondisi yang umum terjadi pada tekanan yang dapat mengakibatkan keempat kondisi tersebut yaitu: (1) *financial stability*, (2) *external pressure*, (3) personal *financial need*, dan (4) *financial targets.*

Kesempatan (Opportunity)

Sementara itu, seperti telah dijelaskan pada bagian sebelumnya bahwa kesempatan merupakan peluang yang menyebabkan pelaku secara leluasa dapat menjalankan aksinya yang disebabkan oleh pengendalian internal yang lemah, ketidakdisplinan, kelemahan dalam mengakses informasi, tidak ada mekanisme audit serta sikap yang apatis. Hal yang perlu digarisbawahi adalah tentang "pengendalian internal". Pengendalian internal yang tidak baik (tidak kuat) akan memberikan peluang kepada orang-orang untuk melakukan kecurangan. Sementara itu, SAS No. 99 menyebutkan bahwa peluang/kesempatan pada *financial statement fraud* dapat terjadi pada tiga kategori tersebut meliputi *nature of industry, ineffective monitoring, dan organizational structure.*

Rasionalisasi (Rationalization)

Rasionalisasi merupakan elemen yang sangat penting dalam terjadinya fraud, dimana pelaku selalu mencari pembenaran atas perbuatannya. Sikap atau karakter yang dimiliki pelaku fraud, akan menentukan rasionalisasi atas pembenaran kecurangan yang dilakukan, contohnya bagi mereka yang umumnya tidak jujur, mungkin lebih mudah untuk merasionalisasi penipuan.

Kemampuan (Capability)

Dalam kenyataannya ternyata ada satu faktor lain yang perlu dipertimbangkan, yaitu Individual capability. Individual capability merupakan sifat dan kemampuan pribadi

seseorang yang mempunyai peranan besar yang memungkinkan melakukan suatu tindak kecurangan. Pada elemen *Individual Capability* terdapat beberapa komponen kemampuan untuk menciptakan *fraud* yaitu (Vousinas, 2019):

1. posisi/fungsi seseorang dalam perusahaan,
2. kecerdasan *(brain),*
3. tingkat kepercayaan diri/ego *(confident/ego),*
4. kemampuan pemaksaan *(coercion skills),*
5. kebohongan yang efektif *(effective lying),* dan
6. kekebalan terhadap stres *(immunity to stress).*

Dalam *fraud diamond,* sifat-sifat dan kemampuan individu memainkan peran utama dalam terjadinya *fraud.* Berbagai kecurangan besar tidak akan terjadi tanpa orang-orang yang memiliki kemampaun individu yang tinggi *(capability).* Walaupun peluang membuka jalan untuk melakukan tindakan fraud serta insentif dan rasionalisasi dapat menarik orang ke arah itu, akan tetapi seseorang harus memiliki kemampuan untuk melihat celah melakukan fraud sebagai kesempatan dan untuk mengambil keuntungan dari itu, yang mana tidak hanya sekali, tetapi secara terus menerus. Dengan demikian, *fraud* terjadi karena adanya kesempatan untuk melakukannya, tekanan dan rasionalisasi yang membuat orang mau melakukannya dengan kemampuan individu yang dimiliki.

Pada intinya *fraud diamond* adalah alasan seseorang melakukan *fraud* karena adanya kesempatan, tekanan dan rasionalitas yang mana ketiga alasan tersebut dapat terjadi jika seseorang memiliki kemampuan *(capability). Fraud Diamond* ini yang dapat menjadi alasan seseorang melakukan kecurangan terhadap laporan keuangan *(fianancial statement).*

Fraud Pentagon

Dalam perkembangannya muncul teori baru yang mengupas lebih mendalam mengenai faktor-faktor pemicu *fraud* yaitu teori **Fraud Pentagon** (Crowe's fraud pentagon theory). Teori ini dikemukakan oleh Crowe Howarth pada tahun 2011. Teori fraud pentagon merupakan perluasan dari teori *fraud triangle* yang sebelumnya dikemukakan oleh Cressey (Bawakes *et al.* 2018). Dalam teori ini Howarth menambahkan dua elemen *fraud* lainnya yaitu *kompetensi* dan *arogansi (competence and arrogance).* Kondisi perusahaan yang kini semakin berkembang dan kompleks dibanding dulu, serta para pelaku *fraud* yang kini lebih cerdik dan mampu mengakses berbagai informasi perusahaan menyebabkan teori *fraud* perlu dikembangkan dari *fraud triangle* menjadi *fraud pentagon.* Lima elemen dalam *fraud pentagon* meliputi *pressure, opportunity, rationalization, competence/capability, and arrogance.*

Gambar 5. Fraud Pentagon

Dalam *fraud pentagon* terdapat penambahan dua elemen lain selain yang termasuk dalam *fraud triangle* yaitu *"capability"* (kemampuan) dan *"arrogance"* (superioritas). Dalam kenyataannya ternyata ada satu faktor lain yang perlu dipertimbangkan, yaitu *individual capability. Individual capability* adalah sifat dan kemampuan pribadi seseorang yang mempunyai peranan besar yang memungkinkan melakukan suatu tindak kecurangan. Sedangkan *"arrogance"* atau sikap superioritas dan keserakahan dalam sebagian dirinya yang menganggap bahwa kebijakan dan prosedur perusahaan sederhananya tidak berlaku secara pribadi. Dengan sifat seperti ini, seseorang dapat melakukan kecurangan dengan mudah karena merasa/menganggap dirinya paling unggul diantara yang lain dan menganggap kebijakan organisasi tidak berlaku untuknya.

Korupsi

Kata korupsi sebenarnya berasal dari bahasa latin *"corruptio"* atau *"corruptus"* yang mempunyai arti busuk, rusak, menggoyahkan, memutarbalik, dan menyogok. Menurut para ahli bahasa, *corruptio* berasal dari kata kerja *corrumpere*, yaitu suatu kata dari Bahasa Latin yang lebih tua. Kata tersebut selanjutnya menurunkan istilah *"corruption"* atau *"corrups"* (Inggris), *corruption* (Perancis), *corruptie/korruptie* (Belanda) dan korupsi (Indonesia).

Secara harfiah korupsi merupakan sesuatu yang jelek, jahat, dan bersifat merusak. Apabila membicarakan tentang korupsi, memang akan menemukan kenyataan semacam itu karena korupsi menyangkut segi-segi moral, sifat keadaan yang busuk, jabatan karena pemberian, faktor ekonomi dan politik, serta penempatan keluarga atau golongan ke dalam kedinasan di bawah kekuasaan jabatannya. Dengan demikian, secara harfiah dapat ditarik kesimpulan bahwa sesungguhnya istilah korupsi memiliki arti yang sangat luas. Dalam ilmu politik, korupsi secara umum didefinisikan sebagai penyalahgunaan jabatan dan administrasi, ekonomi atau politik, baik yang disebabkan oleh diri sendiri maupun orang lain, yang ditujukan untuk memperoleh keuntungan pribadi, sehingga menimbulkan kerugian bagi masyarakat umum, pemerintah, perusahaan, atau pribadi lainnya.

Sementara itu, pengertian lain mengenai korupsi adalah tindakan seseorang yang menyalahgunakan kepercayaan dalam suatu masalah atau organisasi untuk mendapatkan keuntungan pribadi. Tindakan korupsi ini terjadi karena beberapa faktor yang terjadi di kalangan masyarakat. Untuk lebih memperjelas pemahaman tentang arti kata korupsi, berikut ini dijelaskan beberapa definisi korupsi dalam undang-undang Indonesia, antara lain meliputi:

1. Setiap orang yang secara melawan hukum melakukan perbuatan memperkaya diri sendiri atau orang lain atau suatu korporasi yang dapat merugikan keuangan negara atau perekonomian negara (pasal 2 Nomor 31 Tahun 1999).
2. Setiap orang yang dengan tujuan menguntungkan diri sendiri atau orang lain atau suatu korporasi, menyalahgunakan kewenangan, kesempatan atau sarana yang ada padanya karena jabatan atau kedudukan yang dapat merugikan keuangan negara atau perekonomian negara (pasal 3 Nomor 31 Tahun 1999).
3. Makna korupsi pada tipe ketiga ini tertuang pada beberapa pasal Undang-Undang Nomor 20 Tahun 2001, yaitu:
   a. Memberi atau menjanjikan sesuatu kepada pegawai negeri atau penyelenggara negara dengan maksud supaya pegawai negeri atau penyelenggara negara tersebut berbuat atau tidak berbuat sesuatu dalam jabatannya, yang bertentangan dengan kewajibannya; atau memberi sesuatu kepada pegawai

negeri atau penyelenggara negara karena atau berhubungan dengan sesuatu yang bertentangan dengan kewajiban, dilakukan atau tidak dilakukan dalam jabatannya (pasal 5 ayat 1).

b. Memberi atau menjanjikan sesuatu kepada hakim dengan maksud untuk mempengaruhi putusan perkara yang diserahkan kepadanya untuk diadili; atau memberi atau menjanjikan sesuatu kepada seseorang yang menurut ketentuan peraturan perundang-undangan ditentukan menjadi advokat untuk menghadiri sidang pengadilan dengan maksud untuk mempengaruhi nasihat atau pendapat yang akan diberikan berhubung dengan perkara yang diserahkan kepada pengadilan untuk diadili (pasal 6 Ayat 1).
c. Pasal 7 Ayat 1 point 1 sampai 4, 8, 9, 10 point 1 sampai 3, 11 dan 12 point 1 sampai 9. Selain yang terdapat pada Undang-undang Nomor 20 Tahun 2001 juga terdapat pada Undang-Undang Nomor 31 Tahun 1999, yaitu pada pasal 13.
d. Pada pengertian ini korupsi digambarkan sebagai percobaan, korupsi digambarkan pada pasal 15, 16 dan 17 Undang-Undang Nomor 31 Tahun 1999.
e. Pada pengertian ini korupsi digambarkan sebagai tindakan murni dengan kata lain bahwa membantu pelaku tindak korupsi dalam penyidikan. Pengertiaan ini tertuang dalam pasal 21 sampai 24 Undang-Undang Nomor 31 Tahun 1999.

Dari pengertian korupsi yang dipaparkan tersebut, maka dapat disimpulkan bahwa korupsi merupakan perbuatan yang buruk seperti penggelapan uang, penerimaan uang sogok dan lain sebagainya dengan tujuan untuk memperkaya diri sendiri atau orang lain atau korporasi, yang mengakibatkan kerugian keuangan pada negara. Atau tindakan penyelewengan atau penggelapan uang baik itu uang negara atau uang lainnya yang dilakukan untuk keuntungan pribadi atau orang lain. Selain itu, ada satu faktor tambahan lain terkait dengan aktivitas korupsi ini, yaitu aktivitas yang "dirahasiakan". Jadi, pada umumnya tindakan korupsi ini dilakukan secara diam-diam atau dirahasiakan, dimana orang lain diluar diri si-pelaku korupsi atau kelompok pelaku korupsi biasanya tidak mengetahui aktivitas kecurangan yang telah dilakukan. Mereka membuat "skenario" yang sedemikian rupa sehingga tindakan kecurangan yang dilakukannya tidak diketahui oleh siapapun termasuk orang terdekat sekalipun di luar diri si-pelaku atau kelompok pelaku korupsi.

Penyebab Korupsi

Begitu banyak prolematika kehidupan yang terjadi dari hal yang sederhana sampai hal yang rumit untuk dipecahkan masalahnya. Setiap kejadiaan yang terjadi pasti memiliki sebab, dan sebab tersebutlah yang memicu terjadinya berbagai asumsi tentang akibat yang ditimbulkan oleh sebab kejadian tersebut. Tak ubahnya manusia dan jin diciptakan oleh sang khaliq untuk beribadah kepada-Nya. Begitu juga dengan yang sangat marak terjadi di Indonesia yaitu kasus korupsi. Hal ini dapat kita lihat dari berbagai media masa seperti siaran televisi, banyak siaran di televisi menyebutkan tentang kasus korupsi yang terjadi di Indoensia. Sejalan dengan hal tersebut, media kabar (koran) juga membahas tentang isu korupsi yang terjadi di Indoensia. Beberapa media masa menempatkan kasus korupsi di halaman pertama dari banyaknya berita yang dimuat di dalamnya, hal ini mungkin dipicu oleh negara kita yang merupakan negara hukum yangmana pantas untuk membincangkan kasus tersebut sebagai kabar utamanya. Dari kejadian tersebut banyak sekali asumsi yang beredar dikalang tokoh politik maupun pengamat politik "mengapa korupsi bisa terjadi?". Beberapa asumsipun bermunculan untuk kasus tersebut.

Ada lima hal yang memicu korupsi bisa terjadi, Hal pertama adalah sistem birokrasi yang masih "corrupt", Hal yang kedua adalah sistem hukum yang belum kuat dan tegas. "KUHAP dibaca SUAP jadinya ada markus (makelar kasus) dimana-mana. Hal ketiga adalah penghasilan yang besar. Semakin kaya seorang pejabat, semakin banyak pejabat tersebut korupsi. Hal yang ke empat pengawasan yang tidak efektif. Penyebab korupsi yang terakhir adalah kurangnya taat hukum sudah menjadi budaya. Dalam banyak hal, penyebab seseorang melakukan korupsi adalah karena ketergodaannya akan dunia materi atau kekayaan yang tidak mampu ditahannya. Ketika dorongan untuk menjadi kaya tidak mampu ditahan, sementara akses ke arah kekayaan bisa diperoleh melalui cara berkorupsi, maka jadilah seseorang melakukan tindak korupsi. Tegasnya, orang yang melakukan korupsi dikarenakan ketamakannya akan harta. Walaupun demikian, sebagai seorang manusia ketidakpuasan terhadap kebutuhan hidup merupakan sifat dasar alami manusia.

Permasalahan tentang korupsi saat ini tengah menjadi perbincangan hangat di kalangan masyarakat Indonesia, terutama pada media masa lokal dan nasional. Maraknya korupsi di Indonesia seakan sulit untuk diberantas dan telah menjadi budaya yang mengakar kuat di masyarakat pada semua lapisan. Pada dasarnya, di Indonesia korupsi merupakan suatu pelanggaran hukum yang kini telah menjadi suatu kebiasaan berdasarkan data *transparency International* Indonesia.

Banyak kasus korupsi di Indonesia sampai saat ini belum bisa teratasi dengan baik. Pada era demokrasi ini, korupsi akan mempersulit pencapaian *good governance* dan pembangunan ekonomi. Terlebih lagi pernah terjadi perebutan kewenangan antara KPK dan Polri. Sebagai institusi yang sama-sama menangani korupsi, seharusnya KPK dan Polri bisa bekerja sama dalam memberantas korupsi. Tumpang tindih kewenangan seharusnya tidak terjadi jika dapat dikoordinasikan secara baik. Penyebab terjadinya korupsi ditengarai bermacam-macam, antara lain masalah ekonomi, yaitu rendahnya penghasilan yang diperoleh jika dibandingkan dengan kebutuhan hidup masa kini dan gaya hidup yang konsumtif, budaya memberi tips (uang pelicin), budaya malu yang rendah, sanksi hukum yang lemah dan tidak mampu menimbulkan efek jera, penerapan hukum yang tidak konsisten dari institusi penegak hukum, serta kurangnya pengawasan hukum. Dalam upaya pemberantasan korupsi, diperlukan kerja sama semua pihak maupun semua elemen masyarakat, tidak hanya institusi terkait saja.

Di Indonesia, beberapa institusi yang diberi kewenangan untuk memberantas korupsi, antara lain Komisi Pemberantasan Korupsi (KPK), Kepolisian, *Indonesia Corruption Watch* (ICW) serta Kejaksaan. Keberadaan KPK merupakan salah satu langkah yang sangat berani pemerintah dalam usaha pemberantasan korupsi di Indonesia. Dalam menangani kasus korupsi, yang harus ditekankan adalah oknum pelaku dan hukum. Kasus korupsi dilakukan oleh oknum-oknum yang tidak bertanggung jawab sehingga membawa dampak buruk pada nama instansinya hingga pada pemerintah dan negara. Hukum diciptakan untuk mengatur, dan setiap lembaga/badan di lingkungan pemerintahan telah memiliki kewenangan hukum sesuai dengan perundangan yang ada. Namun demikian, banyak terjadi tumpang tindih kewenangan yang diakibatkan oleh banyaknya campur tangan politik buruk yang dibawa oleh oknum perorangan maupun instansi/organisasi. Untuk mencapai tujuan pembangunan nasional, maka korupsi harus diberantas atau ditekan, baik dengan cara preventif maupun represif. Penanganan semua kasus korupsi harus mampu memberikan efek jera kepada pelaku agar tidak terulang kembali. Selain dari itu, sebagai warga Indonesia yang baik kita wajib memiliki budaya malu yang tinggi agar segala tindakan yang merugikan negara seperti korupsi dapat diminimumkan. Indonesia adalah negara hukum, sehingga semua warga negara Indonesia memiliki derajat dan

perlakuan yang sama di mata hukum. Terkait dengan hal tersebut, dalam penindakan hukum bagi pelaku korupsi haruslah tidak boleh pilih kasih, baik bagi pejabat ataupun masyarakat kecil. Dengan demikian, diperlukan sikap jeli pemerintah dan masyarakat sebagai aktor inti penggerak demokrasi di Indonesia, terutama dalam memilih para pejabat yang akan menjadi wakil rakyat. Tidak hanya itu, semua elemen masyarakat juga berhak mengawasi dan melaporkan kepada institusi terkait jika terindikasi adanya tindak pidana korupsi.

Dampak Korupsi

Berkaitan dengan dampak yang diakibatkan dari tindak pidana korupsi, setidaknya terdapat dua konsekuensi. Konsekuensi negatif dari korupsi sistemik terhadap proses demokratisasi dan pembangunan yang berkelanjutan. Konsekuensi dari kedua hal tersebut dapat dijelaskan sebagai berikut:

1) Korupsi mendelegetimasikan proses demokrasi dengan mengurangi kepercayaan publik terhadap proses politik melalui politik uang.
2) Korupsi mendistorsi pengambilan keputusan pada kebijakan publik, membuat tiadanya akuntabilitas publik, dan menafikkan *the rule of law*. Hukum dan birokrasi cenderung hanya melayani kepada kekuasaan dan pemilik modal.
3) Korupsi meniadakan sistem promosi dan hukuman yang berdasarkan kinerja karena hubungan *patron-client* dan nepotisme.
4) Korupsi mengakibatkan proyek-proyek pembangunan dan fasilitas umum bermutu rendah dan tidak sesuai dengan kebutuhan masyarakat, sehingga mengganggu pembangunan yang berkelanjutan.
5) Korupsi mengakibatkan sistem ekonomi lemah karena produk yang tidak kompetitif dan penumpukan beban hutang luar negeri.

Dari penjelasan tersebut, dapat kita simpulkan bahwa dampak korupsi sangat berbahaya karena efek dari aktivitas korupsi ke semua bidang strategis suatu negara baik ekonomi, politik, sosial dan budaya. Sementara itu, kasus korupsi di Indonesia sudah mencapai posisi yang sangat rawan karena praktik korupsi sudah menjadi budaya dan kebiasaan pada semua level baik di lingkungan organisasi pemerintahan maupun organisasi bisnis. Untuk itu pemerintah diharapkan segera melakukan langkah strategik untuk penanggulangan korupsi khususnya di lembaga pemerintahan. Sehubungan dengan hal tersebut, pada bagian berikutnya akan dibahas beberapa tindakan atau strategi yang dapat dilakukan untuk menekan tindakan korupsi dan fraud pada umumnya di Indonesia.

Pencegahan dan Pendeteksian Fraud

Pencegahan fraud dapat dianalogikan dengan sebuah penyakit, yaitu lebih baik dicegah dari pada diobati. Jika menunggu terjadinya *fraud* baru ditangani itu artinya sudah ada kerugian yang terjadi dan telah dinikmati oleh pihak-pihak tertentu, bandingkan bila kita berhasil mencegahnya, tentu kerugian belum semuanya beralih kepada para pelaku *fraud* tersebut. Selanjutnya, apabila *fraud* sudah terjadi maka biaya yang dikeluarkan jauh lebih besar untuk memulihkannya daripada melakukan pencegahan sejak dini.

1. Membangun struktur pengendalian yang baik
   Dalam memperkuat pengendalian intern di perusahaan, COSO *(The Committee of Sponsoring Organizations of The Treadway Commission)* pada bulan September 1992 memperkenalkan suatu rerangka pengendalian yang lebih luas daripada model

pengendalian akuntansi tradisional, serta mencakup manajemen risiko di dalamnya, yaitu pengendalian intern yang terdiri atas 5 (lima) komponen yang saling terkait yaitu:

a. Lingkungan pengendalian *(control environment),* merupakan tanggung jawab dari manajemen puncak untuk menyatakan dengan jelas nilai-nilai integritas dan kegiatan tidak etis yang tidak dapat ditoleransi.
b. Penaksiran risiko *(risk assessment),* dalam hal ini manajemen perusahaan harus mengidentifikasi dan menganalisis semua faktor yang menciptakan resiko bisnis dan harus menentukan bagaimana caranya mengelola resiko tersebut.
c. Standar Pengendalian *(control activities),* untuk mengurangi terjadinya kecurangan, manajemen harus merancang kebijakan dan prosedur untuk mengidentifikasi resiko tertentu yang dihadapi perusahaan.
d. Informasi dan komunikasi *(information and communication),* Sistem pengendalian internal harus dikomunikasikan dan diinfokan kepada seluruh karyawan perusahaan dari level atas hingga level bawah.
e. Pemantauan *(monitoring),* Sistem pengendalian internal harus dipantau secara berkala. Apabila terjadi kekurangan yang signifikan, harus segera dilaporkan kepada manajemen puncak dan juga kepada dewan komisaris.

2. Mengefektifkan aktivitas pengendalian
   a. Review kinerja, aktivitas pengendalian ini mencakup review atas kinerja sesungguhnya dibandingkan dengan anggaran, prakiraan, atau kinerja periode sebelumnya. Selain itu, juga meliputi tindakan menghubungkan satu rangkaian data yang berbeda operasi.
   b. Pengolahan informasi, berbagai aktivitas pengendalian dilakukan untuk meyakinkan ketepatan, kelengkapan, dan otorisasi transaksi. Terdapat dua jenis pengelompokan pengendalian sistem informasi yaitu pengendalian umum dan pengendalian aplikasi. Pengendalian umum biasanya mencakup pengendalian atas operasi pusat data, pemrosesan dan pemeliharaan perangkat lunak sistem, keamanan akses, pengembangan serta pemeliharaan sistem aplikasi. Pengendalian ini berlaku untuk mainframe, minicomputer dan lingkungan pemakai akhir. Pengendalian ini membantu menerapkan bahwa transaksi adalah sah, diotorisasi semestinya, dan diolah secara lengkap dan akurat.
   c. Pengendalian fisik, aktivitas pengendalian fisik meliputi berbagai tindakan terkait dengan keadaan fisik aktiva yang meliputi keamanan fisik aktiva, penjagaan yang cukup memadai terhadap berbagai fasilitas yang terlindungi dari akses terhadap aktiva dan catatan, otorisasi untuk akses ke program komputer dan data files, serta perhitungan secara periodik dan pembandingan dengan jumlah yang tercantum dalam catatan pengendali.
   d. Pemisahan tugas, pembebanan tanggung jawab kepada personel yang berbeda untuk memberikan otorisasi, pencatatan transaksi dan penyelenggarakan penyimpanan aset yang ditujukan untuk mengurangi kesempatan bagi seseorang untuk berbuat kecurangan.

3. Meningkatkan kultur organisasi
   Kultur organisasi merupakan norma perilaku dan nilai-nilai yang dipahami dan diterima oleh semua anggota pada suatu organisasi dan digunakan sebagai dasar dalam aturan perilaku dalam organisasi tersebut. Sementara itu menurut Millar *et al.* (2018) kultur organisasi ini juga bisa diartikaan sebagai nilai-nilai yang menjadi pedoman bagi sumber daya manusia untuk menghadapi segala permasalahan

eksternal serta usaha penyesuaian integrasi ke dalam organisasi, dengan demikian setiap anggota organisasi wajib memahami nilai-nilai yang ada dan sebagaimana mereka harus bertingkah laku atau berperilaku.

Meningkatkan kultur organisasi dapat dilakukan dengan mengimplementasikan prinsip-prinsip *Corporate Governance* (CG). Lebih lanjut Grove dan Clouse (2017) mengemukakan prinsip-prinsip Corporate Governance yang meliputi:

a. Keadilan *(Fairness)*
b. Transparansi *(Transparency)*
c. Akuntabilitas *(Accountability)*
d. Tanggung jawab *(Responsibility)*
e. Moralitas *(Morality)*
f. Kehandalan *(Reliability)*
g. Komitmen *(Commitment)*

4. Mengefektifkan fungsi internal audit
   Beberapa hal yang harus diperhatikan oleh manajemen agar fungsi internal audit bisa efektif dan maksimal membantu manajemen dalam melaksanakan tanggungjawabnya dengan memberikan analisa, penilaian, saran dan komentar tentang kegiatan yang diperiksanya yaitu:
   a. Internal audit departemen harus mempunyai kedudukan yang independen dalam organisasi perusahaan.
   b. Internal audit departemen harus mempunyai uraian tugas secara tertulis, sehingga setiap auditor mengetahui dengan jelas apa yang menjadi tugas, wewenang dan tanggungjawabnya.
   c. Internal audit harus mempunyai petunjuk internal audit *(internal audit manual).*
   d. Harus ada dukungan yang kuat dari top manajemen kepada departemen internal audit.
   e. Internal audit departemen harus memiliki sumber daya yang profesional, kompeten, bersikap obyektif dan mempunyai integritas serta loyalitas yang tinggi.
   f. Internal auditor harus bisa bekerjasama dengan akuntan publik.
   g. Menciptakan struktur penggajian yang wajar dan pantas.
   h. Mengadakan rotasi dan kewajiban bagi pegawai untuk mengambil hak cuti.
   i. Memberikan sanksi yang tegas kepada yang melakukan kecurangan dan berikan penghargaan kepada mereka yang berprestasi.
   j. Membuat program bantuan kepada pegawai yang mendapatkan kesulitan baik dalam hal keuangan maupun non-keuangan.
   k. Menetapkan kebijakan perusahaan terhadap pemberian pemberian dari luar harus diinformasikan dan dijelaskan pada semua orang yang dianggap perlu agar jelas mana yang hadiah dan mana yang berupa sogokan dan mana yang resmi.
   l. Menyediakan sumber-sumber tertentu dalam rangka mendeteksi kecurangan karena kecurangan sulit ditemukan dalam pemeriksaan yang biasa-biasa saja.

Dengan melakukan berbagai aktivitas tersebut, peran dan fungsi internal auditor akan dicapai secara maksimal meskipun kemungkinan ada faktor lain yang secara potensial dapat mengganggu peran dan fungsi internal audit baik dari sisi internal maupun eksternal organisasi/perusahaan. Adanya aktivitas internal audit ini dapat menghindari timbulnya resiko kesalahan, penyalahgunaan wewenang, serta berbagai kendala dengan mengembangkan efisiensi dan efektivitas perusahaan.

Sehubungan dengan hal tersebut perusahaan seharusnya menyusun *Standard Operating Procedure* (SOP) pelaksanaan internal audit pada suatu organisasi, serta melakukan pengendalian internal audit di dalam perusahaan dengan tujuan untuk pengembangan perusahaan. *Standard Operating Prosedur* tersebut hendaknya disertai dengan aturan yang dibuat oleh pimpinan tertinggi organisasi/perusahaan sehingga bersifat mengikat untuk dipatuhi seluruh personel di dalam organisasi atau perusahaan.

Pendeteksian Fraud

Membahas kecurangan tiada habisnya, ibarat menutup kebocoran muncul rembesan atau bocaran yang lain, begitu dan begitu seterusnya. Selama ini pendekatan pencegahan kecurangan cenderung lebih banyak menggunakan teori-teori investigasi dan forensik, namun belum banyak yang menggunakan penedekatan moral. Pada bagian ini, akan dicoba untuk ditelaah kembali pencegahan dan pendeteksian *fraud* melalui pendektan teori investigasi dan forensik.

Pendeteksian *fraud* merupakan suatu tindakan untuk mengetahui bahwa fraud terjadi, siapa pelaku, siapa korbannya, dan apa penyebabnya. Kunci pada pendeteksian fraud adalah untuk dapat melihat adanya kesalahan ketidakberesan. *Fraud* (kecurangan) pada hakekatnya tersembunyi dan pelakunya pada umumnya juga akan menyembunyikan jejaknya dengan rapi dan terstruktur. Oleh karena itu pendeteksian fraud juga tidak dapat dilakukan langsung dengan melihat jejak yang ditinggalkannya. Pendeteksian *fraud* dilakukan dengan mengidentifikasi tanda-tanda atau gejala terjadinya fraud. Setiap terjadi fraud selalu diikuti dengan adanya tanda-tanda atau gejala fraud. Oleh karena itu dengan mengenali gejala atau tanda tersebut, maka dapat dikenali pula sinyal atau indikasi adanya aktivitas fraud.

Gejala-gejala atau tanda-tanda terjadinya fraud dapat ditunjukkan dari individu pelaku, dari organisasi, maupun dari luar organisasi. Tanda-tanda dari pelaku tampak dari perubahan gaya hidup dan tindak tanduknya atau perilaku yang mencurigakan. Organisasi yang ada menunjukkan berbagai kondisi yang kondusif terjadinya fraud, terutama sebagai akibat lemahnya pengendalian internal baik dalam rancangan struktur pengendalian maupun dalam pelaksanaan.

Kondisi lain ialah adanya keganjilan-keganjilan dalam akuntansinya dan pada hasil berbagai analisis atas pertanggungjawaban keuangan dan aktivitasnya. Di samping itu, banyak pengaduan dari luar organisasi seperti pelanggan, rekanan, atau dari pemasok. Pendeteksian fraud dapat melalui:

a. Identifikasi gejala dan dengan identifikasi bendera merah *(red flags)*
b. Pendeteksian fraud dengan *critical point of auditing*

Analisis kepekaan *(job sensitivity analysis)*. Para atasan atau manajer suatu unit organisasi, auditor internal, atau *fraud examiner* harus cepat tanggap dan segera melakukan penelaahan lebih lanjut terhadap hasil pendeteksian fraud, sehingga potensi fraud dapat dicegah dan fraud yang telah terjadi dapat dihentikan dan ditindak lanjuti. Adapun langkah awal dari pendeteksian fraud meliputi:

1. Memahami aktivitas organisasi dan mengenal serta memahami seluruh sektor usaha. Pada pemahaman aktivitas organisasi ini, sertakan personel yang berpengalaman dalam tim deteksi, serta lakukan wawancara dengan personel kunci dari organisasi. Pada pemahaman itu diidentifikasi apakah organisasi telah menerapkan pengendalian maupun dalam pelaksanaan. Pengendalian intern bukan saja untuk mencegah *fraud*, tetapi dirancang pula untuk mendeteksi *fraud* secara dini karena pengendalian intern. dapat digunakan sebagai pengendalian detektif.

Berbagai sarana kendali yang ada, dirancang untuk dapat mencegah fraud secara otomatis sehingga setiap tindak *fraud* dapat terdeteksi tanpa menunggu hasil audit. Dari hasil pemahaman aktivitas organisasi tersebut dapat diidentifikasi *fraud* yang terjadi pada aktivitas itu.

2. Memahami tanda-tanda penyebab terjadinya fraud.
   Tanda-tanda penyebab terjadinya fraud berupa berbagai keanehan, keganjilan, dan penyimpangan dari keadaan yang seharusnya serta kelemahan dalam pengendalian intern. Tanda-tanda tersebut diperoleh dari berbagai informasi, tetapi hasilnya masih merupakan tanda-tanda umum yang masih harus dianalisis dan dievaluasi. Bila ada indikasi kuat, dilakukan investigasiterhadap gejala tersebut. Pendeteksian fraud terhadap gejala dan tanda-tanda fraud dapat pula dilakukan terhadap kondisi atau situasi tertentu yang disebut bendera merah *(red flags)* yaitu suatu kondisi yang member isyarat dini terjadinya *fraud (fraud warning sign)*. Seperti halnya pada gejala, tidak semua bendera merah dipastikan terjadi fraud, tetapi setiap fraud selalu tampak adanya kondisi yang member isyarat adanya *fraud* baik dari pelaku,organisasi,maupun jenis fraudnya.
3. Pendeteksian dengan *critical point of auditing* dan teknik analisis kepekaan (*job sensitivity analysis*).
   Critical point of auditing merupakan teknik pendeteksian *fraud* melalui audit atas catatan akuntansi yang mengarah pada gejala atau kemungkinan terjadinya. Teknik analisis kepekaan adalah teknik pendeteksian *fraud* didasarkan pada analisis dengan memandang pelaku potensial. Analisisnya ditujukan pada posisi tertentu apakah ada peluang tindakan *fraud* dan apa saja yang dapat dilakukan.Banyak teknik pendeteksian fraud sesuai dengan jenis *fraud*. Secara umum, upaya mendeteksi *fraud* antara lain dilakukan dengan: Pengujian pengendalian intern. Meliputi pengujian pelaksanaannya secara acak dan mendadak. Hal ini untuk mendeteksi *fraud* yang dilakukan dengan kolusi sehingga pengendalian intern yang ada tidak berfungsi efektif.

Dalam sistem pengendalian intern diatur bahwa pengeluaran barang dari gudang harus didukung dokumen pengeluaran yang disahkan oleh otoritasnya. Karena adanya kolusi dinyatakan barang yang keluar jumlahnya X kg dan kualitas B. Kenyataannya, barang yang keluar sebenarnya sebanyak Y kg dan kualitasnya A. Jejak barang yang keluar direkayasa catatan akuntansi dan dokumennya sehingga bila diteliti tidak terdeteksi bahwa barang yang keluar sebanyak Y kg dengan kualitas A. Apabila dilakukan pengecekan mendadak pada saat barang keluar, barulah kecurangan tersebut terdeteksi. Dalam kasus ini, meskipun pengujian audit keuangan atau audit operasional dilakukan, pada kedua jenis audit itu tidak ada keharusan auditor untuk dapat mendeteksi dan mengungkap adanya *fraud*, akan tetapi auditor harus merancang dan melaksanakan auditnya sehingga *fraud* dapat terdeteksi.

Penggunaan prinsip pengecualian *(exception)* dalam pengendalian dan prosedur. Pengecualian dimaksud antara lain: Adanya pengendalian intern yang tidak dilaksanakan atau dikompromosikan. Transaksi-transaksi yang janggal misalnya: waktu transaksi pada hari minggu atau hari libur lain, jumlah frekuensi transaksi terlalu banyak atau terlalu sedikit. Tempat transaksi terlalu menyimpang dari biasanya. Tingkat motivasi, moral dan kepuasan kerja terus menerus menurun. Sistem pemberian penghargaan yang ternyata mendukung pelaku tidak etis. Dilakukan kaji ulang terhadap penyimpangan dalam kinerja operasi. Dari hasil kaji ulang diperoleh penyimpangan yang mencolok dalam hal anggaran, rencana kerja, tujuan, dan sasaran organisasi. Penyimpangan tersebut bukan karena adanya sebab yang wajar dari aktivitas bisnis

yang lazim. Pendekatan reaksi meliputi adanya pengaduan dan keluhan karyawan, kecurigaan, dan intuisi atasan.

Kewajiban Auditor terhadap Kecurangan Tidak Terdeteksi

Adanya kecurangan tidak terdeteksi kemungkinan disebabkan oleh aktivitas kecurangan yang melibatkan skema canggih, terstruktur dan terorganisasi secara cermat yang dirancang untuk menutupinya, seperti pemalsuan, secara sengaja gagal mencatat transaksi, atau penyajian keliru yang disengaja kepada auditor. Berbagai usaha penyembunyian tersebut kemungkinan akan lebih susah terdeteksi apabila disertai dengan adanya kolusi. Aktivitas kolusi ini dapat menyebabkan auditor percaya bahwa bukti audit meyakinkan, meskipun pada kenyataannya bukti tersebut palsu.

Terkait dengan hal-hal tersebut, maka beberapa hal yang harus dilakukan oleh auditor meliputi: (1) Berusaha mendapatkan keterangan dari pihak manajemen atau bagian audit internal pengetahuan tentang kecurangan aktual, yang diduga dan dicurigai berdampak pada entitas. (2) Mendapatkan pemahaman tentang bagaimana pihak yang bertanggung jawab terhadap tata kelola melakukan pengawasan terhadap proses yang diterapkan oleh manajemen dalam mengidentifikasi dan merespons risiko kecurangan dalam entitas dan pengendalian internal yang telah ditetapkan oleh manajemen untuk mengurangi risiko tersebut. (3) Mengevaluasi apakah hubungan tidak biasa atau tidak terduga yang telah diidentifikasi ketika melaksanakan prosedur analitis, termasuk yang terkait dengan akun pendapatan, dapat mengindikasikan adanya risiko kesalahan penyajian material yang diakibatkan oleh kecurangan. (4) Mengevaluasi apakah informasi yang diperoleh dari prosedur penilaian risiko lain dari aktivitas terkait yang telah dilaksanakan mengindikasikan bahwa terdapat satu atau lebih faktor risiko kecurangan.

Simpulan

Fraud merupakan bentuk kecurangan untuk mendapatkan keuntungan pribadi maupun lembaga/organisasi. Kecurangan yang bersifat kelembagaan lebih kompleks dibandingkan dengan kecurangan yang dilakukan oleh pribadi. Kecurangan/*fraud* mengakibatkan kerugian yang besar. Dalam pemerintahan, kerugian yang diterima bukan hanya kehilangan atau kebocoran uang negara, namun juga berakibat pada menurunnya kepercayaan masyarakat terhadap pemerintah serta menurunnya tingkat investasi.

Maraknya berita mengenai investigasi terhadap indikasi penyimpangan *(fraud)* di dalam perusahaan dan juga pengelolaan negara di surat kabar dan televisi semakin membuat sadar bahwa kita harus melakukan sesuatu untuk membenahi ketidakberesan tersebut. Walaupun saat ini sorotan utama sering terjadi pada manajemen puncak perusahaan, atau terlebih lagi terhadap pejabat tinggi suatu instansi, namun sebenarnya penyimpangan perilaku tersebut bisa juga terjadi di berbagai lapisan kerja organisasi.

Untuk mengatasi permasalahan ini seorang internal auditor dalam pengungkapan terjadinya kecurangan harus memiliki kemampuan mirip dengan yang dimiliki seorang penyidik kriminal dan keberadaan keduanya adalah untuk mencari kebenaran melalui pengungkapan bukti pendukung perbuatan kecurangan *(fraud)*. Dalam pengungkapan kecurangan, seorang internal auditor harus mempunyai rasa ingin tahu yang tinggi serta suka akan tantangan pada hal-hal yang muncul secara tidak lazim. Dengan kata lain keingintahuan terhadap hal-hal yang bertentangan dengan

logika maupun apa yang diharapkan secara wajar merupakan salah satu hal penting yang harus dimiliki oleh seorang internal auditor.

Daftar Bacaan

Abdallah, A., Maarof, M.A. & Zainal A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, (68), 90-113.

Albrecht, W.S., Albrecht, C.C., Albrecht, C.O. dan Zimbelman, M. (2009). *Fraud Examination*, third Edition, South Western, a part of Chengange Learning, USA.

Allen, L. (2018). Accounting for contingent litigation liabilities: What you disclose can be used againts you. *Virginia Law and Business Review*, 12 (2), 312-330.

Bawakes, H.F., Simanjuntak, A.M.A. & Daat, S.C. (2018). Pengujian teori fraud pentagon terhadap fraudulent financial reporting. *Jurnal Akuntansi & Keuangan Daerah*, 13 (1), 114-134.

Beets, M.J & Clark, D. (2017). *Investigation of Fraud and Economic Crime*. Oxford: Oxford University Press.

Grove. H. & Clouse. M. (2017). Corporate governance principles and sustainability. *Corporate Governance and Sustainability Review*, 1 (2), 13-19.

Millar. K., Cadden. T., Yang. Y. & Humphrets. P. (2018). The interplay between lean practices, organisational culture practices and operational performance. *25th International EurOMA Conference*. Budapest. 24-26 June.

Peraturan Otoritas Jasa Keuangan Nomor 39/POJK.03/2019 tentang Penerapan Strategi Anti Fraud Bagi Bank Umum.

Prihartono, Theresia & Mayangsari, S. (2018). Pengaruh integritas, objektivitas, dan kompetensi auditor internal terhadap efektivitas audit internal dengan gaya kepemimpinan demokrasi sebagai variabel moderasi pada Inspektorat Jenderal Kementerian Dalam Negeri. *Jurnal Magister Akuntansi Trisakti*, 5 (1), 63-88.

Vousinas, G.L. (2019), Advancing theory of fraud: the S.C.O.R.E. model, *Journal of Financial Crime*, 26 (1), 372-381.

BAB 2
FINANCIAL STATEMENT FRAUD

Pendahuluan

Setiap jenis perusahaan memiliki laporan keuangan *(financial statement)* yang bertujuan menyediakan semua informasi yang menyangkut posisi keuangan, kinerja, serta perubahan posisi keuangan suatu perusahaan. Informasi ini tentunya bermanfaat bagi berbagai pemakai laporan keuangan untuk pengambilan keputusan secara ekonomi. Laporan keuangan ini harus dipersiapkan secara periodik untuk berbagai pihak yang berkepentingan. Suatu laporan keuangan memberikan informasi keuangan perusahaan yang dapat digunakan dalam pengambilan keputusan ekonomi serta menunjukkan kinerja yg telah dilakukan manajemen *(stewardship)* atau pertanggungjawaban manajemen atas penggunaan sumber-sumber daya yang telah dipercayakan kepadanya. Laporan keuangan merupakan sebuah laporan yang menggambarkan hasil dari proses akuntansi yang digunakan sebagai media komunikasi untuk pihak-pihak yang berkepentingan dengan data/informasi keuangan serta aktivitas perusahaan. Definisi laporan keuangan menurut Osadchy *et al.* (2018) merupakan hasil dari proses akuntansi yang dapat digunakan sebagai alat untuk mengkomunikasikan data keuangan atau aktivitas suatu perusahaan.

Standar Akuntansi (SA) seksi 312 PSA 04 menyebutkan bahwa laporan keuangan mengandung salah saji material apabila laporan keuangan tersebut mengandung salah saji yang dampaknya secara individual atau keseluruhan cukup signifikan, sehingga dapat mengakibatkan suatu laporan keuangan tidak disajikan secara wajar, dalam semua hal yang material, sesuai dengan prinsip akuntansi yang berlaku umum di Indonesia. Salah saji laporan keuangan tersebut dapat terjadi sebagai akibat dari 'kekeliruan' atau 'kecurangan'. Istilah kekeliruan berarti salah saji atau penghilangan secara tidak disengaja jumlah atau pengungkapan dalam laporan keuangan. Menurut SA seksi 312 PSA 06 dinyatakan bahwa kekeliruan dapat mencakup: (1) Kesalahan dalam pengumpulan dan pengolahan data yang menjadi sumber penyusunan laporan keuangan. (2) Estimasi akuntansi yang tidak masuk akal yang timbul dari kecerobohan atau salah tafsir fakta. (3) Kekeliruan dalam penerapan prinsip akuntansi yang berkaitan dengan jumlah, klasifikasi, cara penyajian, ataupun pengungkapan *(disclosure)*.

Lebih lanjut, seperti yang telah dijelaskan di muka bahwa kecurangan (*fraud*) perlu dibedakan dengan kesalahan *(Errors)*. Kesalahan dapat dideskripsikan sebagai "*Unintentional Mistakes*" (kesalahan yang tidak di sengaja). Kesalahan dapat terjadi pada setiap tahapan dalam pengelolaan transaksi, terjadinya transaksi, dokumentasi, pencatatan dari ayat-ayat jurnal, pencatatan debit kredit, pengikhtisaran proses dan hasil laporan keuangan. Kesalahan dapat saja terjadi dalam banyak bentuk matematis,

kritikal, atau dalam aplikasi prinsip-prinsip akuntansi. *'Commission'* merupakan kesalahan prinsip *(error of principle),* seperti perlakuan pengeluaran pendapatan sebagai pengeluaran modal. Sedangkan *'Omission'* berarti bahwa suatu item tidak dimasukkan sehingga menyebabkan informasi tidak benar. Apabila suatu kesalahan adalah disengaja, maka kesalahan tersebut merupakan kecurangan (*fraud*). Istilah "Irregulary" merupakan kesalahan penyajian keuangan yang disengaja atas informasi keuangan.

Kesalahan mempunyai dua bentuk dasar, meliputi: (1) kesalahan akuntansi *(accounting errors)* dan (2) kesalahan sistem *(system errors).* Jika kesalahan akuntansi terjadi, akan mempengaruhi langsung pada kesalahan pelaporan keuangan. Sedangkan kesalahan sistem berhubungan erat dengan lemahnya sistem pengendalian internal, yang pada akhirnya akan menyulitkan pelacakan kesalahan dan ketidakberesan yang terjadi dalam suatu organisasi. Berikut ini akan dijelaskan tentang kesalahan akuntansi dan kesalahan sistem yang sering menjadi ganjalan dalam proses pelaporan dan pertanggungjawaban organisasi.

Kesalahan Akuntansi (Accounting Errors)

Kesalahan tipe ini mempengaruhi secara langsung kesalahan pelaporan keuangan baik disengaja maupun tidak disengaja. Kesalahan akuntansi dikelompokkan menjadi 3 (tiga) jenis, meliputi:

1) Kesalahan karena tidak mencantumkan *(errors of omissions).*
2) Kesalahan karena penyalahgunaan jabatan/wewenang *(errors of commissions)*
3) Kesalahan karena prinsip akuntansi *(errors of principles).*

Ketiga jenis kesalahan tersebut yang meliputi *errors of omissions, errors of commissions,* dan *errors of principles* yang disengaja, secara tipikal timbul dari orang-orang yang dengan sengaja berbuat tidak jujur. Kesalahan tersebut sering terjadi sebagai akibat dari akumulasi ketidakberesan yang terjadi pada suatu organisasi. Secara khusus kesalahan akuntansi ini akan berdampak pada tindakan hukum. Bagi para auditor kesalahan seperti ini sedapat mungkin harus dihindari. Salah satunya adalah dengan mendisain sistem pengendalian intern yang memadai. Sedangkan ketiga kelompok kesalahan tersebut di atas yang sifatnya tidak disengaja lebih cocok bila hanya disebut sebagai kekeliruan *(mistake).* Kekeliruan semacam ini kemungkinan akibat dari kesalahan proses elektronik, sistem dan beban kerja yang berlebihan *(overload),* kesalahpahaman instruksi maupun prosedur yang harus dilakukan *(human errors),* serta kecerobohan dalam memberikan pertimbangan.

Errors of omissions, baik sengaja maupun tidak, pada umumnya terjadi pada fungsi-fungsi pelaksanaan: (1) operasi klerikal; (2) pencatatan transaksi; dan (3) penjurnalan. Sedangkan *errors of commission* bisa timbul ketika para karyawan yang melaksanakan ketiga fungsi tersebut tidak memenuhi syarat, bahkan mengarah pada tindakan penggelapan. Sementara itu, *errors of principles* terjadi karena penerapan metode, teknik dan prosedur akuntansi yang tidak sesuai dengan standar akuntansi keuangan yang berlaku.

Kesalahan Sistem *(System Errors)*

Kesalahan sistem, tidak dengan sendirinya akan berakibat pada kesalahan penyajian laporan keuangan. Namun, dengan semakin meningkatnya kesalahan tersebut akan berakibat pada kelemahan sistem pengendalian intern, yang pada gilirannya akan berdampak pula pada akurasi penyajian laporan keuangan. Kesalahan sistem terdiri dari

dua tipe dasar yaitu (1) kesalahan ketidakpatuhan *(compliance errors)*, dan (2) kesalahan disain sistem *(system design deficiencies)*. Kedua tipe kesalahan tersebut bisa terjadi karena disengaja maupun tidak disengaja.

Kesalahan Ketidakpatuhan *(Compliance Errors)*

Compliance errors yang disengaja *(intensional)*, merupakan perbuatan ketidakpatuhan, karena kegagalan seseorang melaksanakan kebijakan, prosedur dan teknik internal kontrol. Sedangkan *compliance errors* yang tidak disengaja *(unintensional)*, merupakan tindakan yang sifatnya insidental tapi mengarah pada ketidakpatuhan terhadap kebijakan, prosedur dan teknik pengendalian intern. Kesalahan ketidakpatuhan ini bisa terjadi karena beberapa faktor yang antara lain meliputi:

a. Kesalahan menjalankan fungsi peralatan mekanis atau elektronik.
b. Karyawan tidak memahami kebijakan, prosedur dan teknik pengendalian intern.
c. Sistem dan mekanisme kerja *overload*.
d. *Human error* karena kecerobohan atau kekeliruan dalam membuat pertimbangan.

Kesalahan Disain Sistem *(Systems Design Errors)*

Systems design erros yang sifatnya sengaja merupakan kesalahan yang dilakukan seseorang dengan cara mengabaikan pengendalian yang telah ditetapkan, atau sistem yang didisain sudah tidak relevan lagi dengan kondisi yang ada. Sistem tersebut sengaja dibiarkan agar ada peluang untuk melakukan pelanggaran atau kecurangan. Dalam banyak hal, pada umumnya para karyawan atau pegawai akan mengetahui kelemahan sistem yang ada. Hal ini berisiko terjadinya penggunaan peluang karena sitem yang lemah tersebut. Kesalahan sistem lebih berpotensi terjadi pada sistem komputerisasi.

Systems design erros yang sifatnya tidak sengaja, berkaitan dengan kondisi dimana para karyawan bahkan pimpinan tidak menyadari akan sistem yang diterapkan, padahal sistem tersebut salah. Hal ini berpotensi terjadinya akumulasi kesalahan dan pelanggaran, yang baru akan diketahui kalau kesalahan dan ketidaktertiban tersebut sudah menjadi besar.

Sedangkan menurut Amiram *et al.* (2018) kecurangan laporan keuangan mencakup beberapa modus, antara lain: (a) Kegiatan pemalsuan, pengubahan, atau memanipulasi catatan keuangan *(financial record)*, dokumen pendukung atau transaksi bisnis. (b) Aktivitas penghilangan yang disengaja terhadap suaatu peristiwa, transaksi, akun, atau informasi signifikan lainnya sebagai sumber pendukung dari penyajian laporan keuangan. (c) Implementasi atau penerapan yang salah dan disengaja terhadap prinsip-prinsip akuntansi, kebijakan, maupun prosedur yang digunakan untuk mengukur, mengakui, melaporkan dan mengungkapkan peristiwa ekonomi serta transaksi bisnis. (d) Penghilangan dengan disengaja terhadap semua informasi yang seharusnya disajikan dan diungkapkan yang terkait dengan prinsip dan kebijakan akuntansi yang digunakan dalam membuat laporan keuangan.

Penyebab Terjadinya Fraud pada Laporan Keuangan

Pada dasarnya fraud tidak begitu saja terjadi dalam suatu organisasi atau perusahaan, akan tetapi fraud dapat terjadi karena berbagai penyebab dan kemungkinan yang dijadikan alasan untuk melakukan tindakan fraud. Dalam bidang akuntansi, dikenal dua jenis kesalahan yaitu kekeliruan *(error)* yang mengandung unsur ketidaksengajaan, dan kecurangan *(fraud)* yang pada umumnya disengaja atau dilakukan secara terencana.

Kecurangan laporan keuangan atau *fraudulent financial reporting* adalah salah saji atau pengabaian jumlah dan pengungkapan yang disengaja dengan maksud menipu para pemakai laporan keuangan. Kecurangan ini biasanya terjadi ketika sebuah perusahaan *(company)* melaporkan lebih tinggi dari yang sebenarnya *(overstates)* terhadap asset atau pendapatan, atau ketika perusahaan melaporkan lebih rendah dari yang sebenarnya *(understates)* terhadap kewajiban dan beban. Kecurangan laporan keuangan ini bisa dilakukan oleh siapa saja pada level apa-pun dan siapa-pun yang memiliki kesempatan.

Salah satu kasus fraud audit yang paling sering ditemui adalah *earning management* (manajemen laba) dan *income smoothing* (perataan laba). *Earning management* merupakan tindakan untuk memenuhi target laba yang dilakukan oleh para manajemen secara disengaja. *Income smoothing* adalah suatu tindakan manajemen laba yang disengaja dengan memindahkan pos-pos beban dan pendapatan ke dalam beberapa periode yang bertujuan untuk mengurangi fluktuasi laba. Sebagai contoh manajemen melebih sajikan pendapatan dengan cara melebih sajikan aset dan mengakui pendapatan secara tidak tepat. Hal penting yang perlu dicatat pada pengertian ini adalah kedua aktivitas tersebut baik manajemen laba maupun perataan laba dianggap sebagai *fraud* jika keduanya terindikasi mengandung adanya pelanggaran hukum atau peraturan yang berlaku, karena ada kemungkinan aktivitas yang dilakukan tidak mengandung unsur pelanggaran hukum sama sekali. Sebagai contoh sebuah perusahaan berusaha menurunkan nilai labanya dengan menggunakan teknik-teknik atau metode akuntansi tertentu yang secara aturan diperbolehkan karena berharap beban pajak atas perusahaan tersebut berkurang.

Cara Mendeteksi *Fraud*

Laporan hasil audit oleh para pengguna laporan keuangan pada umumnya dipakai sebagai alat untuk menyakinkan bahwa perusahaan yang diaudit dalam keadaan sehat. Sehubungan dengan hal tersebut, seorang auditor dalam melakukan audit harus dapat mengungkapkan salah saji material dan tindakan fraud yang terjadi pada perusahaan yang diaudit. Oleh sebab itu, seorang auditor harus mengetahui dengan pasti cara-cara yang harus dilakukan agar dapat mendeteksi *fraud.*

Menurut Baesens *et al.* (2015) cara mendeteksi kecurangan pada berbagai jenis kasus *fraud* adalah sebagai berikut:

1. Kecurangan Laporan Keuangan *(Financial Statement Fraud)*
   Kecurangan dalam penyajian laporan keuangan umumnya dapat dideteksi melalui analisis laporan Keuangan sebagai berikut:
   a. Analisis vertikal, yaitu teknik yang digunakan untuk menganalisis hubungan antara item-item dalam laporan laba rugi, neraca, atau laporan arus kas dengan menggambarkannya dalam persentase.
   b. Analisis horizontal, yaitu teknik untuk menganalisis persentase-persentase perubahan item laporan keuangan selama beberapa periode laporan.
   c. Analisis rasio, merupakan alat untuk mengukur hubungan antara berbagai nilai item dalam laporan keuangan.
2. Penyalahgunaan Aset *(Asset Misappropriation)*
   Variasi pendeteksian kecurangan jenis ini sangat beragam. Pemahaman terhadap pengendalian intern atas pos-pos tersebut akan sangat membantu dalam mendeteksi kecurangan. Metode-metode yang bisa digunakan antara lain (Eissa *et al.*, 2014):

a. *Analytical Review*, yaitu review atas berbagai akun yang mungkin menunjukkan ketidak biasaan atau kegiatan-kegiatan yang tidak diharapkan.
b. *Stastitical Sampling*, melakukan sampling atas pos-pos tertentu yang dicurigai.
c. *Outsider Complain*, yaitu keluhan dari konsumen, pemasok, atau pihak lain yang merupakan alat deteksi yang baik yang dapat mengarahkan auditor untuk melaksanakan pemeriksaan lebih lanjut.
d. *Site visite observation*, observasi ke lokasi ini pada umumnya dapat mengungkap ada atau tidaknya pengendalian internal pada lokasi-lokasi tersebut.

Penggunaan metode-metode tersebut dapat dilakukan sesuai dengan kasus yang terjadi. Artinya kemungkinan suatu kasus bisa diselesaikan dengan hanya menerapkan satu metode saja, atau kemungkinan lain suatu kasus harus diselesaikan dengan lebih dari satu metode atau kombinasi dari beberapa jenis metode.

3. Korupsi (*Corruption*)
Kecurangan pada kasus ini dapat dideteksi melalui beberapa cara diantaranya keluhan dari rekan kerja yang jujur, laporan dari rekan, atau para pemasok *(supplier)* yang tidak puas dan menyampaikan *complain* atau protes kepada pihak perusahaan. Atas sangkaan terjadinya kecurangan ini kemudian dilakukan analisis terhadap tersangka atau transaksinya.

Deteksi Kecurangan Akuntansi Berdasarkan Pihak yang Berkepentingan dengan Informasi Akuntansi

Pendeteksian terjadinya praktik kecurangan bisa dilakukan dengan mengenali gejala-gejalanya antara lain (Elisabeth & Casey, 2017):

1. Gejala Kecurangan pada Manajemen
Secara umum agak sulit dideteksi, namun gejalanya dapat dikenali yaitu timbulnya ketidakcocokan diantara manajemen puncak; rendahnya moral dan motivasi karyawan; departemen/lembaga akuntansi kekurangan staf; tingkat komplain yang tinggi terhadap organisasi/perusahaan dari pihak konsumen, pemasok, atau badan otoritas; terjadi kekurangan kas secara tidak teratur dan tidak terantisipasi; menurunnya tingkat penjualan atau laba sementara utang dan piutang usaha meningkat; perusahaan/company mengambil kredit sampai batas maksimal untuk jangka waktu yang lama; terdapat kelebihan persediaan yang signifikan; serta terdapat peningkatan jumlah ayat jurnal penyesuaian pada akhir tahun buku.
2. Gejala Kecurangan pada Karyawan atau Pegawai
Gejala kecurangan yang dilakukan oleh karyawan atau pegawai dapat dikenali antara lain yaitu pembuatan ayat jurnal penyesuaian tanpa otorisasi manajemen dan tanpa perincian/penjelasan pendukung, melakukan pengeluaran dokumen pendukung, pencatatan yang salah/tidak akurat pada buku besar, serta terjadi perubahan perilaku dari individu yang melakukan kecurangan. Adapun indikasi adanya pegawai yang melakukan kecurangan dapat dilihat dari beberapa kondisi atau situasi berikut ini:
   a. Perubahan perilaku secara signifikan, seperti: tingkah laku tidak seperti biasanya, bergaya hidup mewah, penggunaan mobil atau pakaian mahal, suka bepergian ke luar negeri, dan lain-lain.
   b. Gaya hidup di atas rata-rata.

c. Sering mengalami trauma emosional di rumah atau tempat kerja.
d. Penjudi berat.
e. Temuan audit atas kekeliruan *(error)* atau ketidakberesan *(irregularities)* dianggap tidak material ketika ditemukan.

Dari indikasi terjadinya praktik kecurangan yang ditunjukkan oleh gejala-gejala tersebut, kita bisa menduga bahwa ada yang tidak beres dengan praktik manajemen keuangan ataupun pelaporan keuangan pada organisasi atau company yang bersangkutan. Dengan demikian, untuk meyakinkan bahwa telah ada aktivitas yang mengarah pada tindakan kecurangan sebaiknya segera dilakukan audit investigasi oleh auditor yang berkompeten dibidang audit investigasi.

Teknik Audit Kecurangan

Audit investigasi diarahkan lebih ke pembuktian ada atau tidak adanya *fraud* dan perbuatan melawan hukum lainnya, oleh karena itu lebih memusatkan kepada 5W (*what, where, when, who, why*) dan 1H (*how*). Audit investigasi juga menggunakan teknik audit yang biasa dilakukan dalam audit laporan keuangan, namun di dalam audit investigasi teknik-teknik audit lebih bersifat eksploratif, mencari "wilayah garapan" atau *probing* (contohnya dengan review analitikal) maupun pendalaman (contohnya dengan konfirmasi atau dokumentasi), sehingga sangat diperlukannya review analitikal pada awal investigasi untuk perbandingan antara apa yang akan dihadapi dengan apa yang layak seharusnya terjadi dan berusaha menjawab sebab terjadinya kesenjangan. Tuanakotta (2015) menyatakan bahwa teknik audit yang lazim dipergunakan dalam aktivitas audit investigasi meliputi hal-hal berikut ini:

1. Memeriksa fisik dan mengamati (*physical examination*)
   Melakukan pemerikasaan fisik, dapat diartikan sebagai penghitungan kembali asset yang berupa uang tunai (mata uang rupiah maupun asing), kertas berharga, persediaan barang, aset tetap, dan barang berwujud lainnya. Mengamati sendiri diartikan sebagai pemanfaatan indera untuk mengetahui sesuatu.
2. Meminta informasi dan konfirmasi (*confirmation*)
   Dalam aktivitas audit investigasi, permintaan konfirmasi harus di barengi, didukung, diperkuat dan dikolaborasikan dengan berbagai informasi dari sumber lain, atau diperkuat dengan cara lain.
3. Memeriksa dokumen (*documentation*)
   Pemeriksaan dokumen pasti dilakukan didalam audit investigatif, tetapi dengan kemajuan teknologi, definisi dokumen menjadi lebih luas, termasuk informasi yang diolah, disimpan dan dipindahkan secara elektronis *(digital).*
4. Review analitikal (*analytical review*)
   a. Menganalisis kemampuan perusahaan yang diaudit dengan membanding-kannya dengan perusahaan saingannya yang seukuran (sepadan) dan melakukan perbandingan dalam perusahaan yang diaudit atas hal yang sama pada masa sekarang dengan masa lalu.
   b. Membandingkan anggaran dengan realisasi dengan perlunya pemahaman mekanisme anggaran, evaluasi atas pelaksanaan anggaran dan insentif (keuangan maupun non-keuangan) yang terkandung dalam sistem anggarannya.
   c. Melakukan analisis vertikal dan horizontal yang merupakan analisis rasio atas laporan keuangan.
   d. Melihat hubungan antara satu data keuangan dengan data keuangan lainnya

dengan melakukan perbandingan antar akun, contohnya penjualan dengan piutang, penjualan dengan rata-rata persedian, dan lainnya.

e. Menggunakan data non-keuangan dengan review analitikal, seperti misalnya mengenal pola hubungan *(relationship-pattern).*

5. Menghitung kembali (reperformance)
   Menghitung kembali tujuannya adalah mengecek kebenaran perhitungan. Dalam audit investigasi, perhitungan yang dihadapi umumnya lebih kompleks dari pada audit laporan keuangan karena didasarkan atas kontrak atau perjanjian yang lebih rumit.

Hubungan Pengendalian Internal dan Kecurangan

Audit internal sangat erat berkaitan dengan masalah pencegahan tindak kecurangan (*fraud)* di dalam suatu organisasi atau perusahaan. Adanya audit internal dalam suatu organisasi atau perusahaan diyakini bermanfaat dalam membantu mencegah terjadinya kecurangan. Namun demikian, audit internal tidak bertanggung jawab atas terjadinya kecurangan, meskipun audit internal merupakan pihak yang memiliki kewajiban yang paling besar dalam masalah pencegahan kecurangan.

Kecurangan *(fraud)* dapat dikurangi bahkan dicegah dengan menciptakan iklim budaya jujur, keterbukaan, dan saling membantu satu sama lain. Selain itu pencegahan kecurangan dapat dihilangkan dengan menghilangkan peluang untuk melakukan kecurangan, misalnya dengan menanamkan kesan bahwa setiap tindakan kecurangan akan mendapat sanksi yang setimpal. Audit internal harus dapat memastikan apakah kecurangan itu memang ada atau tidak. Untuk memastikannya, audit internal akan melakukan evaluasi terhadap sistem pengendalian internal yang dibuat manajemen dan aktivitas karyawan perusahaan berdasarkan kriteria yang tepat untuk merekomendasikan suatu rangkaian tindakan kepada pihak manajemen.

Simpulan

Kecurangan yang terjadi di setiap negara mempunyai jenis yang berbeda-beda karena praktik kecurangan antara lain sangat dipengaruhi oleh kondisi hukum, politik, sosial dan budaya di negara yang bersangkutan. Negara dengan penegakan hukum yang sudah berjalan baik dan kondisi ekonomi masyarakat secara umum cukup atau lebih dari cukup, cenderung memiliki lebih sedikit modus operandi praktik kecurangan.

Kesempatan urttuk melakukan kecurangan berasal dari tidak adanya fungsi pengawasan yang mencukupi di dalam perusahaan. Selain itu, keberadaan fungsi pengawasan tersebut tidak dengan sendirinya menjamin dapat dideteksinya terjadinya perbuatan-perbuatan kecurangan, namun fungsi pengawasan tersebut juga arus dijalankan secara efektif. Disamping itu, perlu adanya penegakan supremasi hukum dengan membawa pihak-pihak yang seandainya terbukti melakukan kecurangan diproses secara hukum untuk memberikan efek jera atas perbuatan yang dilakukan.

Contoh Kasus

PT KF melakukan release laporan keuangan perusahaan per 31 Desember 2001, dengan melaporkan adanya laba bersih sebesar Rp.132 Milyar. Laporan keuangan.tersebut di audit oleh Hans Tuanakotta & Mustofa. Kementerian BUMN dan Bapepam menilai bahwa laba bersih tersebut terlalu besar dan mengandung unsur rekayasa sehingga dilakukan audit ulang oleh auditor yang sama tetapi berbeda partner. Pada 3 Oktober

2002 laporan keuangan PT KF untuk periode 2001 disajikan kembali *(restated)*, karena telah ditemukan kesalahan yang cukup mendasar. Pada laporan keuangan yang baru, keuntungan yang disajikan hanya sebesar Rp.99,56 miliar, atau lebih rendah sebesar Rp.32,6 milyar, atau 24,7% dari laba awal yang dilaporkan. Berdasarkan hasil pemeriksaan Bapepam (pada waktu itu) diperoleh bukti sebagai berikut:
Terdapat kesalahan penyajian dalam laporan keuangan PT. KF, yang mengakibatkan *overstated* laba pada laba bersih untuk tahun yang berakhir 31 Desember 2001 sebesar Rp.32,7 milyar, yang merupakan 2,3% dari penjualan, dan 24,7% dari laba bersih PT. KF. Kesalahan-kesalahan tersebut terdiri atas:

1. Kesalahan berupa *overstated* pada unit industri bahan baku:
   a. Unit industri bahan baku, kesalahan berupa overstated pada penjualan sebesar Rp.2,7 miliar.
   b. Unit logistik sentral, kesalahan berupa overstated pada persediaan barang sebesar Rp.23,9 miliar.
   c. Unit pedagang besar farmasi (PBF), kesalahan berupa overstated pada persediaan barang sebesar Rp.8,1 miliar.
2. Kesalahan berupa overstated pada penjualan sebesar Rp.10,7 miliar.
   Kesalahan-kesalahan penyajian tersebut dilakukan oleh Direksi periode 1998 – Juni 2002 dengan cara:
   a. Membuat dua daftar harga persediaan yang berbeda masing-masing diterbitkan pada tanggal 1 Februari 2002 dan 3 Februari 2002, dimana keduanya merupakan master price yang telah diotorisasi oleh pihak yang berwenang yaitu Direktur Produksi PT KF. Master price per-3 Februari 2002 merupakan master price yang telah disesuaikan nilainya *(mark up)* dan dijadikan dasar sebagai penentuan nilai persediaan pada unit distribusi PT KF per 31 Desember 2001.
   b. Melakukan pencatatan ganda atas penjualan pada unit PBF dan unit bahan baku. Pencatatan ganda dilakukan pada unit-unit yang tidak disampling oleh akuntan.
      Sehubungan dengan temuan tersebut, maka sesuai dengan Pasal 102 Undang-undang Nomor 8 tahun 1995 tentang Pasar Modal jo Pasal 61 Peraturan Pemerintah Nomor 45 tahun 1995 jo Pasal 64 Peraturan Pemerintah Nomor 45 tahun 1995 tentang Penyelenggaraan Kegiatan di Bidang Pasar Modal maka PT KF dikenakan sanksi administratif berupa denda yaitu sebesar Rp 500.000.000,- (lima ratus juta rupiah).

Sesuai Pasal 5 huruf n Undang-Undang No.8 Tahun 1995 tentang Pasar Modal, maka:

1. Direksi Lama PT KF (Persero) Tbk. periode 1998 – Juni 2002 diwajibkan membayar sejumlah Rp.1.000.000.000,- (satu miliar rupiah) untuk disetor ke Kas Negara, karena melakukan kegiatan praktek penggelembungan atas laporan keuangan per 31 Desember 2001.
2. Sdr. LSW, Rekan KAP HTM selaku auditor PT KF (Persero) Tbk. diwajibkan membayar sejumlah Rp.100.000.000,- (seratus juta rupiah) untuk disetor ke Kas Negara, karena atas risiko audit yang tidak berhasil mendeteksi adanya penggelembungan laba yang dilakukan oleh PT KF (Persero) Tbk. tersebut, meskipun telah melakukan prosedur audit sesuai dengan Standar Profesional Akuntan Publik (SPAP), dan tidak diketemukan adanya unsur kesengajaan. Tetapi, KAP HTM tetap diwajibkan membayar denda karena dianggap telah gagal menerapkan Persyaratan Profesional yang disyaratkan di SPAP SA Seksi 110 – Tanggung Jawab & Fungsi Auditor Independen, paragraf 04 Persyaratan Profesional, dimana disebutkan bahwa persyaratan profesional yang dituntut dari auditor independen adalah orang yang memiliki pendidikan dan pengalaman berpraktik sebagai auditor independen.

Faktor penyebab dilakukan kecurangan laporan keuangan dalam kasus tersebut dilandasi hal-hal sebagai berikut:

- Untuk menarik investasi melalui penjualan saham
- Untuk mendapatkan bonus yang berhubungan dengan kinerja perusahaan
- Untuk menunjukkan adanya kenaikan laba bersih sehingga kinerja perusahaan terlihat baik.

Daftar Bacaan

Amiram, D., Bozanic, Z., Cox, J.D., Dupont, Q., Karpoff, J.M. & Sloan, R. (2018). Financial reporting fraud and other forms of misconduct: A multidisciplinary review of the literature. *Review of Accounting Studies*, (23), 732-783.

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C. & Zimbelman, M.F. (2011). *Fraud Examination*. South Western: Cengage Learning. E-Book.

Amrizal. (2004), *Pencegahan dan Pendeteksian kecurangan oleh internal auditor*. BPKP. (31 Januari 2012).

Baesens, B., Vlasselaer, V.V and Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques*, New Jersey: John Wiley and Sons.

Eissa, A., Wells. C. & Rudolf, N. (2014). *Fraud: A Practitioner's Handbook*. London: Bloomsbury Publishing. PLS.

Elisabeth, P. & Casey, E. (2017). An intelligence led approach to addressing cyber fraud: Proactive fraud auditing. *Journal of Financial Compliance*, 1 (1), 64-71.

Osadchy, E. A., Akhmetshin, E. M., Amirova, E. F., Bochkareva, T. N., Gazizyanova, Yu. Yu., & Yumashev, A. V. (2018). Financial statements of a company as an information base for decision-making in a transforming economy. *European Research Studies Journal*, 21(2), 339-350.

Tuanakotta, T. M. (2015). *Akuntansi Forensik dan Audit Investigatif*, Ed.2. Jakarta: Salemba Empat.

BAB 3
PENCUCIAN UANG

Pendahuluan

Tindak pidana pencucian uang atau yang sering disebut juga dengan *"money laundry"* merupakan salah satu jenis tindak pidana *white collar crime* atau kejahatan kerah putih, dimana tindak pidana pencucian uang ini merupakan kelanjutan dari kejahatan-kejahatan lain, yang biasanya dilakukan oleh perorangan maupun korporasi dalam batas wilayah suatu negara maupun yang dilakukan melintasi batas wilayah lain. Kejahatan-kejahatan yang lain tersebut di atas antara lain berupa tindak pidana korupsi, penyuapan, penyelundupan barang, penyelundupan tenaga kerja, penyelundupan imigran, baik dalam bidang Perbankan, bidang pasar modal, bidang asuransi, narkotika, psikotropika, perdagangan manusia, perdagangan senjata gelap, penculikan, terorisme, pencurian, penggelapan, penipuan, pemalsuan uang, perjudian, prostitusi, di bidang perpajakan, di bidang kelautan, di bidang lingkungan hidup, dan kemungkinan juga tindak pidana lainnya. Hasil tindak pidana tersebut menghasilkan harta kekayaan yang sangat besar jumlahnya. Hasil dari harta kekayaan yang berasal dari berbagai kejahatan tersebut pada umumnya tidak langsung dibelanjakan atau digunakan oleh pelaku kejahatan, karena apabila langsung digunakan akan mudah dilacak oleh aparat penegak hukum.

Pada umumnya, para pelaku tindak pidana pencucian uang terlebih dahulu mengupayakan menyimpan harta kekayaan hasil tindak pidana tersebut ke dalam suatu sistem keuangan, terutama ke dalam sistem perbankan, yang diharapkan dapat menyembunyikan atau menyamarkan asal usul harta kekayaan yang diperoleh dari tindak pidana, sehingga tidak dapat dilacak oleh penegak hukum. Karena harta kekayaan hasil kejahatan tersebut bagi organisasi kejahatan ibarat darah dalam satu tubuh, dimana apabila aliran harta kekayaan melalui sistem perbankan Internasional yang dilakukan diputus, maka organisasi kejahatan tersebut lama kelamaan akan menjadi lemah, berkurang aktivitasnya, bahkan menjadi mati. Oleh sebab itu, bagi organisasi kejahatan ada dorongan untuk melakukan pencucian uang agar asal usul harta kekayaan yang sangat dibutuhkannya tersebut sulit atau tidak dapat dilacak oleh penegak hukum.

Pengertian Pencucian Uang

Menurut UU No. 25/ 2003 Pasal 1 ayat (1) ***Pencucian Uang*** merupakan perbuatan menempatkan, mentransfer, membayarkan, membelanjakan, menghibahkan, menyumbangkan, menitipkan, membawa keluar negeri, menukarkan, atau perbuatan

lainnya atas harta kekayaan yang diketahuinya atau patut diduga merupakan hasil tindak pidana dengan maksud untuk menyembunyikan, atau menyamarkan asal-usul harta kekayaan sehingga seolah-olah menjadi harta kekayaan yang sah.

Departemen Kehakiman A.S. mendefinisikan pencucian uang sebagai "proses dimana seseorang menyembunyikan keberadaan, sumber ilegal, atau aplikasi pendapatan ilegal dan kemudian menyamarkan pendapatan itu agar membuatnya tampak sah". Ungkapan *'pencucian uang'* menyiratkan bahwa uang yang *'kotor'* karena dihasilkan secara ilegal adalah *'dicuci'*, atau dibuat terlihat bahwa itu berasal dari sumber yang sah atau legal. Berbagai transaksi digunakan untuk mengambil uang ini yang berasal secara ilegal melalui proses dimana asal usul uang dan rincian transaksi menjadi terpisah dari aktivitas ilegal (Masciandaro, 2017).

Sebagaimana definisi di muka, secara umum dapat kita pahami bahwa pencucian uang ialah suatu kegiatan illegal untuk menutupi kejahatan lain yang sebenarnya dari hasil mengambil sejumlah material (yang dapat diukur dalam satuan uang) untuk tujuan tertentu. Hal ini sejalan dengan pendapat Ackerman & Palifka (2018) yang menyatakan bahwa dana-dana dari hasil tindak kejahatan biasanya disamarkan, disembunyikan atau direkayasa seolah-olah berasal dari kegiatan yang legal.

Undang-Undang Terkait dengan Pencucian Uang

Seperti yang telah disebutkan pada bagian definisi bahwa pencucian uang merupakan suatu bentuk perbuatan illegal, pastinya perbuatan ini tergolong dalam tindak pidana untuk ranah hukum. Oleh karena itu terdapat undang- undang yang dibuat kebijakan khusus untuk membuat pelaku pencucian uang diproses secara hukum. Tindak pidana itu sendiri merupakan segala sesuatu yang melanggar hukum atau sebuah tindak kejahatan. Pelaku kriminalitas disebut seorang kriminal. Biasanya yang dianggap kriminal adalah seorang pencuri, pembunuh, perampok, atau teroris.

Berikut adalah Undang-Undang Pencucian Uang (di Indonesia) yang menjadi acuan tentang pencucian uang yaitu UU No. 15 tahun 2002 yang kemudian direvisi menjadi UU No. 25 Tahun 2003. Adapun UU Pencucian uang membahas tentang: Ketentuan Umum Tindak Pidana Pencucian Uang, tentang Pusat Pelaporan dan Analisis Transaksi (PPATK) serta tentang *Know Your Customer Principles* (KYC). Namun perlu diketahui bahwa Undang-Undang Pencucian Uang di Indonesia diatur dalam UU No. 15/2002 dan kemudian dilakukan revisi menjadi UU No. 25/2003. Tentunya ketika revisi ini akan dilakukan memiliki tujuan agar kebijakan hukum yang mengatur seputar pencucian uang dapat lebih spesifik dan memiliki kompleksitas penangan hukum lebih maksimal serta akan memberikan manfaat positif terhadap pertahanan dan keamanan negara terkait pencucian uang. Berikut ini merupakan tabel olahan tentang Undang-Undang Pencucian Uang yang direvisi:

Tabel 1. Undang-Undang tentang Pencucian Uang Sebelum dan Setelah Revisi

UU No 15 Thn 2002 Tindak Pidana Pencucian Uang	UU Pencucian Uang Yang Telah Direvisi
Pasal 1 ayat 4 Penyedia Jasa Keuangan adalah setiap orang yang menyediakan jasa di bidang keuangan termasuk tetapi tidak terbatas pada bank, lembaga pembiayaan, perusahaan efek, pengelola reksa dana, kustodian, wall amanat, lembaga penyimpanan dan penyelesaian, pedagang valuta asing, dana pensiun, dan perusahaan asuransi.	**Pasal 1 ayat 1** Penyedia Jasa Keuangan yaitu perbuatan menempatkan, mentransfer, membayarkan, membelanjakan, menghibahkan, menyumbangkan, menitipkan, membawa keluar negeri, menukarkan atau perbuatan lainnya atas harta kekayaan yang diketahuinya atau patut diduga merupakan hasil tindak pidana dengan maksud untuk menyembunyikan, atau menyamar asal usul harta kekayaan sehingga seolah-olah menjadi harta kekayaan yang sah

UU No 15 Thn 2002 Tindak Pidana Pencucian Uang	UU Pencucian Uang Yang Telah Direvisi
Pasal 1 ayat 6 Transaksi keuangan mencurigakan merupakan transaksi yang menyimpang dari profil dan karakteristik serta kebiasaan pola transaksi dari nasabah yang bersangkutan, termasuk transaksi keuangan oleh nasabah yang patut diduga dilakukan dengan tujuan untuk menghindari pelaporan transaksi yang bersangkutan yang wajib dilakukan oleh Penyedia Jasa Keuangan sesuai dengan ketentuan Undang-undang ini.	**Pasal 1 ayat 7** Transaksi keuangan mencurigakan adalah: a. transaksi keuangan yang menyimpang dari profil, karakteristik, atau kebiasaan pola transaksi dari nasabah yang bersangkutan; b. transaksi keuangan oleh nasabah yang patut diduga dilakukan dengan tujuan untuk menghindari pelaporan transaksi yang bersangkutan yang wajib dilakukan oleh Penyedia Jasa Keuangan sesuai dengan ketentuan Undang-Undang ini; atau c. transaksi keuangan yang dilakukan atau batal dilakukan dengan menggunakan Harta Kekayaan yang diduga berasal dari hasil tindak pidana.
	Pasal 1 ayat 8 Transaksi keuangan yang dilakukan secara tunai adalah transaksi penarikan, penyetoran, atau penitipan yang dilakukan dengan uang tunai atau instrumen pembayaran lain yang dilakukan melalui Penyedia Jasa Keuangan
Pasal 2 Hasil tindak pidana adalah Harta Kekayaan yang berjumlah Rp 500.000.000,00 (lima ratus juta rupiah) atau lebih atau nilai yang setara, yang diperoleh secara langsung atau tidak langsung dari kejahatan: a. korupsi; b. penyuapan; c. penyelundupan barang; d. penyelundupan tenaga kerja; e. penyelundupan imigran; f. perbankan; g. narkotika; h. psikotropika; i. perdagangan budak, wanita, dan anak; j. perdagangan senjata gelap; k. penculikan; l. terorisme; m. pencurian; n. penggelapan; o. penipuan, yang dilakukan di wilayah Negara Republik Indonesia atau di luar wilayah Negara Republik Indonesia dan kejahatan tersebut juga merupakan tindak pidana menurut hukum Indonesia.	**Pasal 2** Hasil tindak pidana adalah Harta Kekayaan yang diperoleh dari tindak pidana: a. korupsi; b. penyuapan; c. penyelundupan barang; d. penyelundupan tenaga kerja; e. penyelundupan imigran; f. di bidang perbankan; g. di bidang pasar modal; h. di bidang asuransi; i. narkotika; j. psikotropika; k. perdagangan manusia; l. perdagangan senjata gelap; m. penculikan; n. terorisme; o. pencurian; p. penggelapan; q. penipuan; r. pemalsuan uang; s. perjudian; t. prostitusi; u. di bidang perpajakan; v. di bidang kehutanan; w. di bidang lingkungan hidup; x. di bidang kelautan; atau y. tindak pidana lainnya yang diancam dengan pidana penjara 4 (empat) tahun atau lebih, yang dilakukan di wilayah Negara Republik Indonesia atau di luar wilayah Negara Republik Indonesia dan tindak pidana tersebut juga merupakan tindak pidana menurut hukum Indonesia.
	Pasal 2 ayat 2 Harta Kekayaan yang dipergunakan secara langsung atau tidak langsung untuk kegiatana terorisme dipersamakan sebagai hasil tindak pidana sebagaimana dimaksud pada ayat (1) huruf n.

Sifat Money Laundering

1. Pemilihan Tempat *Money Laundering*
   Ketika *money laundering* dilakukan, pelaku tidak melakukannya melalui jalur khusus yang dibuat melainkan pelaku melakukannya dengan melihat *'peluang'* yang dapat menciptakan *'kesan legal'* untuk mencuci uang agar tidak menimbulkan kecurigaan kepada pihak-pihak tertentu. Apabila pihak-pihak tertentu tersebut mengetahui (pihak tersebut dapat berupa aparat hukum negara) menjadi *boomerang* bagi pelaku, maka untuk itu pelaku biasanya menggunakan jasa lembaga-lembaga tertentu.

   Seperti yang diungkapkan Kartika (2019) mengenai sektor-sektor potensial yang digunakan oleh pelaku untuk melakukan perbuatan pencucian uang mereka pada umumnya meliputi sektor-sektor berikut: sektor perbankan, pasar modal, dan lembaga keuangan non-bank dengan memanfaatkan dan menggunakan jasa- jasa dan *instrument* yang ditawarkan, dan inilah yang dianggap oleh pelaku sebagai peluang untuk melakukan pencucian uang *(money laundering)*.
2. Pelaku *Money Laundering*
   Pelaku aktivitas *money laundering* secara potensial dapat dilakukan oleh siapa saja ataupun kelompok-kelompok manapun. Hal ini dikarenakan hasil dari pencucian uang 'memberikan hasil' yang tidak sedikit bagi para pelaku. Sebagaimana menurut Masciandaro (2017) bahwa organisasi bisnis dan individu dapat mencuci uang melalui transaksi kompleks yang melibatkan jaringan perusahaan *'shell'* atau kepercayaan yang sering berbasis di luar negeri. Pada umumnya, penjahat yang melakukan aktivitas pencucian uang adalah pedagang obat bius, penggelapan, politisi korup dan pejabat publik, mafia, teroris, dan penipu. Dengan demikian, pencucian uang tidak hanya terkait dengan pengedar narkoba dan mafia, tetapi juga dengan individu maupun organisasi yang menonjol yang sangat terhormat di mata masyarakat.
3. Proses *Money Laundering*
   Sebagaimana menurut Albrecht *et al.* (2011: 583) terdapat tiga tahap ketika proses pencucian uang dilakukan, meliputi:
   a. Tahap Penempatan (*Placement*)
      Pada tahap penempatan, pencucian menyisipkan "uang kotor" ke lembaga keuangan yang sah. Pada umumnya, tindakan ini melibatkan pembuatan setoran tunai ke bank. Hal ini seringkali merupakan tahap paling mengerikan dari proses pencucian uang karena setoran tunai yang sangat besar menimbulkan bendera merah dan bank diminta untuk melaporkan rincian mengenai transaksi tunai besar kepada pemerintah.
   b. Tahap Layering
      Tahap *layering* adalah langkah paling kompleks dalam skema pencucian uang. Tujuan dari tahap ini adalah membuat uang kotor sulit dilacak. *Layering* melibatkan berbagai transaksi keuangan sehingga sulit untuk mengikuti arus dana. Lapisan dapat terdiri dari aktivitas seperti membuat transfer kawat antar rekening yang berada di negara yang berbeda dengan nama yang berbeda. Ini juga termasuk aktivitas membuat banyak transfer bank-ke-bank, membuat simpanan dan penarikan untuk terus memvariasikan jumlah uang di rekening, menukarkan uang ke mata uang baru, dan membeli barang bernilai tinggi (misalnya rumah, mobil, perhiasan, dan lainnya) untuk mengubah bentuk aset.
   c. Tahap Integrasi (Integration)
      Sampai pada tahapan ini, uang masuk kembali ke ekonomi arus utama dalam bentuk yang tampak sah, sehingga tampaknya berasal dari transaksi yang legal.

Transaksi ini mungkin melibatkan penjualan aset lain (misalnya: perkebunan, real estate, pertambangan, dan lainnya) yang dibeli selama tahap *layering* atau memberikan dana ke bisnis dimana si pelaku pencucian seharusnya "berinvestasi". Begitulah uang/dana tersebut diperkenalkan kembali sebagai sesuatu yang "bersih" ke dalam arus ekonomi. Pencucian uang bisa menggunakan dana untuk konsumsi pribadi. Jika jejak dokumen dari tahap sebelumnya tidak ada, sangat sulit untuk mengungkap skema pencucian di tahap integrasi. Pada gambar 4 berikut ini dijelaskan ilustrasi yang mendeskripsikan tahap-tahap dari proses pencucian uang.

Gambar 6. Tahapan Proses Pencucian Uang

Dampak *Money Laundering* (Bagi Negara)

Dikarenakan pencucian uang merupakan tindakan yang dilakukan oleh pelaku *money laundering* atas hasil yang diperoleh melalui tindakan-tindakan sebagaimana disebutkan dalam UU No. 23/2003 pada BAB I pasal 2 ayat (1) hasil tindak pidana yang dilakukan *money laundering* berasal dari: korupsi, penyuapan, penyelundupan barang, penyelundupan tenaga kerja, penyelundupan imigran, bidang perbankan, bidang pasar modal, bidang asuransi, narkotika, psikotropika, perdagangan manusia, perdagangan senjata gelap, penculikan, terorisme, pencurian, penggelapan, penipuan, pemalsuan uang, perjudian, prostitusi, bidang perpajakan, bidang kehutanan, bidang lingkungan hidup dan bidang kelautan. Oleh karena itu, tentunya dampak yang ditimbulkan meliputi segala hal terutama yang berkaitan dengan segala bentuk tindak pidana yang telah dilakukan dari bermacam-macam bentuk tindak pidana berdasarkan pasal 2 tersebut.

Namun demikian, untuk lebih spesifik maka dampak dari pencucian uang dapat digambarkan melalui salah satu peristiwa (tingkat internasional) yang mana Indonesia mengalami dampak dari prosedur yang seharusnya dimiliki oleh suatu negara ketika lingkup globalisasi telah menetapkan suatu mekanisme khusus menanggapi perihal

pencucian uang menjadi permasalahan global. Berikut ilustrasi dampak yang dirasakan oleh pemerintah Indonesia:

Pada Bulan Juni 2001 Indonesia dimasukkan ke dalam daftar *Non-Cooperative Countries and Territories* (NCCTs) bersama-sama 19 negara lainnya. Kelemahan yang disoroti oleh *Financial Action Task Force* (FATF) adalah tidak adanya undang-undang yang menetapkan pencucian uang sebagai tindak pidana, tidak adanya ketentuan 'Prinsip Mengenal Nasabah' atau *Know Your Customer Priciples* (KYC) untuk lembaga keuangan non-bank, rendahnya kualitas SDM dalam penanganan kejahatan pencucian uang dan kurangnya kerjasama internasional. Dimasukannya Indonesia dalam daftar NCCTS mendorong pemerintah mengambil langkah-langkah untuk mengatasi kelemahan yang telah disoroti oleh FATF. Pemerintah Indonesia selanjutnya mengesahkan UU No. 15/ tahun 2002 tentang Tindak Pidana Pencucian Uang. Pemerintah juga telah mengeluarkan ketentuan KYC bagi lembaga keuangan non bank termasuk perusahaan sekuritas. Bank Indonesia juga telah menyempurnakan ketentuan KYC utuk perbankan dengan mengeluarkan pedoman standar yang wajib menjadi acuan perbankan (Tuanakotta, 2014).

Dari kejadian di atas tampak bahwa permasalahan tentang tindak pidana pencucian uang memiliki dampak bagi suatu negara khususnya bagi Indonesia.Hal ini berkenaan dengan segala bentuk transaksi yang bersifat multilateral. Sebagaimana menurut Martha *et al.* (2010: 78-79) "kita mengklasifikasikan orang lain ke dalam kelompok-kelompok dan kita juga mengklasifikasikan diri kita sendiri ke dalam kelompok-kelompok". Kelompok-kelompok yang menjadi anggotanya disebut *in-groups* dan kelompok yang tidak menjadi anggota kelompoknya disebut *out-groups.* Sebelum kategorisasi, misalnya individu-individu tidak pernah memikirkan diri mereka sebagai seorang anggota dari sebuah kelompok yang cenderung merendahkan, atau bahwa orang lainnya adalah anggota-anggota dari sebuah kelompok yang meninggikan. Lebih lanjut tidak ada peluang bagi kelompok- kelompok ini untuk saling berinteraksi, sehingga menghilangkan segala kemungkinan bahwa anggota-anggota kelompok akan jadi menyukai *in-groups* dan tidak menyukai *out-groups.*

Lembaga Yang Menangani *Money Laundering*

Permasalahan mengenai tindak pidana pencucian uang perlu ditangani agar suatu negara mampu meminimalisir tindak pidana ini. Klasifikasi lembaga yang menangani tindak pidana pencucian uang dibagi menjadi dua skala, meliputi:

1. Skala Internasional

   Menurut Imron & Yulianti (2019) di tingkat internasional, upaya melawan kegiatan pencucian uang dilakukan dengan membentuk *Financial Action Task Force* (FATF) *on Money Laundering* dalam G- 7 Summit di Perancis pada Bulan Juli 1989. FATF saat ini beranggotakan 29 negara/territorial ditambah dua organisasi regional yaitu *The European Commision* dan *The Gulf Cooperation Council* yang mewakili pusat-pusat keuangan terutama di Amerika, Eropa dan Asia. Salah satu peran FATF adalah menetapkan kebijakan dan langkah yang diperlukan untuk melawan pencucian uang. FATF mengeluarkan berbagai rekomendasi pencegahan dan pemberantasan pencucian uang dan rekomendasi khusus untuk memberantas pembiayaan terorisme.

   Rekomendasi tersebut diakui berbagai negara sebagai standar internasional dalam memberantas kegiatan pencucian uang. Negara-negara yang berdasarkan penilaian FATF tidak memenuhi rekomendasi tersebut dimasukkan dalam daftar *Non-Cooperative Countries and Territories* (NCCTs). Negara yang masuk dalam

NCCTs dapat dikenakan *counter measures*, misalnya berupa penolakan *Letter of Credit* yang diterbitkan di negara yang terkena *counter measures*.

2. Skala Nasional

Khusus negara Indonesia tindak pidana pencucian uang ditangani oleh suatu lembaga independen yang didirikan untuk menangani hal tersebut. Adapun lembaga yang menangani pencucian uang di Indonesia terbagi menjadi:

a. Lembaga Khusus (PPATK)

Sebagaimana menurut Purnomo (2017) di Indonesia lembaga yang bertugas menangani Pencucian Uang ialah Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) yang dibentuk sebagai lembaga independen dalam melaksanakan tugas dan kewenangannya untuk mecegah dan memberantas tindak pidana pencucian uang. Berikut ini merupakan beberapa tugas dari PPATK:

1) Mengumpulkan, menyimpan, menganalisis, dan mengevaluasi informasi yang diperoleh oleh PPATK.
2) Memantau catatan dalam buku daftar pengecualian yang dibuat oleh penyedia jasa keuangan.
3) Membuat pedoman mengenai tata cara pelaporan transaksi keuangan yang mencurigakan.
4) Memberi nasehat dan bantuan kepada instansi yang berwenang tentang informasi yang diperoleh oleh PPATK.
5) Mengeluarkan pedoman dan publikasi kepada penyedia jasa keuangan tentang kewajibannya sesuai ketentuan peraturan perundang-undangan dan membantu mendeteksi perilaku nasabah yang mencurigakan.
6) Memberikan rekomendasi/saran/masukan kepada pihak Pemerintah mengenai upaya-upaya yang terkait dengan pencegahan dan pemberantasan tindak pidana pencucian uang.
7) Melaporkan hasil analisis transaksi keuangan yang berindikasi tindak pidana pencucian uang kepada kepolisian dan kejaksaan.
8) Membuat dan memberikan laporan mengenai hasil analisis transaksi keuangan dan kegiatan lainnya enam bulan sekali kepada Presiden, Dewan Perwakilan Rakyat dan lembaga yang berwenang melakukan pengawasan terhadap penyedia jasa keuangan.

b. Lembaga Independen Lainnya

Yang dimaksud lembaga independen lainnya di sini ialah Komisi Pemberantasan Korupsi (KPK). Karena KPK termasuk ke dalam lembaga independen negara yang menangani kasus pencucian uang.

Secara lebih khusus pada lembaga independen lainnya, muncul adanya "sosok profesi" yang disebut dengan Akuntan Forensik. Dalam beberapa literature dapat digarisbawahi bahwa peran akuntan forensik pada sebuah lembaga independen seperti KPK untuk melakukan investigasi terhadap suatu kasus pencucian uang dengan menggunakan suatu metode yang dikenal dengan sebutan *'follow the money'*. Pada hakikatnya teknik investigasi untuk mengungkap kasus pencucian uang ini secara merata digunakan pada lembaga independen di negara manapun.

Tuanakotta (2014: 373) menjelaskan bahwa *follow the money* secara harfiah berarti "mengikuti jejak-jejak yang ditinggalkan dalam suatu arus uang atau arus dana". Jejak-jejak ini membawa penyidik atau akuntan forensik ke arah pelaku *fraud*. Ketentuan perundang-undangan mengenai tindak pidana pencucian uang mengingatkan kita bahwa bukan kejahatan utamanya saja (seperti korupsi, penyuapan, penyeludupan barang dan manusia, pencurian, prostitusi, terorisme

dan lain-lain) yang merupakan tindak pidana, tetapi juga pencucian uangnya adalah tindak pidana. Teknologi informasi merupakan faktor yang sangat menetukan dalam teknik *follow the money*, lebih tepatnya teknologi informasi yang disebut computer forensik.

c. Lembaga Keuangan (Bank dan Non-Bank)
Menurut Setiawan (2018) sistem pada lembaga keuangan sangat rawan bagi kegiatan pencucian uang. Mengingat perbankan paling dominan dalam sistem keuangan Indonesia, maka penanganan sistem perbankan dari kegiatan pencucian uang perlu mendapat perhatian khusus. Untuk itu Bank Indonesia pada tanggal 12 Mei 1999 mengeluarkan ketentuan yang melarang setoran modal bank dengan menggunakan dana yang berasal dari dana untuk tujuan pencucian uang. Ketentuan setoran modal dimaksud berlaku baik bagi dalam rangka pendirian bank baru maupun tambahan setoran modal. Dalam penerapannnya, ketentuan ini mewajibkan investor membuat surat pernyataan bahwa dana untuk setoran modal atau tambahan setoran modal bank tidak berasal dari atau untuk tujuan pencucian uang.

Selanjutya tanggal 18 Juni 2001, Bank Indonesia mengeluarkan ketentuan Prinsip Mengenal Nasabah atau *Know Your Customer Principles* (KYC) yang mewajibkan bank untuk mengenal profil dan karakteristik transaksi nasabahnya sebagai uapaya awal mencegah bank digunakan sebagai sarana pencucian uang. Hal ini sejalan dengan prinsip-prinsip prudential banking berdasarkan *Basle Core Principles for Effective Banking Supervision*, yang mana merupakan praktek internasional yang mewajibkan bank-bank memiliki pedoman manajemen risiko.

Risiko yang akan terjadi apabila bank dimanfaatkan untuk sarana pencucian uang meliputi risiko operasional, risiko hukum, risiko konsentrasi dan risiko reputasi. Pada bulan Januari 2003 Departemen Keuangan dan Badan Pengawas Pasar Modal mengeluarkan ketentuan KYC bagi Lembaga Keuangan Non-Bank yang berada di bawah pengawasan instansi tersebut. Departemen Keuangan (Direktorat Jenderal Lembaga Keuangaan) memiliki kewenangan pengawasan terhadap perusahaan asuransi, dana pension, lembaga pembiayaan dan pegadaian. Sedangkan BAPEPAM mengawasi perusahaan efek (saat ini OJK), pengelola reksa dana dan *custodian*. Pada Bulan Desember 2001 Bank Indonesia menyempurnakan ketentuan KYC dengan standar minimum yang wajib dijadikan acuan bank-bank di Indonesia. Peraturan mengenai KYC mewajibkan para penyedia jasa keuangan untuk menetapkan kebijakan dan prosedur mengenai penerimaan dan identifikasi calon nasabah, pemantauan rekening dan transaksi nasabah serta manajemen risiko.

Penyedia jasa keuangan juga diwajibkan menyampaikan laporan transaksi keuangan mencurigakan (*Suspicious Transaction Reports*) disingkat TSR, yaitu transaksi yang menyimpang dari profil dan karakteristik serta kebiasaan pola transaksi nasabah. Penyedia jasa keuangan wajib meyampaikan laporan transaksi keuangan secara tunai (*Cash Transaction Reports*) disingkat CTR untuk transaksi RP 500 juta ke atas. STR dan CTR disampaikan kepada PPATK. Berdasarkan STR dan CTR akan dievaluasi dan dianalisis oleh PPATK. Apabila dijumpai indikasi pelanggaran pidana, PPATK akan meneruskannya kepada Kepolisian dan Kejaksaan (sebagai lembaga penyidik) untuk dilakukan penyidikan.

Simpulan

Tindak pidana pencucian uang merupakan kejahatan yang dapat merusak citra negara. Baik citra negara pada skala nasional bahkan skala internasional. Dengan demikian, kebutuhan akan pengusutan tuntas tindak pidana ini memerlukan sumber daya manusia yang produktif serta berwawasan tinggi untuk melakukan pemberantasan terhadap tindak pidana pencucian uang. Selain itu hubungan internasional dalam mengusut tindak pidana pencucian uang sangat diperlukan sebagai power dalam menangani kasus-kasus pencucian uang yang mana dari tindakan ini akan berkaitan dengan tindak pidana lainnya.

Contoh Kasus

"TCW Gunakan 300 Perusahaan Garap Proyek Pemerintah"

JAKARTA - Tersangka kasus pencucian uang, TCW alias Wawan diduga menggunakan 300 perusahaan untuk menggarap sejumlah proyek pemerintah. Hal itu terungkap dalam proses penyidikan kasus dugaan tindak pidana pencucian uang (TPPU) yang menjadikan TCW sebagai tersangka. "Ada 300 perusahaan yang diduga digunakan TCW untuk menggarap proyek," kata Kabag Pemberitaan dan Publikasi KPK, Priharsa dalam konferensi pers di Gedung KPK, Jakarta, Kamis (10/3).

Priharsa mengatakan, sebagian perusahaan yang digunakan untuk menggarap proyek pemerintah merupakan perusahaan yang sengaja didirikan TCW dengan mengatasnamakan anak buahnya. Sementara sebagian lainnya merupakan perusahaan yang telah berdiri dan TCW hanya meminjam nama untuk ikut proses lelang.

"Sebagian (perusahaan) diatasnamakan anak buahnya, dan sebagian pinjam bendera," ungkapnya.

Diungkapkan Priharsa, ratusan perusahaan tersebut digunakan TCW untuk menggarap berbagai proyek di Banten. Tak hanya proyek yang menggunakan milik Pemprov Banten, perusahaan-perusahaan ini juga menggarap sejumlah proyek pemerintah pusat di Banten. Meski demikian, Priharsa mengaku belum mengetahui secara pasti total nilai dari proyek-proyek yang digarap TCW dengan menggunakan ratusan perusahaan tersebut.

"Nilai (proyeknya) belum tahu karena belum dapat info dari penyidik. Ini masih didalami," jelasnya.

Untuk mengusut hal ini, penyidik telah memeriksa sejumlah nama yang berkaitan dengan ratusan perusahaan tersebut. Penyidik juga memanggil sejumlah nama untuk mengusut jual beli tanah dan mobil.

"Beberapa nama yang kami panggil adalah nama yang digunakan untuk buat perusahaan dan menggarap proyek Pemprov Banten dan instansi vertikal di Provinsi Banten. Penyidik juga fokus ke beberapa nama yang berkaitan transaksi tanah dan jual beli mobil," paparnya. Kemarin, penyidik KPK memanggil 12 nama sebagai saksi untuk mengusut kasus TPPU TCW. Mereka adalah MA (pihak swasta), YMK (swasta), MLI (swasta), ICR (swasta), JL (swasta), AS (Direktur PT. Dini Usaha Mandiri), ASH (Direktur CV. Radefa), ASHD (pemilik PT. Dini Usaha

Mandiri), RA (Direktur. PT. Palugada Mandiri), YS (Direktur PT. Adca Mandiri), dan TA (Direktur PT Sumber Agung Putra), serta FAS (karyawan PT. Plaza Otoprima).

Kasus pencucian uang merupakan pengembangan penyidikan kasus dugaan suap sengketa Pilkada Lebak Banten di MK yang menjerat TCW sebelumnya. Tak hanya itu, TCW juga menjadi tersangka kasus dugaan korupsi pengadaan alat kesehatan di Tangerang Selatan, serta pengadaan alkes di Pemerintah Provinsi Banten.

Dalam kasus pencucian uang ini, TCW disangka melanggar Pasal 3 dan Pasal 4 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Selain itu, TCW juga dijerat dengan Pasal 3 Ayat (1) dan atau Pasal 6 Ayat (1) serta UU Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang junto Pasal 55 Ayat 1 ke-1 KUHP. (sumber: https://www.kpk.go.id)

Daftar Bacaan

Ackerman S.R., Palifka B.J. (2018) Corruption, Organized Crime, and Money Laundering. In: Basu K., Cordella T. (eds) Institutions, Governance and the Control of Corruption. *International Economic Association Series*. Palgrave Macmillan, Cham.

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C. & Zimbelman, M.F. (2011). *Fraud Examination*. South Western: Cengage Learning.

Depag RI. (1987). *Al-Qur'anulkarim*. Bandung: PT. Sygma Examedia Arkanleema. https://www.kpk.go.id

Imron, A. & Yulianti, S. (2019). Penegakan, pencegahan dan pemberantasan tindak pidana pencucian uang atas national risk assessment. *Jurnal Surya Kencana Dua*, 6 (1), 682-711.

Kartika, P.P. (2019). Data elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana pencucian uang. *Indonesian Journal of Criminal Law*, 1 (1), 33-46.

Martha L. C. (2010). *Pengantar Psikologi Politik*. Edisi Kedua. Jakarta: Rajawali.

Masciandaro, D. (2017). *Global Financial Crime: Terrorism. Money Laundering and Offshore Centres*. Global Finance Series. Milan: Routledge.

Presiden Republik Indonesia. (2002). Undang- Undang Republik Indonesia Nomor 15 Tentang Tindak Pidana Pencucian Uang. Jakarta.

Presiden Republik Indonesia. (2003). Undang- Undang Republik Indonesia Nomor 25 Tentang Tindak Pidana Pencucian Uang. Jakarta.

Presiden Republik Indonesia. (2010). Undang- Undang Republik Indonesia Nomor 8 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Jakarta.

Purnomo, B.H. (2017). The role of internal audit in governance, risk management, and controls for fraud prevention at PPATK. *Asia Pasific Fraud Journal*. 2 (1), 15-26.

Setiawan, M.R. (2018). Implementasi prinsip mengenal nasabah sebagai upaya pencegahan tindak pidana pencucian uang. *Jurnal Hukum Diversi*, 3 (2), 139-156.

Tuanakotta, T.M. (2007). *Akuntansi Forensik dan Audit Investigatif.* Jakarta: Lembaga Penerbit Fakultas Ekonomi Universitas Indonesia.

Tuanakotta, T.M. (2014). *Akuntansi Forensik dan Audit Investigatif*, Edisi 2. Jakarta: Salemba Empat.

BAB 4
BANKING FRAUD

Pendahuluan

Seiring perkembangan dunia usaha yang semakin kompleks, berkembang pula praktik kejahatan dalam bentuk kecurangan (*fraud*) ekonomi. Jenis *fraud* yang terjadi pada berbagai negara bisa berbeda, karena dalam hal ini praktik *fraud* antara lain dipengaruhi kondisi hukum di negara yang bersangkutan. Pada negara-negara maju dengan kehidupan ekonomi yang stabil, praktik *fraud* cenderung memiliki modus yang sedikit dilakukan. Adapun pada negara-negara berkembang seperti Indonesia, praktik *fraud* cenderung memiliki modus banyak untuk dilakukan. *Fraud* dapat terjadi pada sektor swasta maupun sektor publik. Pada sektor swasta, banyak terdapat penyimpangan dan kesalahan yang dilakukan seseorang dalam menafsirkan catatan keuangan. Hal itu menyebabkan banyaknya kerugian yang besar bukan hanya bagi orang-orang yang bekerja pada perusahaan, akan tetapi pada investor-investor yang menanamkan dananya pada perusahaan tersebut.

Fraud atau kecurangan adalah suatu tindakan atau perbuatan yang dengan maksud disengaja menggunakan sumber daya organisasi/perusahaan secara tidak wajar untuk memeroleh keuntungan pribadi sehingga merugikan pihak organisasi/perusahaan yang bersangkutan atau pihak lain. Dalam industri perbankan, *fraud* dapat diartikan sebagai tindakan sengaja melanggar ketentuan internal meliputi (1) Kebijakan, (2) Sistem dan (3) Prosedur yang berpotensi merugikan bank baik material maupun moril.

Bank Indonesia (BI) berupaya melakukan pencegahan fraud dengan mensyaratkan perbakan melakukan penerapan pelaksanaan tata kelola perusahaan yang baik (*Good Corporate Governance*/GCG). *Good Corporate Governance* menjadi acuan di dalam beberapa kebijakan BI seperti pembatasan kepemilikan saham pengendali, transparansi informasi suku bunga dasar kredit, dan lain-lain.

Pembahasan Beberapa Istilah di Dunia Perbankan

1. **Pengertian Bank**
   Menurut Asikin (2015), bank merupakan salah satu badan usaha lembaga keuangan yang bertujuan memberikan kredit dan jasa, adapun pemberian kredit itu dilakukan baik dengan modal sendiri ataupun dengan dana yang dipercayakan oleh pihak ketiga maupun dengan jalan mengedarkan alat-alat pembayaran baru berupa uang. Menurut Undang-undang Republik Indonesia nomor 7 tahun 1992 tentang perbankan sebagaimana telah diubah dengan undang-undang nomor 10 tahun 1998, bank merupakan badan usaha yang menghimpun dana dari masyarakat dalam

bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak.

2. **Produk Bank**
   Seperti telah diketahui, bank memiliki tiga fungsi yaitu menghimpun dana, menyalurkan dana, hingga menyediakan layanan jasa kepada masyarakat. Tentu saja seluruh fungsi tersebut dihadirkan demi menyediakan berbagai manfaat untuk masyarakat melalui produk-produk yang dikeluarkan. Setiap produk memiliki karakteristik yang berbeda. Berikut ini merupakan lima jenis produk bank yang bermanfaat dan sering digunakan oleh masyarakat.
   a. Tabungan
      Produk keuangan yang satu ini merupakan kegiatan operasional bank yang paling populer dan sering digunakan oleh masyarakat. Tabungan sering digunakan masyarakat untuk menyimpan uang secara lebih aman dari pada di rumah atau organisasi. Saat ini tabungan tidak hanya terdiri dari satu produk saja, namun telah berkembang menjadi banyak meliputi tabungan haji, tabungan rencana, tabungan berjangka, dan lainnya. Karakteristik pada tabungan antara lain adanya buku tabungan, ATM, setoran awal, biaya bulanan, hingga bunga.
   b. Giro
      Giro merupakan suatu produk bank untuk menghimpun dana dari pihak ketiga. Biasanya suku bunga giro terbilang jauh lebih rendah apabila dibandingkan dengan tabungan serta deposito. Mengapa demikian? Simpanan giro bisa diambil sewaktu-waktu hingga batas akhir limit yang telah ditentukan oleh pihak bank. Giro identik dengan tiga hal, yaitu jenis nasabah, jenis penarikan, dan syarat pembukaan rekening.
   c. Deposito
      Produk yang satu ini memiliki fungsi serupa giro. Namun pencairannya membutuhkan waktu tertentu. Biasanya penarikan di luar waktu tersebut hanya akan menimbulkan risiko bagi nasabah berupa pinalti atau pemotongan dana dari uang yang disimpan di dalam deposito. Dalam deposito ada beberapa karakteristik, yaitu jatuh tempo dan batas waktu penyimpanan.
   d. Kredit
      Kredit memungkinkan seseorang atau badan usaha untuk membeli produk, kemudian pembayarannya dalam jangka waktu tertentu. Beberapa karakteristik yang tidak pernah terlepas dari kredit adalah adanya jangka waktu, suku bunga yang telah disepakati, jaminan, cara pembayaran, biaya administrasi, hingga asuransi jiwa.
   e. Pinjaman
      Ada beberapa bank yang menyediakan layanan pinjaman. Layanan ini biasanya mengunggulkan sistem peminjaman tanpa kartu kredit. Kamu tinggal membayar pada jangka waktu yang telah ditentukan. Sebagai contoh, Amar Bank menyediakan layanan peminjaman secara online dengan cepat dan mudah pada produknya yang bernama **Tunaiku**. Produk ini tidak menggunakan agunan serta kartu kredit.

3. **Jenis-jenis Kredit Perbankan**
   Seperti yang telah dijelaskan sebelumnya bahwa 5 produk bank yang bermanfaat dan sering digunakan oleh masyarakat diantaranya tabungan, giro, deposito kredit dan pinjaman. Dari kelima produk bank tersebut terdapat yang namanya kredit, menurut Nainggolan *et al.* (2019) "Kredit bank adalah semua realisasi pemberian kredit dalam bentuk rupiah maupun valuta asing kepada pihak ketiga bukan bank

termasuk kepada pegawai bank sendiri serta pembelian surat berharga yang disertai dengan *note purchase agreement*/pengambilalihan tagihan dalam rangka anjak piutang dan cerukan". Ditinjau dari penggunaannya, maka pemberian kredit bank dapat berbentuk Kredit Modal Kerja, Kredit Investasi, dan Kredit Konsumsi (Nurjannah & Nurhayati, 2017).

1. Kredit Modal Kerja
   Kredit Modal kerja yaitu kredit jangka pendek yang diberikan untuk membiayai kebutuhan modal kerja dari suatu perusahaan.
2. Kredit Investasi
   Kredit Investasi yaitu kredit jangka menengah dan jangka panjang dalam rangka membiayai pengadaan aktiva tetap suatu perusahaan.
3. Kredit Konsumsi
   Kredit konsumsi yaitu kredit yang diberikan kepada masyarakat dengan ciri sebagai berikut:
   a. Nilai kredit tergantung pada barang yang dibeli
   b. Sumber pembelian tidak dari barang yang dibeli tetapi dari penghasilan/profesi yang bersangkutan.
   c. Penilaian kredit sangat ditekankan pada penilaian atas agunan.

Beberapa contoh dari kredit konsumsi yaitu: Kredit Kepemilikan Rumah (KPR), Kredit Profesi Guru (KPG), Kredit mahasiswa Indonesia dan Kredit asrama mahasiswa.

4. *Fraud* Dalam Dunia Perbankan

Banyak macam cara yang dapat dilakukan oleh orang yang tidak bertanggung jawab dalam melakukan *fraud* atau kecurangan, modus operandinya pun sangat beragam, berikut ini diuraikan beberapa *fraud* dalam dunia perbankan, diantaranya meliputi:

a) *Fraud* di Bidang Kredit
   Aktivitas lainnya yang rawan *fraud* adalah perkreditan, yakni memberikan kredit fiktif atau agunan fiktif, antara lain dengan memanfaatkan berkas kredit yang lunas. Kemudian, aktivitas *accounting*. Unit *accounting* melakukan perubahan parameter bunga sehingga biaya dana meningkat dan dipindahkan ke rekening tabungan yang bersangkutan.

Tabel 2. Fraud Actual Credit Card

Fraud Actual Credit Card	Des-12		Jan-13		%	
	Kerugian (juta)	Jumlah Kasus	Kerugian (juta)	Jumlah Kasus	Kerugian (juta)	Jum Ka
Kartu Palsu	231.6	20	244.1	42	5.0	
Kartu hilang/dicuri	80.7	850	13	1011	(8 4)	
Kartu Tidak diterima	27.1	4	77.2	11	184.0	
Fraud Aplikasi	457.4	47	919.3	45	101.0	
Transaksi tanpa menggunakan kartu	1.649.9	651	2.019.6	635	22.0	
Lainnya	18.5	2	139.1	5	649.0	
Total	2.465.5	1.554	3.412	1.752	38	
Total Transaksi	18.356.567	20.067.650	17.960.041.7	20.021.962	(3.2)	(0.2)

Sumber: Laporan Bulanan Sistem Pembayaran - Bank Indonesia Periode Feb 2013

b) *Fraud* di Bidang *Operation*
Dalam operasional perbankan, beberapa aktifitas yang diidentifikasikan rawan *fraud,* antara lain aktivitas pendanaan. Dalam hal ini, pegawai bank menarik dana dari rekening nasabah dengan memanfaatkan kepercayaan nasabah. Pejabat bank dan petugas *customer service* menerima titipan penyetoran deposito *(door to door)* dan diterbitkan bilyet deposito, namun tercatat dalam pembukuan bank. Uang setoran digunakan untuk kepentingan pribadi. *Fraud* lain dilakukan dengan menyetujui pencairan deposito *prime customer* tanpa didiukung dengan bilyet asli. Contoh kasus Citibank – Melinda Dee, dan Bank Mega – PT. Elnusa.

c) *Fraud* di Bidang Teknologi dan Informasi
Penggandaan kartu kredit yang menggunakan teknologi marak digunakan. Penggunaan teknologi *chip* masih dalam proses masa transisi sehingga masih rentan terhadap pencurian informasi. Kasus pencurian data nasabah Bank Mandiri di merchant *"body shop"* menyebabkan nasabah dirugikan sebesar Rp.7,5 Miliar. Pencurian data pada saat swipe menyebabkan data diduplikasi dan digunakan untuk bertransaksi di luar negeri (Amerika Serikat dan Meksiko).

Dari laporan tersebut, jumlah kasus *fraud actual* kartu kredit di Januari 2013 yang tercatat sebanyak 1.752 kasus dengan kerugian mencapai Rp.3,41 Miliar. Jumlah kasus ini meningkat sebesar 13% dengan kerugian 38% apabila dibandingkan dengan periode sebelumnya di Desember 2012.

Tabel 3. Fraud Actual Debit Card

Fraud Actual Debit Card	Des-12		Jan-13		
	Kerugian (juta)	Jumlah Kasus	Kerugian (juta)	Jumlah Kasus	
Kartu Palsu	12.1	2	500.3	94	4
Kartu hilang/dicuri	0.8	702	2	752	
Kartu Tidak diterima	-	0	-	0	-
Fraud Aplikasi	-	0	-	0	-
Transaksi tanpa menggunakan kartu	-	0	-	0	-
Lainnya (tertelan, dsb)	4.0	78	-	81	-
Total		782	502	927	2
Total Transaksi		269.581.159	-	249.407.261	
Nilai Transaksi	277.232.809		291.301.584,0		

Sumber: Bank Indonesia 2013

Sementara untuk kartu debet periode Januari 2013, tercatat 927 kasus dengan nilai kerugian mencapai Rp.502 juta. Jumlah kasus dan nilai kerugian mengalami kenaikan masing sebesar 18,54 % dan 2.886 % dibandingkan dengan periode Desember 2012. Untuk uang elektronik dan Kegiatan Usaha Pengiriman Uang tidak ada kasus fraud yang dilaporkan.

5. Kebijakan Manajemen Bank Dalam Mencegah *Fraud*

Untuk mencegah terjadinya kejahatan perbankan dapat dilakukan dengan Kebijakan Manajemen bank. Menurut Lester A. Pratt dalam *Bank Frauds Their Detection and Prevention* kebijakan ini dapat dilakukan melalui langkah-langkah berikut:

a) Kebijakan Personalia. Kebijakan ini meliputi peraturan seleksi, pelatihan, promosi dan penggajian dari pegawai dan pejabat bank. Program dimaksud harus dilakukan secara hati-hati untuk mencegah kejahatan. Peraturan tentang promosi pegawai harus menempatkan dan keahlian seseorang di atas senioritas. Penggajian pejabat dan pegawai bank harus seiring dengan meningkatnya pendapatan dan pertumbuhan suatu institusi sesuai dengan kompetensi serta partisipasi seorang pegawai atau pejabat dalam jabatannya untuk mendukung kesuksesan bank.

b) Kebijakan Pengawasan. Kebijakan tentang fungsi pengawasan menetapkan cara yang aman dan lazim dalam setiap kegiatan usaha bank untuk mencapai tujuan organisasi, baik pengawasan melekat sejara berjenjang, audit intern, Direktur/Unit Kepatuhan dan Unit Manajemen Risiko. Hal yang penting dalam aktivitas pengawasan adalah penilaian atas efisiensi, ekonomis dan keamanan dalam setiap fungsi departemen.

c) Tanggung Jawab Direksi. Setidaknya ada lima tanggung jawab yang wajib diemban direksi dalam rangka mencegah terjadinya bank *fraud*, yaitu:

   (1) Direksi bertanggung jawab melakukan pengawasan terhadap seluruh kegiatan bank dan memastikan usaha bank berjalan dengan baik.

   (2) Direksi bank bukan penjamin atas kebenaran dan kelakuan yang patut dari pejabat eksekutifnya, namun mereka harus melakukan pengawasan terhadap tindak-tanduk eksekutif banknya dengan seksama.

   (3) Direksi harus menaruh perhatian terhadap penerapan prinsip kehati-hatian dalam setiap kegiatan usaha bank.

   (4) Direksi bank harus mengetahui setiap fakta yang mencurigakan, sehingga harus menempatkan orang yang dapat dipercaya sebagai pengawas.

   (5) Direksi tidak diharapkan memantau kegiatan rutin perbankan setiap hari, tetapi mereka harus mempunyai pengetahuan pelaksanaan kegiatan usaha bank pada umumnya, dan memberikan arahan kepada hal-hal yang penting.

Simpulan

Dengan mengetahui berbagai jenis fraud di sektor perbankan, serta menjalankan berbagai langkah tentang kebijakan perbankan dalam menangani fraud seperti yang telah dijelaskan dalam bab ini, maka pengendalian internal terhadap manajemen perbankkan menjadi lebih kuat. Sistem pengendalian internal yang kuat menyebabkan kemungkinan terjadinya fraud akan lebih kecil. Hal ini karena pengendalian internal yang efektif dapat mencegah kerugian atau pemborosan pengolahan sumber daya perusahaan. Selain itu, pengendalian internal juga dapat menyediakan informasi tentang bagaimana menilai kinerja perusahaan dan manajemen perusahaan serta menyediakan informasi yang akan digunakan sebagai pedoman dalam perencanaan.

Contoh Kasus

"Kredit Fiktif Rockit Aldeway"

Direktorat Tindak Pidana Ekonomi Khusus (Tipideksus) Bareskrim Polri membongkar kasus pembobolan bank yang terjadi selama kurun waktu Maret-Desember 2015. Nama HS mendadak tenar, khususnya di lingkungan industri perbankan Tanah Air. Ketenarannya karena pria keturunan India itu membobol dana tujuh bank senilai Rp. 836 miliar bermodus penarikan kredit modal kerja berbekal dokumen *purchase order* (PO) fiktif, lewat perusahaan miliknya PT Rockit Aldeway. Perusahaan ini merupakan produsen batu split.

Tipideksus Bareskrim Mabes Polri menyebutkan bahwa dari total dana yang ditilap HS, sebanyak Rp 398 miliar merupakan dana bank pelat merah, dan Rp 438 milik bank swasta. HS sendiri sudah ditangkap. Tim Bareskrim berhasil menangkapnya di kawasan bisnis Sudirman, Jakarta. HS terkejut atas upaya paksa yang Tim Bareskrim lakukan. Dia berdalih masalahnya sudah diselesaikan di sidang penundaan kewajiban pembayaran utang (PKPU). Dari dokumen yang diperoleh, korban kejahatan HS berjumlah total 32 pihak, terdiri dari institusi dan perseorangan. Adapun tujuh bank yang menjadi korbannya adalah PT Bank Mandiri Tbk, PT Bank Negara Indonesia Tbk, PT Bank Commonwealth, PT Bank Muamalat Tbk, HSBC Indonesia, PT Bank Ekonomi Raharja Tbk dan PT Bank QNB Kesawan Tbk (*lihat tabel*).

Tidak banyak yang mengenal sosok HS. Posisi terakhir dia adalah direktur utama dan juga pemegang 99% saham Rockit. Sisa saham 1% dipegang Dewi Suganda, wanita berusia 46 tahun yang juga Komisaris Rockit. Dari dokumen yang dimiliki, Dewi tercatat menyandang gelar S1 dari Universitas La Trobe, Melbourne Australia. Sementara HS merupakan alumnus University of Massachusettsat Amherst. Karier di sektor keuangan pun telah HS lakoni sejak lama. Sejak 1996-2002, HS berkarier di HSBC Indonesia. Berbagai jabatan mulai dari *corporate dealer treasury* hingga *manager fixed income & forex sales*, pernah diembannya. Maka tidak heran jika aksi yang dijalankan HS membobol tujuh bank berjalan mulus.

Kredit Fiktif

Modus pengajuan kredit modal kerja berbekal 10 berkas PO fiktif Rockit yang dikendalikan HS memang efektif menggasak ratusan miliar rupiah dana bank. Bareskrim menangkap seseorang oknum bankir berinisial "D" yang ditahan

karena ikut memuluskan aksi kejahatan HS. Dari aksinya, oknum D memperoleh imbalan Rp 700 juta dari HS.

Setelah memperoleh kredit sekitar tahun 2015, di tengah perjalanan Rockit dan HS mengajukan permohonan penundaan kewajiban pembayaran utang (PKPU) secara sukarela bernomor 106/PKPU/2015/PN JKT.PST pada tanggal 28 Desember 2015. Selang sehari, 29 Desember, sidang pertama PKPU langsung digelar dan majelis hakim langsung memutus dengan mengabulkan permohonan PKPU Rockit dan HS. Majelis hakim pun lantas menetapkan keduanya dalam keadaan PKPU sementara, selama 45 hari dan menunjuk Yana Supriatna sebagai pengurus PKPU.

Di tengah perjalanan, muncul kreditur baru Rockit bernama Trilium Global Pte Ltd yang mengaku memiliki tagihan senilai Rp1,02 triliun. Tak banyak informasi mengenai Trillium Global yang baru berdiri pada tahun 2012 lalu. Perusahaan yang bergerak dibidang investasi itu berdomisili di Negeri Merlion, Singapura. Hingga akhirnya akta perdamaian tidak disepakati dan voting para kreditur akhirnya memutuskan Rockit dipaksa menutup perusahaannya alias pailit pada 9 Februari 2016. Profil Trilium yang masih menjadi misteri, memiliki andil besar dalam kelancaran pailit Rockit. Namun, pihak Bareskrim mencium ada aroma tidak sedap soal keberadaan Trilium. Dari keterangan sejumlah pihak, terkait Trilium. Ternyata perusahaan itu terafiliasi dengan tersangka sendiri (HS). Bareskrim terus melakukan pengembangan pemeriksaan dan telah memeriksa 43 saksi, termasuk dari kalangan bankir yang menjadi korban. Namun Agung belum bisa menyampaikan apakah Bareskrim sudah menetapkan tersangka baru.

Di sisi lain, Wakil Ketua Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) Ediana Rae menyatakan terus berkoordinasi dengan pihak Bareskrim untuk mengungkap kasus ini.

Langkah Perbankan

Agung menyatakan, pihaknya memulai pemeriksaan kasus Rockit pasca mendapat laporan dari empat bank yang menjadi korban. Laporan terakhir diterima Bareskrim pada Februari 2017. Manajemen Bank Mandiri yang menjadi salah satu kreditur Rockit telah melaporkan HS dan Rockit ke polisi pada sekitar bulan September-Oktober 2016. Total nilai utang Rockit dan HS ke Bank Mandiri mencapai Rp 249,32 miliar. Adapun total nilai tagihan seluruh kreditur tak kurang dari Rp 1,89 triliun. Di pihak lain, Endy Abdurrahman, Direktur Utama Bank Muamalat menyatakan jumlah pinjaman yang diberikan perusahaannya ke Rockit mencapai Rp 100 miliar. Agunan yang sudah dikuasai dan menjadi milik Muamalat secara sah dan hukum mencapai Rp 91 miliar.

Adapun juru bicara Bank HSBC Indonesia dan Bank Ekonomi, yakni Daisy Primayanti menyatakan belum dapat memberikan komentar, mengingat permasalahan ini sedang ditangani oleh pihak Kepolisian. Dari data yang dimiliki mengindikasikan penyaluran kredit HSBC ke Rockit mencapai Rp 49,74 miliar dan Bank Ekonomi Rp 48 miliar.

PT Bank Negara Indonesia Tbk (BNI) juga menjadi korban Rockit. Tahun 2016 lalu, Elia Massa Manik, SEVP Remidial Recovery BNI pernah menyebut nilai tagihan BNI mencapai sekitar Rp 170 miliar. Adapun data yang diperoleh menyebutkan total kredit BNI sekitar Rp 148 miliar.

Otoritas Jasa Keuangan (OJK) Meradang

Aksi Rockit Aldeway membobol dana di tujuh bank dengan skema kredit modal kerja berbekal dokumen *purchase order* (PO) fiktif, membuat Otoritas Jasa Keuangan (OJK) meradang. OJK menegaskan, tak akan melindungi oknum bankir yang kelak terbukti ikut terlibat dalam kasus ini. Proses penyelidikan kasus perusahaan perdagangan batu split itu dengan internal tujuh bank sebagai pemberi kredit, masih dilakukan oleh lembaga pengawas perbankan. Selain itu, KPK juga akan melakukan *fit and proper test* kepada semua orang perbankan yang terlibat.

Jika terbukti oknum perbankan tersebut terlibat dalam kolusi pemberian kredit, mereka akan dicopot dari jabatannya dan ditutup masa karier mereka di industri perbankan. Dan jika oknum perbankan tersebut terbukti melakukan tindak pidana perbankan, maka yang bersangkutan akan dipidanakan oleh pihak banknya. Tidak hanya itu, OJK juga akan memberikan sanksi kepada bank. Irwan Lubis, Deputi Komisioner Pengawas Perbankan OJK, meminta kepada bank-bank yang terlibat dalam kasus tersebut untuk memperlambat pemberian kredit di kuartal I 2017, serta memperdalam verifikasi data dalam setiap pemberian kredit kepada debitur. OJK meminta perlambatan menyalurkan kredit untuk menjaga risiko.

Wasit perbankan ini juga meminta kepada bank untuk teliti dalam memberikan kredit serta melengkapi pedoman standar kebijakan perkreditan, manajemen kredit menjalankan sistem komite kredit, dan melakukan verifikasi data agar terhindar dari *fraud* atau kolusi di perbankan.

Penundaan Kewajiban Pembayaran Utang (PKPU) Jadi Modus

Rockit sendiri sebenarnya bukan perusahaan batu split yang benar-benar bodong. Sejumlah dokumen yang diperoleh menerangkan, sedikitnya ada 10 perusahaan yang disebut-sebut punya hubungan bisnis dengan Rockit (*lihat tabel*).

Perusahaan/Pengusaha yang disebut menjadi konsumen produk PT Rockit Aldeway

Nama Perusahaan
PT Adaro Indonesia
PT Petrosea
PT Cakrawala Sejahtera
CV Tamara Bakti Usaha
PT Servo Lintas Raya
PT Gajah Tunggal
PT Multi Tambang Jaya
PT Tradindo Megah Lestari
Dicky Hermawan
Agustinus Dhea Wea

Perusahaan/pengusaha yang disebut menjadi pemasok batu bagi PT Rockit Aldeway

Nama Perusahaan
CV Batu Berlian
PT Daz Pratama
CV Bas
CV Berkah Jaya
Koperasi Batu Manunggal
PT Arsindo
Asa Kalimaya
Lain-lain

Sumber: Kontan

Salah satu konsumen terbesar Rockit adalah PT Adaro Indonesia, yang tak lain anak usaha dari PT Adaro Energy Tbk (ADRO). Febrianti Nadira *Head of Corporate Communication* Adaro Energy membenarkan kabar itu. "PT Adaro

Indonesia pernah menggunakan jasa PT Rockit Aldeway, bersama-sama dengan vendor sejenis lainnya untuk pengadaan material batu pecah, split pada proyek perbaikan infrastruktur di wilayah tambang Adaro beberapa tahun lalu," tutur wanita yang biasa disapa Ira itu. Sayangnya, Ira tidak memiliki data berapa nilai proyek yang dikerjakan perusahaan bermodal dasar Rp 15 miliar itu bagi Adaro.

Aksi Rockit terbilang cukup lihai. Pasca memperoleh kredit, perusahaan ini lantas membawa dirinya sendiri dalam kondisi penundaan kewajiban pembayaran utang (PKPU). Kemunculan Trilium Global Pte Ltd pada masa PKPU yang mengaku memiliki tagihan Rp 1,02 triliun ke Rockit menambah kecurigaan adanya *kongkalikong*. Pada akhirnya-pun Rockit pailit.

Direktorat Tindak Pidana Ekonomi Khusus (Tipideksus) Bareskrim Mabes Polri menyatakan sudah mendapatkan banyak bukti atas dugaannya. Karena aksinya itu, dia kini tidak lagi menghirup udara bebas. Hari-harinya kini hanya bisa dilewatinya dibalik jeruji besi. Kedua tersangka yang telah ditangkap sejak 23 Februari lalu itu, disangka dengan sejumlah pasal, yaitu Pasal 49 ayat (2) UU Nomor 10 Tahun 1998 tentang Perbankan, Pasal 263 dan 378 KUHP tentang pemalsuan, serta Pasal 3 dan 5 UU Nomor 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang, dengan ancaman penjara 15 tahun.

Dari kasus tersebut dapat kita telaah dan beri berbagai perspektif yang tentunya akan berbeda-beda bagi setiap orang, tergantung dari latar balakang bidang yang ditekuni. Secara umum, ada beberapa hal penting terkait dengan kasus tersebut, meliputi:

1. Dalam kasus ini adanya pelanggaran ketentuan internal bank dalam pengajuan kredit yang meliputi kebijakan, sistem, dan prosedur yang dilakukan oleh pihak internal.
2. Sesuai aturan, seorang manajer representatif kredit seharusnya mengecek dokumen permohonan yang diajukan. Hasil pengecekan itu nantinya akan menjadi bahan acuan bagi kepala cabang untuk diteruskan ke bagian risiko, untuk dicek kembali risiko kreditnya. Dari hasil pengecekan, barulah diketahui apakah permohonan disetujui atau tidak. Dalam kasus ini seharusnya Bank yang bersangkutan mempunyai internal kontrol yang berlapis, serta berintegritas sehingga tidak terjadi kasus seperti yang pada akhirnya merugikan Bank itu sendiri. Selanjutnya, meskipun berbagai bank memiliki persyaratan pengajuan pinjaman dana yang berbeda-beda untuk calon debiturnya, alangkah baiknya pihak bank lebih teliti lagi dalam melakukan pengecekan berkas/dokumen apakah real ataukah fiktif.
3. Dari pembahasan yang telah dipaparkan pada bagian terdahulu, dapat ditarik kesimpulan bahwa, *Banking Fraud*, dapat dilakukan oleh pihak internal maupun pihak eksternal. Dalam kasus di muka, Banking Fraud ini dilakukan oleh orang dalam yaitu manajer bank yang berinisial D dan pihak luar yang bernama Harry Suganda, yang pernah berkarier di bank. Karena itu diduga dia tahu banyak mengenai seluk beluk perbankan. Jadi yang melakukan fraud sebenarnya adalah orang-orang pintar yang mempunyai kuasa dan jabatan.

Daftar Bacaan

Asikin. Z. (2015). *Pengantar Hukum Perbankan Indonesia*. Cetakan ke-1. Jakarta: PT. Raja Grafindo Persada

Lester A. P. (1947). *Bank Frauds Their Detection and Prevention*. New York: Ronald Press.

Nainggolan, N.A., Pandia, F.I. & Ansori. (2019). Pengaruh profitabilitas, ukuran perusahaan dan inflasi terhadap risiko kredit bank persero periode 2014-2018. *Jurnal Akuntansi, Keuangan dan Perbankan*, 6 (2), 1176-1184.

Nurjannah & Nurhayati. (2017). Pengaruh penyaluran kredit investasi, kredit modal kerja dan kredit konsumtif terhadap pertumbuhan ekonomi Indonesia. *Jurnal Samudra Ekonomi dan Bisnis*, 8 (1), 590-601.

Petrucelli, J.R. (2012). *Detecting Fraud in Organizations. Techniques, Tools, and Resources*. New Jersey: John Wiley & Sons.Inc.

Pratt, L.A. (2015). *Embezzlement Controls for Business Enterprises*, Fidelity and Deposit Company of Maryland. https://onlinelibrary.wiley.com/doi/abs/10.1002/978111920 5135.app1.

Simorangkir, O.P. (2008). *Seluk Beluk Bank Komersial*, Jakarta: Aksara Persada Indonesia

Tuanakotta, T. M. (2015). *Akuntansi Forensik dan Audit Investigatif*, Ed.2. Jakarta: Salemba Empat.

Undang-Undang Republik Indonesia Nomor 7 Tahun 1992 Tentang Perbankan Sebagaimana Telah Diubah dengan Undang-Undang Nomor 10 Tahun 1998

http://www.amarbank.co.id

http://keuangan.kontan.co.id

BAB 5
INTERNET FRAUD

Pendahuluan

Teknologi informasi dan komunikasi terus berkembang seiring dengan perkembangan pola berfikir umat manusia sebagai mahluk sosial yang mempunyai naluri ingin tahu, ingin mengenal, ataupun berkomunikasi. Inovasi dibidang teknologi informasi dan komunikasi telah berhasil menemukan dan menciptakan antara lain telepon, handpone, komputer dan internet. Perkembangan dan pemanfaatan teknologi informasi dan komunikasi seperti internet, maka manusia dapat mengetahui apa yang terjadi didunia ini dalam hitungan detik, dapat berkomunikasi dan mengenal orang dari segala penjuru dunia tanpa harus berjalan jauh dan bertatap muka secara langsung. Inilah yang dikenal orang dengan sebutan dunia maya atau Cyber Space. Perkembangan teknologi informasi ini banyak manfaat yang positif dalam memudahkan umat manusia untuk melakukan kegiatan-kegiatan melalui dunia cyber, seperti: e-travel yang berhubungan dengan pariwisata, e-banking yang berhubungan dengan perbankan electronic mail atau e-mail, e-commerce yang berhubungan dengan perdagangan. Dalam paper ini akan berfokus kepada fraud di *e-commerce*.

Pemanfaatan teknologi informasi dan komunikasi disamping memberi manfaat bagi kemaslahatan masyarakat, disisi lain memiliki peluang untuk digunakan sebagai alat untuk melakukan kejahatan. Kejahatan yang dilakukan menggunakan teknologi informasi dan komunikasi dapat terjadi pada kejahatan biasa maupun yang secara khusus menargetkan kepada sesama infrastruktur teknologi informasi dan komunikasi sebagai korbannya, dimana dampak dari kejahatan yang muncul dari penggunaan teknologi informasi dan komunikasi secara negatif dapat menyebabkan runtuhnya sistem tatanan sosial, lumpuhnya perekonomian nasional suatu negara, lemahnya sistem pertahanan dan keamanan serta juga dapat memiliki peluang untuk digunakan sebagai alat teror.

Pengertian Internet

Sejalan dengan kemajuan teknologi informatika yang demikian pesat, melahirkan internet sebagai sebuah fenomena dalam kehidupan umat manusia. Internet, yang didefinisikan oleh The U.S. Supreme Court sebagai: *"international network of interconnected computers"* (Reno v. ACLU, 1997), telah menghadirkan kemudahan-kemudahan bagi setiap orang bukan saja sekedar untuk berkomunikasi tapi juga melakukan transaksi bisnis kapan saja dan di mana saja. Saat ini berbagai cara untuk dapat berinteraksi di "dunia maya" ini telah banyak dikembangkan. Salah satu contoh adalah lahirnya teknologi *wireless application protocol* (WAP) yang memungkinkan

telepon genggam mengakses internet, membayar rekening bank, sampai dengan memesan tiket pesawat.

Pengertian *Cyber Crime*

Dalam beberapa literatur, *cyber crime* sering diidentikkan sebagai computer crime. The U.S. Department of Justice memberikan pengertian computer crime sebagai: *"...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution "*. Pengertian lainnya diberikan oleh Organization of European Community Development, yaitu: *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data"*. Sementara itu, Testa *et al.* (2017) mengartikan "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Cyber crime atau kejahatan komputer dapat dibedakan menjadi dua:

1. *Computer fraud* merupakan bentuk kejahatan yang dilakukan pada suatu sistem berbasis Komputer maupun jaringan internet.
2. *Computer crime* merupakankegiatan kejahatan yang menggunakan media komputer dalam melakukan pelanggaran hukum tersebut.

Internet sebagai hasil rekayasa teknologi bukan hanya menggunakan kecanggihan teknologi komputer tapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya. Apalagi pada saat internet sudah memasuki generasi kedua, perangkat komputer konvensional akan tergantikan oleh peralatan lain yang juga memiliki kemampuan mengakses internet. Untuk itu, ada upaya untuk memperluas pengertian computer agar dapat melingkupi segala kejahatan di internet dengan peralatan apapun, seperti pengertian computer dalam The Proposed West Virginia Computer Crimes Act, yaitu: *"an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or type-setter, a portable hand-held calculator, or other similar device"*. Namun begitu, tetap saja pada prakteknya pemahaman publik akan pengertian computer adalah perangkat komputer konvensional (PC, Notebook, Laptop) yang biasa terlihat.

Risiko Kecurangan dalam E-Commerce

Kecurangan dapat terjadi dalam lingkungan manapun, beberapa aspek dari lingkungan e-business memperlihatkan risiko yang unik.Karakteristik ini merupakan pendorong perekonomian berbasis internet yang menciptakan tekanan dan memberikan ruang kesempatan secara khusus untuk kecurangan e-commerce. Seperti jenis kecurangan lainnya, kecurangan baru ini dilakukan ketika tekanan, kesempatan, dan rasionalisasi muncul bersamaan. Elemen-elemen e-commerce membuat adanya peningkatan risiko atau risiko unik yang dapat dilihat dalam tabel berikut:

Tabel 4. Elemen-Elemen Risiko Kecurangan dalam E-Commerce

Tekanan ✓ Pertumbuhan dramatis, yang membuat besarnya kebutuhan akan arus kas ✓ Aktivitas merger atau ekuisisi, yang menciptakan tekanan untuk "meningkatkan hasil keuangan yang dilaporkan" ✓ Meminjam atau mengeluarkan saham; tekanan tambahan untuk "mengolah pembukuan *(cook the books)*" ✓ Produk baru yang membutuhkan system pemasaran yang lebih intensif dan mahal saat pasar yang ada tidak lagi ada ✓ Model bisnis yang cacat atau tidak terbukti dengan tekanan arus kas yang besar
Kesempatan ✓ Teknologi yang baru dan inovatif, dengan pengembangan keamanan sering tertinggal daripada pengembangan transaksi ✓ Kompleksnya system informasi yang menciptakan kesulitan dalam aplikasi pengendalian ✓ Transfer informasi dalam jumlah besar, sebuah faktor yang menciptakan risiko atas pencurian dan risiko identitas seperti pengawasan illegal dan akses yang tidak terotorisasi ✓ Pemindahan kontak pribadi, yang memudahkan pemalsuan identitas atau penyamaran. Tidak adanya "toko secara fisik yang minim aktivitas *online (brick and mortar)*" dan fasilitas fisik lainnya yang memfasilitasi pemalsuan sistus dan transaksi bisnis. ✓ Ketidakmampuan untuk membedakan perusahaan besar dan/atau perusahaan yang dibentuk dari perusahaan baru atau perusahaan yang lebih kecil, sehingga mudah untuk melakukan penipuan terhadap konsumen dengan memalsukan identitas dan/atau pemaparan kegiatan bisnis ✓ Transfer elektronik atas ketersediaan dana, memungkinkan kecurangan dalam skala besar lebih mudah untuk dilakukan ✓ Luasnya keterbatasan yang disepakati, yang menyebabkan pencurian lebih mudah dilakukan dengan menggunakan informasi yang dicuri atau dipalsukan
Peningkatan Kecenderungan terhadap Rasionalisasi ✓ Jarak yang dirasakan mengurangi kontak pribadi antara pelanggan dan pemasok ✓ Transaksi antara pembeli dan penjual anonym atau yang tidak diketahui – anda tidak dapat melihat siapa yang anda sakiti ✓ Pemikiran ekonomi baru berpendapat bahwa metode akuntansi secara tradisional tidak lagi diterapkan

Risiko-risiko Kecurangan E-Commerce dalam Organisasi

Hampir sebagian besar risiko kecurangan e-commerce yang sering ditemukan di dalam organisasi. Setelah pelaku mendapat *firewall* dan pemeriksaan keamanan, jauh lebih mudah untuk masuk ke dalam system, mencuri uang dan informasi, dan menyebabkan kerusakan. Pelaku yang mempunyai akses dari dan ke dalam perusahaan, mengetahui lingkungan pengendalian, memahami mekanisme jaminan keamanan, dan menemukan cara untuk melewati prosedur keamanan. Salah satu permasalahan sangat serius adalah penyalahgunaan wewenang yang telah diberikan kepada para pengguna.

Pencurian uang biasanya merupakan tujuan utama dalam kecurangan secara tradisional. Dalam lingkungan berbasis elektronik, pencurian data umumnya menjadi kekhawatiran yang pertama kali muncul karena data memiliki banyak cakupan manfaat yang menguntungkan. Pertama, data dapat dikonversikan menjadi kas secara lebihmudah. Kedua, informasi tersebut dapatdireplokasi, memungkinkan pelaku dengan mudah menyalin data daripada menghapusnya seperti yang dilakukan dalam kecurangan secara tradisional. Tindakan pencurian sering meninggalkan sangat sedikit jejak karena sumber data tetap lengkap dan dapat digunakan seperti biasa. Kemudian replikasi atas data yang merupakan sebuah alasan bahwa kecurangan e-commerce sering kali tidak dapat terdeteksi pada periode waktu yang panjang, kecuali perusahaan secara hati-hati melakukan pengawasan terhadap akses *logbook*, area tempat tindakan replikasi, yang hamper tidak pernahmereka perhatikan. Ketiga, data dapat ditransfer dengan mudah dan cepat ke beberapa lokasi di dunia. Jika pelaku menggunakan ponsel atau koneksi pribadi lainnya menggunakan jaringan internet untuk mentrasfer data, kegiatan pendeteksian menjadi sangat sulit untuk dilakukan. Hal ini disebabkan karena banyak manajer memiliki keahlian teknis yang minim untuk dapat mencegah dan mendeteksi adanya pencurian data. Manajer TI dan penyedia jaminan keamanan perlu menyadari poin penting dalam infrastruktur *e-business*, tempat data dengan mudah dicuri.

Kata sandi bisa menjadi salah satu poin kelemahan dan kegagalan perusahaan dalam menghadapi ancaman pihak luar, karena dalam banyak system, pemilihan kata sandi tertinggal/tersisa untuk pengguna akhir dan tidak dapat sepenuhnya dikendalikan. Peretas sering menggunakan teknik perekayasaan sosial untuk mendapatkan akses kata sandi. Pesan instan, catatan blog, dinding facebook, dan jejaring sosial lainnya memberikan kepada para pelaku sebuah metode baru dalam mengumpulkan informasi. Bahkan, ketika kebijakan perusahaan mengharuskan adanya perubahan kata sandi secara berkala, banyak pengguna sengaja tidak menambahkan urutan nomor atau karakter lainnya untuk mengganti kata sandi terakhir mereka.

Komunikasi yang tidak terenkripsi antar pengguna sering menjadi ancaman bahwa banyak pegawai tidak mendapatkan apresiasi. *Sniffing* adalah mencatat, menyaring, dan melihat informasi yang ada melalui lini jaringan; merupakan sebuah metode yang umum dalam mengumpulkan informasi dari komunikasi yang tidak terenkripsi. *Sniffing* dengan mudah dilakukan pada sebagian besar jaringan oleh peretas yang menjalankan secara bebas aplikasi yang tersedia seperti *Wireshack* dan *tpcdump*.

Meskipun *firewall*, penyaring *spam*, dan aplikasi virus melindungi organisasi dari serangan eksternal, laptop pegawai dan perangkat telepon genggam memberikan risiko yang cukup sulit untuk diatur. Salah satu praktik penipuan terbaru untuk orang yang sering melakukan perjalanan bisnis disebut *wartrapping*. Dalam penipuan jenis ini, peretas dapat mengetahui lokasi orang tersebut seperti di bandara dan membuat poin akses melalui laptop mereka via internet. Laptop mereka terlihat seperti jaringan nirkabel yang secara regular dapat menghubungkan satu sama lain. Ketika orang tersebut membuka laptop mereka, kartu nirkabel mereka terhubung secara otomatis ke titik-titik akses internet "gratis" ini. Banyak yang berfikir mereka terhubung ke jaringan nirkabel bandara yang resmi lewat komputer peretas. Saat orang tersebut melakukan pencarian lewat internet, mengecek surel, dan menggunakan jaringan perusahaan mereka, peretas mencuri kata sandi dan informasi penting lainnya.

Munculnya perangkat *Universal Serial Bus* (USB), meningkatnya memori di telepon, dan perangkat keras eksternal yang tersedia secara portabel menimbulkan ancaman keamanan di berbagai bidang. Kapasitas yang besar memungkinkan dengan

cepat mengunduh informasi dari jaringan internal dalam jumlah yang signifikan. Perangkat ini, termasuk ponsel berkamera dan pemutar music seperti iPod, telah terpasang pada banyak instansi militer karena potensi ancaman yang mereka hadapi.

Vandalism selalu menjadi risiko dengan sistem internal. Dari adanya penolakan terhadap usaha pada sistem lokal untuk penghapusan dokumen terhadap kerusakan secara fisik, vandalism adalah cara mudah bagi pegawai untuk membahayakan sistem internal. Vandalism dapat terlihat jelas, atau dapat sangat sulit ditemukan, tersembunyi berminggu-minggu atau berbulan-bulan sebelum dampaknya diketahui.

Risiko-Risiko E-Commerce di Luar Organisasi

a. *Spyware*
   Tipe *malware* yang sama dengan *Trojan horse* yaitu menginstal perangkat lunak untuk pengawasan sebagai tambahan perangkat lunak yang biasa diunduh atau dibeli oleh pengguna. *Spyware* lebih dtujukan agar dapat mengangkat informasi keuangan atau informasi sensitif lainnya dari direktori internal dan dokumen serta mengirimkannya ke entitas eksternal.
b. *Phishing*
   Phishing adalah metode umum yang digunakan peretas untuk menggali informasi pribadi atau informasi perusahaan dari pegawai. *Phisher* mengirim surel atau *pop-up messages* kepada pengguna dengan menanyakan informasi pribadi dengan cara yang kreatif. Pada umumnya korban banyak yang terkena perangkap yaitu memberikan berbagai informasi pribadi kepada pelaku *phishing*.
c. *Spoofing*
   Spoofing mengubah informasi dalam *header* surel atau alamat IP. Pelaku menyembunyikan identitas mereka hanya dengan mengubah informasi dalam *header*, selanjutnya mereka memungkinkan melakukan akses yang tidak terotorisasi.
d. Pemalsuan identitas
   Untuk transaksi elektronik yang sedang dilakukan, setiap pihak dalam transaksi harus yakin benar bahwa identitas yang diklaim oleh pihak lain adalah otentik. Ancaman ini kurang mendapat perhatian dalam pengaturan pertukaran data elektronik (*Electronic Data Interchange* – EDI), karena EDI secara sederhana menggunakan jalur akses yang relatif terbatas, jalur khusus, dan penyedia jaringan bernilai tambah yang dibuat sebagai perantara. Dalam hal ini, keaslian atau keotentikan menjadi sesuatu yang sangat penting yang harus mendapat perhatian besar atas transaksi yang dilakukan melalui saluran elektronik yang dimiliki publik dalam *e-business*.

Tambahan permintaan basis data (SQL) dan bahasa pemrograman antar situs (XSS) menyajikan risiko-risiko bahwa banyak situs yang tidak didesain untuk ditangani. Dalam tambahan permintaan basis data (SQL), peretas mengirim instruksi terkait basis data setelah data secara regular disertakan dalam formulir pendaftaran *online*. Sejak banyak system *back-end* secara sederhana menyiarkan perintah dari formulir ke basis data, tambahan permintaan basis data (SQL) dilakukan oleh basis data perusahaan. Perintah ini mungkin menyisipkan catatan yang tidak terotorisasi yang memberikan akses kepada peretas, atau dapat secara sederhana menyoroti tabel dengan nama yang umum (seperti tabel pengguna dan tabel pelanggan). XXS adalah metode dalam menambahkan *JavaScript* dan instruksi pencarian lainnya ke dalam data yang ada di situs. Ketika instruksi ini diinterpretasikan oleh pengguna, maka perilaku yang tidak terotorisasi terjadi. Contoh yang umum adalah pengalihan pengguna ke situs yang palsu dan pembajakan pengguna ID *cookie* untuk akses yang tidak terotorisasi.

Salah satu kecurangan yang paling umum dalam bisnis secara tradisional adalah "*bust-out*" atau kebangkrutan yang direncanakan. Hal itu merupakan bentuk yang paling sederhana, dimana pelaku membangun bisnis, membeli persediaan secara kredit, menjualnya dengan harga rendah, dan menghilang dengan uang sebelum tagihan dibayar.

Pesan surel dan kunjungan ke situs dapat dibajak karena perbedaan yang hampir tidak terlihat dalam nama induk internet yang sering tidak diketahui oleh pengguna internet. Contohnya *"computer.com"* dan *"computer.org"* merupakan dua nama induk yang sama sekali berbeda yang dapat dengan mudah membingungkan. Jika dua nama dimiliki oleh entitas yang berbeda, salah satu situs dapat meniru yang lainnya dan menipu pengguna, karena dalam pikiran mereka, mereka sedang berurusan dengan situs atau alamat surel yang asli. Banyak perusahaan membeli semua nama domain untuk semua bentuk nama perusahaan mereka, termasuk yang salah eja, untuk mencegah tipe kesalahan situs ini yang dipergunakan pihak lain untuk membantu pengguna menemukan situs asli.

Mencegah Kecurangan Melalui Aktivitas Pengendalian

Aktivitas pengendalian adalah kebijakan dan prosedur yang memastikan bahwa tindakan yang diperlukan telah diambil terhadap adanya resiko dan terjadinya kecurangan. Aktivitas pengendalian umumnya gagal pada lima tipe berikut ini:

1. Pemisahan tugas yang memadai.
   Pengendalian ini berguna untuk memastikan bahwa individu yang mengotorisasi transaksi berbeda dengan individu yang secara aktual mengeksekusi transaksi tersebut. Pada bagian ini, umumnya kecurangan yang sering terjadi pada transaksi pembelian dan penjualan adalah *kickback* dan penjualan. Untuk itulah pentingnya pemisahan tugas yang memadai, agar dapat mencegah penyuapan karena pelanggan tidak sepenuhnya memiliki pengendalian atas transaksi.
2. Otoritas yang sesuai atas transaksi dan aktivitas.
   Otorisasi yang sesuai adalah pengendalian lain yang memiliki peranan dalam e – business. Pengendalian Otorisasi yang paling umum adalah kata sandi, *firewall*, akta, dan tanda tangan digital, dan biometrika.
   a. Kata Sandi
      Merupakan bagian penting dari jaminan keamanan dari sejumlah sistem elektronik, tapi kata sandi yang merupakan *Achilles' heel* karena keterlibatan banyak orang. Kata sandi yang dapat dikompromikan memungkinkan adanya transaksi yang telah dibuat tidak terotorisasi. Untuk mencegah kecurangan, organisasi seharusnya secara jelas mengkomunikasikan kebijakan yang dimilikinya terkait pemulihan, perubahan dan pengungkapan kata sandi. Dalam lingkungan sistem elektronik, tidak ada pengendalian untuk mencegah kecurangan yang lebih baik dilakukan selain penggunaan kata sandi secara bijak dan pelatihan yang memadai bagi penggunanya.
   b. Akta dan Tanda Tangan Digital
      Seperti tanda tangan dalam dokumen kertas yang berfungsi sebagai otorisasi atau verifikasi, tanda tangan digital meyakinkan kembali pengguna bahwa transaksi valid. Akta dan Tanda Tangan Digital kemudian mencegah adanya pemalsuan identitas dan pemalsuan peran dan beberapa hal penting lain.
   c. Biometrika

Merupakan penggunaan nilai–nilai unik dari bagian tubuh manusia untuk memberikan jaminan keamanan atas pengendalian akses. Karena setiap orang memiliki karakteristik biologis yang unik (contohnya, pola iris dan retina mata, sidik jari, pita suara, struktur wajah dan bentuk tulisan tangan), ilmuwan dan perusahaan teknologi yang mengembangkan peralatan keamanan khusus yang memiliki potensi untuk secara akurat membuktikan kebenaran suatu identitas. Akses dan izin untuk melakukan transaksi diberikan atau ditolak didasarkan dari seberapa mirip pembahasan selanjutnya terkait referensinya.

3. Dokumentasi dan kegiatan pencatatan yang memadai.
   Dokumentasi dan pencatatan faktur penjualan, order pembelian, pencatatan tambahan, jurnal penjualan, kartu jam kerja pegawai, dan cek merupakan objek fisik dimana transaksi dicatat, diklasifikasikan, dan diikhtisarkan. Dalam *e-business*, dokumen–dokumen ini disajikan dalam bentuk elektronik. Kurangnya dokumentasi yang tercetak *(hard copy)*, merupakan pokok utama dari *e-business*, menciptakan kesempatan baru untuk melakukan kecurangan. Dokumentasi dan pencatatan biasanya merupakan pengendalian investigatif, bukan pengendalian preventif. Dokumentasi dan pencatatan merupakan jejak penelusuran audit dan memungkinkan auditor dan pemeriksa kecurangan untuk melakukan investigasi atas dugaan adanya kesalahan yang dilakukan.
   Transaksi elektronik yang utama dan pengendalian dokumentasi adalah enkripsi, yang melindungi informasi rahasia atau sensitif (seperti cek atau transaksi pembelian atau transaksi penjualan) dari kegiatan "*sniffing*" atau upaya pencurian.
4. Pengendalian fisik atas aset dan pencatatan.
   Perusahaan yang telah terkomputerisasi membutuhkan sesuatu yang khusus untuk melindungi peralatan, program, dan arsip data yang ada pada komputer. Tiga kategori pengendalian meliputi melindungi peralatan teknologi informasi *(hardware)*, melindungi program *(software)*, serta melindungi arsip data dari kecurangan. Seperti jenis lainnya dari aset, pengendalian fisik yang dipergunakan untuk melindungi fasilitas komputer contohnya adalah penguncian pintu ruangan penyimpanan terminal komputer dan ruangan penyimpanan yang memadai serta aman untuk perangkat lunak dan arsip data. Sebagai tambahan untuk jaminan keamanan berbasis perangkat lunak, perangkat keras dan perangkat lunak yang mencakup infrastruktur TI harus secara fisik terjamin keamanannya. Terkadang infrastruktur fisik sangat sensitif dan penting untuk kegiatan operasional *e-business*, oleh karena itu sistem perlu ditempatkan dalam lokasi yang terisolasi dengan akses keamanan tingkat tinggi.
5. Pengecekan yang indenpenden atas kinerja.
   Pengecekan yang independen secara khusus penting dalam pencegahan kecurangan dalam kegiatan *e-business*. Kebutuhan pengecekan ini muncul karena adanya perubahan sistem pengendalian internal dari waktu ke waktu, personel lupa atau gagal dalam mengikuti prosedur, atau menjadi kurang berhati-hati kecuali jika seseorang melakukan observasi dan evaluasi atas kinerja mereka. Perlu diingat bahwa kemungkinan besar transaksi yang mengandung kecurangan muncul ketika pengendalian tidak berfungsi.

   Kecurangan elektronik, khususnya jika dilakukan oleh perusahaan yang berskala kecil, sering dilakukan oleh seseorang yang mempunyai kedudukan tinggi dalam organisasi, dan cukup sering mewakili organisasi, dimana orang tersebut pada suatu saat melakukan perlawanan terhadap organisasi. Karena manajemen biasanya terlibat, manajemen dan dewan direksi atau mitra bisnis harus diinvestigasi untuk menentukan *eksposure* mereka terhadap motivasi untuk melakukan tindak

kecurangan. Untuk mencegah terjadinya kecurangan, memperoleh pemahaman yang lengkap dan detail tentang manajemen atau mitra bisnis dari organisasi, serta mengetahui apa motivasi mereka merupakan hal yang sangat penting. Untuk itu perlu dilakukan pengujian/evaluasi terhadap beberapa hal dalam rangka mendapatkan pemahaman tersebut. Secara khusus ada tiga unsur utama yang harus diuji, yaitu:

a. Latar Belakang
   - Apakah ada organisasi lain di masa lalu yang membuat pihak manajemen dan dewan direksi pernah memiliki keterikatan?
   - Apakah ada situasi atau keadaan tertentu dimasa lalu yang pernah membuat pihak manajemen dan dewan direksi pernah memiliki keterikatan?
b. Motivasi
   - Apa yang sesungguhnya menjadi pemicu dan hal–hal yang dapat memotivasi pemimpin organisasi?
   - Apakah mereka dibawah tekanan untuk membuat hasil yang tidak realistis?
c. Pengaruh Pengambilan Keputusan
   - Apakah kompensasi utama mereka berdasarkan pada kinerjanya?
   - Apakah setiap perjanjian utang atau tekanan keuangan lainnya ada?

Kemampuan manajemen untuk mempengaruhi keputusan merupakan hal penting untuk dipahami, karena ketika kecurangan hanya dilakukan satu atau dua individu yang memiliki kekuatan utama dalam hal pembuatan keputusan, maka akan jauh lebih mudah mengatasinya.

Mendeteksi Kecurangan E-Business

Pendeteksian kecurangan dapat disebabkan faktor data dengan semua jenis kecurangan yang mungkin terjadi diidentifikasi, selanjutnya teknologi dan aktivitas terkait lainnya digunakan untuk melihat gejala kecurangan. Oleh karena itu, pemeriksaan kecurangan harus:

1. Berusaha untuk memahami bisnis atau kegiatan operasional organisasi.
2. Mengidentifikasi kecurangan apa yang dapat terjadi dalam kegiatan operasional.
3. Menentukan gejala – gejala yang paling mungkin muncul saat terjadinya kecurangan.
4. Menggunakan basis data dan sistem informasi untuk mencari gejala tersebut.
5. Melakukan analisis terhadap hasil.
6. Melakukan investigasi terhadap gejala–gejala untuk menentukan apakah hal tersebut disebabkan oleh kecurangan secara aktual atau faktor lainnya.

Metode pendeteksian kecurangan ini memiliki kemampuan sangat baik dalam mendeteksi kecurangan *e-business*. Salah satu teknik terbaik untuk mengimplementasikan jenis pendeteksian kecurangan adalah penggunaan teknologi dalam menangkap kecurangan yang berbasis teknologi. Banyak alat peretas yang digunakan untuk menyelesaikan dan menangkap pelaku daripada untuk meretas ke dalam sistem. Sehingga menjadi sangat penting bagi investigator kecurangan *e-commerce* untuk memahami alat dan metode yang digunakan pelaku.

Pengetahuan mengenai server situs, surel klien dan server terkait, serta program yang didesain untuk mengganggu seperti Nmap, Airsnort, dan Wireshark penting untuk menangkap pelaku dan mengamankan sistem. Investigator kecurangan *e-commerce* ada baiknya jika mengambil beberapa pelatihan yang terkait dengan sistem informasi atau ilmu jaringan komputer dan program jaminan keamanan. Hal ini karena saat ini

banyak server dan infrastruktur internet yang dimiliki perusahaan berbasis Unix, sehingga pengetahuan terkait Unix/Linux dinilai sangat penting. Selain itu, aplikasi yang dimiliki klien seringkali berbasis Windows, sehingga pengetahuan yang terkait dengan kekuatan dan kelemahan keamanan dalam Windows juga menjadi penting.

Bahasa pemrograman komputer, yang ditulis dalam bahasa seperti *Perl, Python, Ruby,* dan *Bash,* dapat memantau log dan sistem untuk mengetahui kemungkinan adanya kerusakan sistem. Oleh karena itu berbagai sistem pendeteksian gangguan terhadap sistem dan program yang berbeda (*Instrusion Detection System* – IDS) banyak tersedia dalam pasar saat ini. Penggunaan dan pengawasan terhadap sistem yang ada secara berhati-hati seharusnya dilakukan oleh setiap organisasi. Hal ini merupakan salah satu usaha untuk meminimalkan terjadinya penyalahgunaan penggunaan sistem komputer perusahaan yang akan berakibat munculnya tindakan *fraud.*

Keuntungan transaksi *e-business* adalah bahwa informasi terkait transaksi yang didapatkan secara elektronik dalam basis data dapat dianalisis dalam berbagai macam cara. Data ini membuat pendeteksian kecurangan berlangsung lebih cepat dibandingkan sebelumnya, tapi teknik ini membutuhkan lebih banyak tenaga ahli komputer. Aspek yang paling sulit mendeteksi kecurangan *e-business* adalah menentukan secara benar jenis kecurangan yang dapat terjadi dan gejala-gejala keterjadiannya. Gejala hanya merupakan bukti tidak langsung yang dianggap terbaik. Mungkin ada penjelasan logis dan jelas untuk faktor-faktor yang muncul sebagai gejala. Bagaimanapun juga, transaksi *e-business* dapat menyebabkan kecurangan lebih mudah dilakukan, tapi juga membuatnya lebih mudah terdeteksi.

Selain dengan teknologi di atas, melakukan pencegahan dan pendeteksian secara sosial adalah hal yang penting. Kegiatan audit secara teratur atas perilaku pengguna dalam sistem harus dilakukan dengan mengamati bagaimana pengguna berinteraksi dengan sistem yang mereka gunakan. Para staf atau pegawai perlu mendapatkan pelatihan tentang apa itu kecurangan *e-commerce* sehingga mereka dapat melihat apakah terjadi permasalahan seperti itu pada perusahaan mereka. Pengguna juga perlu mendapatkan pelatihan bahwa sementara anomali komputer mungkin tidak bernilai signifikan, mereka dapat menyoroti permasalahan secara mendalam. Seperti misalnya informasi terkait kasus kecurangan dalam sistem tradisional, informasi tersebut dapat berguna dalam mengatasi kecurangan secara eletronik apabila pegawai memiliki pengetahuan yang memadai serta memahami apa yang harus mereka cari.

Simpulan

Kecurangan E-Commerce merupakan salah satu permasalahan yang paling siginifikan dalam bisnis saat ini. Dengan mempertimbangkan kemampuan yang dibutuhkan untuk melakukan pendeteksian dan investigasi kecurangan E-Commerce, maka setidaknya kita dapat melakukan pencegahan peretasan sistem tersebut. Penggunaan dasar-dasar jaminan keamanan yang telah teruji akan sangat membantu mencegah terjadinya kecurangan dalam E-business. Mengenai hal tersebut pendekatan yang dapat dilakukan adalah: (1) Memahami risiko kecurangan E-Commerce; (2) mengambil langkah-langkah untuk mencegah kecurangan dalam E-Commerce; serta (3) mendeteksi kecurangan E-business.

Untuk memperjelas pemahaman tentang konsep internet fraud, berikut ini disajikan kasus yang dapat dijadikan latihan untuk memecahkan persoalan terkait dengan internet fraud.

Contoh Kasus

Fraud pada Situs Tiket.Com

Terungkapnya kasus ini berawal dari pengaduan PT Global Tiket Network kepada polisi tentang adanya peretasan pada sistem aplikasi jual beli tiket daring Tiket.com yang tersambung dengan sistem penjualan tiket pada maskapai penerbangan PT Citilink Indonesia (www.citilink.co.id) pada 11-27 Oktober 2016.

Dari hasil pemeriksaan, diketahui tersangka MKU berperan menawarkan penjualan tiket pesawat melalui akun HJ pada jejaring sosial Facebook. MKU memiliki username dan password untuk masuk ke server Citilink yang didapatkannya dengan cara meretas situs Tiket.com bersama tersangka SH. Tersangka melakukan login terhadap server Citilink dengan menggunakan username dan password milik travel agen Tiket.com dengan tujuan mendapatkan kode booking tiket pesawat Citilink untuk dijual ke pembeli.

Sementara tersangka AL bertugas memasukkan data pesanan tiket pesawat Citilink dari pembeli yang selanjutnya data tersebut dimasukkan ke aplikasi penjualan maskapai Citilink dengan menggunakan *username* dan *password* milik travel agen Tiket.com dan setelah kode booking pesawat didapat, selanjutnya kode booking tersebut dikirim ke pihak pembeli. Tersangka lainnya NTM bertugas mencari calon pembeli melalui akun Facebook bernama Nokeyz Dhosite Kashir. Setelah mendapatkan calon pembeli, data calon pembeli diberikan kepada tersangka AL untuk diproses dengan prosedur yang sama. Untuk menarik minat pembeli mereka menjualnya dengan harga diskon 30 sampai 40 persen. Dari bisnis haram ini kawanan SH cs meraup keuntungan sekitar Rp 1 miliar.

Keempat tersangka termasuk SH awalnya berkenalan melalui Facebook karena memiliki kegemaran memainkan permainan yang sama. Dua tersangka MKU dan AL lulusan SMA. Kalau NTM mahasiswa yang tidak meneruskan kuliahnya. Sehari-harinya profesinya sebagai gamer. Sedangkan SH Pendidikan formalnya hanya sampai bangku SMP, bahkan tidak lulus. Dalam pengungkapan kasus ini, penyidik menyita barang bukti, tujuh unit ponsel, tiga kartu ATM, dua surat izin mengemudi (SIM), dua KTP, dua unit laptop, satu buku tabungan Bank BCA dengan saldo Rp 212 juta, satu unit router wifi, satu kartu mahasiswa (KTM) dan satu unit sepeda motor.

Pihak tiket.com mengalami kerugian sebesar Rp 4.124.000.982 karena pelaku meretas, mengambil serta menjual jatah deposito tiket pesawat pada server Citilink Indonesia. Pihak Citilink juga merugi Rp 1.973.784.434 karena ada sejumlah orang yang membeli tiket dari sindikat peretas tersebut melakukan pembatalan dan refund. Sebelumnya tiga orang berinisial MKU (19), Al (19) dan NTM (27) itu ditangkap di Jalan Siaga Dalam Gang Kemuning Nomor 12 RT 19 Kelurahan Damai, Kecamatan Balikpapan Selatan, Kota Balikpapan, Kalimantan Timur. Sementara yang sebelumnya buron yaitu SH ditangkap petugas di rumah orang tuanya di kawasan Situ Gintung, Cirendeu, Ciputat, Tangerang Selatan, Banten, pada Kamis (30/3/2017) siang.

Ahli keamanan internet Alfons Tanujaya menilai kasus peretasan situs Tiket.com yang berakibat kerugian miliaran rupiah bisa terjadi ke situs komersial lain di Indonesia. Dari sudut pandang Alfons, pemilik situs komersial dalam negeri terlalu mengabaikan terhadap standar keamanan. Menurut Alfons (2015), kejadian itu sebenarnya tidak mengagetkan. Ia mengklaim sistem

keamanan perusahaan teknologi di Indonesia saat ini pada umumnya sudah rentan. Masih banyak yang sekadar pakai *username* dan *password*, padahal itu sudah ketinggalan," kata Alfons kepada CNN Indonesia.com. Standar keamanan yang rendah yang diterapkan perusahaan teknologi dianggap mudah memancing aksi peretasan yang berujung kerugian finansial. Alfons bahkan menilai jika tak ada perubahan sistem keamanan username & password, cuma waktu yang menentukan kapan kasus serupa akan terulang.

Masih menurut Yusuf dan Anggriawan (2015), perusahaan teknologi Indonesia sebaiknya mulai menerapkan *Two Factor Authentification* (TFA) atau bisa disebut verifikasi dua lapis. TFA dianggap telah menjadi standar baku terkini sistem keamanan. TFA sudah diterapkan pada situs-situs terkenal seperti Google, Facebook, serta Twitter. Dengan TFA, sebuah situs tidak akan hanya meminta username dan password, namun juga meminta satu informasi yang hanya bisa dimiliki dan diketahui oleh pemilik akun yang asli. Verifikasi dua lapis sebenarnya sudah dipakai oleh kalangan perbankan untuk mencegah kerentanan saat terjadi transaksi elektronik. Sistem token seperti yang dimiliki BCA misalnya merupakan contoh penerapan TFA ini.

Kemungkinan solusi yang dapat dilakukan

a) Memahami risiko kecurangan E-commerce, yang muncul baik dari dalam maupun dari luar. Risiko dari dalam seperti: tekanan, kesempatan, peningkatan kecenderungan terhadap rasional. Sedangkan risiko dari luar meliputi: *Sniffing, Wartrapping, Spyware, Phishing, dan Spoofing.*
b) Mengambil langkah-langkah untuk mencegah kecurangan dalam E-commerce melalui aktivitas pengendalian seperti halnya menerapkan *Two Factor Authentification* (TFA) atau bisa disebut verifikasi dua lapis.
c) Mendeteksi Kecurangan E-business, dan segera melakukan antisipasi secara tepat dan strategik.

Daftar Bacaan

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C., Zimbelman, dan Mark F. (2012). *Fraud Examination.* Fourth edition (USA: South-Western Cengage Learning).

Gema. A.J. (2013). *"Cybercrime: Sebuah Fenomena di Dunia Maya".* http://www.interpol.go.id/id/ kejahatan-transnasional/kejahatan-dunia-maya/89-cybercrime-sebuah-fenomena-di-dunia-maya

Koong, K., Liu, L., Qin, H. and Ying, T. (2017), Occurrences of online fraud complaints: 2002 through 2015, *International Journal of Accounting & Information Management*, 25 (4), 484-504. https://doi.org/10.1108/IJAIM-12-2016-0113.

Kovács, L. and David, S. (2016), Fraud risk in electronic payment transactions, *Journal of Money Laundering Control*, 19 (2), 148-157. https://doi.org/10.1108/JMLC-09-2015-0039.

Norris, G., Brookes, A. & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34, 231-245.

Tara. J. (2013). *"Fenomena Kejahatan Penipuan Internet dalam Kajian Hukum Republik Indonesia".* http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-

dunia-maya/92-fenomena-kejahatan-penipuan-internet-dalam-kajian-hukum-republik-indonesia

Testa, A., Maimon, D., Sobesto, B. & Cukier, M. (2017). Illegal Roaming and File Manipulation on Target Computers. Assessing the Effect of Sanction Threats on System Trespassers' Online Behaviors. *Criminology and Public Policy*, 16 (3), 689-726.

Yusuf, R. & Anggriawan, E. (2015). *Penerapan metode smart authentication dalam layanan e-banking menggunakan two channel authentication dan qr-code pada perangkat mobile android.* Seminar Nasional Sistem Informasi Indonesia (SESINDO).

http://www.cnnindonesia.com/teknologi/20170331170940-185-204118/pakar-keamanan-ti-kasus-tiketcom-berpotensi-terulang/

http://www.tribunnews.com/techno/2017/03/30/server-dibobol-tiket-hasil-curian-di-tiketcom-dijual-dengan-diskon-40-persen

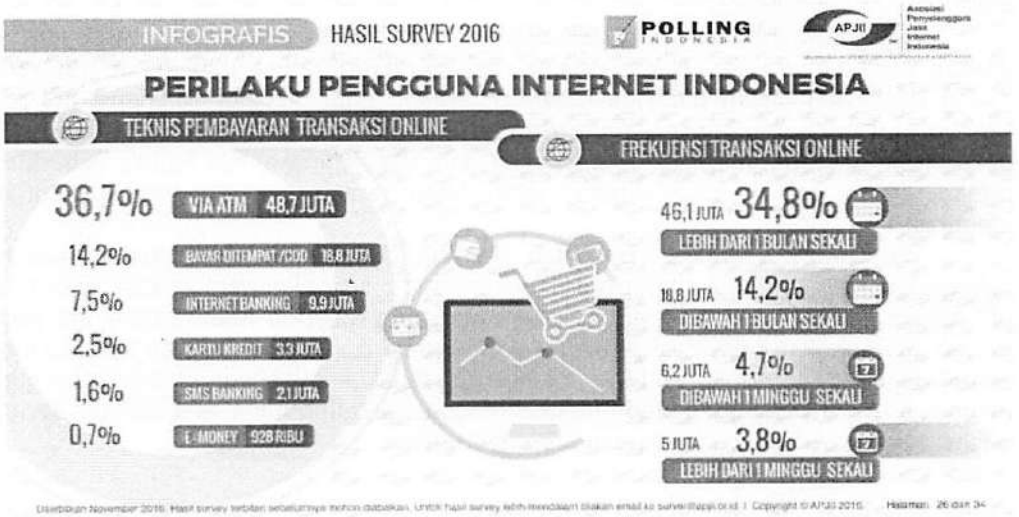
http://www.cnnindonesia.com/teknologi/20170331145137-185-204065/begini-cara-hacker-bobol-situs-tiketcom/

BAB 6
PENCURIAN IDENTITAS

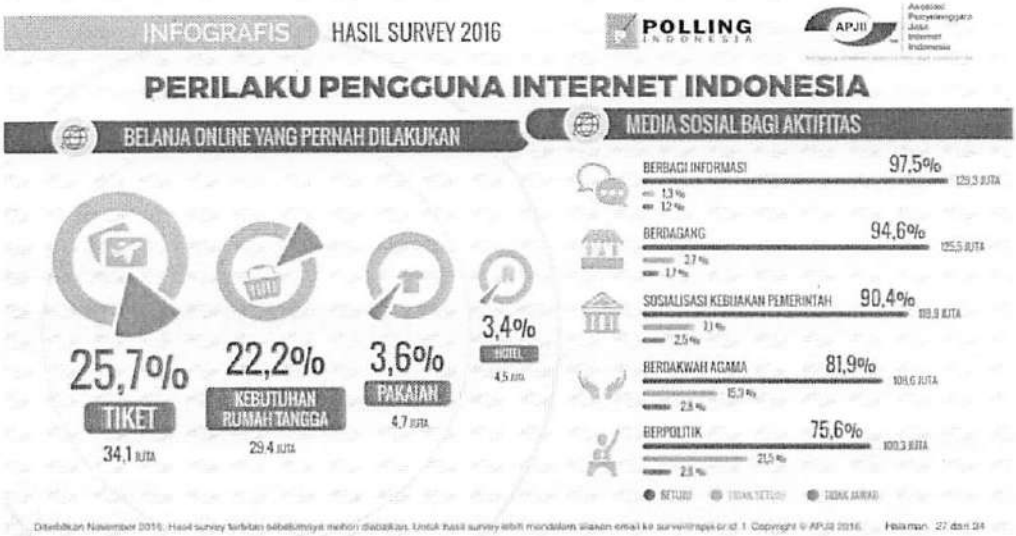
Pendahuluan

Saat ini pemakaian dunia maya khususnya internet merupakan hal yang sangat penting dalam kehidupan sehari–hari. Hampir seluruh transaksi dilakukan menggunakan internet. Internet merupakan sistem jaringan yang menghubungkan seluruh komputer yang ada di sekuruh dunia guna mendapatkan informasi yang diperlukan, dapat digunakan untuk berinteraksi dengan orang lain yang sangat jauh sekalipun. Penggunaan internet dalam kehidupan sehari–hari sebagai contoh adalah transaksi perbankan, transaksi jual beli dan segala kebutuhan informasi yang diperlukan manusia dapat dicari dengan menggunakan internet.

Di Indonesia, penggunaan internet sangat besar, ini dapat dilihat dari hasil survey berikut:



Gambar 7. Teknis Pembayaran Transaksi on Line di Indonesia (Survey 2016) (https://proxsisgroup.com diakses tanggal 02/05/2019)



Gambar 8. Survey belanja on Line (Survey tahun 2016)
(https://proxsisgroup.com diakses tanggal 02/05/2019)

Dengan adanya internet sangat membantu kehidupan manusia, akan tetapi ada beberapa hal yang merugikan dalam penggunaan internet salah satunya adalah masalah mengenai privasi. Dengan adanya internet, privasi seseorang seolah menyempit. Dengan mengakses internet memaksa seseorang untuk mengisi data–data yang bersifat umum maupun pribadi, seperti alamat rumah, nomor telepon, alamat e-mail, dan nomor rekening bank.

Kejahatan internet yang berkaitan dengan privacy, sebagai contoh adalah *identity theft* dan *stalking*. Penggunaan *password* merupakan salah satu perlindungan paling sederhana dalam menjaga identitas pribadi tetap menjadi konsumsi pribadi. Namun saat ini, penggunaan password tidak lagi cukup efektif karena ada beberapa pihak yang mampu membobol *password* dan menggunakannya untuk keperluan pribadi. Dalam bab ini, akan dibahas lebih dalam tentang *identity theft* (pencurian identitas).

Pencurian identitas bukanlah bentuk kejahatan baru, korbannyapun kebanyakan berasal dari orang-orang yang tanpa sengaja memberikan informasi pribadinya kepada pihak lain, entah secara langsung maupun tidak. Bagi Anda yang pernah memberikan informasi pribadi, yakni memberikan nama lengkap serta nomor identitas (seperti nomor KTP, SIM, atau tanda pengenal lainnya) pada *telemarketer*, atau mengisi formulir pengajuan kredit melalui tenaga marketing bank, atau bahkan secara online, Anda harus waspada dengan *identity theft* ini.

Modus Operandi Pencurian Identitas

Para pelaku kejahatan jenis ini akan mengumpulkan informasi tentang calon korbannya yang kini cukup mudah didapat dengan berbagai macam cara dan mereka akan berpura-pura menjadi Anda dengan menggunakan informasi tersebut. Informasi ini akan mereka gunakan untuk berbagai macam hal yang menguntungkan bagi mereka, misalnya membuat kartu kredit baru dengan nama Anda, mengajukan kredit/cicilan

baru, dan masih banyak lagi kemungkinan perbuatan curang yang dapat mereka lakukan.

Tagihan kartu kredit palsu, misalnya, dapat dikirim pada alamat lain sesuai dengan kehendak si pelaku, biasanya dengan alasan bahwa Anda telah pindah rumah sehingga tidak sesuai dengan alamat yang terkait dengan nomor identitas Anda. Sehingga dengan begitu Anda tidak akan mendeteksi adanya tagihan lain yang menggunakan nama dan akun rekening Anda karena tagihannya tidak pernah sampai langsung ke tangan Anda.

Jika demikian, Siapa yang dirugikan?

Anda mungkin tidak merasa bahwa identitas Anda telah disalahgunakan hingga berbulan-bulan lamanya, sampai Anda ditagih/dihubungi langsung oleh bank yang bersangkutan karena telah menunggak pembayaran hingga sekian waktu lamanya. Bila hal ini terjadi, para pelaku kejahatan juga akan sulit terlacak dan bahkan tidak akan ditindak pidana. Sebenarnya para pelaku pencurian identitas ini tidak menarget Anda sebagai korban. Pada beberapa negara, bila terbukti ada pencurian identitas yang terjadi dengan menggunakan nama Anda, maka Anda tidak akan dikenai pasal atau hukuman apapun, dan Anda tidak perlu membayar tagihan yang dibebankan kepada Anda. Sebenarnya Anda tidak dirugikan secara finansial. Korban yang sebenarnya dalam hal ini adalah pihak bank, pertokoan dan penyedia layanan.

Namun kejadian ini tetap akan merugikan reputasi dan nilai kredit Anda, karena waktu yang harus Anda habiskan untuk membersihkan nama baik sekaligus nilai kredit bisa berlangsung cukup lama dan menguras tenaga. Bayangkan berapa banyak surat dan klarifikasi yang harus Anda tulis dan lakukan pada pihak-pihak yang bersangkutan bahwa kredit yang diajukan pada mereka bukanlah berasal dari Anda pribadi tetapi merupakan ulah orang-orang yang tidak bertanggung jawab.

Pengertian Pencurian Identitas *(Identity Theft)*

Pencurian Identitas dalam Arti Sempit

Pencurian identitas dalam arti sempit berarti bahwa seseorang mengambil suatu kartu pengenal/segala jenis pengenal milik orang lain untuk kemudian dia gunakan pada dirinya sendiri sebagai identitas pengenal orang yang dicuri tersebut. Saat ini pencurian identitas yang terjadi banyak dilakukan karena motif yang beragam, dimulai dari kepentingan untuk mencapai tujuan ekonomi yang mereka inginkan, penipuan, sampai sekedar melampiaskan motif dendam semata.

Pencurian Identitas dalam Arti Luas

Pencurian identitas dalam arti luas berarti bahwa seseorang telah menjadi sangat depresi atau mengalami gangguan kejiwaan *(psikopat)* dengan meniru atau mencuri identitas orang lain yang dia ingat, benci, atau sukai. Pencurian identitas sangat merugikan karena orang yang dicuri identitasnya mungkin citranya akan buruk di mata orang lain.

Pencurian Identitas Secara Umum

Secara umum pencurian identitas merupakan suatu bentuk dari kecurangan di dalam dunia IT dimana seseorang berpura-pura menjadi "orang lain" dengan berbekal identitas orang lain tersebut, biasanya hal ini dilakukan dengan tujuan untuk

memperoleh akses atau mengambil alih kartu kredit dan keuntungan lainnya dari orang tersebut.

Kategori Pencurian Identitas

a. *Bussines / Commercial Identity Theft* (Pencurian Identitas Bisnis / Komersial)
   Tipe ini menggunakan nama bisnis ataupun identitas bisnis orang lain untuk memperoleh keuntungannya sendiri.
b. *Criminal Identity Theft* (Pencurian Identitas Pidana).
   Tipe ini beraksi sebagai orang lain ketika akan melakukan tindakan kejahatan
c. *Financial Identity Theft* (Pencurian Identitas Keuangan)
   Tipe ini menggunakan identitas orang lain untuk memperoleh kredit, barang serta layanan yg dimiliki oleh orang tersebut.
d. *Identity Cloning* (Kloning Identitas)
   Tipe ini menggunakan identitas serta informasi yang dimiliki orang lain didalam kehidupannya sehari-hari.
e. *Medical Indentity Theft* (Pencurian Identitas Medis)
   Tipe ini menggunakan identitas orang lain untuk memperoleh layanan kesehatan dan obat-obatan.

Cara yang Digunakan dalam Pencurian Identitas

Cara Pencurian Identitas Secara Umum

Pada dasarnya, secara umum para pelaku pencurian identitas tidak menarget Anda sebagai korban. Pada beberapa negara, bila terbukti ada aktivitas pencurian identitas yang terjadi dengan memakai nama Anda, maka Anda tidak akan dikenai pasal atau hukuman apapun, selain itu Anda tidak perlu membayarkan tagihan yang dibebankan pada Anda. Dengan demikian Anda tidak dirugikan secara finansial. Korban yang sebenarnya dalam hal ini adalah pihak bank dan pertokoan. Berikut ini berbagai cara yang kemungkinan dapat dilakukan oleh para pelaku terkait dengan upaya pencurian identitas secara umum:

a. Menggali informasi data diri seseorang dari "sampah" *(Dumpster Diving)*.
b. Mengambil data personal dari perangkat-perangkat elektronik dan media penyimpanan termasuk PC, server, PDA, Handphone, USB Disk, dan *hard disk* yang tertera di situs-situs publik.
c. Menggunakan data publik dari individu warga negara yang di publish pada tempat-tempat pendaftaran umum seperti pada pemilihan umum.
d. Mencuri kartu kredit atau akun bank, KTP, *passpor* dengan cara mencopet atau membobol rumah korban.
e. Skimming informasi dari para pemegang kartu kredit.
f. Mencuri informasi personal dari computer dengan menggunakan *malware*, seperti *trojan horse, keylogging*, dan lain-lain.
g. Hacking pada jaringan komputer, sistem dan database, sringkali dilakukan dalam skala besar.
h. Browsing pada situs-situs jejaring sosial untuk melihat detail informasi dari korban.
i. Mengalihkan yang tertuju pada korban ke email pelaku.
j. Berpura-pura sebagai *customer service representative* atau pekerja *help-desk* dengan mendekati korban untuk memperoleh data-data pribadi korban.

Cara Pencurian Identitas Kartu Kredit

Kehadiran kartu kredit memang memudahkan sebuah transaksi. Akan tetapi, diperlukan kewaspadaan yang tinggi pada saat menggunakannya. Berbagai tindak kejahatan kartu kredit dapat ditemukan di mana saja, salah satu yang marak saat ini adalah dengan cara *skimming*. Skimming merupakan tindak kajahatan kartu kredit dengan cara mengkopi data kartu milik nasabah dan menyalinnya ke kartu yang baru. Berikut cara yang umum dilakukan oleh pelaku kejahatan kartu kredit terkait dengan metode *skimming*:

a. Data dan nomor awalnya didapat dengan cara *skimming* artinya merekam secara elektronik data pada ***magnetic stripe*** skimming ini biasanya dikerjakan dengan sebuah alat sebesar bungkus rokok dan tergantung ada berbagai model yang dijual di pasaran, biasanya si pelaku kejahatan dalam mencuri data dan nomor dari kartu kredit asli akan menitipkan *skimming* tersebut di restoran, hotel, toko, maupun tempat-tempat pembayaran dengan alat bantu gesek, yang artinya harus ada keterlibatan orang dalam dari tempat-tempat tersebut. Pada umumnya, modus operandinya si kasir menyembunyikan ***SKIMMER*** di bawah meja dan melakukan dua kali penggesekan tanpa sepengetahuan pemilik kartu.
b. Cara lain pencurian data pemilik kartu kredit asli adalah bisa dengan cara memasang semacam **CHIP** pada terminal **POS** (***point of sale***) yaitu sebuah alat gesek kartu kredit yang digunakan untuk keperluan pembayaran pada restoran, toko, hotel, super market, dan lainnya dimana si-pelaku kejahatan di sini bisa petugas service terminal **POS**, karyawan pada terminal **POS**, atau orang lain yang menitipkan. Intinya bahwa **CHIP** harus dipasang oleh petugas yang menangani terminal POS, misalkan pada saat service.
c. Dengan cara ***SKIMMING*** dan **CHIP *Information*** ini maka *Card Verification Value (CVV)* yang mempunyai tiga digit angka yang berfungsi sebagai pengaman kartu kredit akan ikut terekam.

Kasus Pencurian Data Kartu Kredit dan Kartu Debit

Global	Indonesia
Pencurian Data Kartu Kredit dan Kartu Debit Di Perusahaan Retail "Target" di US	**Pencurian Data Kartu Kredit Dan Kartu Debit di Merchant Body Shop**
• Hacker berhasil mengakses informasi kartu debit dan kredit pelanggan selama thaksgiving dan christmas shopping season (27 November – 15 Desember 2013) sebanyak 40 juta data pelanggan. • Data yang berhasil diambil : nama, alamat, nomor telepon, alamat email, pin untuk kartu debit • Software yang digunakan untuk meretas data tersebut ternyata dapat diperoleh secara mudah hanya dengan harga $1800 - $2300 • Software tersebut tidak terdeteksi sebagai malware oleh firewall.	• Pada 5 Maret 2013, terdeteksi *fraud counterfeit* kartu debit di Amerika Serikat (AS) dan Meksiko yang kemudian pada 7 Maret 2013 juga Filipina, Turki, Malaysia, Thailand dan India. • Kejahatan dengan menyalahgunakan kartu kredit diduga dilakukan melalui praktik double swipe, di EDC dan pada alat lain (cash register) untuk kepentingan merchant. Data kedua dimasukkan oleh pihak tertentu ke suatu jaringan dan disebarluaskan, serta disalahgunakan. • Korban yaitu nasabah Bank BCA, Mandiri dan Citibank. Bank BCA mengalami kerugian sekitar Rp 1 miliar.

Sumber : http://www.forbes.com/sites/paularosenblum/2014/01/17/the-target-data-breach-is-becoming-a-nightmare/, 2014
http://www.infobanknews.com/2013/03/bca-siap-ganti-kerugian-nasabah-korban-pencurian-data-kartu/, 2013

Tabel 4. Kasus Pencurian Data Kartu Kredit & Debit

Pencegahan Pencurian Identitas

Era milenium salah satunya ditandai dengan menyatunya identitas dengan kehidupan perbankan. Apabila identitas pribadi kita hilang, maka orang lain sangat berpeluang untuk mengganggu kehidupan finansial kita bahkan sampai uang kita yang tersimpan di Bank habis sama sekali. Ada berbagai cara untuk melakukan praktik jahat seperti ini, dimulai dari mengintip kode-kode rahasia seseorang ketika melaksanakan transaksi pembelian secara online, mengakses sistem perbankan seseorang melalui saluran internet, mengacak-acak akun e-mail milik seseorang dengan memasukkan enkripsi tertentu, dan lain-lain. Pada umumnya, kasus pencurian identitas selalu dibarengi dengan aktivitas pencurian uang. Banyak kasus yang kita temui terkait dengan tindakan pencurian identitas ini. Kita bisa mencarinya di Google, melihat di TV, maupun media masa lain tentu akan ditemukan banyak kasus pencurian semacam itu. Untuk menghindari kasus pencurian identitas ini, ada berbagai cara yang bisa kita lakukan, diantaranya meliputi hal-hal berikut:

1. Hindari menyimpan, meletakkan serta membuang berbagai benda yang mengandung informasi penting seperti komputer pribadi, *hardisk, flashdisk,* lembaran dan kartu berharga di sembarang tempat.
2. Memproteksi segala jenis informasi pribadi dan informasi rahasia lainnya dengan tidak memberikan kepada pihak manapun baik dalam bentuk digital maupun fisik, kecuali untuk keperluan yang telah ditetapkan dan dilindungi oleh undang-undang, termasuk nomer telepon dan alamat email yang biasa digunakan untuk keperluan penting.
3. Hindari penggunaan perangkat keras dan perangkat lunak tanpa pengetahuan yang cukup tentang keamanan penggunaan perangkat tersebut.
4. Selalu menggunakan perangkat lunak yang asli *(original)* dan berlisensi resmi.
5. Menggunakan software antivirus yang terupdate pada perangkat teknologi informasi yang dimiliki.
6. Mengamankan jaringan baik jaringan internet, LAN dan jaringan nirkabel *(wireless)* yang dimiliki dengan menggunakan *firewall, Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS) serta WPA/2 untuk jaringan tanpa kabel *(wireless).*
7. Menggunakan sosial media dengan bijaksana dengan menerapkan aturan *privacy* yang cukup dan tidak melakukan posting atau sharing informasi dan urusan pribadi secara berlebihan.
8. Menjalankan manajemen *password* dengan baik, diantaranya dengan melakukan penggantian *password* secara berkala, tidak menggunakan *password* yang sama utamanya pada layanan sangat penting dan rahasia dan tidak mencatat atau menyimpan *password* dalam bentuk file, jika diperlukan gunakan *two factors auth* untuk lebih memperkuat autentikasi.
9. Hindari menggunakan komputer dan jaringan publik untuk keperluan rahasia/privat. Utamanya komputer dan jaringan yang tidak jelas sistem keamanannya, seperti penggunaan komputer warnet, jaringan wifi gratis di café-café dan lainnya.
10. Tidak mengunjungi atau membuka tautan-tautan mencurigakan dan yang tidak perlu, utamanya tautan pada spam di mailbox, tautan yang bergambar pornografi, tautan download gratis untuk software yang sebenarnya berbayar dan lainnya.
11. Tidak mudah percaya menerima suatu penawaran, baik secara langsung, melalui telepon, SMS, WhatsApp ataupun melalui internet.
12. Mengenali ciri penyedia layanan terpercaya baik offline maupun online, dengan melihat beberapa review, *track record* melalui media dan hanya menggunakan layanan yang terpercaya utamanya yang meminta identitas pribadi dan keuangan.

13. Hanya bertransaksi keuangan dengan penyedia layanan online yang telah memiliki sertifikat atau terverifikasi seperti menggunakan *Secure Sockets Layer* (SSL), *Verified by Visa*, *Authorize.net* dan lainnya.
14. Senantiasa melakukan pengecekan laporan saldo dan transaksi keuangan secara berkala.
15. Hanya menghubungi *helpdesk* yang resmi untuk bantuan dan pengaduan layanan yang digunakan.
16. Membiasakan diri mempelajari atau setidaknya membaca setiap aturan, peringatan, TOS dan SLA yang tertulis dalam layanan digunakan.

Upaya Penyedia Layanan dalam Memerangi Identity Theft

Beberapa usaha dapat dilakukan untuk menghindari adanya praktik pencurian identitas ini oleh penyedia layanan. Usaha-usaha tersebut diantaranya meliputi:

1. Konsisten menjalankan aktifitas organisasi sesuai dengan aturan yang ada.
2. Melakukan kontrol dan monitoring aset dan layanan secara maksimal.
3. Membuat Rencana Kontinjensi *(Contingency Planning)* dan menjalankannya apabila terjadi insiden.

Undang – Undang Informasi dan Transaksi Elektronik

Peraturan perundang–undangan tentang informasi dan transaksi elektronik yang diatur dalam UU No 11 pasal 28 tahun 2008, menjelaskan:

1. Penggunaan setiap informasi melalui media elektronik yang menyangkut data tentang hak pribadi seseorang harus dilakukan atas persetujuan pemilik data tersebut.
2. Dikecualikan dari ketentuan sebagaimana dimaksud dalam ayat (1) adalah penggunaan informasi yang bersifat umum dan tidak bersifat rahasia melalui media elektronik.

Pembaharuan peraturan perundang–undangan tentang informasi dan transaksi elektronik adalah UU No. 19 tahun 2016.

Simpulan

Pencurian identitas *(identity theft)* bukanlah merupakan sebuah bentuk kejahatan baru, korbannya pun kebanyakan berasal dari orang-orang yang tanpa sengaja memberikan informasi pribadinya kepada pihak lain, baik secara langsung maupun tidak langsung. Seseorang yang pernah memberikan informasi pribadi, misalnya memberikan nama lengkap serta nomor identitas (seperti nomor KTP, SIM, atau tanda pengenal lainnya) kepada telemarketer, atau melakukan pengisian formulir pengajuan kredit melalui tenaga marketing bank, atau bahkan secara online, maka orang tersebut harus waspada dengan adanya aktivitas *identity theft* ini. Para pelaku kejahatan macam ini akan mengumpulkan segala bentuk informasi tentang calon korbannya yang kini sangat mudah didapatkan dengan berbagai macam cara, dan mereka akan berpura-pura menjadi diri si korban dengan menggunakan informasi tersebut. Hal ini akan mereka pergunakan untuk berbagai macam hal yang menguntungkan mereka, seperti membuat kartu kredit baru, mengajukan kredit/cicilan baru, dan lain-lain.

Contoh Kasus

Pemalsuan Kredit Fiktif di Bank Syariah Mandiri

Kepala Divisi Humas Mabes Polri Irjen Pol Ronny F Sompie Mengatakan pihaknya tengah mengkaji pidana pemalsuan dalam kasus pengelapan dana bermodus kredit fiktif pada Bank Syariah Mandiri (BSM), Bogor, Jawa Barat. "Pasal pemalsuan KUHP juga berlaku seperti hanya UU Perbankan selain di kaji," kata Ronny di Jakarta, kamis (24/10). Pasal pemalsuan dokumen rencananya akan diikutsertakan dalam pidana yang menjerat keempat tersangka penggelapan dana bermodus kredit fiktif senilai Rp 102 miliar. Hasil sementara penyilidikan 197 identitas nasabah dipalsukan, dalam hal ini yang dipalsukan adalah Kartu Tanda Penduduk (KTP) serta data persyaratan pengajuan kredit ke bank BSM.

Kendati demikian polisi harus menyelidiki kasus ini lebih dalam. Apakah dokumen nasabah itu aspal (asli tapi palsu) atau memang benar-benar palsu. Polisi perlu bukti dari para ahli-ahli terkait. Dalam hal ini polisi berhasil mengungkap kasus penggelapan dana senilai Rp.102 milyar di kantor cabang pembantu BSM bogor jawa Barat. Empat tersangka yang kini ditahan di rumah tahanan bareskrim polri, yakni Kepala Cabang Utama BSM Bogor berinisial MA, Kepala Cabang Pembantu BSM Bogor berinisial CH, Accounting Officer BSM berinisial JL serta IP sebagai debitur. Penangkapan keempatnya dilakukan Rabu (23/10) atas laporan yang disampaikan pada tanggal 12 September 2013 dari Bank Syariah Mandiri Pusat.

Sementara itu, barang bukti berupa sembilan unit mobil mewah dan satu unit motor gede telah disita kepolisian sejak Rabu (23/10) siang. Kesepuluh kendaraan yang disita terdiri atas Honda Freed warna putih bernomor polisi F 630CW, Toyota Fortuner warna putih F 1030 DO, Honda CRV warna hitam F 1299 L, Honda Jazz putih F 39 A, Mercedes Benz putih B 741 NDH, Mercedes Benz SLK kuning B 1 ADG, Toyota Alphard putih B 1650 RL, Hummer hitam B 741 FKD dan Toyota Altis F 1649 DK, serta satu unit motor gede Honda Goldwings F6B hitam tanpa plat nomor.

Atas perbuatannya, SD dipersangkakan Pasal 64 UU Nomor 21 Tahun 2008 tentang Tindak Pidana Perbankan Syariah, Pasal 264 ayat 1 KUHP atas pemalsuan dokumen oleh notaris, serta Pasal 3 dan atau Pasal 5 UU Nomor 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang. Sebelumnya, polisi telah menetapkan enam tersangka dalam kasus kredit fiktif itu, diantaranya Kepala Cabang Utama BSM Bogor berinisial MA, Kepala Cabang Pembantu BSM Bogor berinisial HH, Account Officer BSM Bogor berinisial JL, serta tiga debitur meliputi IP, HG dan RA. Dalam kasus itu, IP bersama HG dan RA yang bertindak sebagai debitur mengajukan akad murabahah untuk pembiayaan perumahan. Mereka mengajukan kredit atas nama 197 nasabah dengan data palsu dan berhasil mencairkan Rp.102 miliar untuk kepentingan pribadi. Sekitar Rp.43 miliar telah dibayarkan ke pihak bank sehingga perseroan masih merugi Rp.59 miliar. Keenam tersangka lainnya dipersangkakan Pasal 63 Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah dan Pasal 3 dan 5 UU Nomor 8 Tahun 2010 tentang Pemberantasan Tindak Pidana Pencucian Uang.

Kejadian pemalsuan dokumen identitas 197 nasabah dalam kasus penggelapan dana bermodus kredit fiktif senilai Rp. 102 miliar di Kantor Cabang

Pembantu Bank Syariah Mandiri Bogor, membawa dampak rusaknya reputasi bank yang berakibat menurunnya tingkat kepercayaan stakeholder antara lain regulator, nasabah, masyarakat, manajemen bank dan pegawai terhadap bank sebagai akibat persepsi negatif yang dapat mempengaruhi keberlangsungan usaha bank. Terkait dengan hal tersebut, Bank syariah harus mengetatkan pengawasan. Apalagi BSM adalah bank berbasissyariah, internal audit harus benar-benar dipastikan berjalan. Bank juga harusmelakukan perbaikan terus-menerus. Pihak BSM seharusnya menindak lanjuti permasalahan didalam perusahaannya agar tidak ada lagi yang merasa dirugikan apalagi jumlah kerugian yg masih ada. Selain itu, masalah yang terjadi seharusnya tidak ditutupi, masalah tersebut harus segera diselesaikan.

Pada kasus kredit fiktif pada bank syariah mandiri cabang Bogor ini terdapat pelanggaran kode etik profesi. Seperti prinsip tanggung jawab, kepentingan publik, integritas, dan obyektifitas. Dikarenakan adanya pelanggaran internal perusahaanyang terjadi, adanya kerjasama antara pihak bank dengan pihak eksternal untukmelakukan kecurangan dengan modus pengajuan kredit oleh 197 nasabah yang di ajukan oleh iyan permana selaku debitur, yang ternyata dari 113 nasabah tersebut menggunakan data-data palsu untuk memperoleh keuntungan pribadi. Yang mana pada awalnya dilakukan pengajuan kredit untuk pengerjaan proyek pembangunan perumahan sebagaimana yang diajukan oleh debitur namun pada kenyataannya tidak demikian. Dalam kasus ini tersangka dapat menampung uang hasil kejahatannya senilai Rp.102 miliar. Dari kasus yang terjadi merupakan bukti bahwa fungsi pengawasan internal bankdan regulator masih lemah karena masih bisa dibobol. Baik itu karena standard operating procedure (SOP) tidak benar-benar berjalan, atau karena ada bagian-bagian tertentu yangtidak dijalani. Bisa juga karena tidak adanya evaluasi dan monitoring yang rutin dan kuatdari pihak BSM pusat ketika SOP berjalan. Tetapi apabila melihat modus pembobolan yang terjadi di KCP BSM Bogor, seharusnya tidak perlu terjadi abila manajemen peka dan mulai bisa mendeteksi sedini mungkin, sehingga kerugian tidak membesar. Dampak yang terjadi dari kasus ini selain menyebabkan kerugian dan rusaknya reputasi bank syariah mandiri, berakibat pula pada hilangnya kepercayaan masyarakat kepada bank yang berbasis syariah tersebut. Upaya-upaya yang dapat dilakukan untuk mencegah kasus di muka dapat dilakukan dengan:

- Melaksanakan sistem tata kerja dan penempatan profesi secara profesional dan integritas moral yang tinggi.
- Menerapkan sanksi pidana yang maksimal dan secara tegas agar para tersangka merasa takut akan hukuman yang akan didapat jika melakukan kolusi,
- Perlunya pengawasan yang rutin dan kuat dari pihak BSM pusat. Agar para profesiakuntan dan petinggi bsm tersebut tidak memiliki kesempatan untuk melakukan kecurangan,
- Perlu diberlakukan penerapan etika dalam profesi akuntan.

Dengan berbagai upaya tersebut akan semakin jelas *Standard Operating Procedure* (SOP) kerja dari suatu institusi/organisasi sehingga nampak jelas hak dan kewajiban masing-masing pihak dalam organisasi. Tidak ada pekerjaan ataupun tanggung jawab yang tumpang tindih antar unit ataupun individu dalam organisasi. Selain itu, semakin jelas pula aturan sanksi

apabila ada pelanggaran prosedur ataupun etika dalam organisasi. Kemudian pada akhirnya fungsi pengendalian dan pengawasan tetap dijalankan agar semua yang menjadi tujuan dan harapan organisasi dapat tercapai dengan proses yang benar *(on the right track).*

Daftar Bacaan

Fahriani, N., Devi, P.A.R. & Aditama, D. (2017). Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer. *Prosiding Seminar Nasional Teknologi dan Rekayasa Informasi.* Universitas Brawijaya, Jawa Timur.

Latumahina, R.E. (2014). Aspek hukum perlindungan data pribadi di dunia maya. *Jurnal Gema Aktualita*, 3 (2), 14-25.

Petrucelli, J.R. (2012). *Detecting Fraud in Organizations. Techniques, Tools, and Resources.* New Jersey: John Wiley & Sons, Inc.

Randa, R & Reyns, B.W. (2018). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the national crime victimization survey. *Journal Deviant Behavior,* (39), 205-223.

Zaem, R.N., Manoharan, M., Yang, Y. & Barber, K.S. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers and Security,* (65), 50-63.

https://proxsisgroup.com/cyber-crime-indonesia/

http://www.jurnalsecurity.com/mengenal-kejahatan-kartu-atm-dan-kartu-kredit/

BAB 7
KEJAHATAN FRAUD

Pendahuluan

Secara umum *Fraud Related Crime* Merupakan kejahatan yang bisa dilakukan dengan banyak cara dan dilakukan di berbagai bidang–bidang tertentu. Hal ini dilakukan dengan cara memakai nama palsu, tipu muslihat dan rangkaian kebohongan dengan maksud dan tujuan untuk menipu orang lain, perusahaan atau organisasi demi keuntungan diri sendiri. Pada bab sebelumnya telah dibahas tentang berbagai jenis fraud dengan berbagai cara pencegahan dan penanggulangannya. Bab ini membahas berbagai jenis kejahatan fraud yang saat ini masif dilakukan baik di Indonesia disertai dengan beberapa contoh kasus pendek terkait dengan jenis fraud yang dilakukan.

Jenis – jenis Kejahatan Fraud

Pencurian Identitas Pribadi

Pada era serba *online* saat ini semuanya serba mudah, praktis dan cepat. Jika menginginkan membeli barang yang ada di luar negeripun cukup belanja via online. Sangat praktis dan mudah yaitu tinggal membuka aplikasi belanja *e-commerce*, mendaftar, kemudian mengisi data diri secara lengkap seperti nama, alamat email, serta nomor telepon selulair. Dalam hitungan menit, kita sudah bisa langsung belanja barang yang diinginkan. Terkait dengan pembayaran, kita tidak perlu repot karena ada banyak pilihannya, mulai dari menggunakan kartu kredit, kartu debit, ATM, transfer bank via internet/mobile banking, hingga melalui dompet digital perusahaan pembayaran yang bekerjasama dengan *e-commerce* tersebut.

Namun demikian, dibalik semua kemudahan bertansaksi dan belanja *online* tersebut, ada hal yang perlu diwaspadai yaitu pencurian data pribadi. Dalam hal ini, pencuri bisa menggunakan nomor kartu kredit, nomor Jaminan Sosial, nomor KTP/SIM untuk membuka rekening cek dan kredit, dan selanjutnya mengajukan pinjaman, membayar tagihan, dan biaya barang melalui telepon atau Internet. Penuntutan membutuhkan identifikasi tersangka, yang hampir tidak mungkin dilakukan dalam kasus-kasus semacam ini, karena sangat sulit melacak identitas pelaku. Administrasi Jaminan Sosial melaporkan bahwa saat ini keluhan tentang penyalahgunaan *Social Security Number* (SSN) telah meningkat drastis dalam beberapa tahun ini.

Contoh:

Kasus kejahatan pencurian identitas atau menggunakan data orang lain dalam pengajuan pinjaman dana daring (online) diungkap Tim Subdit 2 Cyber Crime Polda Kalimatan Barat. Tersangka yakni RH (36) dengan korban sekitar 80-an warga dan perusahaan berbasis aplikasi penyedia layanan pesawat serta hotel yang memiliki fasilitas *paylater*.

Kronologi pengungkapan kasus ini berawal dari adanya laporan beberapa anggota masyarakat yang merasa dirugikan karena telah menjadi korban penipuan. Mereka merasa tidak pernah memanfaatkan jasa *paylater* (pinjaman) namun mendapat tagihan. Modus tersangka yaitu dengan mengumpulkan fotokopi KTP dan foto pemilik KTP hingga terkumpul sebanyak 80 buah sepanjang bulan Maret sampai dengan Mei 2019. Tersangka kemudian mengunggah identitas warga yang merupakan para korban kejahatan identitas ini ke akun aplikasi penyedia *paylater*. Hasil pengajuan 80 data orang tersebut, yang mendapat persetujuan sebanyak 70 dan mendapatkan limit pinjaman sebesar Rp.1 juta sampai dengan Rp.8 juta dalam bentuk poin pemesanan tiket pesawat dan reservasi kamar hotel. Setelah mendapat persetujuan, si pelaku kejahatan selanjutnya menjual tiket pesawat dan kamar hotel dengan menggunakan limit pinjaman dari para korban. Si pelaku menjual tiket maupun kamar hotel dengan harga murah melalui media sosial. Misalnya, harga tiket pesawat yang normalnya Rp. 1,2 juta dijual dengan harga Rp 800 ribu dengan menggunakan akun *paylater* orang lain (korban). Setelah menjual tiket pesawat dan kamar hotel, pemilik akun *paylater* wajib membayarkan cicilan pinjaman ke bank yang telah bekerja sama dengan perusahaan aplikasi. Total uang yang didapat tersangka atas kejahatan identitas ini mencapai Rp 350 juta. Namun uang hasil penjualan ini justru digunakan tersangka untuk kepentingan pribadi. Sementara para korbannya mendapat tagihan untuk penggunaan yang tak pernah dilakukan.

Dalam kasus ini, polisi menyita 11 lembar fotokopi KTP korban, uang tunai Rp 1.250.000, dua unit telepon genggam, satu buah kartu sim seluler, satu keping ATM dan 38 buah informasi debitur dari OJK.

Pabrikasi Cek Palsu

Pengeluaran sebuah cek dapat dilakukan dari komputer dengan menggunakan program seperti *Versa Check*, dimana pelaku menyalin nomor *routing* dari suatu pemeriksaan yang valid. Cek ini terlihat seperti cek yang sah/legal yang berasal dari tindakan yang telah sesuai prosedur dan bisa dikeluarkan oleh pelaku bisnis untuk bertransaksi dengan pihak lain.

Contoh:

Subdit Resmob Polda Metro Jaya membekuk dua pelaku penipuan dengan modus menyebar amplop berisi cek palsu senilai Rp 4,7 Miliar. Dua pelaku yang dibekuk adalah YM (45) dan WW (39). Keduanya dibekuk di Tajur Halang Kabupaten Bogor, Jawa Barat, pada 8 Agustus 2019 lalu. Kabid Humas Polda Metro Jaya Kombes Argo Yuwono mengatakan kedua pelaku membuat dokumen cek palsu dan SIUP atas nama PT SB yang juga fiktif atau palsu dan diperbanyak. Selanjutnya, dengan motor mereka menyebarkan paket dokumen tersebut ke perkampungan di kawasan Jakarta Timur, Bekasi, dan Bogor, terutama di depan warung atau tempat usaha. Hal ini dilakukan dengan tujuan orang yang menemukannya akan diperdayai oleh pelaku. Di dalam dokumen tersebut ada nomor telepon si pelaku. Di sana disebutkan bahwa pelaku adalah seorang pimpinan perusahaan.

Di saat seseorang/penemu cek palsu tersebut menghubungi pelaku, maka pelaku mengaku sebagai direktur sebuah perusahaan dan berterimakasih kepada korban (penemu cek). Selanjutnya, pelaku menjanjikan akan memberikan upah ratusan juta dari nilai cek senilai Rp 4,7 miliar yang ada dalam dokumen yang ditemukan korban. Akan tetapi, pelaku meminta korban mengirimkan uang sekitar Rp 5 Juta sampai Rp 6 Juta kepada korban dengan dalih agar cek yang dimaksud bisa cair. Karena dijanjikan sebagian nilai dari cek akan diberikan ke korban, beberapa korban terperdaya dan mengirim uang kepada pelaku.

Uang Palsu, Wesel, dan Cek Perjalanan

Telah terjadi peningkatan dalam produksi uang palsu, wesel, dan cek perjalanan. Kesemuanya ini juga dihasilkan dari suatu perangkat komputer dengan memanfaatkan fasilitas teknologi informasi yang semakin canggih. Hal ini kemungkinan bisa dilakukan oleh banyak orang karena saat ini perangkat keras komputer sangat murah dan terjangkau untuk semua lapisan masyarakat, sehingga siapapun bisa masuk ke dalam "bisnis" yang cukup murah dengan harapan pendapatan yang tinggi ini.

Internet Scam

Scammer merupakan seseorang atau sekelompok orang yang melakukan penipuan dengan cara yang sangat licik dan kotor. Mereka menipu lewat dunia maya (internet) ataupun dunia nyata. Jenis-jenis scammers secara umum antara lain seperti iklan jual beli online, hadiah, *business*, uang dalam paket, computer kena virus, cinta maya, survey dapat duit, travel, dan masih banyak lagi. Berikut ini beberapa contoh dari masing-masing jenis *scammers* tersebut:

Iklan Jual beli

Anda pasang iklan penjualan rumah di internet. Selanjutnya ada orang yang berniat membelinya dan kasih *down payment* (DP) tanpa lihat rumahnya terlebih dahulu. Kejadian selanjutnya yang umum terjadi adalah dengan berbagai alasan atau modus tertentu, Anda sebagai penjual malah diminta pergi ke sebuah ATM untuk transfer uang ke mereka. Hal seperti ini biasanya dilakukan oleh orang Indonesia.

Hadiah

Anda dinyatakan dapat hadiah dari sebuah perusahaan yang sangat terkenal seperti Telkomsel, Indosat, XL, Bank Pemerintah/swasta, serta perusahaan terkenal dengan pemberitahuannya memakai website gratisan yang mirip website aslinya. Akan tetapi, ujung-ujungnya anda di suruh kirim uang untuk biaya administrasi atau biaya lainnya kepada pengirim berita tersebut.

Business

Menawarkan masker di media sosial (internet) dengan harga dibawah rata-rata, jika uang sudah dikirim maka akun pembeli langsung diblok. Pelaku seorang wanita NL asal Jawa Timur ditangkap polisi karena menipu pembeli masker sebanyak Rp 11.4 juta. Dia mencari mangsa melalui *Face Book* dengan berpura pura berjualan masker dan beberapa kebutuhan pokok lainnya.

Uang Dalam Paket

Seorang wanita bernama Rieke (nama samaran) (28) ditangkap petugas Polres Jakarta Selatan karena menipu dengan modus jualan secara online melalui Facebook. Kini, polisi tengah mencari otak kejahatan itu pelaku berinisial AG.

Kasat Reskrim Polres Jakarta Selatan AKBP Bismo mengatakan, kasus tersebut berawal saat Facebook korban, BI (41) yang di-invite oleh akun Fred Harper. Setelah terjadi perkenalan, akun tersebut mengirim pesan bakal mengirimkan barang ke korban dari Inggris melalui Security Cargo Network UK. Selanjutnya, akun tersebut menyampaikan informasi bahwa dibutuhkan biaya 1.200 poundsterling atau Rp.9.500.000 untuk membayar pajak dan ongkos kirim. Untuk meyakinkan korban, akun Fred Harper mengirim bukti pengiriman barang dari Security Cargo Network UK itu dan foto-foto barang yang dikirim, berupa perhiasan, jam tangan, tas, dan kotak yang berisi uang.

Besoknya, akun tersebut kembali mengirim pesan kalau korban akan mendapatkan telepon dari nomor 085772006xxx yang mengatasnamakan perwakilan Security Cargo Network UK di Indonesia bernama Rieke. Tak lama, Rieke pun menghubungi korban dan memintanya untuk mentransfer uang ke Bank BNI atas nama AS nomor rekening 0488336xxx. Setelah ditransfer dan korban menunggu kedatangan barang tersebut, pelaku kembali menghubungi dan menyatakan paket kirimannya tertahan di Bandara Soetta karena banyak terdapat perhiasan dan uang. Pelaku lantas menawarkan bantuan dengan syarat korban harus mengirim uang sebesar Rp.30 juta sebagai pembuatan sertifikat agar paketannya bisa keluar. Pada saat itu, korban mulai curiga dan mengecek bukti pengiriman barang dan foto-foto barang itu yang mana ternyata fiktif belaka.

Computer Kena Virus

Modusnya adalah seseorang menelpon kita dengan menggunakan fasilitas skype atau *random call.* Orang tersebut mengaku dari Microsoft atau perusahaan software lainnya dan mengatakan bahwa komputer anda kena virus berbahaya. Selanjutnya, Anda dipandu untuk melakukan hal "ini itu" yang pada akhirnya diminta membayar biaya perbaikan atau biaya lainnya, padahal sebenarnya komputer Anda tidak apa-apa atau normal-normal saja.

Menurut West & Bhattacharya (2016) langkah-langkah pencegahan fraud yang efektif tidak hanya dirancang untuk melindungi organisasi (perusahaan) dan pelanggannya, tapi juga menjaga agar pelanggan tetap dapat berinteraksi dengan cepat, mudah, dan sesuai dengan keinginan. Terdapat sebuah ungkapan *"mencegah lebih baik dari pada mengobati".* Ungkapan tersebut sangat tepat digunakan untuk mengatasi fraud karena secara umum yang sebenarnya terjadi jauh lebih besar daripada yang terungkap. Akar permasalahan dari fraud adalah fraud *by need, by greed,* dan *by opportunity.* Untuk yang *by need* dan *by greed* bisa ditekan dengan proses rekruitmen yang tepat, selanjutnya selalu dilakukan "kesadaran akan fraud" *(fraud awarenenss)* serta contoh yang baik dari pimpinan. Untuk yang *by opportunity* bisa ditekan dengan sebuah sistem pengendalian internal yang memadai. Selanjutnya, pada bagian berikut ini dipaparkan beberapa jenis *cyber fraud* lainnya yang akhir-akhir ini sudah mulai marak dilakukan di Indonesia serta cara yang dapat digunakan untuk mencegahnya.

Carding

Cyber fraud jenis ini merupakan kegiatan berbelanja dengan menggunakan nomor dan identitas kartu kredit orang lain, yang didapatkan secara ilegal, biasanya dilakukan dengan mencuri data di internet. Sebutan pelakunya adalah Carder. Sebutan lain untuk kejahatan jenis ini adalah *cyberfraud* atau penipuan di dunia maya.

Ada beberapa langkah yang dapat dilakukan untuk mengantisipasi tindak kejahatan carding, diantaranya sebagai berikut:

a. Jika kita bertransaksi di toko, restoran, atau hotel menggunakan kartu kredit, pastikan kita mengetahui bahwa kartu kredit hanya digesek pada mesin EDC *(Electronic Data Capture)* yang dapat kita lihat secara langsung.
b. Jika kita melakukan transaksi belanja atau reservasi hotel secara *online*, pastikan bahwa website tersebut aman dengan dilengkapi teknologi enskripsi data (https) serta memiliki reputasi yang bagus. Ada baiknya juga jika kita "tidak melakukan transaksi *online* pada area ***hotspot***" karena pada area tersebut rawan terjadinya *intersepsi* data.
c. Jangan sekali-kali memberikan informasi terkait dengan kartu kredit milik kita beserta identitas kita kepada pihak manapun, sekalipun hal tersebut ditanyakan oleh pihak yang mengaku sebagai petugas bank.
d. Simpanlah surat tagihan kartu kredit yang dikirim oleh pihak bank setiap bulannya atau jika kita ingin membuangnya maka sebaiknya hancurkan terlebih dahulu dengan menggunakan alat penghancur kertas (*paper shredder*). Hal ini karena surat tagihan memuat informasi berharga kartu kredit Anda.
e. Apabila menerima tagihan pembayaran atas transaksi yang tidak pernah kita lakukan maka segera laporkan-kepada pihak bank penerbit sesegera mungkin untuk dilakukan investigasi.

Hacking

Merupakan kegiatan yang dilakukan oleh individu, organisasi, atau negara untuk mendapatkan akses tidak sah ke komputer dan sistem pihak lain yang bergantung pada teknologi. Tujuan dari aktivitas ini adalah mencuri data-data penting yang akan dipakai untuk tindak kejahatan finansial dan lainnya melalui fasilitas teknologi informasi yang ada. Aktivitas *hacking* dapat melibatkan modifikasi atau perubahan pada software atau hardware untuk melakukan aktivitas yang tidak dimaksudkan oleh penciptanya. Terdapat beberapa hal yang harus kita ingat untuk menjaga program/website kita dari hack, yaitu membuat kata sandi atau *password* yang lebih kuat dari *password* sebelumnya, jangan install plugins yang sekiranya tidak diperlukan dalam website atau program kita, pastikan semuanya terupdate secara berkala, dan gunakan layanan pemantau situs untuk menjaga website/program kita.

Cracking

Merupakan *hacking* untuk tujuan jahat. Seorang *cracker* beraksi dengan mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, si *hacker* lebih fokus pada prosesnya. Sedangkan *cracker* lebih fokus untuk menikmati hasilnya. Beberapa cara yang kemungkinan dapat dilakukan untuk mencegah ulah *cracker*, yaitu dengan 3 cara berikut:

a. Membuat *password* yang susah ditebak orang lain tetapi mudah diingat kita.
b. Mengkombinasikan *password* dengan menggunakan angka dan huruf.
c. Jangan membuat *password* tentang diri kita atau yang terkait dengan diri kita, misalnya tanggal lahir, tempat lahir, nomor telepon, alamat rumah, nomor pegawai, dan lainnya.

Defacing

Merupakan kegiatan mengubah halaman situs/website/blog milik pihak lain, seperti yang terjadi pada situs Menkominfo dan Partai Golkar, Bank Indonesia serta situs KPU saat pemilu 2004 yang lalu.

Cara mengatasi website/blog yang terkena *defacing* sebagai berikut:

a. Download source & database yang ada diwebsite untuk backup. Hal ini berjaga-jaga apabila langkah yang kita lakukan gagal, tetapi apabila konfigurasi & lengkap dijamin 100% berhasil, terkecuali ada sesuatu yang terlewatkan.
b. Download source CMS versi terbaru dari website penyedia CMS, misalkan: www.drupal.org, www.joomla.org, www.wordpress.org, dan lain-lain.
c. Lakukanlah perbaikan database secara lokal, berjaga-jaga apabila *backdoor* ada di database. Biasanya didalam database ada acces user tidak dikenal yang akses levelnya sama dengan Administrator.
d. Install CMS yang tadi sudah didownload diweb hosting. Kemudian lakukanlah konfigurasi: database, *file permission, directory permission.* Jangan menggunakan *default configuration*, modifikasilah konfigurasi-konfigurasi yang ada agar lebih powerfull.
e. Kemudian instalasi component: Themes, Plugin, Component, dan lainnya. Gunakanlah yang paling update, atau *source* baru dari komponen yang akan diinstal (*Fresh Install Component).*
f. Kemudian update database, dengan login ke Database Control Panel (php myadmin, DB Admin, c-Panel Database, dan sebagainya). Setelah melakukan login, maka importlah database tersebut.
g. Gantilah secara berkala username Administrator & Password dengan menggunakan nama yang unik atau tidak lazim, jangan menggunakan user yang bersifat umum seperti: admin, user, administrator, 12345, abcde, dan lainnya. Gunakanlah yang lebih *powerfull* dan susah untuk ditebak untuk menghindari *bruteforce,* gunakanlah alias untuk menampilkan username administrator di *web content.*

Phising

Merupakan kegiatan memancing pemakai komputer di internet *(user)* agar mau memberikan informasi data diri pemakai *(username)* dan kata sandinya *(password)* pada suatu website yang sudah di-*deface. Phising* ini biasanya diarahkan kepada pengguna *online banking.*

Berikut ini merupakan beberapa cara yang dapat diterapkan dengan mudah agar terhindar dari aktivitas *phishing.*

a. Amankan browser Anda, dengan dimulai dari set kemanan di browser Anda.
b. Instal ekstensi keamanan pada browser. Ekstensi seperti *Netcraft Extension* berfungsi untuk mengidentifikasi website yang berbahaya.

c. Waspada terhadap email yang mengarahkan Anda kepada suatu website palsu dan meminta login akun. Cek dan cermati email si pengirim, pastikan email pengirim sesuai dengan email resmi.
d. Berhati-hatilah terhadap *pop-up* ketika Anda sedang mengakses halaman tertentu. Terlebih jika pop-up tersebut meminta akses login atau informasi pribadi seperti token, nomor kartu kredit, nomor identitas, dan lain-lain.
e. Pastikan Anda mengetahui dan mengakses website asli akun yang Anda miliki. Pada *address bar website* resmi biasanya terdapat icon kunci dan keterangan *Secure Socket Layer* (SSL) *Certificate* yang valid. SSL adalah salah satu komponen penting yang harus dimiliki website. Dengan SSL, transfer data di dalam website menjadi lebih aman dan terenkripsi. Website resmi biasanya menggunakan fitur keamanan SSL. Layanan keamanan SSL ini diperlukan untuk validasi keaslian website dan keamanan transaksi, juga meningkatkan kepercayaan para pengguna.

Spamming

Merupakan pengiriman berita atau iklan lewat surat elektronik *(e-mail)* yang tidak dikehendaki. Secara umum, arti *spam* adalah aktivitas mengirimkan pesan kepada orang lain dengan memakai perangkat elektronik secara terus-menerus dengan jumlah yang masif tanpa dikehendaki oleh penerimanya. Aktivitas *spam* ini disebut dengan *spamming*, sementara itu pelakunya disebut dengan *spammer*. Pada umumnya pesan yang dikirim oleh spammer berisi iklan atau informasi yang sebenarnya tidak dibutuhkan oleh si penerima. Namun, pengirim spam tetap melakukannya karena memiliki tujuan tertentu yang ingin didapatkan dari si penerima spam.

Untuk mengatasi spam langkah-langkah yang bisa diambil meliputi:

a. Memakai antivirus yang mendukung anti spam
b. Memberi filter untuk spam pada router ato server email dan semacamnya
c. Gunakan firewall bawaan OS dan personal firewall
d. Aktifkan anti-relay atau non-aktifkan relay sistem pada server e-mail
e. Gunakan fasilitas mail filtering yang ada di Outlook Express

Malware

Merupakan perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya. Istilah *malware* diambil dari gabungan potongan dua kata yaitu *malicious* "berniat jahat" dan *software* "perangkat lunak". Tujuannya tentu untuk merusak atau mencuri data dari perangkat yang dimasuki. *Malware* biasanya disusupkan dengan sengaja ke dalam jaringan internet. Jika secara manual memasukkan ke dalam komputer korban tentu saja sangat sulit karena terkendala oleh sistem keamanan komputer atau jaringan komputer. Oleh karena itu kebanyakan peretas melakukan aksinya menggunakan bantuan jaringan internet.

Cara untuk mengatasi Malware sangat mudah yaitu dengan 2 cara sederhana berikut ini:

1. Memasang aplikasi pendukung untuk *Scanner Malware* pada Personal Computer (PC) atau komputer kita.
2. Lakukan *scanning* paling tidak 1 minggu 3 kali pada PC atau komputer.

Dengan melakukan cara-cara tersebut di atas paling tidak kita sudah mencoba melakukan pencegahan dan pendeteksian terjadinya tindakan praktik *malware*. Hal ini

harus dilakukan secara teratur dan terus-menerus karena perkembangan teknologi terus berlanjut yang membutuhkan cara-cara baru yang ter-up-date baik dari sisi software maupun hardwarenya.

Cara Mengatasi Kejahatan Fraud

Secara umum semua jenis kejahatan/kecurangan yang memanfaatkan fasilitas teknologi informasi dapat dicegah atau ditanggulangi. Meskipun demikian, terkadang tidak mudah atau harus dilakukan dengan disiplin dan teratur. Berikut disajikan berbagai cara yang dapat dilakukan untuk mengatasi kemungkinan terjadinya kejahatan fraud.

1. Lindungi cek dan kartu kredit Anda. Mereka lebih bernilai dari pada uang tunai untuk penjahat.
2. Jangan memasukkan nomor SIM Anda di cek Anda. Hal ini membuat mudah untuk mendapatkan ID palsu dibuat.
3. Simpan semua tanda terima kartu kredit dengan aman. Banyak penjahat menggunakan tanda terima penerimaan tersebut untuk melakukan penipuan.
4. Jangan meninggalkan dompet, atau cek di dalam mobil atau kendaraan Anda.
5. Jangan pernah memberikan nomor kartu kredit atau debit Anda kepada orang lain yang menghubungi Anda baik via telepon, email, maupun media lainnya. Berikan keterangan seperlunya hanya jika Anda benar-benar sedang berhubungan dengan petugas bank penerbit kartu kredit/debit Anda. Artinya jika Andalah yang menghubungi mereka, sehingga yakin bahwa Anda telah berhubungan dengan petugas bank penerbit kartu Anda.

Contoh:

Pemalsu Kartu Kredit

Direktorat Reserse Kriminal Umum Polda Metro Jaya menangkap IS (30), karena diduga memalsukan kartu kredit. Pria itu ditangkap di penginapannya di daerahCipulir, Jakarta Selatan. Kepala Unit V Resmob Ajun Komisaris Handik Zusen mengatakan penangkapan tersangka dilakukan setelah menerima laporan dari salah satu bank yang merasa dirugikan atas aktivitas IS. "Tersangka menggunakan data elektronik pengguna kartu kredit WNA," ujarnya dalam sebuah keterangan, Rabu, 10 Desember 2014.

Pelaku menggunakan kartu kredit palsu untuk berbelanja kebutuhan pribadinya. Pelaku membeli *handphone* di beberapa toko. Di antaranya tercatat di Toko Bee Cell, Bless Cell, dan Cantik Cell. Modus pemalsuan yang digunakan pelaku adalah dengan memanfaatkan mesin *electronic data capture* (EDC) salah satu bank. "Dengan EDC, pihak bank bersangkutan dirugikan lantaran harus menanggung klaim pembayaran kartu kredit," katanya. Dari tangan tersangka, polisi mengamankan sejumlah barang bukti. Di antaranya adalah 8 ponsel Samsung, 3 kartu ATM, 2 kartu kredit BNI, 4 kartu kredit BII, dan 2 kartu kredit Bank Mega.

Kasus carding yang terjadi di Cipulir mengindikasikan bahwa kejahatan *carding* bisa terjadi pada siapa saja. Kasus ini membuktikan bahwa carding mempunyai karakteristik Global, yaitu pelaku dan korban carding terjadi dilintas negara yang mengabaikan batas batas geografis dan waktu. Pelaku melakukan transaksi menggunakan kartu kredit palsu untuk berbelanja kebutuhan pribadinya. Pelaku membeli beberapa *handphone*, dan bisa untuk dijual lagi. Dalam hal ini, pihak bank

yang bersangkutan dirugikan lantaran harus menanggung klaim pembayaran kartu kredit.

Banyak elemen penting yang seharusnya ikut terlibat untuk memerangi kejahatan *carding* di Indonesia, pihak-pihak terkait tersebut diantaranya sebagai berikut:

a. Pihak Bank selaku penerbit kartu kredit harus menggunakan teknologi chip, bukan lagi swipe yang secara kriptografi lebih lemah. Dengan menggunakan kartu kredit dengan sistem chip, maka kejahatan kartu kredit lebih sulit ditembus daripada swipe.
b. Pihak Bank harus menyediakan fasilitas-fasilitas pendukung untuk menghindari kerugian yang lebih besar setelah terjadi penyalagunaan kartu kredit, misalnya saja ketika akan terjadi transaksi, pengguna akan mendapatkan SMS untuk melakukan konfirmasi. Hal lain yang bisa juga dilakukan diantaranya seperti memberikan laporan yang *update* setiap kali transaksi baik itu pengiriman melalui SMS ataupun melalui email, dan layanan cepat untuk melakukan pemblokiran ketika terjadi sesuatu yang tidak diinginkan.
c. Bagi pemilik kartu kredit, pengetahuan sebanyak mungkin tentang penggunaan kartu kredit yang benar sangatlah penting, misalnya tidak mudah memberikan data-data kartu kredit kepada pihak lain, sekalipun yang meminta mengaku sebagai representatif sebuah bank.
d. Sanksi tegas bagi pelaku *carding*, karena kejahatan *carding* bisa terjadi secara Internasional dan dapat dilakukan secara kolektif kolegial, agar dapat memberikan efek jera untuk pelaku *carding*.
e. Pihak Kepolisian seharusnya semakin aktif dan tanggap terhadap kasus *cyber crime* khususnya *carding* dengan melakukan rekrutmen polisi khusus dunia maya *(cyber police)* dengan kompetensi yang baik, serta pelatihan-pelatihan tentang kejahatan dunia cyber yang kian lama semakin canggih.
f. Pihak *merchant* yang mempekerjakan karyawan harus secara aktif memberikan penjelasan dan pengetahuan akan kejahatan dunia maya termasuk sosialisasi akan undang-undang Teknologi Informasi dan Transaksi Elektronik kepada karyawan sejak menjalani OJT (*on job training*). Hal ini akan membuat karyawan menjadi lebih sadar hukum khususnya yang terkait dengan *cyber crime*.
g. Pihak *Internet Service Provider* (ISP) harus proaktif memblok laman-laman yang secara terang-terangan mendukung terjadinya kejahatan carding di dunia maya, seperti laman penjualan data kartu kredit hingga tutorial melakukan carding.
h. Pihak-pihak yang menggunakan sarana kartu kredit sebagai media transaksi elektronik wajib menggunakan protokol keamanan yang tidak mudah dibobol oleh peretas.

Simpulan

Perlunya pendekatan secara teknologi dengan pengamanan *software, hardware,* kemudian dilakukan upaya sosialisasi tentang komputer dan internet di tengah-tengah masyarakat, selain itu pendekatan kultur juga bisa dilakukan dengan cara menerapkan etika. Dalam berinteraksi dengan orang lain dengan menggunakan internet, diliputi oleh suatu aturan tertentu yang dinamakan *Netiquette* atau etika dalam berkomunikasi melalui internet. Meskipun belum ada ketetapan yang baku mengenai bagaimana etika berinteraksi di internet, etika dalam berinteraksi di dunia nyata *(real life)* dapat dipakai sebagai acuan, selain upaya pencegahan juga dilakukan penegakan hukum terhadap kejahatan *cyber crime*.

Daftar Bacaan

Claudia, G. (2018). Akuntansi forensik untuk bedah kasus korupsi. *Jurnal Ekonomi, Manajemen, Akuntansi dan Perpajakan,* 1 (1), 95-109.

Enggarani, N.S. (2016). Penanggulangan Kejahatan Internet di Indonesia. *Jurnal Ilmu Hukum,* 15 (2), 149-168.

Harjoto, M. (2017), Corporate social responsibility and corporate fraud. *Social Responsibility Journal,* 13 (4), 762-779. https://doi.org/10.1108/SRJ-09-2016-0166.

Homer, E. (2019), Testing the fraud triangle: a systematic review, *Journal of Financial Crime,* 27 (1), 172-187, https://doi.org/10.1108/JFC-12-2018-0136

Ishak, R. (2010). (Kadit Serse Polda Jateng), pada seminar tentang Hacking yang diadakan oleh Majalah NeoTek pada bulan Agustus 2010 di Semarang.

Manning, P., Stokes, P., Visser, M., Rowland, C. and Tarba, S. (2018), Dark open innovation in a criminal organizational context: the case of Madoff's Ponzi fraud, Management Decision, 56 (6), 1445-1462. https://doi.org/10.1108/MD-05-2017-0535.

Nawawi, A., & Barda, (2007), *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* Jakarta: Kencana Predana Media Group

West, J & Bhattacharya, M. (2016). Intelligent financial fraud detection: *A comprehensive review. Computers and Security,* (57), 47-66.

http://akuntansipublikums.blogspot.co.id

BAB 8
AKUNTANSI FORENSIK

Pendahuluan

Pada awalnya, akuntansi forensik digunakan untuk keperluan pembagian warisan atau dalam rangka pengungkapan motif pembunuhan. Pada mulanya ilmu akuntansi diterapkan dalam berbagai permasalahan hukum, sehingga istilah yang dipakai adalah akuntansi forensik (bukan audit forensik). Pada perkembangannya, sampai saat ini-pun kadar akuntansi pada berbagai penyelesaian kasus hukum masih nampak, misalnya pada perhitungan ganti rugi dalam pengertian sengketa, maupun kerugian akibat kasus korupsi, atau secara sederhana akuntansi forensik menangani fraud khususnya dalam cakupan *corruption* dan *misappropriation of asset*. Dengan demikian, akuntansi forensik dapat diartikan sebagai penggunaan ilmu akuntansi untuk kepentingan bidang hukum. Artinya, akuntansi dapat dimanfaatkan dalam kancah perseteruan selama proses pengadilan, atau dalam proses peninjauan *judicial* atau administratif.

Masih banyak orang yang memahami profesi terkait dalam peraturan di atas dengan sebutan dokter forensik, akan tetapi *"ahli lainnya"* yang dalam hal ini termasuk akuntan belum banyak dikenal sebutannya sebagai akuntan forensik. Pada dasarnya, akuntan forensik bertugas memberikan pendapat hukum dalam pengadilan (litigation), selain itu juga berperan dalam bidang hukum di luar pengadilan *(non-litigation)* misalnya dalam membantu merumuskan alternatif penyelesaian perkara dalam sengketa, perumusan perhitungan ganti rugi serta upaya menghitung dampak pemutusan/pelanggaran kontrak. Untuk menjadi seorang akuntan forensik harus memperhatikan hal-hal sebagai berikut:

a) Pengetahuan dasar akuntansi dan audit yang kuat.
b) Pengenalan perilaku manusia dan organisasi (human and organization behaviour).
c) Pengetahuan tentang aspek yang mendorong terjadinya kecurangan (meliputi: *incentive, pressure, attitudes, rationalization, opportunities*).
d) Pengetahuan tentang hukum dan peraturan.
e) Pengetahuan tentang kriminologi dan viktimologi *(profiling)*.
f) Pemahaman yang baik terhadap pengendalian internal.
g) Kemampuan berpikir seperti layaknya seorang pencuri *(think as a theft)*.

Jika kita telaah dengan seksama, yang menjadi perbedaaan utama antara akuntansi forensik dan audit konvensional lebih terletak pada mindset (kerangka pikir). Metodologi kedua jenis bidang tersebut tidak jauh berbeda. Akuntansi forensik lebih menekankan pada keanehan *(exeption, oddities, irregularities)* dan pola tindakan *(product of conduct)* dari pada kesalahan *(errors)* dan keteledoran *(ommisions)* seperti pada audit umum. Prosedur utama dalam akuntansi forensik menekankan pada *analytical review* serta teknik wawancara mendalam *(in depth interview)* walaupun

seringkali masih juga menggunakan teknik audit umum seperti pengecekan fisik, rekonsiliasi, konfirmasi dan lain sebagainya. Pada umumnya, akuntansi forensik memfokuskan pada area-area tertentu (contohnya penjualan, atau pengeluaran tertentu) yang diindikasikan telah terjadi tindak kecurangan baik dari laporan pihak dalam organisasi ataupun orang ketiga *(tip off)*, atau petunjuk terjadinya kecurangan *(red flag)*, maupun petunjuk yang lain. Dari berbagai referensi menunjukkan bahwa sebagian besar tindak kecurangan dapat terbongkar karena *tip off* atau ketidaksengajaan *(accident)*.

Mengapa Akuntansi Forensik?

Berdasarkan berbagai fakta dan berbagai referensi, fraud sangatlah merugikan berbagai pihak karena dapat mengganggu jalannya pemerintahan pada suatu negara maupun proses bisnis pada sebuah organisasi bisnis, bahkan dapat menghancurkan keduanya. Fraud yang berupa korupsi lebih luas daya penghancurnya. Pada dasarnya cakupan akuntansi forensik adalah fraud dalam arti yang luas. *Association of Certified Fraud Examiners* mengelompokkkan fraud kedalam tiga kelompok yaitu *corruption* (korupsi), *asset misappropriation* (penjarahan aset), dan *fraudulent financial statement* (laporan keuangan yang dengan sengaja dibuat menyesatkan). Dalam kaitannya dengan fraud, akuntan forensik menjadi spesialis yang lebih khusus dibandingkan dengan akuntan pada umumnya yang berspesialisasi dalam bidang pengauditan. Mereka menjadi *fraud auditor* atau *fraud examiner* yang memiliki spesialisasi dalam bidang fraud.

Selama ini, yang menjadikan fokus utama berkaitan dengan masalah fraud pada umumnya maupun masalah korupsi pada khususnya adalah kelemahan penerapan *corporate governance* atau kelemahan penerapan governance di sektor korporasi. Hal yang sama juga terjadi di sektor pemerintahan, yaitu lemahnya penerapan governance pada sektor pemerintahan atau *public governance*. Di Indonesia hal ini sangat jelas terlihat dalam perkara-perkara korupsi dari para penyelenggara negara dan dari kajian mengenai integritas yang dibuat KPK. Salah satu dampak kelemahan governance adalah adanya fraud atau perkara korupsi yang melibatkan para penyelenggara negara. Sedangkan dampak kelemahan governance di korporasi lebih kepada pengaruh di pasar modal yaitu harga saham perusahaan akan lebih rendah dimana seharusnya mempunyai nilai yang lebih tinggi kalau mereka mempunyai tata kelola perusahaan yang baik (*good corporate governance*).

Akuntansi forensik merupakan pemakaian keahlian dalam bidang audit dan akuntansi yang dipadu dengan kemampuan investigatif untuk memecahkan suatu masalah/sengketa keuangan atau dugaan fraud yang pada akhirnya akan diputuskan oleh pengadilan/arbitrase/ tempat penyelesaian perkara lainnya. Kasus korupsi, pada dasarnya merupakan sengketa keuangan antara Negara melawan warganya yang secara resmi telah ditunjuk untuk mengelola pemerintahan. Tingkat korupsi yang tinggi akan menjadi pendorong yang sangat kuat berkembangnya praktik-praktik akuntansi forensik di Indonesia. Akuntansi forensik sangat dibutuhkan karena adanya potensi fraud yang dapat menghancurkan pemerintahan, dunia bisnis, dunia pendidikan, departemen maupun sektor yang lain. Tindakan fraud terjadi karena berbagai sebab, diantaranya Corporate Governance yang rendah, lemahnya *enforcement*, kelemahan dalam bidang penegakan hukum, ketidaktaatan terhadap standar akuntansi serta faktor lainnya.

Survei Integritas oleh KPK

Komisi Pemberantasan Korupsi (KPK) secara rutin setiap tahun selalu melakukan survei integritas. Survei tersebut merupakan wewenang KPK dalam melaksanakan tugas koordinasi dan supervisi. Lembaga ini berwenang melakukan pengawasan, penelitian, atau penelaahan terhadap semua instansi yang melaksanakan aktivitas layanan publik. Berbeda dengan indeks tentang korupsi yang dibahas sebelumnya, indeks integritas yang diterbitkan KPK tidaklah semata-mata didasarkan atas persepsi saja. Tujuan survei ini adalah sebagai berikut:

1. Melakukan kajian dan berusaha menemukan akar permasalahan terjadinya kasus korupsi di sektor pelayanan publik.
2. Mengubah perspektif layanan, yang semula orientasi lembaga penyedia layanan publik ke perspektif pelanggan.
3. Memberikan dorongan kepada organisasi/lembaga publik mempersiapkan upaya pencegahan korupsi yang efektif di wilayahnya serta layanan yang rentan terjadinya korupsi.

Survei KPK tersebut juga menemukan banyak informasi terkait dengan aktifitas pegawai dalam melakukan tindakan pengungkapan kecurangan. Beberapa informasi menarik yang muncul misalnya beberapa pegawai takut melaporkan dugaan korupsi di lembaganya dikarenakan khawatir akan dikucilkan, diberi sanksi atau kariernya dihambat. Sehubungan dengan hal tersebut pihak KPK dan pemerintah selanjutnya memberikan jaminan yang pasti untuk memberikan perlindungan kepada pelapor baik dirinya maupun keluarganya.

Perlindungan hukum merupakan sebuah bentuk layanan publik yang wajib diberikan oleh pihak pemerintah untuk memberikan rasa aman kepada setiap warga negara. Berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, telah dinyatakan bahwa negara bertanggung jawab atas perlindungan hak asasi manusia. Hal tersebut tercantum dalam pasal 28 ayat (4) UUD 1945 yaitu: "Perlindungan, pemajuan, penegakan, dan pemenuhan hak asasi manusia adalah tanggung jawab negara, terutama pemerintah." Selanjutnya, sebagai dasar perlindungan saksi ataupun korban tercantum dalam Pasal 28G Ayat (1) yang berbunyi,"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Perlindungan terhadap para saksi maupun korban merupakan jaminan hak yang diberikan oleh Negara sehingga memiliki implikasi kewajiban pemerintah dalam melindungi hak saksi dan korban, baik dalam pengaturan substansi hukum maupun dalam penerapan norma yang telah ditetapkan.

Lingkup Akuntansi Forensik

Praktik Di Sektor Swasta

Akuntansi forensik dimulai sesudah ditemukan indikasi awal adanya fraud. Audit investigasi merupakan bagian awal dari akuntasi forensik. Adapun valuation analysis berhubungan dengan akuntansi atau unsur perhitungan. Misalnya dalam menghitung kerugian negara karena tindakan korupsi. Jasa-jasa forensik pada sektor swasta meliputi: *Fraud & Finansial Investigations, Analitik dan Forensic Technology, Fraud Risk Management, FCPA Reviews and Investigations, Anti Money Laundering Services,*

Whistleblower Hotline, Litigations Support, Intelectual Property Protection, Client Training, serta *Business Intelligence Services.* Tahapan-tahapan dalam jasa *asset recovery* yaitu: mengumpulkan bukti dan menelusuri aset, mengamankan aset, proses peradilan, melaksanakan putusan, mengembalikan aset.

Beberapa contoh jasa yang diberikan oleh Akuntan forensik antara lain sebagai berikut:

a. ***Analytic & Forensic Technology,*** jasa ini juga dikenal sebagai ahli komputer forensik *(data imaging dan data mining)* dimana bidang keahliannya diantaranya memulihkan data komputer yang telah hilang atau sengaja dihilangkan untuk menyembunyikan jejak tindakan kejahatan atau kecurangan.
b. ***Fraud risk management,*** jasa dalam bidang ini mirip sekali dengan FOSA *(Fraud-Oriented System AUdit)* dan COSA *(Corruption-Oriented System Audit)* dimana dalam jasa ini mempunyai perangkat analisis yang lengkap seperti perangkat lunak yang telah dilindingi hak ciptanya, misalnya: Anonymous, T-Tect, Tip-Offs, Dtermine, dan lain-lain.
c. ***Whistleblower Hotline,*** Suatu kantor akuntan menggunakan software yang dilindungi Undang-Undang hak cipta seperti *Tip-OffAnonymous.* Kebanyakan tindak kecurangan (fraud) terungkap karena pelaku wistleblower memberikan informasi (*Tip-Off*) secara diam-diam (*Anonymous*) tentang adanya fraud yang tengah berlangsung.
d. ***Anti money laundering services,*** jasa ini diberikan oleh suatu kantor akuntan yang mana orientasinya berfokus pada potensi pelanggaran terhadap Undang-Undang pencucian uang.
e. ***Business intelligence services,*** dalam hal ini kata intelligence mempunyai sebuah kesan bahwa suatu kantor akuntan memberikan jasa mata-mata atau melaksanakan sebuah pekerjaan detektif. Sebenarnya hal utama yang dilakukan adalah pemeriksaan latar belakang seseorang atau suatu entitas. Pada umumnya, jasa ini diperlukan oleh perusahaan yang akan melakukan akuisisi, merger atau melakukan penanaman dana pada perusahaan lain. Aktivitas seperti ini pada intinya untuk melakukan pemeriksaan terhadap identitas dan latar belakang seseorang maupun suatu entitas.

Asset Recovery

Asset recovery merupakan berbagai usaha pemulihan kerugian dengan cara menemukan dan menguasai kembali aset/harta yang telah dijarah, misalnya dalam suatu kasus korupsi, penggelapan, serta pencucian uang *(money laundry).* Adapun tahap-tahap dalam pelaksanaan *asset recovery* dapat dijelaskan sebagai berikut:

a. **Pengumpulan Bukti dan Penelusuran Aset.** Untuk mendapatkan bukti, pemeriksa harus mengidentifikasi dan menelusuri aset atau *"follow the money"* sampai diperoleh hubungan antara aset tersebut dengan tindakan kriminal yang dimaksud, atau setidaknya sampai dengan lokasi atau tempat aset yang dimaksud dapat dikatahui. Adapun beberapa teknik yang dapat dipakai dalam pengumpulan bukti maupun penelusuran aset diantaranya meliputi:
   1) merencanakan tindakan investigatif,
   2) membuat profil subjek,
   3) mendapatkan bukti keuangan dan bukti-bukti lain,
   4) mengorganisasikan data: membuat profil keuangan,
   5) menganalisis data: membandingkan aliran kas dengan profil rekening,
   6) melaksanakan kerja sama internasional.
b. **Pengamanan Aset.** Pengamanan aset diwujudkan dengan sebuah tindakan pemblokiran yang menurut pasal 1 Undang-undang Nomor 1 Tahun 2006 adalah

pembekuan untuk sementara harta kekayaan untuk kepentingan penyidikan, penuntutan, atau pemeriksaan di sidang pengadilan dengan tujuan untuk mencegah dialihkan atau dipindahtangankan kepada orang tertentu, atau orang lain tidak berurusan dengan harta kekayaan yang telah diperoleh, atau mungkin telah diperoleh dari dilakukannya tindak pidana tersebut.

c. **Proses Peradilan**. Proses utama dalam tahapan peradilan ini adalah pengumpulan bukti yang dilaksanakan melalui penyitaan. Definisi penyitaan menurut Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana Pasal 1 ayat (16) adalah serangkaian tindakan penyidik untuk mengambil alih dan/atau menyimpan di bawah penguasaannya benda bergerak atau tidak bergerak, berwujud atau tidak berwujud untuk kepentingan pembuktian dalam penyidikan, penuntutan dan peradilan.
d. **Pelaksanaan Putusan.** Pada waktu proses peradilan telah membuahkan putusan yang menginstruksikan penyitaan aset, maka banyak langkah wajib yang ditempuh untuk melaksanakan putusan tersebut. Akan tetapi, mengingat tindakan pidana saat ini telah merambah ke dunia internasional, maka semakin mudah bagi para pelaku fraud menyembunyikan dan melarikan harta hasil tindak pidananya ke luar negeri. Sehubungan dengan hal tersebut, maka diperlukan kerja sama internasional dalam pelaksanaan program pengembalian aset tindak pidana.
e. **Pengembalian Aset.** Untuk mengembalikan harta atau aset hasil tindak pidana korupsi, terdapat beberapa alternatif mekanisme yang bisa dilakukan, yaitu: (i) pengembalian aset melalui pengambilalihan dengan jalur pidana, (ii) pengembalian aset melalui pengambilalihan dengan jalur perdata, serta (iii) pengembalian aset melalui jalur administrasi atau politik. Disamping itu, dalam proses pengembalian aset hasil tindak pidana korupsi yang dilaksanakan oleh Kejaksaan Agung dan KPK sebagai aparat berwenang dalam penegakan hukum juga mengenal dua mekanisme pengembalian aset, meliputi; (i) pengembalian aset melalui perampasan aset tanpa pemidanaan, serta (ii) pengembalian aset secara sukarela. Dalam hal pengembalian harta/aset hasil tindak pidana korupsi, KPK memiliki wewenang sebatas pengembalian aset dengan jalur pidana dan penyerahan secara sukarela, apabila diharuskan menempuh jalur di luar pidana maka kejaksaan selaku pengacara negara menerapkan mekanisme selanjutnya, baik secara perdata maupun mekanisme jalur administratif dan politik.

Expert Witness

Penyediaan jasa forensik yang berupa penampilan saksi ahli *(expert witness)* pada proses pengadilan di negara-negara Anglo Saxon sudah sangat lazim, sehigga seolah-olah secara teknis "*akuntasi forensik*" mempunyai pengertian menyiapkan seorang akuntan untuk menjadi saksi ahli dalam proses ligitasi, sebagai bagian dari tim penuntut umum atau pembela dalam perkara yang berkenaan dengan fraud. Akan tetapi, dalam perkembangan selanjutnya istilah "akuntasi forensik" bermakna sama dengan prosedur akuntansi investigatif.

Sebenarnya, yang menjadi masalah utama dalam jasa *expert witness* adalah pengujian terhadap kompetensi. Oleh karena itu, dikenal dua metode yaitu *Daubert test* dan *Frye test. Daubert test* merupakan pemenuhan kondisi-kondisi yang meliputi:

a) teknik atau teori sudah diuji secara ilmiah,
b) teknik atau teori sudah dipublikasi dalam publikasi ilmiah dimana sesama rekan dapat menelaahnya,
c) tingkat kesalahan dalam menerapkan teknik tersebut dapat ditaksir dengan memadai atau diketahui,

d) teknik atau teori sudah diterima dalam masyarakat atau asosiasi ilmuwan terkait.

Sementara itu, *Frye test* hanya mensyaratkan bahwa keterangan saksi ahli didasarkan pada prinsip atau metode yang sudah diterima publik atau asosiasi ilmuwan terkait. Masalah yang muncul dalam penggunaan akuntan forensik sebagai ahli di persidangan khususnya dalam tindak pidana korupsi, pada umumnya adalah kompetensi dan independensi. Masalah kompetensi dan independensi ini sering dipertanyakan oleh tim pembela atau pengacara terhadap akuntan forensik yang membantu penuntut umum. Sebaliknya, pada umumnya tidak ada atau jarang ada pertanyaan mengenai kompetensi dan independensi akuntan forensik yang membantu tim pembela (pengacara).

Praktik di Sektor Pemerintahan

Di Indonesia, akuntansi forensik pada sektor publik lebih menonjol daripada akuntansi forensik pada sektor swasta/bisnis. Secara umum akuntansi forensik pada sektor publik khususnya sektor pemerintahan tidak banyak berbeda, hanya terdapat beberapa perbedaan pada tahapannya yang mana dari seluruh rangkaian akuntansi forensik terbagi-bagi pada berbagai lembaga seperti lembaga pemeriksaan keuangan negara, lembaga pengawasan internal pemerintahan, lembaga pengadilan, dan berbagai lembaga LSM (Lembaga Swadaya Masyarakat) yang berfungsi sebagai *pressure group*. Sedangkan dimensi yang membedakan akuntansi forensik di sektor publik dan swasta antara lain meliputi landasan penugasan, imbalan, hukum, ukuran keberhasilan, pembuktian dan teknik audit investigatif. Pada Tabel 5 berikut ini disajikan perbandingan antara akuntansi forensik di sektor publik dan sektor swasta.

Tabel 5. Akuntansi Forensik di Sektor Publik dan Swasta

Dimensi	Sektor Publik	Sektor Swasta
Landasan Penugasan	Amanat Undang-Undang	Penugasan tertulis secara spesifik
Imbalan	Lazimnya tanpa imbalan	Fee dan biaya
Hukum	Pidana umum dan khusus, hukum administrasi negara	Perdata, arbitrase, administratif, dan aturan intern perusahaan
Ukuran Keberhasilan	Memenangkan perkara pidana dan memulihkan kerugian	Memulihkan kerugian
Pembuktian	Dapat melibatkan instansi lain di luar lembaga yang bersangkutan	Bukti intern, dengan bukti ekstern yang terbatas
Teknik Audit Investigatif	Sangat bervariasi karena kewenangan relatif besar	Relatif lebih sedikit dibanding pada sektor publik, kreativitas dalam pendekatan lebih menentukan
Akuntansi	Tekanan pada kerugian negara dan kerugian keuangan negara	Penilaian bisnis

Atribut dan Kode Etik Akuntan Forensik serta Standar Audit Investigatif

Atribut

Dalam melaksanakan suatu aktifitas investigasi terhadap dugaan adanya fraud pada sebuah instansi atau organisasi diperlukan beberapa pengetahuan khusus dan strategi agar kegiatan investigasi berjalan secara efektif. Bagi auditor pemula, sebaiknya

memperhatikan dan melakukan hal-hal berikut ini guna tercapainya efektifitas investigasi yang dilakukan:

1. Berusaha menghindari pengumpulan fakta dan data yang berlebihan secara prematur.
2. Mampu membuktikan niat pelaku melakukan kecurangan.
3. Kreatif dan berpikir seperti layaknya si pelaku kejahatan, serta jangan mudah ditebak dalam hal arah pemeriksaan, penyelidikan, atau investigasi yang dilakukan.
4. Mengetahui persis bahwa banyak kecurangan dilakukan dengan persekongkolan.
5. Dalam aktifitas penyusunan strategi, perlu mempertimbangkan apakah kecurangan dilakukan di dalam pembukuan atau di luar pembukuan.

Dengan memperhatikan hal-hal tersebut di atas, dapat ditarik rumusan penting yang sangat bermanfaat dalam rangka pelaksanaan audit investigatif, yaitu (a) Dari awal upayakan menduga siapa pelaku fraud, (b) fokus pada pengambilan bukti dan barang bukti untuk pengadilan, (c) kreatif, jangan mudah ditebak, (d) Investigator harus memiliki intuisi yang tajam untuk merumuskan teori mengenai persekongkolan, (e) kenali pola fraud. Disamping beberapa rumusan penting tersebut, penting bagi pelaksanaan investigasi diketahui beberapa karakteristik pemeriksa fraud berdasarkan *Association of Certified Fraud Examine* (ACFE). Hal ini untuk meyakinkan bahwa pemeriksa fraud benar-benar memiliki tingkat profesionalisme yang tinggi dengan kompetensi yang meyakinkan sehingga hasil audit dapat dipercaya oleh berbagai pihak. Adapun karakteristik pemeriksa fraud berdasarkan *Association of Certified Fraud Examiner* meliputi:

1. Memiliki kemampuan mengumpulkan fakta-fakta dari berbagai saksi secara *fair*, tidak memihak, sahih dan akurat, serta pelaporan secara lengkap dan akurat.
2. Mempunyai kepribadian yang menarik dan mampu memotivasi orang lain untuk membantunya.
3. Mampu berkomunikasi dalam "bahasa" mereka.
4. Memiliki kemampuan teknis untuk mengerti konsep-konsep keuangan dan mampu untuk menarik kesimpulan.

Dari beberapa karakter akuntan forensik tersebut, Howieson (2018) menyatakan beberapa hal yang harus dimiliki oleh seorang akuntan forensik, diantaranya meliputi: kreatif; rasa ingin tahu; tak mudah menyerah; memiliki akal sehat, business sense; dan percaya diri. Dengan memiliki berbagai sifat tersebut, diharapkan seorang akuntan forensik akan dapaat menyelesaikan berbagai kasus terkait dengan tindakan fraud yang terjadi pada suatu entitas bisnis maupun sektor publik.

Kode Etik

Kode etik merupakan bagian dari dari kehidupan berprofesi yang mengatur hubungan antara anggota profesi dengan sesamanya, dengan pemakai jasanya dan stakeholder lainnya, dan dengan masyarakat luas. Kode etik berisi nilai-nilai luhur yang amat penting bagi eksistensi profesi. Profesi bisa eksis karena ada integritas (sikap jujur walaupun tidak diketahui orang lain), rasa hormat dan kehormatan, dan nilai-nilai luhur lainnya yang menciptakan rasa percaya dari pengguna dan stakeholders lainnya.

Salah satu contoh kode etik organisasi profesional yaitu kode etik Komisi Pemberantasan Korupsi (KPK), mengingat lembaga tersebut merupakan lembaga audit forensik yang paling efektif di Indonesia. KPK mendefinsikan kode etik sebagai norma yang wajib dipatuhi dan dilaksanakan oleh Pegawai Komisi dalam menjalankan tugas-

tugas organisasi maupun menjalani kehidupan pribadi. Kode etik pimpinan KPK adalah penjabaran dari nilai-nilai dasar perilaku prilaku pribadi yang wajib dilaksanakan oleh seluruh pimpinan KPK.

Carmichael (2018) merumuskan beberapa standar untuk melaksanakan investigasi terhadap dugaan adanya fraud. Konteks yang mereka rujuk adalah investigasi atas fraud yang dilakukan oleh pegawai pada suatu perusahaan. Adapun standar-standar tersebut meliputi:

1. Seluruh investigasi harus dilandasi praktik yang diakui *(accepted best practices)*
2. Pengumpulan berbagai bukti dengan prinsip kehati-hatian *(due care)*, sehingga bukti-bukti tersebut dapat diterima di pengadilan.
3. Pastikan semua jenis dokumentasi dalam keadaan aman, terlindungi dan diindeks serta jejak audit tersedia dengan jelas dan rapi.
4. Pastikan bahwa para investigator mengerti benar hak-hak asasi pegawai dan senantiasa menghormatinya
5. Beban pembuktian terdapat pada yang menduga pegawainya melakukan kecurangan, serta pada penuntut umum yang mendakwa pegawai tersebut, baik dalam kasus hukum dan administratif maupun hukum pidana.
6. Usahakan kuasai seluruh substansi investigasi dan kuasai juga seluruh target yang sangat kritis ditinjau dari segi waktu.
7. Catat atau rekam semua tahapan kunci dalam proses investigasi, termasuk diantaranya proses perencanaan pengumpulan bukti dan barang bukti, wawancara, kontak dengan pihak ketiga, pengamanan terhadap segala hal yang bersifat rahasia, ikuti tata cara atau protokol yang ada, dokumentasi dan penyelenggaraan catatan, melibatkan dan atau melapor ke polisi, penuhi kewajiban hukum serta persyaratan pelaporan yang benar.

Tatanan Kelembagaan Terkait dengan Penanggulangan Fraud di Indonesia

Undang Undang Dasar 1945 telah menjelaskan tentang lembaga negara atau lembaga penyelenggara negara, baik di tingkat pusat maupun di daerah. Pada tingkat pusat terdapat beberapa kelompok kelembagaan antara lain kelompok lembaga yang mencerminkan perwakilan rakyat, presiden dan wakil presiden yang mewakili kekuasaan pemerintahan negara, dan kelompok yang mewakili kekuasaan kehakiman oleh Mahkamah Agung dan badan peradilan yang berada di bawahnya. Ketiga kelompok tersebut adalah merupakan perwujudan konsep *trias politica* dalam ketatanegaraan. Badan Pemeriksa Keuangan (BPK) tidak termasuk dalam kekuasaan tersebut karena BPK lebih dikenal dalam sistem ketatanegaraan negara-negara demokrasi.

Lembaga Pemberantasan Korupsi

Komisi Pemberantasan Korupsi (KPK) yang berdiri pada tanggal 29 Desember tahun 2003, dimana lembaga ini bukanlah lembaga pemberantasan korupsi yang pertama di Indonesia. Motivasi KPK didirikan karena kelemahan aparat penegak hukum pada bidang penyelidikan dalam menghadapi tuntutan konvensi pemberantasan korupsi PBB. Selain KPK tersebut, pada masa pemerintahan presiden Susilo Bambang Yudhoyono (SBY) dibentuk juga *Tim Pemburu Koruptor* dan *Timtas Tipikor* yang dikomandani oleh Pimpinan Kejaksaan Agung.

Komisi Pemberantasan Korupsi (KPK) merupakan lembaga negara yang dibentuk dengan tujuan meningkatkan daya guna dan hasil guna terhadap upaya

pemberantasan tindak pidana korupsi. Lembaga ini bersifat independen dan bebas dari pengaruh kekuasaan manapun dalam pelaksanaan tugas dan wewenangnya. Lembaga ini dibantuk berdasarkan Undang-Undang Republik Indonesia Nomor 30 Tahun 2002 mengenai Komisi Pemberantasan Tindak Pidana Korupsi. Dalam menjalankan tugasnya, KPK berpedoman kepada lima asas, yaitu: kepastian hukum, keterbukaan, akuntabilitas, kepentingan umum, dan proporsionalitas. Lembaga ini bertanggung jawab kepada publik serta menyampaikan laporannya secara terbuka dan berkala kepada Presiden, DPR, dan BPK.

Tugas dan Wewenang Komisi Pemberantasan Korupsi (KPK)

1. Melakukan koordinasi dengan instansi yang berwenang dalam melakukan pemberantasan tindak pidana korupsi (Tipikor). Dalam melaksanakan tugas koordinasi tersebut, KPK memiliki kewenangan untuk (1) mengkoordinasikan penyelidikan, penyidikan, dan penuntutan tipikor; (2) menetapkan sistem pelaporan dalam kegiatan pemberantasan tipikor; (3) meminta informasi tentang kegiatan pemberantasan tipikor kepada instansi yang terkait; (4) melaksanakan dengar pendapat atau pertemuan dengan instansi yang berwenang melakukan pemberantasan tipikor; dan (5) meminta laporan instansi terkait mengenai pencegahan tipikor.
2. Melaksanakan supervisi terhadap seluruh instansi yang berwenang untuk melakukan pemberantasan tindak pidana korupsi. Dalam melaksanakan tugas supervisi tersebut, KPK berwenang untuk:
   a. Melakukan pengawasan, penelitian, atau penelaahan terhadap instansi yang menjalankan tugas dan wewenangnya yang berkaitan dengan pemberantasan tipikor, serta instansi yang tugasnya melaksanakan pelayanan publik.
   b. Mengambil alih penyidikan atau penuntutan terhadap pelaku tipikor yang sedang dilakukan oleh kepolisian atau kejaksaan.
3. Penyelidikan, penyidikan dan penuntutan terhadap tindak pidana korupsi.
   Komisi Pemberantasan Korupsi mempunyai wewenang untuk melakukan penyelidikan, penyidikan, dan penuntutan atas kasus tipikor.
4. Melaksanakan aktivitas penyadapan dan merekam pembicaraan.
5. Memerintahkan kepada instansi terkait untuk melarang seseorang melakukan perjalanan ke luar negeri, diantaranya meliputi:
   a. Meminta informasi kepada lembaga keuangan/bank tentang keadaan keuangan si tersangka atau terdakwa yang sedang diperiksa;
   b. Meminta kepada bank atau lembaga keuangan lainnya untuk melakukan blokir terhadap rekening yang diduga hasil tindak korupsi milik tersangka, terdakwa, atau pihak lain yang terkait;
   c. Memerintahkan kepada atasan tersangka untuk memberhentikan sementara tersangka dari jabatannya;
   d. Meminta informasi terkait dengan kekayaan dan perpajakan tersangka atau terdakwa kepada instansi yang terkait;
   e. Menghentikan sementara suatu transaksi keuangan, transaksi perdagangan, dan perjanjian lainnyaatau pencabutan sementara perizinan, lisensi serta konsesi yang dilakukan atau dimiliki tersangka/terdakwa yang diduga berdasarkan bukti awal yang cukup ada hubungannya dengan tindak pidana korupsi yang sedang diperiksa;

f. Meminta bantuan instansi penegak hukum negara lain (interpol) untuk melakukan pencarian, penangkapan, dan penyitaan barang bukti tersangka/terdakwa di luar negeri;
g. Meminta bantuan kepolisian atau instansi lain yang terkait untuk melakukan penangkapan, penahanan, penggeledahan, dan penyitaan dalam perkara tindak pidana korupsi yang sedang ditangani.

6. Pencegahan tipikor. Dalam melaksanakan tugas-tugas pencegahan tindak pidana korupsi, KPK mempunyai wewenang untuk:
   a. melakukan pendaftaran dan pemeriksaan terhadap laporan harta kekayaan penyelenggara negara;
   b. menerima laporan dan menetapkan status gratifikasi;
   c. menyelenggarakan program pendidikan antikorupsi pada setiap jenjang pendidikan;
   d. merancang dan mendorong terlaksananya program sosialisasi pemberantasan tindak pidana korupsi;
   e. melakukan kampanye antikorupsi kepada masyarakat umum;
   f. melakukan kerja sama bilateral atau multilateral dalam pemberantasan tindak pidana korupsi.
7. Pemantauan penyelenggaraan pemerintahan negara. Dalam melaksanakan tugas monitor, KPK memiliki kewenangan untuk:
   a. melakukan pengkajian terhadap sistem pengelolaan administrasi di semua lembaga negara dan pemerintah;
   b. memberi saran kepada pimpinan lembaga negara dan pemerintah untuk melakukan perubahan jika berdasarkan hasil pengkajian, sistem pengelolaan administrasi tersebut berpotensi korupsi;
   c. melaporkan kepada Presiden Republik Indonesia, Dewan Perwakilan Rakyat Republik Indonesia, danBadan Pemeriksa Keuangan, jika saran Komisi Pemberantasan Korupsi mengenai usulan perubahan tersebut tidak diindahkan.

Kewajiban KPK

KPK berkewajiban:

1. memberikan perlindungan terhadap saksi atau pelapor yang menyampaikan laporan ataupun memberikan keterangan mengenai terjadinya tindak pidana korupsi;
2. memberikan informasi kepada masyarakat yang memerlukan atau memberikan bantuan untuk memperoleh data lain yang berkaitan dengan hasil penuntutan tindak pidana korupsi yang ditanganinya;
3. menyusun laporan tahunan dan menyampaikannya kepada Presiden Republik Indonesia, Dewan Perwakilan Rakyat Republik Indonesia, dan Badan Pemeriksa Keuangan;
4. menegakkan sumpah jabatan;
5. menjalankan tugas, tanggung jawab, dan wewenangnya berdasarkan asas-asas di atas.

Anti Corruption Agencies

Lembaga semacam KPK yang secara generik dikenal sebagai Anti-Corruption Agencies (ACA), tidak hanya ada di Indonesia. Di banyak negara Agency ini disebut Commission

atau Komisi (seperti KPK). Namun ada juga yang menyebutkan Biro, seperti di Singapura, atau Badan, seperti di Malaysia. Ada dua model ACA, yakni multy agency model dan single-agency model. Negara menerapkan multy agency model, memanfaatkan lembaga-lembaga penegak hukum yang sudah ada dan membangun satu lembaga khusus. Indonesia adalah contoh negara yang menerapkan multy agency model. Kebanyakan negara Eropa Barat dan Amerika Serikat juga menerapkan multy agency model.

Landskap Audit Pemerintahan

Terdapat beberapa faktor yang dapat melemahkan proses audit pada lembaga pemerintahan. Pertama, BPK menghadapi kendala-kendala sumber daya yang parah. Kedua, tidak adanya undang-undang audit negara modern yang menyebabkan banyak kerancuan dan menjadi tempat di mana organisasi-organisasi yang ingin menghindari audit bisa bersembunyi. Banyak organisasi, terutama militer, telah menolak untuk diaudit BPK. Ketiga, parlemen, Departemen Keuangan, dan departemen-departemen teknis tidak mempunyai proses yang digariskan secara jelas untuk menindaklanjuti temuan-temuan audit dan mengambil alih langkah perbaikan, dan sebagai akibatnya tidak terjadi tindak lanjut yang sistematis. Keempat, seperti telah dicatat sebelumnya, BPK tidak berwenang mengumumkan hasil temuannya.

Selanjutnya, di lain sisi pihak Badan Pemeriksaan Keuangan dan Pembangunan (BPKP) memberikan layanan kepada instansi pemerintah baik Departemen/Lembaga Pemerintah Non-Departemen (LPND) maupun Pemerintah Daerah. Cakupan layanan yang diberikan oleh BPKP adalah:

1) Audit atas berbagai kegiatan unit kerja di lingkungan departemen/Lembaga Pemerintah Non-Departemen (LPND) maupun pemerintah daerah.
2) Policy evaluation.
3) Optimalisasi penerimaan negara.
4) Asistensi penerapan Sistem Akuntansi Pemerintah Pusat dan Daerah.
5) Asistensi penerapan *good corporate governance.*
6) *Risk management based audit.*
7) Audit investigatif atas kasus berindikasi korupsi.

Terdapat tiga pendapat mengenai pembaruan landskap audit pemerintah, yakni:

a) Bubarkan BPKP dan sebarkan SDM-nya ke Inspektorat Jenderal dan Badan Pengawasan Daerah (Bawasda).
b) Manfaatkan BPKP yang melakukan fungsi Inspektorat Jenderal dan Bawasda (Badan Pengawasan Daerah).
c) BPKP sebagai *think thank* saja, tidak usah besar namun efektif dalam memacu Inspektorat Jenderal dan Bawasda.

Tentunya pendapat-pendapat atau usulan tersebut terdapat pro dan kontra yang perlu dipertimbangkan dengan seksama. Dalam mempertimbangkan pro dan kontra tersebut perlu diperhatikan aspek kemanfaatan bagi masyarakat Indonesia terutama dalam kaitannya dengan pencegahan dan penanggulangan tindak kecurangan pada lembaga pemerintahan Indonesia.

Pengadilan Tipikor

Dari berbagai butir yang diajukan dalam permohonan *judicial review,* hanya ada satu butir yang dikabulkan oleh Mahkamah Konstitusi, yaitu pembentukan Pengadilan Tindak Pidana Korupsi dengan Undang-undang Nomor 30 Tahun 2002. Selanjutnya

Mahkamah Konstitusi memutuskan Pengadilan Tipikor harus dibentuk dengan berdasarkan undang-undang tersendiri sebelum akhir Desember 2009.

Dari pantauan *Indonesian Corruption Watch* (ICW) selama lima tahun terakhir, komitmen pengadilan umum justru dipertanyakan. Banyak terdakwa kasus korupsi yang diadili pengadilan umum, yang semuanya terdiri atas hakim karier, justru dibebaskan. Ini berbeda dari Pengadilan Tipikor, yang memadukan hakim karier dan hakim *ad hoc*, yang mana selama ini tidak pernah membebaskan terdakwa korupsi dari hukuman. Pemantauan ICW pada sejumlah pengadilan umum selama lima tahun terakhir sejak 2010, menunjukkan jumlah terdakwa kasus korupsi yang bebas di pengadilan umum kecenderungannya meningkat, dan terdakwa hukumannya cenderung ringan.

Akuntansi atau Audit Forensik?

Pada awal permulaannya, di negara Amerika Serikat akuntansi forensik dimanfaatkan untuk menentukan pembagian warisan atau mengungkapkan motif pembunuhan. Seperti misalnya pembunuhan seorang isteri oleh suami untuk mendapatkan hak waris atau klaim asuransi, pembunuhan mitra dagang untuk menguasai perusahaan, dan berbagai contoh lainnya. Bermula dari penerapan akuntansi untuk memecahkan persoalan hukum, maka istilah yang dipakai adalah akuntansi forensik (bukan audit forensik). Saat inipun kadar akuntansinya masih terlihat, misalkan dalam perhitungan ganti rugi, baik dalam konteks keuangan Negara, maupun di antara pihak-pihak dalam suatu sengketa perdata. Pada mulanya, akuntansi forensik merupakan perpaduan yang paling sederhana antara bidang akuntansi dan hukum. Contoh, penggunaan akuntan forensik dalam penggantian harta gono-gini. Di sini sangat terlihat unsur akuntansinya, unsur menghitung besarnya harta yang akan diterima pihak (mantan) suami dan (mantan) isteri. Segi hukumnya dapat diselesaikan di dalam atau di luar pengadilan, secara litigasi atau non-litigasi. Dalam kasus yang lebih pelik, ada satu bidang tambahan yaitu bidang audit.

Akuntansi forensik sebenarnya telah dipraktekkan di Indonesia sejak lama. Praktek ini tumbuh pesat, tidak lama setelah terjadinya krisis keuangan tahun 1977. Akuntansi forensik dilaksanakan oleh berbagai instansi atau lembaga seperti Badan Pemeriksa Keuangan (BPK), Komisi Pemberantasan Korupsi (KPK), Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), Badan Pengawasan Keuangan dan Pembangunan (BPKP), Bank Dunia (untuk proyek-proyek pinjamannya), dan kantor-kantor akuntan publik (KAP) di Indonesia.

Penerapan Akuntansi Forensik di Indonesia

Pada bulan Oktober 1997, pemerintah Indonesia telah menjajagi kemungkinan untuk meminjam dana baik dari IMF maupun World Bank untuk menanggulangi krisis keuangan yang pada waktu itu semakin parah. Sebagai prasayarat pemberian bantuan, IMF dan World Bank mewajibkan adanya proses *Agreed Upon Due Dilligence* (ADDP) yang dikerjakan oleh akuntan asing dibantu beberapa akuntan Indonesia. Temuan ADDP ini sangat mengejutkan karena dari sampel Bank Besar di Indonesia menunjukkan perbankan kita melakuan overstatement asset sebesar 28%-75% dan *understatement* kewajiban sebesar 3%-33%. Temuan ini segera membuat panik pasar dan pemerintah yang berujung pada likuidasi 16 bank swasta. Likuidasi tersebut kemudian diingat menjadi langkah yang buruk karena menyebabkan adanya penarikan besar-besaran dana tabungan dan deposito pada bank-bank swasta karena hancurnya kepercayaan

publik pada pembukuan perbankan. ADPP tersebut tidak lain dari penerapan akuntansi forensik atau audit investigatif.

Di Indonesia, Istilah akuntansi forensik baru populer setelah keberhasilan Pricewaterhouse Coopers (PwC) yaitu sebuah kantor Akuntan Besar dunia *(The Big Four)* membongkar kasus Bank Bali. Kantor akuntan PwC dengan software khususnya mampu menunjukkan arus dana yang sangat rumit, yang berbentuk seperti diagram cahaya yang mencuat dari matahari. Kemudian PwC meringkasnya menjadi arus dana dari orang-orang tertentu. Sayangnya keberhasilan ini tidak diikuti dengan keberhasilan sistem pengadilan. Metode yang digunakan dalam audit tersebut adalah *follow the money* atau mengikuti aliran uang hasil korupsi Bank Bali dan *in depth interview* yang selanjutnya mengarahkan kepada berbagai pejabat dan pengusaha yang terlibat dalam kasus ini.

Kasus yang lain terjadi pada tahun 2006, dimana Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) mampu membuktikan kepada pengadilan bahwa AW terlibat dalam penggelapan L/C BNI senilai Rp 1.3 Triliun, dengan menggunakan metode *follow the money* yang mirip dengan metode PwC dalam kasus Bank Bali. Dalam kasus lain dengan metode yang sama PPTK juga berhasil mengungkapkan beberapa transaksi "ganjil" yaitu 15 pejabat kepolisian kita yang memiliki saldo rekening milyaran rupiah padahal penghasilan mereka tidak sampai menghasilkan angka sefantastis itu.

Simpulan

Akuntan Forensik merupakan akuntan yang menjalankan kegiatan evaluasi dan penyelidikan, dan dari hasil tersebut dapat digunakan dalam proses pengadilan hukum. Meskipun demikian Akuntan forensik juga mempraktekkan keahlian khusus dalam bidang akuntansi, auditing, keuangan, metode-metode kuantitatif, bidang-bidang tertentu dalam hukum, penelitian, dan ketrampilan investigatif dalam mengumpulkan bukti, menganalisis, dan mengevaluasi materi bukti serta menginterpretasi dan mengkomunikasikan hasil temuan tersebut. Akuntan forensik mempunyai tugas memberikan pendapat hukum dalam pengadilan *(litigation),* dan juga bisa berperan dalam bidang hukum di luar pengadilan *(non-litigation).* misalnya dalam membantu merumuskan alternatif penyelesaian perkara dalam sengketa, perumusan perhitungan ganti rugi dan upaya menghitung dampak pemutusan/pelanggaran kontrak. Selain itu, akuntansi Forensik merupakan aplikasi keterampilan investigasi dan analitik yang bertujuan untuk memecahkan berbagai masalah keuangan melalui cara-cara yang sesuai dengan standar yang ditetapkan oleh pengadilan atau hukum. Dengan demikian investigasi dan analisis yang dilakukan harus sesuai dengan standar yang ditetapkan oleh pengadilan atau hukum yang memiliki yurisdiksi yang kuat.

Contoh Kasus

PT Petral Group

PT Petral Group berdiri pada tahun 1969 oleh dua pemegang saham dari Petra Oil Marketing Corporation Limited yang terdaftar di Bahama dan kantor di Hong Kong, serta Petral Oil Marketing Corporation yang terdaftar di California, AS. Kedua perusahaan pemegang saham itu kemudian merger di tahun 1978 menjadi Petra Oil Marketing Limited yang terdaftar di Hong Kong. Antara tahun 1979-1992 Petra Oil Marketing Limited dimiliki perusahaan

Zambesi Invesments Limited (Hong Kong) dan Pertamina Energy Services Pte Limited (Singapura) dan diakusisi di tahun 1998 oleh PT Pertamina (Persero) dan pada 2001 mengubah namanya menjadi PT Pertamina Energy Trading Ltd (Petral) sesuai dengan persetujuan pemegang saham. Aktivitas utama Petral adalah melakukan jual-beli minyak, dengan fokus pembelian minyak untuk dijual ke Pertamina. Semua aktivitas itu dilakukan di Singapura. Pada tahun 2012 pendapatan usaha perusahaan ini mencapai US$ 33,292miliar, dan membukukan laba bersih US$ 46 juta. Petral memiliki 55 perusahaan yang terdaftar sebagai mitra usaha terseleksi. Pengadaan minyak untuk Petral memang diselenggarakan secara tender terbuka, namun Petral juga melakukan pengadaan minyak dengan pembelian langsung. Alasannya, ada jenis minyak tertentu yang tidak dijual bebas atau pembelian minyak secara langsung dapat lebih murah dibandingkan dengan mekanisme tender terbuka.

Kasus Patral bermula ketika anak perusahaan pertamina ini mendapatkan opini wajar tanpa pengecualian dari kantor akuntan public PWC Singapura yang telah selesai diaudit oleh PwC pada 16 Januari 2015. Anggota Tim Reformasi Tata Kelola Minyak dan Gas, Agung Wicaksono, mengatakan dalam pertemuannya dengan Pertamina Energy Trading Ltd (Petral) pada Rabu, 17 Desember 2014 terungkap persoalan dalam bisnis Petral yang belum selesai. Menurut Agung, Petral tidak mengetahui identitas pemilik perusahaan pemenang lelang pengadaan minyak yang selama ini bekerja sama dengan mereka. Petral selama ini menjadi *trading arm* atau entitas yang bertugas menangani jual-beli produk minyak pertamina. Petral menjadi sorotan karena dituding sebaga sarang mafia yang memburu rantai dari impor minyak. Petral dituding tidak transparan dalam menyelenggarakan impor. Hal ini menyebabkan kerugian Negara dari kacaunya tata kelola impor migas.

Kecurangan Petral merupakan persoalan yang skalanya luar biasa besar, dan teknik nya sangat canggih dan rumit sehingga mampu berjalan selama puluhan tahun tanpa terdeteksi oleh auditor. Karena rantai perdagangan yang besar dalam skala internasional, rasanya tidak cukup jika hanya dilakukan audit investigatif. Bahkan dikatakan bahwa ketika ada diskon minyak bumi sebesar USD 1,3 per barrel, namun yang kemudian dilaporkan ke negara hanya sebesar USD 0,3 per barel. Jika dikalikan dengan jumlah barel yang diimpor, tentu kerugiannya sangat besar untuk negara. Kemudian ada skandal Petral lain yaitu ketika melakukan impor zatapi. Disebutkan bahwa tender zatapi lebih mahal USD 12,3 per barrel dibandingkan harga yang seharusnya. Total impor zatapi saat itu 600.000 barel.

Setelah berbagai pemberitaan media, Pertamina menunjuk kantor akuntan publik Korda Mentha untuk melakukan audit forensik atas anak perusahaannya yaitu Petral. Audit Forensik dilaksanakan pada 1 Juli hingga 30 Oktober 2015 untuk periode Januari 2012 hingga Mei 2015.

Dalam laporan audit forensik yang dilakukan oleh auditor independenKondaMentha, ditemukan hal sebagai berikut:

1) Terbukti tercatat dalam berbagai dokumentasi Petral bahwa ada pihakketiga yang ikut campur pada proses pengadaan dan jual beli minyak mentah dan produksi BBM di Pertamina Energy Service Pte Ltd yang merupakan anak usaha Petral yang bertugas melakukan pengadaan imporminyak dan Bahan Bakar Minyak (BBM).
2) Pihak ketiga berhasil mempengaruhi personal-personal di PES untuk memuluskan mengatur tender dan harga.

3) Akibat dari ikut campurnya pihak ketiga, Petral dan Pertamina tidakmemperoleh harga terbaik ketika melakukan pengadan minyak maupun jual beli produk BBM.

Dalam prosesnya, auditor independen Kordha Mentha mengakui ada beberapa pegawai yang tidak kooperatif dalam memberikan informasi kepada auditor. Hasil dari audit forensik mengindikasikan bahwa memang ada pertukaran informasi via e-mail dari para pegawai kepada vendor. Audit forensik terhadap Pertamina Energy Trading Ltd (Petral) menyebutkan terjadi anomali dalam pengadaan minyak pada 2012-2014. Berdasarkan temuan lembaga auditor Korda Mentha, jaringan mafia minyak dan gas (migas) menguasai kontrak suplai minyak senilai US$ 18 miliar atau sekitar Rp 250 triliun selama tiga tahun.

Dalam kasus ini, adatiga poin yang berhasil ditemukan oleh auditor forensik, yaitu: (1) Terbukti tercatat dalam berbagai dokumentasi Petral bahwa ada pihak ketiga yang ikut campur pada proses pengadaan dan jual beli minyak mentah dan produksi BBM di Pertamina. Energy Service Pte Ltd yang merupakan anak usaha Petral yang bertugas melakukan pengadaan impor minyak dan Bahan Bakar Minyak (BBM); (2) Pihak ketiga berhasil mempengaruhi personal-personal di PES untuk memuluskan mengatur tender dan harga dan (3) Akibat dari ikut campurnya pihak ketiga, Petral dan Pertamina tidak memperoleh harga terbaik ketika melakukan pengadan minyak maupun jual beli produk BBM. Dalam kasus ini, audit forensik tidak diminta untuk menghitung berapa kerugian negara, meskipun sebenarnya hal itu bisa saja. Dari audit forensik ini akhirnya diputuskan bahwa Petral akan dilikuidasi dan perannya digantikan oleh Intregated Supply Chain (ISC)

Daftar Bacaan

Association of Certified Fraud Examiner. https://www.acfe.com/.

Badan Pengawasan Keuangan dan Pembangunan http://www.bpkp.go.id/sumbar/konten/278/ produk-layanan.bpkp

Badan Pengawasan Keuangan dan Pembangunan. *Kawal Akuntabilitas Keuanan dan Pembangunan.* http://www.bpkp.go.id/konten/10/pusat-layanan.bpkp

Carmichael, D.R. (2018). Audit Versus Fraud Examination. *Thè CPA Journal,* 88 (2), 48-53.

Crain, M.A., Hopwood, W.S., Gendler, R.S., Young, G.R., & Pacini, C. (2019). *Essentials of Forensic Accounting.* Durham: Association of International Certified Proffessional Accounting.

Crumbley, D.L., Lester, E.H. & Stevenson, S. (2011). *Forensic and Investigative Accounting,* 5th Edition. Chicago: CCH.

Howieson, B. (2018), What is the 'good' forensic accountant? A virtue ethics perspective. *Pacific Accounting Review,* 30 (2), 155-167.

Komisi Pemberantasan Korupsi. *Fungsi dan Tugas.* https://www.kpk.go.id/id/tentang-kpk/ struktur- organisasi/93-tentang-kpk/fungsi-dan-tugas/31-fungsi-dan-tugas

Petrucelli, J.R. (2012). *Detecting Fraud in Organizations. Techniques, Tools, and Resources.* New Jersey: John Wiley & Sons.

Singleton, T.W., Singleton, A.J., Bologna, G.J & Lindquist, A.J. (2006). *Fraud Auditing and Forensik Accounting,* Third Edition. New Jersey: John Wiley & Sons.

Undang-Undang RI No.46 tahun 2009, tentang Pengadilan Tindak Pidana Korupsi.

BAB 9
AUDIT INVESTIGATIF

Pendahuluan

Audit investigatif merupakan suatu bentuk audit atau pemeriksaan yang mempunyai tujuan untuk mengidentifikasi dan mengungkap berbagai kecurangan atau kejahatan dengan menggunakan pendekatan, prosedur dan teknik-teknik yang umumnya digunakan dalam suatu penyelidikan atau penyidikan terhadap suatu tindak kejahatan. Oleh karena tujuan audit investigasi tersebut untuk mengidentifikasi dan mengungkap kecurangan atau kejahatan, maka pendekatan, prosedur dan teknik yang dipakai dalam audit investigatif relatif berbeda dengan pendekatan, prosedur dan teknik yang digunakan di dalam audit keuangan, audit kinerja maupun audit dengan tujuan tertentu lainnya.

Pada pelaksanaan audit investigatif, auditor memulai aktivitas audit dengan praduga/indikasi akan adanya kemungkinan terjadinya kecurangan dan kejahatan yang akan diidentifikasi dan diungkap melalui audit yang akan dilaksanakan. Hal ini tentunya akan mempengaruhi beberapa kondisi setelahnya, misalnya siapa yang akan diwawancarai terlebih dahulu atau dokumen apa yang harus dikumpulkan terlebih dahulu. Selain hal tersebut, dalam pelaksanaan audit investigatif, jika diberi atau memiliki kewenangan, auditor dapat menggunakan prosedur dan teknik yang umumnya digunakan dalam proses penyelidikan dan penyidikan tindak kejahatan, seperti misalnya pengintaian dan penggeledahan serta observasi lapangan.

Auditor sebagai pelaksana Audit Investigasi

Audit investigatif terhadap indikasi tindak pidana korupsi dapat dilakukan oleh auditor di lembaga negara dan lembaga pemerintah serta auditor di lembaga non-pemerintah. Pelaksanaan audit investigatif di lembaga negara dan lembaga pemerintah terikat kepada ketentuan yang terdapat pada Standar Pemeriksaan Keuangan Negara (SPKN). Sementara itu, pelaksanaan audit investigatif oleh auditor di lembaga non-pemerintah dapat mengacu kepada standar pemeriksaan yang dikeluarkan oleh lembaga yang memiliki otoritas untuk mengeluarkan standar seperti itu, di Indonesia misalnya Institut Akuntan Publik Indonesia (IAPI) atau standar audit lainnya tergantung kepada keterikatan antara auditor dengan pemberi mandat audit.

Kualifikasi Auditor

Pada dasaarnya, audit investigatif seharusnya dilaksanakan oleh seseorang yang telah memiliki pengalaman yang cukup serta keahlian dalam melaksanakan audit investigatif. Oleh karena itu, auditor yang belum mempunyai pengalaman dan keahlian harus mendapat bimbingan dari auditor lain yang telah memiliki pengalaman dan keahlian melaksanakan audit investigatif. Auditor investigatif juga perlu mempunyai pemahaman yang cukup tentang hal-hal yang akan diaudit terutama menyangkut regulasi/peraturan yang berlaku serta proses bisnis yang berkaitan dengan hal-hal yang akan diaudit. Secara khusus, auditor yang akan melaksanakan audit investigatif juga harus mempunyai pemahaman yang cukup tentang ketentuan-ketentuan hukum terkait dengan hal-hal yang akan diaudit maupun ketentuan-ketentuan hukum yang berkaitan dengan pengungkapan tindak kejahatan misalnya Kitab Undang-Undang Hukum Acara Pidana (KUHP).

Lebih lanjut Chukwu *et al.* (2019) menjelaskan beberapa karakter yang seharusnya dimiliki oleh seorang auditor forensik, yaitu diantaranya meliputi: (1) Kreatif, yaitu kemampuan untuk melihat sesuatu yang oleh orang lain dianggap situasi bisnis yang normal namun sebenarnya ada masalah yang tersembunyi, dan mempertimbangkannya dengan interpretasi lain. (2) Memiliki rasa ingin tahu yang tinggi, dalam hal ini mempunyai keinginan untuk menemukan apa yang sesungguhnya terjadi dalam suatu rangkaian peristiwa dan situasi. (3) Tidak mudah menyerah, dimana auditor forensik seharusnya mempunyai kemampuan untuk maju terus pantang mundur, meskipun fakta nampaknya tidak mendukung, serta ketika dokumen atau informasi sulit diperoleh. (4) Akal sehat, yaitu kemampuan untuk mempertahankan perspektif dunia nyata. (5) *Business sense,* meliputi kemampuan untuk dapat memahami bagaimana bisnis sesungguhnya berjalan, tidak hanya sekedar memahami bagaimana transaksi dicatat. (6) Percaya diri, yakni kemampuan untuk mempercayai diri dan temuan yang didapatkan, sehingga dapat selalu bertahan jika dilakukan berbagai pengujian atau pembuktian silang.

Auditor harus paham benar bahwa banyak kecurangan dilaksanakan dengan persekongkolan. Suatu pengendalian intern yang bagaimanapun baiknya, tidak dapat selalu mencegah hal ini. Salah satu strategi yang dapat dilakukan untuk menemukan kecurangan dalam melakukan aktivitas audit investigasi adalah auditor harus proaktif dalam mempertimbangkan apakah kecurangan dilakukan di dalam pembukuan atau di luar pembukuan. Adapun kecurangan di dalam pembukuan dapat berupa pembayaran yang dilakukan beberapa kali untuk transaksi yang sama, sedangkan untuk kecurangan di luar pembukuan dapat berupa *kickback*, atau suap yang diambil dari harga beli yang sudah dinaikkan nilainya *(mark up).* Demikianlah berbagai modus operandi kecurangan yang kemungkinan dapat dilakukan, sehingga auditor harus memahami benar tentang hal tersebut supaya pelaksanaan audit yang dilakukan optimal.

Pendekatan-Pendekatan pada Audit Investigasi

Seperti halnya pada aktivitas penyelidikan dan penyidikan, pelaksanaan audit investigatif dapat dilakukan secara REAKTIF atau PROAKTIF.

1. Audit investigatif dikatakan bersifat **"reaktif"** apabila auditor melaksanakan audit setelah mendapatkan informasi dari pihak lain berkaitan dengan kemungkinan adanya tindak kecurangan atau kejahatan. Audit investigatif yang bersifat reaktif pada umumnya dilaksanakan setelah auditor menerima atau mendapatkan informasi dari berbagai sumber, misalnya dari auditor lain yang melaksanakan audit

reguler, dari pengaduan masyarakat, atau karena adanya permintaan dari aparat penegak hukum. Karena sifatnya yang reaktif maka auditor tidak akan melaksanakan audit apabila tidak tersedia informasi yang cukup mengenai adanya dugaan atau indikasi kecurangan dan kejahatan.

2. Audit investigatif dikatakan bersifat **"proaktif"** apabila auditor secara aktif mengumpulkan informasi dan menganalisis informasi tersebut untuk menemukan kemungkinan adanya tindak kecurangan dan kejahatan sebelum melaksanakan audit investigatif. Secara aktif auditor mencari, mengumpulkan dan menganalisis segala informasi yang diperoleh untuk menemukan kemungkinan adanya kecurangan dan kejahatan. Audit investigatif yang bersifat proaktif ini perlu dilakukan pada area atau bidang-bidang yang memiliki potensi kecurangan atau kejahatan yang tinggi. Audit yang bersifat proaktif dapat menemukan kemungkinan adanya kecurangan dan kejahatan secara lebih dini sebelum kondisi tersebut berkembang menjadi kecurangan atau kejahatan yang lebih besar. Selain itu, audit investigatif yang bersifat proaktif ini juga dapat menemukan kejahatan yang sedang atau masih berlangsung sehingga pengumpulan bukti untuk penyelidikan, penyidikan dan penuntutan kejahatan lebih mudah dilaksanakan.

Hasil dari sebuah aktivitas audit investigatif, baik yang bersifat reaktif maupun proaktif dapat dipakai sebagai dasar penyelidikan dan penyidikan kejahatan oleh para aparat penegak hukum. Berdasarkan hasil audit tersebut, para aparat penegak hukum selanjutnya mengumpulkan berbagai bukti yang relevan sesuai dengan kaidah hukum yang berlaku untuk kepentingan penuntutan dan pemeriksaan di pengadilan. Selanjutnya, sangat penting diketahui mekanisme dalam pelaksanaan audit investigatif agar pelaksanaan audit lancar dan mencapai hasil yang maksimal.

Mekanisme dalam Melakukan Audit Investigasi

Salah satu usaha keras yang dilakukan pihak pemerintah untuk menanggulangi tindak korupsi adalah dengan melakukan audit investigasi. Audit Investigasi menjadi sangat penting jika hasil audit menunjukkan bukti adanya pelanggaran hukum materiil dan formil (Hukum pidana materiil adalah hukum pidana yang memuat bentuk-bentuk perbuatan yang dilarang serta ancaman hukuman bagi siapa saja yang melanggarnya, dalam hal ini KUHP. Hukum pidana formil merupakan hukum acara pidana yang mengatur tata cara menjalankan hukum pidana materiil, dalam hal ini KUHAP, maka hasil laporan audit investigatif akan diserahkan kepada kejaksaan untuk diproses secara hukum. Pelaksanaan audit investigasi tidak berjalan sendiri, akan tetapi melibatkan berbagai pihak, mulai dari pimpinan, para pejabat struktural, tim konsultan hukum, dan auditor investigatif. Berikut ini dipaparkan mekanisme dalam melaksanakan audit investigasi.

1. Mengumpulkan data dan informasi serta menganalisis adanya indikasi korupsi.
   Audit investigatif proaktif dimulai dengan aktivitas pengumpulan data dan informasi yang berkaitan dengan permasalahan yang akan diaudit. Terdapat dalam jumlah yang besar data dan informasi yang dapat dikumpulkan dari berbagai sumber untuk mengidentifikasi adanya indikasi kecurangan dan kejahatan, seperti: data aliran dana keluar perusahaan, data kekayaan orang-orang yang menjadi *key person* pada suatu perusahaan, informasi dari media massa, dan lain-lain. Selanjutnya, berbagai jenis data dan informasi tersebut dianalisis sesuai dengan tujuan dari audit investigatif yang akan dilaksanakan.

2. Mengembangkan hipotesis terkait dengan kejahatan serta merencanakan audit; diantaranya: (a) Lakukan analisis terhadap perkembangan produk perusahaan di pasaran, bandingkan dengan perusahaan sejenis, analisis rugi sebabnya apa?. (b) Dapatkan informasi mengenai siapa yang berwenang/melakukan otorisasi uang keluar dengan nominal yang signifikan, dan lain-lain.
3. Melaksanakan audit dengan tertib untuk mengumpulkan bukti-bukti yang mendukung hipotesis. Dalam melaksanakan audit investigatif, auditor harus menerapkan pendekatan yang relatif berbeda dengan pendekatan yang dilaksanakan dalam audit non-investigatif, diantaranya meliputi:
   a. Auditor melakukan wawancara terhadap saksi yang mendukung pelaksanaan audit serta melakukan analisis terhadap semua dokumen yang tersedia;
   b. Auditor menggunakan bukti tidak langsung yang tersedia untuk meyakinkan saksi-saksi supaya bisa memperoleh seluruh bukti yang secara langsung menunjukkan terjadinya kecurangan ataupun kejahatan;
   c. Apabila telah mendapatkan bukti-bukti yang cukup, selanjutnya auditor dapat melakukan wawancara terhadap orang-orang yang diduga melakukan kecurangan atau kejahatan terutama untuk membuktikan adanya unsur niat atau kesengajaan.
   d. Auditor juga harus mampu mengidentifikasi dan mengungkap adanya indikasi/keberadaan fraud dengan mengungkapkan hal-hal berikut ini:
      1) What/ Apa yang menjadi masalah indikasi fraud dalam perusahaan?
      2) Who/ Siapa yang diduga/ terindikasi melakukan fraud?
      3) Where/ Dimana indikasi suatu fraud terjadi?
      4) When/ Kapan pelaku melakukan fraud tersebut?
      5) Why/ Mengapa fraud bisa terjadi di perusahaan?
      6) How(how much)/ Bagaimana fraud bisa terjadi? dan berapa besar kerugian akibat fraud tersebut?
   e. Auditor harus mendokumentasikan semua hasil auditnya dalam kertas kerja audit, kertas kerja akan direview oleh *team leader* dan manajer audit (*Partner in Charge*) dan dikumpulkan serta disusun secara sistematis dalam suatu tempat penyimpanan dokumen.
   f. Jika auditor telah melakukan program kerja pemeriksaan yang diperlukan serta mengumpulkan bukti-bukti yang dapat menjawab pertanyaan 5W+H, maka auditor dapat menghentikan audit dan menyusun Laporan Hasil Audit Investigatif segera.
4. Setelah selesai melaksanakan audit, selanjutnya Ketua Tim Audit menyusun laporan audit investigatif, yang disusun dengan memperhatikan ketentuan penyusunan laporan audit investigatif sebagai berikut:
   a. Akurat dalam arti bahwa seluruh materi laporan seperti misalnya terkait dengan kecurangan atau kejahatan yang terjadi serta informasi penting lainnya, termasuk penyebutan nama, tempat, atau tanggal telah benar dan sesuai dengan bukti-bukti yang sudah dikumpulkan;
   b. Jelas dalam arti bahwa laporan harus disampaikan secara sistematik, ringkas, padat dan setiap informasi yang disampaikan mempunyai hubungan yang logis. Selainitu, semua istilah yang bersifat teknis harus sebisa mungkin dihindari, namun bila tidak bisa dihindari harus dijelaskan secara memadai;
   c. Berimbang dalam arti bahwa laporan tidak sedikitpun mengandung adanya bias atau prasangka dari auditor yang menyusun laporan atau pihak-pihak lain yang dapat mempengaruhi auditor. Laporan hanya memuat fakta-fakta dan tidak memuat opini atau pendapat pribadi auditor.

d. Relevan dalam arti bahwa laporan hanya mengungkapkan informasi maupun data-data yang berhubungan langsung dengan kecurangan atau kejahatan yang terjadi, sehingga informasi lain di luar yang terkait langsung dengan kecurangan atau kejahatan yang terjadi dikeluarkan dari laporan;
e. Tepat waktu dalam arti bahwa laporan harus disusun segera mungkin setelah pekerjaan lapangan selesai dilaksanakan dan segera disampaikan kepada para pihak yang berkepentingan.

Berdasarkan mekanisme tersebut, audit investigasi secara garis besar dapat dibagi ke dalam enam tahapan yang meliputi tahap pra-perencanaan, tahap perencanaan, tahap pengumpulan bukti, tahap evaluasi buksi, tahap pelaporan, serta tahap tindak lanjut. Tahapan-tahapan ini sedikit berbeda dengan tahapan-tahapan yang dilakukan dalam pemeriksaan operasional yang biasa dilakukan. Secara garis besar proses pelaksanaan pemeriksaan (audit) investigatif tersebut, meliputi:

Tahap Pra-Perencanaan
Audit investigatif merupakan suatu respon terhadap sinyalemen atau informasi awal yang masuk ke unit kerja investigasi. Sinyalemen atau informasi awal ini dapat bermacam-macam sumbernya seperti pengaduan masyarakat, tindak lanjut terhadap rekomendasi temuan pemeriksaan operasional, informasi dari media massa, serta permintaan dari Menteri untuk melakukan audit investigasi atau audit tertentu. Pada umumnya, pengaduan dari masyarakat belum memuat informasi yang spesifik/detail namun masih bersifat umum dan tendensius. Sehubungan dengan hal tersebut, informasi awal ini perlu terlebih dahulu dianalisis atau ditelaah secara teliti dan detail supaya dapat segera ditentukan layak atau tidak untuk selanjutnya dilaksanakan audit investigatif. Analisis yang dilakukan sebaiknya tidak tergesa-gesa dan memerlukan kajian tim yang lengkap dan detail, karena hasil analisis menentukan dilakukan atau tidaknya audit investigasi pada suatu kasus.

Tahap Perencanaan
Salah satu hal yang membedakan antara audit investigasi dengan audit operasional adalah adanya penyusunan hipotesis yang merupakan bagian dari tahapan perencanaan. Hipotesis ini disusun berdasarkan hasil analisis dari berbagai kemungkinan penyimpangan yang dikembangkan berdasarkan informasi yang tersedia, dan atas jawaban dari pertanyaan: siapa , apa, mengapa, dimana, bilamana, dan bagaimana (5W-1H) yang dihasilkan dari kegiatan penelaahan awal. Selain menyusun hipotesis, dalam tahapan ini juga berbicara tentang penyusunan program audit, perencanaan sumber daya dan penerbitan Surat Tugas.

Tahap Pengumpulan Bukti
Terdapat satu ungkapan yang harus dipertimbangkan oleh auditor investigasi yaitu "*tidak ada bukti tidak ada kasus*". Pengertian dari ungkapan ini adalah bahwa bukti merupakan unsur yang sangat penting dalam mengungkapkan sebuah kasus penyimpangan tindak pidana korupsi. Pada umumnya audit investigatif akan bermuara pada proses hukum, untuk itu auditor investigasi diharapkan mampu memahami berbagai bukti yang bisa dianggap sebagai bukti hukum. Perlu diketahui bahwa tidak semua bukti audit bisa diakui dan dipakai sebagai bukti hukum persidangan. Agar auditor dapat memperoleh berbagai bukti yang dibutuhkan, auditor diharapkan mampu memahami berbagai jenis teknik pengumpulan bukti. Teknik-teknik pengumpulan bukti pada audit investigatif tidak jauh berbeda dengan teknik pengumpulan bukti audit operasional.

Tahap Evaluasi Bukti
Bukti-bukti yang telah berhasil dikumpulkan melalui implementasi berbagai teknik audit selanjutnya dianalisis untuk melihat kesesuaian bukti dengan hipotesis. Melalui analisis bukti inilah auditor bisa mengembangkan dan mencari bukti-bukti lainnya yang dapat digunakan untuk mendukung bukti yang telah diperoleh sebelumnya. Analisis bukti tersebut dapat menggambarkan sebuah rangkaian kejadian atau peristiwa. Dari rangkaian beberapa analisis bukti tersebut akan diperoleh gambaran secara keseluruhan peristiwa yang telah terjadi. Rangkaian analisis bukti ini selanjutnya dievaluasi secara berkala untuk mengetahui apakah ada kesesuaian dengan hipotesis yang telah dibangun. Dalam tahap evaluasi bukti ini, memungkinkan adanya perubahan hipotesis apabila hasil evaluasi bukti tidak mendukung hipotesis yang telah ditetapkan sebelumnya akan tetapi mengarah pada permasalahan yang sebelumnya tidak diperkirakan. Hasil evaluasi bukti inilah yang akan menentukan apakah kasus tersebut terbukti atau tidak.

Tahap Pelaporan
Tahapan yang paling penting dalam sebuah kegiatan audit investigasi adalah proses dokumentasi. Proses dokumentasi ini pada umumnya disusun dalam bentuk laporan tertulis. Penyusunan laporan audit investigatif ini juga merupakan bukti bahwa auditor investigasi telah melakukan tugasnya sesuai dengan prosedur yang berlaku dan profesionalisme yang dimilikinya. Pelaporan ini harus mampu mengungkapkan seluruh fakta yang ada dan menghindari sejauh mungkin mengungkapkan hal-hal yang masih bersifat subyektif serta bias. Adapun laporan yang baik seharusnya mampu menjawab pertanyaan 5W-1H (siapa, apa, mengapa, dimana, bilamana, dan bagaimana).

Tahap Tindak Lanjut
Tahapan terakhir dalam seluruh proses audit investigasi adalah tahap tindak lanjut *(follow-up)*. Proses aktivitas tindak lanjut ini harus dilakukan secara proporsional apalagi untuk sebuah kasus yang berindikasikan tindak pidana korupsi. Tahap tindak lanjut ini bertujuan untuk memastikan apakah hasil temuan audit investigasi telah ditindaklanjuti oleh pihak yang bertanggung jawab dalam kasus tersebut.

Pembagian tahap audit investigasi ini secara teori memang terlihat terpisah dan terbagi dalam beberapa tahapan. Akan tetapi, dalam praktik pelaksanaannya batas-batas antar tahapan tersebut tidak dilaksanakan secara terkotak-kotak. Tahapan-tahapan ini lebih dipahami sebagai sebuah kerangka berfikir auditor dalam melakukan audit investigasi yang efektif sehingga mampu mencapai tujuan pemeriksaan yang diharapkan. Sedapat mungkin pelaksanaan berbagai tahapan ini dilakukan secara berjenjang, maksudnya adalah sebelum masuk kepada tahapan berikutnya, auditor seharusnya menyelesaikan dulu secara tuntas proses tahapan sebelumnya. Hal ini karena tahapan proses sebelumnya akan memberikan pijakan untuk melaksanakan tahapan-tahapan proses selanjutnya. Dengan demikian, dapat kita simpulkan bahwa audit investigasi mempunyai peranan yang sangat penting dalam pengungkapan tindak pidana korupsi. Peran tersebut dilakukan dengan berbagai cara, meliputi: mendeteksi kasus dan modus operandi, menetapkan sebab-sebab penyimpangan dan rekomendasi, melakukan identifikasi terhadap pihak-pihak yang diduga terkait atau bertanggungjawab dengan tindak pidana korupsi, serta melakukan perhitungan jumlah kerugian keuangan negara yang terjadi.

Pada umumnya laporan audit investigasi tebal serta banyak lampirannya. Terkait dengan hal tersebut, sebaiknya laporan ini tidak dilampirkan dalam suatu dakwaan karena terdapat kemungkinan terjadi salah jumlah maupun terdapat angka

yang berbeda antara hal satu dengan lainnya. Satu contoh, pernah dalam sebuah perkara pidana korupsi, jaksa melampirkan laporan audit investigasi dalam dakwaannya. Namun demikian pada akhirnya terdakwa diputus bebas, hal ini karena beberapa pertimbangan keputusan bebas oleh hakim yang antara lain karena penjumlahan angka dalam laporan audit yang salah, terdapat perbedaan angka kerugian negara antara halaman laporan audit yang satu dengan yang lainnya serta angka dalam laporan audit tidak sama dengan lampiran laporan audit.

Selanjutnya, laporan hasil audit investigasi diserahkan kepada aparat penegak hukum untuk ditingkatkan menjadi proses penyidikan. Hal ini dilakukan jika sudah terpenuhi 2 unsur alat bukti yang memadai yaitu laporan hasil audit investigasi dan keterangan ahli, yakni tim audit investigasi itu sendiri. Setelah surat perintah penyidikan *(sprindik)* diterbitkan, maka aparat penegak hukum kemudian meminta tim audit untuk melakukan audit forensik. Audit forensik didefinisikan sebagai tindakan menganalisa serta membandingkan antara kondisi di lapangan dengan suatu kriteria, untuk menghasilkan informasi atau bukti kuantitatif yang dapat dipakai untuk proses litigasi (proses pengadilan). Karena sifat dasar audit forensik berfungsi untuk memberikan bukti di muka pengadilan, maka fungsi utama dari audit forensik adalah untuk melakukan audit investigasi terhadap tindak kriminal dan untuk memberikan keterangan saksi ahli *(litigation support)* di pengadilan.

Audit investigasi mempunyai tujuan untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, supaya dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh pelaku tindak kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sembari mencari berbagai pihak terkait yang terlibat baik secara langsung maupun tidak langsung dengan perbuatan yang tidak menyenangkan dimaksud. Tanggung jawab pelaksanaan audit investigasi adalah pada lembaga audit atau satuan pengawas, sedangkan audit forensik berada pada pribadi auditor (Kumar & Vijayalaksmi, 2018). Apabila berbagai keterangan yang diberikan kepada penyidik atau keterangan di sidang pengadilan palsu, maka auditor akan dikenai sanksi.

Sehubungan dengan hal di atas, sangatlah jelas perbedaan antara audit investigasi dengan audit forensik. Tujuan audit investigasi adalah mengadakan audit lebih lanjut atas temuan audit sebelumnya, serta melaksanakan audit untuk membuktikan kebenaran berdasarkan pengaduan atau informasi dari masyarakat atau *whistleblower.* Sedangkan audit forensik bertujuan untuk membantu penyidik dalam rangka membuat terang *(clear)* perkara pidana khusus yang sedang dihadapi penyidik, serta mengumpulkan bukti-bukti baik berupa dokumen/surat untuk mendukung dakwaan jaksa.

Audit investigasi sangat penting dilakukan karena sebuah permasalahan yang terkait dengan tindakan kecurangan dapat diselesaikan dengan bantuan audit investigasi. Dengan melakukan audit investigasi akan segera diketahui penyebab permasalahan yang terjadi. Untuk mendapatkan hasil investigasi yang maksimal, seorang *fraud auditor* harus menguasai pendekatan, mekanisme serta tahapan-tahapan audit investigasi. Selain hal tersebut beberapa teknik investigasi seperti teknik penyadapan, penyamaran, wawancara, serta teknik merayu untuk mendapatkan informasi sangat penting dipahami oleh seorang auditor investigasi. Lebih lengkap lagi apabila seorang auditor investigasi juga mengerti bahasa tubuh dalam membaca posisi auditee yaitu jujur atau berbohong, serta menguasai juga berbagai software terkait dengan pengauditan seperti CAAT *(Computer Assisted Audit Tools).*

Simpulan

Audit investigasi merupakan audit khusus yang dilaksanakan berkaitan dengan adanya indikasi tindak pidana korupsi, penyalahgunaan wewenang, serta ketidaklancaran suatu pembangunan. Audit investigasi ini dilakukan oleh seorang auditor yang dikenal sebagai Auditor Investigatif. Audit investigasi ini merupakan suatu proses mencari, menemukan serta mengumpulkan bukti secara sistematis yang bertujuan mengungkapkan terjadi atau tidaknya suatu perbuatan dan pelakunya guna dilakukan tindakan hukum lebih lanjut. Pelaksanaan audit investigasi ini berbeda dengan pelaksanaan audit pada umumnya, karena audit ini berkaitan langsung dengan proses litigasi. Hal ini mengakibatkan tugas dari seorang auditor investigasi lebih berat daripada tugas seorang auditor dalam audit umum (general audit). Selain diharuskan memahami konsep pengauditan dan akuntansi, auditor investigatif juga harus memahami hukum terkait dengan kasus penyimpangan atau kecurangan yang mengakibatkan terjadinya kerugian negara.

Contoh Kasus

Kasus Proyek Hambalang

Pembangunan Pusat Pendidikan Pelatihan dan Sekolah Olah Raga Nasional (P3SON) yang rencananya akan di bangun di Hambalang, Sentul, Bogor, Jawa Barat, didalam audit BPK, ditulis bahwa proyek senilai Rp 1,2 triliun ini dibiayai oleh APBN atas dari usulan Kementrian Pemuda dan Olahraga. Direktorat Jenderal Olahraga Departemen Pendidikan Nasional hendak membangun Pusat Pendidikan Pelatihan Olahraga Pelajar Tingkat Nasional *(National Training Camp Sport Center).*

Pada tahun 2004 dibentuklah tim verifikasi yang mempunyai tugas mencari lahan yang representatif untuk mensukeskan rencana tersebut. Hasil tim verifikasi ini menjadi bahan pertimbangan pada Rapim Ditjen Olahraga Depdiknas untuk memilih lokasi yang dianggap paling cocok bagi pembangunan pusat olahraga tersebut. Tim verifikasi mensurvei lokasi yang dinilai layak untuk membangun pusat olahraga itu. Lokasi yang dianggap representatif di Karawang, Hambalang, Cariu, Cibinong, dan Cikarang. Pada akhirnya tim memberikan penilaian tertinggi pada lokasi desa Hambalang, Citeureup, Bogor. Karena lahan di Hambalang itu sudah memenuhi semua kriteria penilaian tersebut di atas. Sehingga lokasi tersebut dipilih untuk dibangun.

Dalam menindaklanjuti pemilihan Hambalang, Dirjen Olahraga Depdiknas langsung mengajukan permohonan penetapan lokasi Diklat Olahraga Pelajar Nasional kepada Bupati Bogor. Bupati Bogor menyetujui dengan mengeluarkan Keputusan Bupati Bogor nomor 591/244/Kpes/Huk/2004 tanggal 19Juli 2004. Tetapi, PVMBG menyarankan untuk tidak mendirikan bangunan di lokasi tersebut karena memiliki risiko bawaan yang tinggi bagi terjadinya bencana alam berupa gerakan tanah.

Pokok Permasalahan

Nilai proyek ini kemudian melejit hingga Rp 2,5 triliun saat Kemenpora dipimpin oleh Menteri Andi Mallarangeng. terungkap dalam audit Hambalang, bahwa pada tanggal 8 Februari 2010 dalam Raker antara Kemenpora dengan Komisi X,

Menpora menyampaikan rencana Lanjutan Pembangunan tahap I P3SON di Bukit Hambalang hanya senilai Rp 625.000.000.000. Permintaan itu diajukan karena dalam DIPA Kemenpora TA 2010 baru tersedia Rp125 miliar. Menpora AM menyampaikan bahwa usulan tersebut merupakan bagian rencana pembangunan P3SON di Bukit Hambalang Sentul yang secara keseluruhan memerlukan dana sebesar Rp 2,5 triliun. Ketua Badan Pemeriksa Keuangan (BPK) menyebut total kerugian negara akibat Proyek Hambalang sebesar Rp 463,67 miliar. BPK menyimpulkan ada indikasi kerugian negara sebesar Rp 463,67 miliar akibat adanya indikasi penyimpaangan dan penyalahgunaan wewenang yang mengandung unsur-unsur pidana yang dilakukan pihak-pihak terkait dalam pembangunan P3SON Hambalang. Pelanggaraan terletak pada beberapa tahapan. Pertama, proses pengurusan hak atas kepemilikan tanah dan ganti rugi tanah. Kedua, proses pengurusan izin pembangunan. Ketiga, proses pelelangan mega proyek hambalang. Keempat, proses persetujuan RKA-KL dan persetujuan Kontrak Tahun Jamak. Kelima, pelaksanaan pekerjaan konstruksi dan keenam, pembayaran dan aliran dana dengan adanya rekayasa akuntansi.

Dalam hasil audit forensik kasus hambalang Ketua Badan Pemeriksa Keuangan (BPK) memaparkan sejumlah hasil audit terhadap kasus Hambalang ke DPR. Laporan audit investigasi kasus Hambalang dilakukan dua tahap. Laporan Hasil Pemeriksaan (LHP) kasus Hambalang tahap I dilakukan pada 30 Oktober 2012. Hasilnya disampaikan ke DPR. Dalam LHP tahap I, BPK menyimpulkan bahwa adanya indikasi penyimpangan terhadap peraturan perundang-undangan dalam proses persetujuan tahun jamak, proses pelelangan, proses pelaksanaan konstruksi, dan dalam proses pencarian uang muka yang dilakukan pihak terkait dalam pembangunan Hambalang yang mengakibatkan timbulnya indikasi kerugian negara sekurang-kurangnya Rp 263,66 miliar. Dalam LHP tahap II, BPK menyimpulkan terdapat indikasi penyimpangan dan/atau penyalahgunaan wewenang yang mengandung penyimpangan yang dilakukan pihak-pihak terkait dalam pembangunan proyek hambalang. Penyimpangan wewenang terjadi pada proses pengurusan hak atas tanah, proses ganti rugi tanah, proses izin pembangunan, proses pelelangan, proses persetujuan RAK K/L dan persetujuan tahun jamak, pelaksanaan pekerjaan konstruksi, pembayaran, dan aliran dana yang di ikuti dengan rekayasa akuntasi dalam proyek Pusat Pendidikan Pelatihan dan Sekolah Olahraga Nasional (P3 SON), Hambalang. Dalam LHP tahap II ini BPK kembali menemukan adanya penyimpangan dalam proses pengajuan dan kerugian negara mencapai Rp 471 miliar.

Terkait dengan persetujuan RAK K/L dan persetujuan tahun jamak, BPK juga menemukan adanya pencabutan Peraturan Menteri Keuangan No 56/2010 yang diganti dengan Peraturan Menteri Keuangan No 194/2011 tentang Tata Cara Pengajuan Persetujuan Kontrak Tahun Jamak dalam Pengadaan Barang/Jasa Pemerintah. Peraturan Menteri Keuangan No 194/2011 diduga diganti secara mendadak bertentangan dengan Pasal 14 UU No 1/2004. Peraturan tersebut dibuat bertujuan untuk melegalisasi dugaan penyimpangan yang telah terjadi. Berbagai indikasi penyimpangan yang dimuat dalam LHP tahap I dan II mengakibatkan kerugian negara sebesar Rp 463,67 miliar.

Kesimpulan tersebut, didasarkan pada fakta-fakta sebagai berikut.

- Kemenpora tidak pernah memenuhi persyaratan untuk melakukan studi amdal sebelum mengajukan izin lokasi. Dan *setplant* dan izin mendirikan bangunan kepada pemkab Bogor atau menyusun dokumen evalusi lingkungan hidup

mengenai proyek Hambalang. Permohonan persetujuan tahun jamak dari Kemenpora kepada Menteri Keuangan atas proyek Pembangunan Hambalang dianggap tidak memenuhi persyaratan sebagai mana yang ditetapkan dalam peraturan yang berlaku. Sehingga sudah seharusnya permohonan tersebut ditolak.

Daftar Bacaan

Crumbley, D.L. (2017). *Forensic and Investigative Accounting*, 8th Edition, Louisiana: Wolters Kluwers.

Chukwu, N., Asaolu, T.O., Uwuigbe, O.R., Umukoro, O.E, Nassar, L. & Alabi, O. (2019). *The impact of basic forensic accounting skills on financial reporting credibility among listed firms in Nigeria*. IOP Conference Series: Earth and Environmental Science. Volume 331, International Conference on Energy and Sustainable Environment 18–20 June 2019, Covenant University, Nigeria.

Hay, D. & Cordery, C. (2018). The value of public sector audit: Literature and history. *Journal of Accounting Literature*, (40), 1-15.

Kumar, D.R & Vijayalaksmi. (2018). A study on role and responsibility of forensic accounting in fraud detecetion and legal disputes. *International Journal of Management and Social Sciences*, 8 (14), 155-167.

Peraturan BPKP RI No. 17 Tahun 2017. *Tentang Pedoman Pengelolaan Kegiatan Bidang Investigasi*.

Sunday, A.A. & Juliana, M.I. (2016). Relevance of forensic auditing as an investigative tool in curbing financial crimes in public sectors organization. *Journal of Accounting and Financial Management*, 2 (3), 40-59.

Tuanakotta, T.M. (2010). *Akuntansi Forensik dan Audit Investigatif*. Edisi-2, Jakarta: Salemba Empat.

Zhang, C., Dai, J. & Vasarhelyi, M.A. (2018). The Impact of disruptive technologies on accounting and auditing education. *The CPA Journal*, 88 (9), 20-26.