

**STRATEGI PENGEMBANGAN UNIT ANTI *FRAUD*
PT BANK BPD DIY DALAM MEMINIMALKAN *FRAUD***



SKRIPSI

Disusun oleh :

Nama : Dewi Kilisuci Anisha Puri

No. Mahasiswa : 14312137

**FAKULTAS EKONOMI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA**

2018

STRATEGI PENGEMBANGAN UNIT ANTI *FRAUD*
PT BANK BPD DIY DALAM MEMINIMALKAN *FRAUD*

SKRIPSI

Disusun dan diajukan untuk memenuhi sebagai salah satu syarat untuk mencapai derajat Sarjana Strata-1 Program Studi Akuntansi pada Fakultas Ekonomi UII

Oleh :

Nama : Dewi Kilisuci Anisha Puri

No. Mahasiswa : 14312137

FAKULTAS EKONOMI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA

2018

PERNYATAAN BEBAS PLAGIARISME

“Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk gelar kesarjanaan di suatu perguruan tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam referesi. Apabila ditemukan dikemudian hari terbukti bahwa pernyataan ini tidak benar maka saya sanggup menerima hukuman/sanksi apapun sesuai peraturan yang berlaku.”

Yogyakarta, 1 Mei 2018

Penulis,



(Dewi Kilisuci Anisha Puri)

STRATEGI PENGEMBANGAN UNIT ANTI *FRAUD*
PT BANK BPD DIY DALAM MEMINIMALKAN *FRAUD*

SKRIPSI

Diajukan Oleh:


Nama: Dewi Kilisuci Anisha Puri

No. Mahasiswa: 14312137

Telah disetujui oleh Dosen Pembimbing

Pada Tanggal 30 April 2018

Dosen Pembimbing,

A handwritten signature in black ink, appearing to read 'Hendi Yogi Prabowo', written over a large, stylized scribble.

(Hendi Yogi Prabowo, S.E., M.For.Accy., Ph.D.)

BERITA ACARA UJIAN TUGAS AKHIR /SKRIPSI

SKRIPSI BERJUDUL

**STRATEGI PENGEMBANGAN UNIT ANTI FRAUD PT BANK BPD DIY DALAM
MEMINIMALKAN FRAUD**

Disusun Oleh : **DEWI KILISUCI ANISHA PURI**

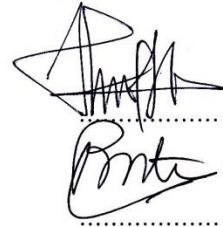
Nomor Mahasiswa : **14312137**

Telah dipertahankan di depan Tim Penguji dan dinyatakan **LULUS**

Pada hari Selasa, tanggal: 5 Juni 2018

Penguji/ Pembimbing Skripsi : Hendi Yogi Prabowo, SE, M.For.Accy., Ph.D.

Penguji : Prapti Antarwiyati, Dra.,MS., Ak, CA.



.....
.....

Mengetahui
Dekan Fakultas Ekonomi
Universitas Islam Indonesia



Dr. D. Agus Harjito, M.Si.

HALAMAN PERSEMBAHAN

Skripsi ini penulis persembahkan untuk :

Kedua orangtua saya (Bapak Purba Wijaya Kusuma dan Ibu Indah Idamansuci) atas segala dukungan, inspirasi, dan doa yang tak hentinya sejak kecil hingga selama penulis menempuh pendidikan tinggi. Tak lupa untuk bude Siti Ari Murti dan Almh. Arifah Hardono serta pakpuh Alm. M.A. Hardono, terimakasih atas segala dukungan materiil maupun immateriil yang diberikan sampai penulis menempuh pendidikan tinggi .

KATA PENGANTAR



Assalamualaikum warrahmatullohi wabarakatuh

Segala puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat dan berkahnya, sehingga penulis dapat menyelesaikan skripsi dengan judul “Strategi Pengembangan Unit Anti *Fraud* PT Bank BPD DIY dalam Meminimalkan *Fraud*” untuk memenuhi salah satu syarat tugas akhir pendidikan sarjana (S1) Akuntansi di Fakultas Ekonomi Universitas Islam Indonesia.

Dalam penyusunan tugas akhir ini, tentunya penulis tidak terlepas dari dukungan, bantuan dan bimbingan banyak pihak. Oleh karena itu, penulis dengan segala kerendahan hati menyampaikan terimakasih kepada :

1. Allah SWT yang tak henti-hentinya menyayangi hamba-Nya, mendengarkan setiap doa, memberikan kemudahan, dan ampunan kepada hamba-Nya.
2. Rasullullah, Nabi Muhammad SAW yang telah membawa manusia dari zaman kegelapan ke zaman terang benderang sehingga membuat kehidupan manusia menjadi lebih baik lagi.
3. Bapak Nandang Sutrisno, SH., M.Hum., LL.M., Ph.D., selaku Rektor Universitas Islam Indonesia, beserta seluruh pimpinan universitas.
4. Bapak Dr. Drs. Dwipraptono Agus Harjito, M.Si., selaku Dekan Fakultas Ekonomi Universitas Islam Indonesia Yogyakarta.
5. Bapak Dekar Urumsah, S.E., S.Si., M.Com., Ph.D., selaku Ketua Program

Studi Akuntansi, Fakultas Ekonomi, Universitas Islam Indonesia.

6. Bapak Hendi Yogi Prabowo, S.E., M.For.Accy., Ph.D., selaku dosen pembimbing skripsi yang telah memberikan ilmu, waktu, dan bimbingannya sehingga penulis dapat menyelesaikan tugas akhir ini.
7. Ibu Primanita Setyono, Ibu Neni Meidawati, Ibu Fitriati Akmila dan Bapak Pandu yang telah memberikan penulis kesempatan untuk belajar sebagai asisten dosen pada mata kuliah yang beliau ampu.
8. Keluarga besar Bani Asmoredjo dan Ki Hadjar Dewantara, khususnya untuk kakekku Alm. H. Rachmad Takim dan nenekku Almh. Hj. Utami serta kakekku Alm. Brigjen TNI R.M. Subroto Aryo Mataram dan nenekku Almh. R.Ay Umiyati Subroto Aryo Mataram yang selalu menjadikan inspirasi bagi penulis agar selalu rendah hati dan memiliki ilmu yang dapat bermanfaat bagi orang banyak.
9. Bapak R.M. Purba Wijaya Kusuma, S.H. dan Ibu Dra, Indah Idamansuci yang telah memberikan banyak dukungan, doa yang tak pernah putus, dan inspirasi utama penulis untuk menyelesaikan studi. Semoga Allah SWT memberikan perlindungan, kebaikan, dan nikmat-Nya kepada kita semua.
10. Kakakku Sekarlangit Dewandaru Aisha Puri yang selalu menjadi tumpuanku, penyemangat, memberi dukungan dalam berbagai kondisi dan selalu rela berkorban untukku. Semoga Allah SWT memberikan perlindungan, kebaikan, dan nikmat-Nya kepadamu.
11. Muhammad Arif Fadhilah yang telah memberikan *support*, ilmu, waktu, dan pelajaran berharga yang diberikan kepada penulis.

12. Sahabat – sahabatku tersayang, Ajeng, Nadia, Lita, Gaffar, Azmi, Luki, Haryan dan Dreza. Terimakasih untuk semua kenangan dan dukungannya sejak awal masuk kuliah hingga lulus. Semoga pertemanan kita akan terjaga hingga tua.
13. Sahabat – sahabatku tercinta Geng LDR, Zea, Nisa, Ely, Aul, Yusi, Dinda, Ovi. Terimakasih atas dukungan kalian sejak SMA, semoga kita dapat selalu menjaga tali silaturahmi.
14. Arvika Shinta, Rizka Dwindi, Luthfi Ikhtiari, Hafiz Addinanto, Azzam, Adam, Talkshow RAKERWIL ISMEI 2016 yang telah menjadi guru terbesar dalam berorganisasi, membangun hubungan teman yang baik. Semoga kita dapat terus menginspirasi dan mencapai yang kita citakan.
15. Asisten dosen ERP Competence Center, Mba Tari, Mba Ratri Dian, Mas Abiyoga, Mas Yusuf Anasta, Vina, Diana, Fika, Mara, Firman, Lulu, terimakasih atas pengalaman yang tak terlupakan di masa – masa akhir perkuliahan dan yang telah saling membantu sehingga memberikan banyak pengalaman bagi penulis.
16. Arma Arba yang telah memberikan segala waktunya untuk saling menginspirasi, saling mendukung meraih cita – cita, memberikan berbagai bentuk semangat. Semoga pertemanan kita terus terjaga sampai tua dan selalu diberikah berkah-Nya yang tak henti kepadamu.
17. Seperjuangan ACCA, Muli, Diana, Daniar, Raina, Fauzan, Fariz yang memberikan pengalaman berharga dalam masa perkuliahan ini sehingga kita semua dapat membagi dan memperluas ilmu bersama – sama.

18. Pejuang skripsi kualitatif, Arba, Muli, Shafira, Desi, Fauzan, dan pejuang lainnya. Terimakasih untuk dukungan dan pembelajarannya.
19. Terimakasih untuk teman – temanku yang sudah membantu dalam pembuatan skripsi ini, untuk Nur Diana terimakasih atas bantuannya, dan untuk Linda, Della, Arrin, Gandhes, Chantika terimakasih atas dukungan dan ilmunya.
20. Teman-teman KKN unit 67. Terimakasih untuk pengalaman kehidupan yang telah kita lewati bersama selama satu bulan.
21. Pihak-pihak lain yang telah membantu dan memberikan pelajaran berharga kepada penulis yang tidak dapat disebutkan satu per satu. Terimakasih atas keikhlasannya dan ilmunya.

Penulis menyadari bahwa skripsi ini terdapat kekurangan dan kelemahan. Untuk itu segala kritik dan saran yang membangun sangat diterima untuk perbaikan penelitian ini. Akhir kata, semoga penelitian ini dapat bermanfaat bagi seluruh pihak yang membutuhkan.

Wassalamualaikum warahmatullahi wabarakatuh

Yogyakarta, 1 Mei 2018

Penulis,

(Dewi Kilisuci Anisha Puri)

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
PERNYATAAN BEBAS PLAGIARISME.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERSEMBAHAN.....	v
KATA PENGANTAR	vi
DAFTAR ISI.....	x
DAFTAR TABEL.....	xv
DAFTAR GAMBAR	xvi
DAFTAR LAMPIRAN.....	xvii
ABSTRAK.....	xix
BAB I.....	1
PENDAHULUAN.....	1
1.1 Pengenalan Bab	1
1.2 Latar Belakang.....	1
1.3 Rumusan Masalah.....	6
1.4 Tujuan Penelitian.....	8
1.5 Fokus Penelitian	9
1.6 Manfaat Penelitian.....	9
1.7 Sistematika Penulisan	10
BAB II.....	13
KAJIAN PUSTAKA.....	13
2.1 Pengenalan Bab	13
2.2 Landasan Teori	13

2.2.1	Fraud	13
2.2.1.1	Pengertian <i>Fraud</i>	13
2.2.1.2	Klasifikasi <i>Fraud</i>	15
2.2.1.3	Perkembangan <i>Fraud</i> di Perbankan Indonesia	29
2.2.2	Strategi Anti <i>Fraud</i>	45
2.2.2.1	Pencegahan	48
2.2.2.2	Deteksi	50
2.2.2.3	Investigasi, Pelaporan dan Sanksi.....	53
2.2.2.4	Pemantauan, Evaluasi, dan Tindak Lanjut.....	54
2.2.3	Pencegahan <i>Fraud</i>	55
2.2.3.1	Mengembangkan Budaya <i>Zero Tolerance</i> pada <i>Fraud</i>	55
2.2.3.3	Pengamanan dengan Teknologi	60
2.2.3.4	Manajemen Sumber Daya Manusia (SDM).....	63
2.2.4	Pendeteksian Fraud	70
2.2.4.1	<i>Whistleblowing System</i>	70
2.2.4.2	<i>Red Flags</i>	74
2.3	Penelitian Terdahulu	79
BAB III.....		88
METODOLOGI PENELITIAN.....		88
3.1	Pengenalan Bab	88
3.2	Jenis Penelitian	88
3.3	Instrumen Penelitian.....	92
3.4	Fokus Penelitian	92
3.5	Sistematika Penelitian	93
3.5.1	Menentukan Topik Penelitian	95
3.5.2	Menentukan Rumusan Masalah	95

3.5.3	Kajian Literatur	96
3.5.4	Pengumpulan Data	96
3.5.5	Analisis Data	97
3.5.5.1	<i>Coding</i>	98
3.5.5.2	<i>Analytical Maps</i>	100
3.5.5.3	<i>Framework Matrices</i>	101
3.5.5.4	<i>Matrix Coding Queries</i>	101
3.5.6	Kesimpulan	102
3.6	Sumber dan Jenis Data	103
3.6.1	Sumber Data Primer	103
3.6.1.1	Wawancara	103
3.6.2	Sumber Data Sekunder	104
3.6.2.1	Dokumen	104
3.7	Pemilihan Responden	105
3.8	Objek Penelitian	108
3.9	Teknik Pengumpulan Data	108
3.10	Teknik Pengujian Keabsahan Data	109
BAB IV		115
HASIL DAN PEMBAHASAN		115
4.1	Pengenalan Bab	115
4.2	Profil Objek Penelitian PT Bank BPD DIY	115
4.2.1	Sejarah Berdirinya PT Bank BPD DIY	115
4.2.2	Produk dan Layanan	122
4.2.3	Struktur Organisasi PT Bank BPD DIY	124
4.3	Struktur dan Mekanisme Penerapan Strategi Anti <i>Fraud</i> pada PT Bank BPD DIY	126

4.3.1	Gambaran Umum <i>Fraud</i> yang Dihadapi PT Bank BPD DIY	126
4.3.2	Struktur Organisasi Unit Anti <i>Fraud</i> PT Bank BPD DIY	128
4.3.3	Analisis Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	130
4.3.3.1	Pilar Pencegahan pada Analisis Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	133
4.3.3.2	Pilar Deteksi pada Analisis Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	142
4.3.3.3	Pilar Investigasi, Pelaporan dan Sanksi pada Analisis Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	146
4.3.3.4	Pilar Pemantauan, Evaluasi dan Tindak Lanjut pada Analisis Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	147
4.3.3.5	Manajemen Risiko pada Analisis Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	149
4.4	Analisis Pengembangan SDM Unit Anti <i>Fraud</i> PT Bank BPD DIY	158
4.4.1	Sertifikasi dan Pelatihan untuk Pegawai	160
4.4.2	Jejak Rekam Pegawai saat Pola Rekrutmen	161
4.4.3	Pengelolaan Teknologi Informasi untuk Mengendalikan <i>Fraud</i>	162
4.4.4	<i>Customer Awareness</i> untuk Mencegah <i>Fraud</i>	163
4.4.5	Pengembangan <i>Whistleblowing system</i> (WBS)	163
4.4.6	Kebijakan Cuti Pegawai	164
4.5	Analisis Kendala yang Dihadapi oleh Unit Anti <i>Fraud</i> PT Bank BPD DIY	164
4.5.1	Penyedia <i>Whistleblowing system</i> (WBS) Dibuat oleh Divisi Teknologi Informasi (TI) Perusahaan Sendiri	166
4.5.2	Kurangnya Kesadaran Melapor Semua Indikasi Kecurangan	166
4.5.3	Jatah Cuti Pegawai yang Tidak Diambil Secara Kolektif	167

4.5.4	Bocornya Rahasia karena Antar Cabang Saling Kenal	168
4.5.5	Belum Adanya Rekrutmen dan Sertifikasi untuk Unit Anti <i>Fraud</i>	168
4.6	Analisis Peningkatan yang Dilakukan Unit Anti <i>Fraud</i> dalam Meminimalkan <i>Fraud</i> PT Bank BPD DIY	169
4.6.1	Audit Teknologi Informasi dan Peningkatan Keamanan	171
4.6.2	Sistem Reward Berupa Promosi, Refresh Anti <i>Fraud Awareness</i> atas Pemahaman <i>Red Flags</i> dan Pembaruan Berupa Aplikasi untuk WBS.....	172
4.6.3	Diadakan <i>Gathering</i> yang Mengurangi Jatah Cuti Bersama dan Melakukan Rotasi Mingguan antar Karyawan	173
4.6.4	Melatih KIC untuk Mempelajari <i>Red Flags</i> Karyawan maupun Transaksi dan Memastikan SOP Dilakukan	174
4.6.5	Dilakukan <i>Training</i> yang Diadakan oleh Badan Bersertifikasi dan Merekrut Pegawai yang Bersertifikasi Akuntan Forensik.....	174
4.7	Kesimpulan Bab	175
	BAB V	177
	PENUTUP.....	177
5.7	Pengenalan Bab	177
5.2	Kesimpulan Penelitian.....	177
5.3	Keterbatasan Penelitian	179
5.4	Saran Penelitian.....	180
	DAFTAR PUSTAKA	181

DAFTAR TABEL

Tabel 2.1 Risiko <i>Internal Fraud</i>	16
Tabel 2.2 Risiko <i>External Fraud</i>	22
Tabel 2.3 Risiko Operasional Bank Umum Posisi Desember 2015.....	30
Tabel 2.4 Jenis dan Kerugian akibat <i>Fraud</i>	32
Tabel 2.5 Pemeriksaan Khusus Bank Triwulan I Tahun 2017.....	33
Tabel 2.6 Pelaku <i>Fraud</i> yang Diduga Tipibank Triwulan I Tahun 2017.....	34
Tabel 2.7 Pemeriksaan Khusus Bank Triwulan II Tahun 2017	35
Tabel 2.8 Pemeriksaan Khusus Bank Triwulan III Tahun 2017	36
Tabel 2.9 Pemeriksaan Khusus Bank Triwulan IV Tahun 2017.....	37
Tabel 2.10 Metode Pencegahan <i>Fraud</i>	58
Tabel 2.11 <i>ACFE Fraud Knowledge Competency</i>	62
Tabel 3.1 Profil Narasumber	103
Tabel 4.1 Komposisi Kepemilikan Saham Awal	115
Tabel 4.2 Komposisi Kepemilikan Saham Disetor	116
Tabel 4.3 Susunan Manajemen	117

DAFTAR GAMBAR

Gambar 2.1 <i>Fraud Triangle</i>	38
Gambar 2.2 <i>Fraud Element Triangle</i>	42
Gambar 3.1 Sistematika Penelitian	90
Gambar 4.1 Struktur Organisasi PT Bank BPD DIY.....	121
Gambar 4.2 Struktur Organisasi Unit Anti <i>Fraud</i> PT Bank BPD DIY	125
Gambar 4.3 <i>Analytical Maps</i> Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	126
Gambar 4.4 <i>Analytical Maps</i> Pengembangan SDM Unit Anti <i>Fraud</i> PT Bank BPD DIY	153
Gambar 4.5 <i>Analytical Maps</i> Kendala yang Dihadapi oleh Unit Anti <i>Fraud</i> PT Bank BPD DIY.....	159
Gambar 4.6 <i>Analytical Maps</i> Peningkatan yang Dilakukan Unit Anti <i>Fraud</i> dalam Meminimalkan <i>Fraud</i> PT Bank BPD DIY	164

DAFTAR LAMPIRAN

Lampiran 1 Wawancara 1 : Ibu Nur Aeni	184
Lampiran 2 Wawancara 2 : Bapak Suwasono Adi Kurniawan.....	197
Lampiran 3 Wawancara 3 : Bapak Zukhroni Ariffin	222
Lampiran 4 Wawancara 4 : Bapak Pandu Kuncoro	227
Lampiran 5 Wawancara 5 : Bapak Muhammad Agus Salam S.	229
Lampiran 6 Wawancara 6 : Bapak Daryoko	232
Lampiran 7 Wawancara 7 : Bapak Andrianto Dwi P.....	235
Lampiran 8 Wawancara 8 : Bapak Ivan Nugroho.....	237
Lampiran 9 Surat Izin Penelitian.....	240
Lampiran 10 Anti <i>Fraud Statement</i>	241
Lampiran 11 Anti <i>Fraud Statement</i> untuk Pegawai.....	242
Lampiran 12 <i>Employee dan Customer Awareness</i>	243
Lampiran 13 <i>Know Your Employee</i>	244
Lampiran 14 <i>Surprise Audit dan Surveillance System</i>	247
Lampiran 15 <i>Whistleblowing System</i>	248
Lampiran 16 <i>Framework Matrix</i> Mekanisme Penerapan Strategi Anti <i>Fraud</i> ..	250
Lampiran 17 <i>Framework Matrix</i> Pengembangan SDM Unit Anti Fraud	275

Lampiran 18 <i>Framework Matrix</i> Kendala yang Dihadapi oleh Unit Anti <i>Fraud</i>	280
Lampiran 19 <i>Framework Matrix</i> Peningkatan yang Dilakukan Unit Anti <i>Fraud</i>	287
Lampiran 20 <i>Matrix Coding</i> Analisis Mekanisme Penerapan Strategi Anti <i>Fraud</i> PT Bank BPD DIY	294
Lampiran 21 <i>Matrix Coding</i> Analisis Pengembangan SDM Unit Anti <i>Fraud</i> PT Bank BPD DIY	298
Lampiran 22 <i>Matrix Coding</i> Analisis Kendala yang Dihadapi oleh Unit Anti <i>Fraud</i> PT Bank BPD DIY	299
Lampiran 23 <i>Matrix Coding</i> Analisis Peningkatan yang Dilakukan Unit Anti <i>Fraud</i> dalam Meminimalkan <i>Fraud</i> PT Bank BPD DIY	300

ABSTRAK

Penelitian ini bertujuan untuk mengetahui penerapan Strategi Anti *Fraud* serta pengembangan SDM yang dilakukan Unit Anti *Fraud* pada PT Bank BPD DIY. Objek dari penelitian ini adalah Unit Anti *Fraud* serta Divisi Manajemen Risiko dan Kepatuhan. Penelitian ini dilakukan dengan metode penelitian kualitatif studi kasus dan menggunakan teknik analisis data *Miles and Huberman*. Teknik pengumpulan data dalam penelitian ini menggunakan wawancara dan dokumen. Pemilihan narasumber dilakukan dengan metode *purposive sampling*, dimana narasumber dipilih dengan kriteria tertentu. Hasil penelitian menunjukkan bahwa penerapan mekanisme Strategi Anti *Fraud* sudah dilaksanakan sesuai dengan Surat Edaran Bank Indonesia No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum, namun masih terdapat kekurangan yang disebabkan oleh kendala dalam penerapannya. Pengembangan SDM terkait penugasan SDM Unit Anti *Fraud* sudah sesuai dengan peraturan Bank Indonesia Nomor 13 tahun 2011, terkait pola rekrutmen seluruh pegawai juga sudah dilakukan jejak rekam pegawai saat rekrutmen, terkait pelatihan khusus SDM Unit Anti *Fraud* sudah bersertifikasi audit internal tetapi masih belum dilakukan sertifikasi khusus anti-*fraud*. Untuk hubungan timbal balik dengan SDM Manajemen Risiko dan Kepatuhan, SDM Unit Anti *Fraud* sudah melakukan koordinasi dalam melakukan identifikasi kerawanan. Kendala yang dihadapi oleh Unit Anti *Fraud* yaitu penyedia *whistleblowing system* yang dibuat oleh Divisi Teknologi Informasi perusahaan sendiri, jatah cuti pegawai yang tidak diambil secara kolektif dan bocornya rahasia surprise audit.

Kata kunci : Strategi Anti *Fraud*, Unit Anti *Fraud*, Pencegahan *Fraud*, Pendeteksian *Fraud*, Pengembangan SDM, *Whistleblowing System*

ABSTRACT

This study aims to determine the application of Anti Fraud Strategy and human resource development conducted by Anti Fraud Unit at PT Bank BPD DIY. The object of this research are the Anti Fraud Unit and the Risk Management and Compliance Division. This research was conducted by qualitative research method of case study and using Miles and Huberman data analysis technique. Data collection techniques in this study using interviews and documents. The selection of resource was done by purposive sampling method, where the source is chosen with certain criteria. The result of this research shows that the application of Anti Fraud Strategy mechanism has been implemented in accordance with Bank Indonesia's Letter No.13 / 28 / DPNP dated December 9, 2011 on Implementation of Anti Fraud Strategy for Commercial Banks, but there are still deficiencies caused by obstacles in its implementation. Human Resource Development related to training for Anti-Fraud Unit Human Resources has accordance with Bank Indonesia regulation number 13 of 2011, related to the recruitment process of all employees has also been traced employee records during recruitment, related to special training of Unit Anti Fraud Human Resources, they have got internal audit certification, but they still have not done special anti-fraud certification. For mutual relationships with Risk Management and Compliance Human Resources, Unit Anti Fraud Human Resources has coordinated in identifying vulnerabilities. Constraints faced by the Anti Fraud Unit are the whistleblowing system providers created by the company's own Information Technology Division, the collective unearned employee's vacation that doesn't taken and leaking of confidential surprise audit.

Keywords : *Anti Fraud Strategy, Anti Fraud Unit, Fraud Prevention, Fraud Detection, Human Resource Development, Whistleblowing System.*

BAB I

PENDAHULUAN

1.1 Pengenalan Bab

Dalam bab ini, peneliti akan menjabarkan latar belakang yang mendasari adanya penelitian mengenai strategi pengembangan unit anti *fraud* dalam meminimalkan *fraud* yang ada. Bab ini juga akan membahas rumusan masalah yang akan dijelaskan pada bab selanjutnya. Selain itu, bab ini juga menjabarkan mengenai fokus penelitian, tujuan penelitian, manfaat dari penelitian ini, serta sistematika dalam penulisan penelitian ini.

1.2 Latar Belakang

Sistem pengendalian internal, tata kelola perusahaan dan manajemen risiko yang diterapkan oleh bank merupakan salah satu cara bank mencegah adanya *fraud*. Peningkatan efektifitas pengendalian internal, tata kelola perusahaan dan manajemen risiko lebih lanjut berguna untuk meminimalisir terjadinya *fraud* dilakukan bank dengan menerapkan strategi anti *fraud*. Strategi anti *fraud* merupakan strategi yang dirancang untuk mengendalikan *fraud* dan memperhatikan jangkauan serta karakteristik *fraud* sehingga dapat diimplementasikan secara komprehensif dalam sistem pengendalian *fraud*. Strategi anti *fraud* adalah bagian dari penerapan manajemen risiko khususnya terkait aspek dalam pengendalian internal. Atas pertimbangan banyaknya terungkap *fraud* di sektor perbankan, maka dibuat lah peraturan untuk

menerapkan strategi anti *fraud* berdasarkan surat edaran Bank Indonesia agar tidak merugikan secara material terhadap bank maupun nasabah.

Menurut Bank Indonesia (2011) dalam Surat Edaran BI No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum, maka ditetapkan:

Bank wajib memiliki dan menerapkan strategi anti *fraud* yang disesuaikan dengan lingkungan internal dan eksternal, kompleksitas kegiatan usaha, potensi, jenis, dan risiko *Fraud*. Penerapan strategi anti *fraud* ditujukan bagi bank konvensional maupun bank umum yang melaksanakan prinsip syariah. Untuk mewujudkan strategi anti *fraud*, bank wajib mengikuti acuan minimal penerapan strategi anti *fraud* yaitu dengan meningkatkan efektifitas pengendalian internal, penerapan manajemen risiko dan tata kelola perusahaan yang baik, sehingga tercipta budaya anti *fraud* di seluruh aspek organisasi. Tumbuhnya *awareness* dalam mencegah dan mendeteksi risiko *fraud* dimulai dari jajaran manajemen agar mampu memberikan arahan serta contoh kepada seluruh organisasi. Strategi anti *fraud* memerlukan sumber daya yang kompeten dalam upayanya dalam mencegah, mendeteksi, serta investigasi dalam mengendalikan *fraud*. Strategi anti *fraud* berupa sistem pengendalian *fraud*, memiliki 4 pilar, sebagai berikut:

1. Pencegahan
2. Deteksi
3. Investigasi, Pelaporan, dan Sanksi;
4. Pemantauan, Evaluasi, dan Tindak Lanjut.

Surat edaran tentang penerapan strategi anti *fraud* merupakan langkah penguatan sistem pengendalian intern Bank dan merupakan pelaksanaan lebih lanjut adanya manajemen risiko bank. Oleh karena itu, dalam menerapkan manajemen risiko, bank harus fokus pada aspek Pengawasan Aktif Manajemen, Struktur Organisasi dan Pertanggungjawaban serta Pengendalian dan Pemantauan.

Menurut Kimani (2011) penipuan dapat dikategorikan dalam dua kelompok besar, yaitu kecurangan internal dan eksternal. Kecurangan internal dilakukan oleh pegawai dan manajer organisasi, yang dilakukan secara individu maupun berkelompok, secara independen maupun bekerjasama dengan pihak diluar organisasi. Kecurangan eksternal dilakukan oleh pihak ketiga organisasi seperti pemasok, pesaing, mitra dan nasabah. Kecurangan eksternal dilakukan oleh orang-orang di luar organisasi. Pelakunya bisa bekerja secara independen atau dapat berkolusi dengan staf untuk menipu Bank. Pelanggar lainnya termasuk calon pelanggan, pemerintah dan organisasi kriminal.

Baru-baru ini, ada beberapa peningkatan dalam mencegah kecurangan media elektronik *banking*. *Financial Fraud Action*, 2011 melaporkan bahwa di Inggris, penipuan pada kartu kredit / debit berada pada level terendah selama 10 tahun terakhir, sementara kerugian penipuan *e-banking* turun 24%. Hal ini disebabkan oleh membaiknya keamanan *e-banking* melalui pendekatan teknologi dan non teknologi (Usman and Shah, 2013).

Dalam beberapa tahun terakhir tercatat beberapa kasus *fraud* yang terjadi dalam dunia perbankan. Di tahun 2017 sendiri ditemukan salah satunya di PT Bank Rakyat Indonesia (Persero) Tbk. Dari yang terbanyak adalah *skimming*, SIM *swap* dengan modus penggantian SIM *card* nomer yang sudah didaftarkan untuk internet banking, serta penyalahgunaan fasilitas internet banking dengan mencuri akun email yang terdaftar.

Di PT Bank Mandiri (Persero) Tbk. ditemukan kejahatan kredit dengan modus melakukan penggelembungan laporan keuangan, jadi ketika perekonomian menurun, penjualan dilaporkan mengalami kenaikan, sehingga ketika perekonomian membaik justru penjualan benar – benar mengalami penurunan. Ditemukan juga kejahatan seperti *phising* atau pencurian identitas dengan kloning data di ATM, serta memalsukan tampilan e-banking bank Mandiri sesuai aslinya sehingga saat nasabah terkecoh sudah memasukkan user id dan password, pelaku segera memindahkan dana yang ada di rekening korban.

Di PT Bank Negara Indonesia (Persero) Tbk. juga terjadi kasus pembobolan data nasabah dengan dilakukan *skimming*, yang kemudian data tersebut digandakan untuk dipergunakan pelaku selama di luar negeri maupun dilakukan penarikan tunai.

Beda halnya di PT Bank Tabungan Negara (Persero) Tbk., terjadi kasus pemalsuan bilyet deposito, kasus ini dilakukan oleh sekelompok orang yang mengatasnamakan pegawai BTN dan menawarkan pinjaman kepada calon nasabah. Pelaku memalsukan seluruh dokumen BTN dan dipergunakan untuk

kepentingannya. Tentu saja hal ini tidak dapat terjadi tanpa bantuan orang internal.

Setelah mendengar berbagai kasus yang terjadi di keempat bank BUMN tersebut, Komisi XI DPR RI meminta kepada setiap bank untuk meningkatkan upaya pencegahan dan identifikasi kerawanan.

Mendeteksi *fraud* cukup dini membantu meminimalkan kerugian dan meningkatkan kemungkinan mengatasi kecurangan yang telah diidentifikasi. Pendeteksian dapat dianggap sebagai pencegah, mencegah kecurangan potensial untuk dilakukan dan membuat organisasi lebih tahan terhadap kecurangan.

Selama tahun 2012, salah satu surat keputusan dan surat edaran direksi adalah dikeluarkannya kebijakan Strategi Anti *Fraud* oleh PT Bank BPD DIY bersamaan dengan dibentuknya *Whistleblowing system*. Strategi anti *fraud* adalah implementasi *Good Corporate Governance* (GCG). Secara umum Dewan Komisaris PT Bank BPD DIY telah menyusun dan menyempurnakan kebijakan *Whistleblowing system* sebagai dasar pedoman dalam menangani pelaporan pelanggaran. Implementasi *Whistleblowing system* secara berkala dipantau efektivitasnya dan dilaporkan secara berkala setiap tahun oleh Direksi melalui Laporan Tahunan. PT Bank BPD DIY juga telah melaksanakan prinsip-prinsip GCG dalam setiap kegiatan usaha Bank pada seluruh tingkatan atau jenjang organisasi, antara lain Direksi telah menjalankan fungsi Satuan Kerja Audit Intern sesuai standar, fungsi Manajemen Risiko dan fungsi Kepatuhan secara independen. Unit Anti *Fraud*

yang bertugas menjalankan strategi anti *fraud* didalam PT Bank BPD DIY merupakan wujud komitmen manajemen bank mengatasi kecurangan yang terjadi di dalam perusahaan yang berguna meminimalkan terjadinya *fraud*.

Dibentuknya Unit Anti *Fraud* berguna untuk mengatasi dampak kerugian *fraud* yang sangat merugikan bank maupun nasabah, serta meningkatkan kepercayaan nasabah terhadap bank. Penelitian ini dilakukan dengan melakukan analisis strategi pengembangan Unit Anti *Fraud* dalam lingkup SDM nya, teknologi, tanggung jawab dan kewajiban setiap bagian dalam unit anti *fraud*. Penelitian ini akan menganalisis strategi PT Bank BPD DIY dalam meminimalkan fraud melalui Unit Anti *Fraud* yang ada di dalam perusahaan, serta bagaimana hubungan timbal balik yang sudah terjalin antara Unit Anti *Fraud* dengan Manajemen Risiko dalam upaya meningkatkan kualitas pendeteksian dan pencegahan *fraud*. Oleh karena PT Bank BPD DIY merupakan Bank yang segera mematuhi kebijakan Bank Indonesia dalam memiliki strategi anti *fraud*, maka peneliti memilih PT Bank BPD DIY sebagai objek penelitiannya.

1.3 Rumusan Masalah

Dari uraian latar belakang tersebut, maka peneliti menentukan rumusan masalah yang dibahas dalam penelitian ini, sebagai berikut:

1. *Bagaimanakah Mekanisme Penerapan Strategi Anti Fraud pada PT Bank BPD DIY ?*

Tujuan dari pertanyaan ini adalah untuk mengetahui bagaimana praktik Unit Anti *Fraud* pada PT Bank BPD DIY. Seperti apa mekanisme penerapannya sehingga diperoleh gambaran mengenai penerapan strategi anti *fraud*.

2. *Bagaimanakah Pengembangan SDM Unit Anti Fraud Bank PT BPD DIY dalam mendeteksi dan mencegah adanya tindakan fraud ?*

Tujuan dari pertanyaan ini adalah untuk mengetahui upaya pengembangan SDM unit anti *fraud*. Seperti apa pelatihan, penugasan dan pola rekrutmen SDM dalam proses peningkatan kinerja mendeteksi dan mencegah tindakan *fraud* sejak unit anti *fraud* dibentuk dan melakukan tugasnya selama ini. Seperti apa hubungan timbal balik antar SDM yang terjalin dengan Manajemen Risiko dan Kepatuhan untuk meningkatkan kualitas pendeteksian dan pencegahan *fraud* dalam meminimalkan tindakan *fraud*.

3. *Kendala Apa yang Dihadapi oleh Unit Anti Fraud PT Bank BPD DIY dalam Meminimalkan Fraud?*

Tujuan dari pertanyaan ini adalah untuk mengkaji kendala yang dihadapi SDM unit anti *fraud* pada proses pendeteksian dan pencegahan *fraud* dalam upaya meminimalkan *fraud* sejak unit anti *fraud* dibentuk dan melakukan tugasnya selama ini, secara independen maupun dengan hubungan timbal balik antar SDM dengan SDM Manajemen Risiko dan Kepatuhan.

4. *Bagaimana Peningkatan yang Dapat Dilakukan oleh Unit Anti Fraud PT Bank BPD DIY dalam Melakukan Tugasnya Meminimalkan Fraud?*

Tujuan dari pertanyaan ini adalah untuk memberikan rekomendasi peningkatan serta perbaikan kinerja SDM maupun perbaikan sarana dan prasarana yang dapat dilakukan dari analisis kendala yang dihadapi SDM sejak unit anti *fraud* dibentuk.

1.4 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang dibahas, penelitian ini memiliki tujuan sebagai berikut:

1. Untuk mengetahui mekanisme penerapan strategi anti *fraud* pada PT Bank BPD DIY.
2. Untuk mengetahui pengembangan SDM oleh unit anti *fraud* melalui pelatihan, penugasan dan pola rekrutmen SDM dalam proses meminimalkan tindakan *fraud* pada PT Bank BPD DIY sejak unit anti *fraud* dibentuk, serta mengetahui hubungan timbal balik antar SDM yang terjalin dengan SDM Manajemen Risiko dan Kepatuhan dalam proses strategi pengembangan SDM untuk meningkatkan kualitas pendeteksian dan pencegahan *fraud*.
3. Untuk menganalisis kendala yang dihadapi SDM unit anti *fraud* dalam proses pendeteksian dan pencegahan *fraud* untuk meminimalkan *fraud* pada PT Bank BPD DIY sejak unit anti *fraud* dibentuk, maupun

selama terjalin hubungan timbal balik antar SDM dengan Manajemen Risiko dan Kepatuhan.

4. Untuk memberikan rekomendasi peningkatan serta perbaikan kinerja SDM maupun perbaikan sarana dan prasarana yang dapat dilakukan oleh unit anti *fraud* PT Bank BPD DIY agar proses meminimalkan *fraud* dapat terus meningkat sejak unit anti *fraud* dibentuk.

1.5 Fokus Penelitian

Dalam melaksanakan penelitian ini, agar tercapai hasil sesuai tujuan penelitian, maka peneliti menentukan fokus penelitian sebagai berikut :

1. Tempat Penelitian : Kantor Pusat PT Bank BPD DIY, Jalan Tentara Pelajar No 7, Yogyakarta.
Telp (0274) 561614
2. Aspek Penelitian : Mekanisme prosedur penerapan strategi anti *fraud* terkait pendeteksian dan pencegahan *fraud* yang dilakukan SDM Unit Anti *Fraud* PT Bank BPD DIY dalam upaya meminimalkan *Fraud*.
3. Waktu Penelitian : 8 Maret 2018 – 15 April 2018
4. Objek Penelitian : Pihak yang bertanggung jawab dalam prosedur penerapan strategi anti *fraud* yaitu Kepala beserta Staff Unit Anti *Fraud*, dan Kepala beserta Staff Divisi Manajemen Risiko dan Kepatuhan PT Bank BPD DIY.

1.6 Manfaat Penelitian

Melalui penelitian ini, diharapkan dapat memberikan manfaat kepada pihak – pihak terkait, antara lain :

1. Bagi peneliti

Penelitian ini diharapkan mampu memberikan pemahaman lebih mendalam serta wawasan baru mengenai mekanisme Unit Anti *Fraud* dalam mendeteksi dan mencegah *fraud* untuk meminimalkan adanya *fraud* pada industri perbankan.

2. Bagi PT Bank BPD DIY

Hasil penelitian ini diharapkan dapat dijadikan bahan pertimbangan untuk membantu mengatasi serta memperbaiki kendala yang ada dalam prosedur pendeteksian dan pencegahan *fraud* dan dapat menjadi masukan untuk meningkatkan strategi anti *fraud* pada PT Bank BPD DIY agar dapat meminimalkan *fraud* untuk jangka waktu kedepan.

3. Bagi pihak lain

Diharapkan hasil dari penelitian ini dapat memberikan kontribusi dalam pengembangan teori dan dapat menjadi referensi untuk penelitian selanjutnya dalam bidang Akuntansi, khususnya dalam bidang Audit. Serta dapat menambah wawasan mengenai kinerja Unit Anti *Fraud* dalam industri perbankan.

1.7 Sistematika Penulisan

Sistematika penulisan pada penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN

Berisi latar belakang tentang penelitian ini. Dari latar belakang tersebut lalu dirumuskan masalah. Selanjutnya

dibahas mengenai tujuan penelitian, manfaat penelitian dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Dalam bab ini berisikan teori-teori yang digunakan sebagai landasan penelitian. Teori ini menjawab permasalahan penelitian yang ada. Bab ini juga membahas penelitian terdahulu yang relevan dengan penelitian ini, kerangka pemikiran dari penelitian ini serta membantu peneliti dalam melakukan penelitian di lapangan.

BAB III METODE PENELITIAN

Dalam bab ini dijabarkan tentang rencana kegiatan yang digunakan dalam penelitian ini. Beberapa hal yang dijelaskan pada bab ini adalah tentang jenis penelitian, fokus penelitian, sistematika penelitian, sumber dan jenis data, pemilihan responden, objek penelitian, teknik pengumpulan data, teknik pengujian keabsahan data dan teknik analisis data.

BAB IV HASIL DAN PEMBAHASAN

Berisikan hasil analisis penelitian yang telah dilakukan. Hasil penelitian tersebut disusun berdasarkan rumusan yang telah dibuat sebelumnya.

BAB V PENUTUP

Dalam bab ini berisikan kesimpulan penelitian, keterbatasan penelitian dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

LAMPIRAN

BAB II

KAJIAN PUSTAKA

2.1 Pengenalan Bab

Bab ini akan membahas seluruh teori yang mendukung dan berkaitan dalam pelaksanaan penelitian yang dilakukan oleh peneliti. Bagian pertama merupakan penjelasan mengenai pedoman seseorang melakukan *fraud*, jenis – jenis *fraud* gambaran umum *fraud* yang terjadi di Indonesia serta dilengkapi dengan analisis *fraud triangle* dan *fraud element triangle*. Bagian kedua akan membahas mengenai strategi anti *fraud* yang dikeluarkan oleh Bank Indonesia, baik latar belakang dikeluarkannya surat edaran maupun pedoman yang dapat diberlakukan oleh setiap bank. Bagian ketiga akan ditekankan untuk membahas proses pencegahan dan pendeteksian *fraud*. Bagian akhir untuk mendukung penelitian ini, penulis menganalisis penelitian terdahulu yang dapat dijadikan sumber acuan temuan penelitian penulis.

2.2 Landasan Teori

2.2.1 Fraud

2.2.1.1 Pengertian *Fraud*

Ruankaew (2016) mengatakan kecurangan atau *fraud* merupakan faktor yang melemahkan yang mempengaruhi pertumbuhan bisnis dan terus menjadi masalah besar bagi banyak

organisasi. Hal ini termasuk suap, menggelapkan uang dari perusahaan, dan mencuri produk.

Menurut *ACFE* (2016) *fraud* bertujuan tertentu dan melanggar hukum yang dilakukan oleh orang-orang dari luar maupun dalam suatu organisasi untuk secara langsung maupun tidak langsung memberikan keuntungan pribadi bahkan kelompok serta merugikan orang lain dengan memberikan laporan yang keliru bahkan memanipulasi laporan kepada pihak lain.

Menurut *Albrecht et al.* (2006) dari beragam jenis kecurangan, kecurangan dapat dikelompokkan dalam dua kelompok utama, yakni kecurangan yang dilakukan terhadap organisasi dan kecurangan yang dilakukan atas nama organisasi. Kecurangan yang dilakukan terhadap organisasi contohnya adalah kecurangan yang dilakukan oleh pegawai, pemasok, pelanggan dan manajemen. Untuk kecurangan yang dilakukan atas nama organisasi contohnya adalah kecurangan investasi.

Menurut *Kimani* (2011) *fraud* atau kecurangan dapat dikategorikan dalam dua kelompok besar, yaitu kecurangan internal dan eksternal. Kecurangan internal dilakukan oleh karyawan dan manajer suatu organisasi, bertindak sendiri atau berkelompok atau melalui kolusi dengan pihak luar. Kecurangan eksternal dilakukan oleh pihak ketiga organisasi seperti pemasok, pesaing, mitra dan pelanggan (nasabah). Pelanggar lainnya

termasuk calon pelanggan, pemerintah dan organisasi kriminal. Kecurangan eksternal dilakukan oleh orang-orang di luar organisasi. Pelakunya bisa bekerja secara independen atau dapat berkolusi dengan staf untuk menipu Bank.

2.2.1.2 Klasifikasi *Fraud*

1. *Internal Fraud*

Kecurangan internal dilakukan oleh karyawan dan manajer suatu organisasi, hal ini bisa dilakukan dengan bertindak sendiri atau berkelompok atau melalui kolusi dengan pihak luar. Statistik Bank Dunia menunjukkan bahwa frekuensi kecurangan internal meningkat drastis dan sejauh ini telah menyebabkan kerugian paling signifikan bagi bank. Ini karena beberapa karyawan dan manajer yang tidak jujur telah menemukan cara untuk mengganti sistem dan atau berkolusi dengan pihak luar untuk menipu bank. Menurut unit kecurangan Bank Dunia, kecurangan manajemen terjadi lebih jarang, namun merupakan kerugian finansial terbesar. Kecurangan manajemen bisa sangat sulit dideteksi karena manajer memiliki akses sebagian besar informasi dan sistem dan memiliki kekuatan untuk menyamarkan tindakan mereka karena mereka tahu bahwa keputusan mereka mungkin tidak perlu dipertanyakan oleh orang lain. Mereka juga dapat mengintimidasi karyawan junior untuk melakukan kecurangan atas nama mereka. Penelitian menunjukkan bahwa kecurangan

internal dilakukan oleh karyawan dan manajemen dan menyumbang 50-80% kecurangan yang dilakukan dalam organisasi (Kimani, 2011).

Hasil penelitian dari Kimani (2011), menunjukkan secara lebih spesifik *internal fraud* yang terjadi dengan kerugian atau dampak yang terjadi terhadap Bank. Skala 1- 5 menunjukkan bahwa skala 1 adalah nilai yang terendah dan skala 5 adalah nilai yang tertinggi. Untuk dampak terhadap bank ditentukan dengan mengalikan luasnya risiko dengan peluang terjadinya risiko.

Tabel 2.1
Risiko *Internal Fraud*

Jenis <i>Fraud</i> Internal	Luasnya Risiko	Peluang Terjadinya	Dampak Terhadap Bank
<i>Cheque Fraud and Fund Transfers</i>	4	2	8
<i>Bribery and Conflicts of Interest</i>	4	2	8
<i>Travel and Entertainment (T&E) Fraud</i>	3	2	6
<i>Theft of Confidential Information</i>	5	1	5
<i>Misuse of Organization Owned Assets</i>	1	3	3

Sumber : Kimani (2011)

a. *Cheque Fraud and Fund Transfers* atau Kecurangan Cek dan Transfer Dana

Beberapa karyawan memilih untuk mencuri cek yang telah ditandatangani dan sudah disiapkan untuk dikirim dan mengubah rincian cek, baik secara manual maupun elektronik. Cek yang berubah kemudian diuangkan oleh karyawan sendiri atau diberikan kepada orang luar bank untuk mencairkannya. Selain itu, karyawan melakukan cara menyembunyikan cek palsu di antara tumpukan cek asli. Penanggung jawab otorisasi cek biasanya cukup sibuk dan mungkin tidak mempunyai waktu untuk memeriksa rincian masing-masing cek secara menyeluruh. Orang tersebut kemudian menandatangani cek dan memberi wewenang untuk segera dikirim. Penipu mengakali penandatanganan dengan memanfaatkan ketidakpedulian penanggung jawab terhadap rincian cek. Beberapa karyawan yang tidak jujur juga melakukan transfer sejumlah uang yang relatif besar dari rekening yang tidak aktif yang berisi sejumlah besar uang ke akun palsu yang dibuat sebelumnya dengan menggunakan dokumen palsu. Mereka memilih untuk mentransfer dana dari rekening yang tidak aktif bertransaksi karena mereka tahu akan memakan waktu sebelum orang yang memiliki akun tersebut mengetahui bahwa ada kejanggalan pada

rekeningnya. Bank mencatat bahwa frekuensi jenis *fraud* yang terjadi tidak begitu tinggi, namun dampaknya terhadap Bank sangat tinggi karena jumlah uang yang sangat besar telah hilang melalui tindakan *fraud* tersebut. Dengan demikian, jenis kecurangan ini perlu segera ditelusuri dan cara untuk menguranginya.

b. *Bribery and Conflicts of Interest* atau Penyuapan dan Benturan Kepentingan

Penyuapan adalah bentuk korupsi dengan menerima hadiah atau sogokan dari pemasok, pelanggan dan rekan bisnis yang potensial. Penyuapan juga bisa berupa penerimaan sogokan dari pejabat pemerintah untuk 'menyelesaikan sesuatu'. Jenis kecurangan ini kebanyakan dilakukan oleh para manajer karena mereka berada dalam posisi yang kuat dan bertanggung jawab dalam membuat keputusan terhadap pemasok dan rekan bisnis yang potensial. Konflik kepentingan muncul ketika seorang karyawan atau manajer juga memiliki kepentingan keuangan namun secara rahasia berbisnis dengan organisasi tempatnya bekerja, seperti konstruksi perusahaan, tempat penyewaan peralatan perusahaan, jasa penggajian, atau vendor luar lainnya. Konflik juga bisa terjadi di mana rekan manajer menerima perlakuan khusus dalam penawaran kontrak. Konsekuensinya

atas hal ini berupa Bank tidak hanya kehilangan banyak uang dan aset tapi juga reputasinya rusak parah karena kasus *fraud* semacam itu biasanya sampai ke media.

c. *Travel and Entertainment (T&E) Fraud* atau Liburan dan Hiburan

Jenis *fraud* ini biasanya sering dilakukan oleh karyawan karena melibatkan akun pengeluaran. Sebenarnya, *fraud* ini dikategorikan sebagai bentuk *fraud* internal paling memakan biaya di banyak organisasi. melihat bahwa *fraud* ini sangat mudah lolos walaupun ada tindakan pencegahan yang efektif sudah dilakukan. Catatan bank menunjukkan bahwa beberapa karyawan memalsukan klaim biaya seperti ongkos atas pemakaian mobil agar mendapat kompensasi lebih dari satu kali. Pada dasarnya, hanya manajer dan beberapa karyawan di Bank yang memiliki hak untuk mengajukan biaya, jenis *fraud* ini tidak terjadi begitu sering.

d. *Theft of Confidential Information* atau Pencurian Informasi Rahasia

Beberapa karyawan memiliki akses terhadap informasi, sistem dan kontrol perusahaan serta dapat memanfaatkan kelemahan kontrol komputer dalam organisasi untuk mengakses dan mencuri informasi rahasia. Dampaknya, pelanggan dan pemegang saham mungkin kehilangan

kepercayaan pada kemampuan manajemen untuk mengamankan informasi rahasia organisasi. Jenis kecurangan ini sangat umum terjadi di Kenya dimana karyawan Bank berkolusi dengan pihak luar untuk merampok Bank saat transportasi uang (Kimani, 2011). Karyawan bank bertindak dengan membocorkan informasi kepada *gangster* bersenjata pada waktu, tempat dan rute saat mobil keamanan yang mengirimkan uang ke tujuan tertentu akan digunakan. Para *gangster* bersenjata kemudian membajak mobil keamanan dan membawa semua uang didalam mobil transportasi uang. Beberapa karyawan juga mampu menggunakan sistem komputer untuk mencuri uang melalui transfer dana dengan memanipulasi proses terkomputerisasi untuk mendapatkan akses ke informasi rahasia. Pengumpulan informasi dapat dilakukan melalui *hacking* ke dalam sistem komputer dan mendownload informasi penting seperti nomor rekening nasabah dan rincian lainnya, dimana karyawan yang melakukannya kemampuan komputer yang luar biasa untuk masuk ke dalam sistem komputer Bank.

e. *Misuse of Organization Owned Assets* atau Penyalahgunaan Aset Organisasi

Jenis kecurangan ini seperti menyalahgunakan mobil, telepon, komputer, alat tulis dan perangkat lunak perusahaan.

Meskipun jenis *fraud* ini dianggap kecil karena biaya organisasi sedikit dan tidak ada uang tunai, hal ini telah menjadi kejadian biasa di bank. Mayoritas karyawan di Bank diketahui menggunakan sumber daya perusahaan untuk keuntungan pribadi.

2. *External Fraud*

Kecurangan eksternal dilakukan oleh pihak ketiga organisasi seperti pemasok, pesaing, mitra dan pelanggan (nasabah). Pelanggar lainnya termasuk calon pelanggan, pemerintah dan organisasi kriminal. Kecurangan eksternal dilakukan oleh orang-orang di luar organisasi. Pelakunya bisa bekerja secara independen atau dapat berkolusi dengan staf untuk menipu Bank (Kimani, 2011).

Hasil penelitian dari Kimani (2011) menunjukkan berbagai jenis kecurangan eksternal yang ditemukan oleh bank dengan kerugian atau dampak yang terjadi terhadap Bank. Skala 1- 5 menunjukkan bahwa skala 1 adalah nilai yang terendah dan skala 5 adalah nilai yang tertinggi. Untuk dampak terhadap bank ditentukan dengan mengalikan luasnya risiko dengan peluang terjadinya risiko.

Tabel 2.2
Risiko *External Fraud*

Jenis <i>Fraud</i> Eksternal	Luasnya Risiko	Peluang Terjadinya	Dampak Terhadap Bank
<i>Money Laundering</i>	4	2	8
<i>Identity Theft and Use of Stolen or Lost Documents</i>	2	3	6
<i>Use of Counterfeit Cards</i>	2	3	6
<i>Theft of Confidential Information</i>	5	1	5

Sumber : Kimani (2011)

a. *Money Laundering* atau Pencucian Uang

Pencucian uang adalah sarana yang digunakan untuk mengkonversi dana yang berasal dari kegiatan ilegal seperti penjualan obat ke dalam penggunaan finansial yang melibatkan instrumen hukum, misalnya deposito bank, investasi saham atau *real estate* (Grosse, 2001). *Barclays Bank of Kenya* contohnya, mengharuskan mereka berurusan dengan pencucian uang dari narkoba, korupsi, aktivitas bajak laut, dan sebagainya. Sayangnya bagi bank, sangat sulit untuk

menentukan dari mana uang tersebut berasal karena gerombolan penjahat sangat cerdas dan telah menemukan cara untuk menyamarkan kesalahan mereka. Kemungkinan bank tidak sadar bertransaksi dengan kelompok kriminal. Jika transaksi semacam itu menjadi pusat perhatian tindak kejahatan di bank, Bank Dunia dapat menghadapi kerusakan parah pada reputasi dan kepercayaan nasabahnya.

Menurut Albrecht *et al.* (2006) Departemen Kehakiman Amerika Serikat mendefinisikan pencucian uang sebagai proses untuk menyembunyikan keberadaan sumber uang ilegal dan kemudian menyamarkan pendapatan tersebut agar tampak legal. Aktivitas ilegal termasuk perdagangan narkoba dan membawa uang ilegal masuk dari negara lain untuk mendanai terorisme. Biasanya pelaku adalah individu dari pihak yang melakukan kegiatan bisnis yang berbasis di luar negeri berupa jaringan atau mafia, dan juga tokoh politisi dan pejabat publik yang memiliki reputasi baik. Skema pencucian uang meliputi tiga langkah, penempatan, pelapisan dan integrasi.

Dalam penelitian Isa *et al.* (2015) pencucian uang adalah salah satu risiko besar di institusi perbankan. Lembaga perbankan membayar denda yang besar karena gagal menilai risiko pencucian uang dengan benar, seperti Bank HSBC

yang berbasis di London yang telah didenda oleh regulator Amerika Serikat dengan harga hampir USD 2 miliar karena telah gagal menghentikan perdagangan obat terlarang dari Jepang yang menggunakan sistem perbankannya untuk mencuci uang (McLaughlin and Pavelka, 2009). Contoh lain yang melibatkan *Standard Chartered Bank* yang didenda sebesar USD \$ 340 juta kepada regulator Amerika Serikat untuk menyelesaikan tuduhan bahwa bank tersebut melanggar undang-undang pencucian uang Amerika Serikat dalam menangani transaksi untuk pelanggan Iran (McLaughlin and Pavelka, 2009).

b. *Identity Theft and Use of Stolen or Lost Documents* atau Pencurian Identitas dan Penggunaan Dokumen yang Dicuri atau Hilang

Pelaku mendapatkan informasi identitas pribadi korban berupa nama, alamat, tanggal lahir, nomor jaminan sosial, kartu identitas, informasi kredit, dan rincian penting lainnya untuk meniru dan menipu korban. Menurut Albrecht *et al.* (2006) contoh teknik pemerolehan informasi, pelaku mengumpulkan informasi seperti mencari di antara tumpukan sampah, mencari rumah atau komputer korban, mencuri surat, membobol mobil atau rumah, memindai informasi kartu kredit dan *phising*. Konsekuensi yang paling merugikan

dari adanya pencurian identitas bukanlah kerugian uang, namun kerugian kredit, reputasi dan informasi yang salah dan sulit untuk diperbaiki.

Kimani (2011) menjelaskan *Barclays Bank of Kenya* terus menjadi korban *fraud* melalui pencurian identitas. Mereka bisa mendapatkannya dari surat, internet, mengambil dokumen dari tempat sampah, mencuri dokumen dari meja kantor, dan seterusnya. Begitu penipu memiliki dokumen yang diperlukan, maka sangat mudah baginya untuk mempresentasikannya ke bank baik ke rekening terbuka, mendapatkan fasilitas kredit atau untuk menarik uang dari rekening korban. Sangat banyak insiden penipu yang menggunakan dokumen dan kartu curian atau kartu hilang yang disaksikan oleh bank setiap tahunnya, karena hilangnya dokumen akan disadari oleh bank dalam waktu yang lama. Hal ini menjadi sangat mudah bagi penipu untuk menggunakan dokumen yang dicuri atau hilang tanpa terdeteksi. Jenis kecurangan ini bisa relatif merugikan jika tidak terdeteksi dengan cepat. Namun, bank mencatat bahwa sejak menarik sejumlah besar uang pada suatu waktu memerlukan beberapa prosedur yang ketat, dan seseorang hanya dapat menarik sejumlah uang tertentu melalui ATM dalam sehari, banyak penipu memilih untuk menarik dan

menghabiskan jumlah uang yang relatif lebih rendah untuk menghindari deteksi cepat.

Setelah pelaku kecurangan mengakses informasi pribadi, mereka menggunakan informasi tersebut untuk kepentingan finansialnya (Albrecht *et al.*, 2006). Beberapa diantaranya adalah :

- 1) Membeli barang besar seperti komputer atau televisi
- 2) Melakukan pinjaman untuk membeli mobil, rumah dan pinjaman lainnya
- 3) Menggunakan cek atau kartu debit fiktif
- 4) Membuka akun bank baru
- 5) Mendaftarkan kebangkrutan atas nama korban
- 6) Melaporkan nama korban ke polisi sebagai pengganti nama mereka
- 7) Membuka akun kredit baru
- 8) Mengubah alamat surat korban.

c. *Use of Counterfeit Cards* atau Penggunaan Kartu Palsu

Kartu debit dan kartu kredit terbuat dari plastik dan dilengkapi dengan informasi seperti nomor kartu, tanggal kadaluwarsa dan nama pemegang kartu. Data dapat dikodekan dan direkam pada satu garis magnetik yang diaplikasikan pada sisi belakang kartu atau juga dapat disimpan dalam *chip* dimana informasi tersimpan dalam

memori permanen *chip mikroprosesor* yang terpasang pada kartu. Penyebab kerugian terbesar dengan penggunaan teknologi strip magnetik adalah peningkatan penyalahgunaan yang dilaporkan di seluruh dunia. Pelaku memiliki wawasan yang luas tentang detail desain kartu strip magnetik, yang membantu mereka mengidentifikasi kelemahan keamanan yang dapat menyebabkan kecurangan.

Sudah umum di industri restoran agar pelayan dapat mengakses informasi pemegang kartu dengan mencatat secara cepat data keuangan yang tertera pada kartu tersebut. Ketika seorang pelayan membawa kartu korban untuk melakukan pembayaran di kasir, dia dapat dengan cepat menuliskan informasi di kartu dan menggunakannya untuk menghasilkan kartu palsu atas nama korban. Hal ini dimungkinkan untuk dilakukan dengan kartu strip magnetik. Terminal ATM yang berada di bawah kendali pelaku digunakan untuk membaca secara tidak sah data keuangan yang dikodekan pada pita magnetik kartu tersebut. Ini adalah perangkat genggam kecil yang ukuran sebesar kotak korek api dan juga dapat diletakkan ke terminal ATM dan dapat membaca garis magnetik kartu dalam beberapa detik. Perangkat ini dapat menyimpan informasi hingga 50 kartu sekaligus, yang kemudian dipindahkan ke departemen

logistik dari sebuah organisasi kriminal dan digunakan untuk membuat kartu strip magnetik palsu.

Pencurian lainnya adalah melalui apa yang disebut *card skimming*. Ini dilakukan melalui pengambilan data dari strip magnetik di bagian belakang kartu ATM. *Skimmers* kecil sering dipasang di dekat pembaca kartu ATM yang terpasang di pabrik, dan mereka dapat menangkap informasi seperti nomor rekening, saldo, dan nomor PIN dari 200 kartu yang digunakan. Banyak bank di negara berkembang mengeluarkan pelanggan mereka dengan kartu strip magnetik. Alasan mengapa kartu strip magnetik masih banyak digunakan adalah karena mayoritas bank belum memasang teknologi *chip* karena tingginya biaya pemasangan dan perawatannya. Namun, kurangnya prosedur verifikasi pemegang kartu juga biasanya memfasilitasi kemungkinan terjadinya kecurangan (Kimani, 2011).

d. *Theft of Confidential Information* atau Pencurian Informasi Rahasia

Kecurangan jenis ini terjadi saat penipu meng-*hack* ke sistem komputer perusahaan dan mencuri informasi rahasia. Mereka kemudian dapat menggunakan informasi ini untuk mencuri pelanggan atau identitas vendor atau untuk memeras organisasi. Padahal jenis kecurangan ini tidak terlalu umum,

meski sudah disaksikan beberapa kesempatan di mana mantan pegawai atau geng kriminal telah meretas ke sistem komputer Bank Dunia dan informasi vital yang diunduh seperti informasi pelanggan, nomor kartu dan sebagainya. Sangat sulit untuk memperkirakan nilai moneter jenis ini *fraud*. Namun, jika terjadi, biaya bank sangat tinggi karena Bank berisiko kehilangan informasi yang berharga untuk para pesaingnya, penjahat dan masyarakat luas.

2.2.1.3 Perkembangan *Fraud* di Perbankan Indonesia

Sejak pengawasan perbankan resmi diambil alih oleh OJK (Otoritas Jasa Keuangan) dari Bank Indonesia, maka laporan tahunan atas perbankan di Indonesia dibuat oleh OJK. *Publish* laporan tahunan perbankan terbaru oleh OJK adalah pada periode 1 Januari 2015 – 31 Desember 2015. Selama tahun 2015, menurut OJK (2015) tercatat sebesar 65,7 % atau 67 bank yang tergolong memiliki risiko operasional *moderate*, risiko tersebut tergolong cukup tinggi di masa mendatang. Risiko tersebut seperti ; ketidaksesuaian pelaksanaan operasional perusahaan dengan ketentuan internal, kelemahan *dual control* yang menyebabkan *fraud* di beberapa kantor cabang, belum sepenuhnya dilaksanakan mitigasi risiko, terdapat rangkap jabatan berkaitan dengan belum tercapainya kebutuhan SDM di beberapa kantor cabang, serta masih adanya permasalahan Teknologi Informasi.

Tabel 2.3**R**

Jenis Bank	Hasil Penilaian					Jumlah Bank
	Low	Low to Moderate	Moderate	Moderate to High	High	
Perseroi	0	1	3	0	0	4
BPD	0	0	16	3	0	19
Campuran	0	7	5	0	0	12
BUSD	0	9	24	0	0	33
BUSND	0	8	5	0	0	13
KCBA	0	3	7	1	0	10
BUS	0	3	7	4	0	11
TOTAL	0	31	67	8	0	102

perasional Bank Umum Posisi Desember 2015

Sumber : Laporan Tahunan Perbankan OJK (2015)

Berdasarkan kelompok bank, sebagian besar *fraud* terjadi pada kelompok Bank Umum Swasta Nasional Devisa (BUSD) yaitu sebanyak 33 bank, lalu pada urutan kedua diikuti oleh kelompok Bank Pembangunan Daerah (BPD) yaitu sebanyak 19 bank dan urutan ketiga oleh kelompok Bank Umum Swasta Nasional Non Devisa (BUSND) sebanyak 13 bank. Kemudian urutan selanjutnya ditempati oleh Bank Campuran sebanyak 12 bank, lalu selanjutnya ditempati oleh Bank Umum Syariah (BUS) sebanyak 11 bank, lalu selanjutnya ditempati oleh Kantor Cabang Bank Asing (KCBA) sebanyak 10 bank, lalu posisi terakhir ditempati oleh Bank Persero sebanyak 4 bank.

Melihat risiko perbankan yang masih cukup tinggi, OJK meminta kepada setiap bank untuk meningkatkan kualitas manajemen risiko dan Sistem Pengendalian Internal (SPI) serta memperhatikan prinsip kehati – hatian. Dalam rangka menguatkan SPI, bank wajib memiliki strategi anti *fraud* yang efektif dan disampaikan kepada OJK setiap semester.

Berdasarkan laporan strategi anti *fraud* yang disampaikan bank terakhir pada semester II tahun 2015, diketahui terdapat beberapa perbuatan *fraud* yang dilakukan oleh *internal* bank secara sendiri sebanyak 331 kasus maupun bersama – sama dengan pihak eksternal yaitu petugas *appraisal*. sebanyak 59 kasus. Pelaku *fraud* antara lain:

1. *Teller*
2. Pejabat Eksekutif
3. Pegawai yang Menangani Kredit

Untuk meminimalkan terjadinya *fraud* maka bank hendaknya tidak hanya melakukan upaya pencegahan namun juga mendeteksi, melakukan investigasi serta memperbaiki sistem dalam mengendalikan fraud.

Tabel 2.4
Jenis dan Kerugian akibat *Fraud*

Jenis Fraud	Jumlah Kerugian
Kecurangan	Rp 97.938.511.000
Manipulasi	Rp 103.148.651.000
Pemberian Bunga Deposito	Rp -
BI Checking	Rp -
Pelanggaran Terkait kredit	Rp 464.127.578.094
Pemalsuan	Rp 26.980.557.074
Penyalahgunaan Kredit	Rp 1.680.138.267
Pemotongan atau Permintaan Uang Insentif Milik Staf Lain	Rp -
Penarikan Tunai Melalui ATM pada Jaringan MEPS - Master Card	Rp 2.900.000.000
Pencurian Informasi Melalui Hacking	Rp 3.295.945.000
Penyalahgunaan Dana Nasabah	Rp 154.176.500.000
Penyalahgunaan Kewenangan	Rp 6.834.896.222.000
Penggelapan	Rp 6.220.322.782
Penggunaan ATM dari PIN	Rp 6.251.511.584
TOTAL KERUGIAN	Rp 7.701.615.936.801

Sumber : Laporan Tahunan Perbankan OJK (2015)

Berdasarkan tabel 2.4 dapat disimpulkan bahwa golongan *fraud* yang menghasilkan kerugian terbanyak yaitu pelanggaran terkait kredit sebesar 43 %, manipulasi sebesar 19,6% dan pemalsuan sebesar 18,6 %.

OJK wajib melakukan pemeriksaan umum setahun sekali secara berkala kepada setiap bank. Selama periode laporan Triwulan I tahun 2017, OJK melakukan pemeriksaan terhadap 522 bank dengan 518 kantor pusat dan 116 kantor cabang.

Dengan 511 bank yang terdiri dari kantor BPR (Bank Perkreditan Rakyat) dan BPRS (Bank Perkreditan Rakyat Syariah), serta 41 adalah kantor BUK (Bank Umum Konvensional) dan BUS (Bank Umum Syariah) (OJK, 2017a). Selain pemeriksaan umum juga dilakukan pemeriksaan khusus secara insidental. Selama periode laporan Triwulan I Tahun 2017, OJK melakukan pemeriksaan khusus pada 96 bank terhadap BUK dan BPR.

Tabel 2.5

Subjek Pemeriksaan	Triwulan I-2017
Setoran Modal	33
Aktivitas Operasional	43
<i>Joint Audit</i>	3
GCG	4
Teknologi dan Informasi	1
<i>Fraud</i>	2
Kesiapan Rencana Bank Devisa	3
Lainnya	7
TOTAL	96

Pemeriksaan Khusus Bank Triwulan I Tahun 2017

Sumber : Laporan Triwulanan I OJK (2017)

Menurut Laporan Triwulanan I OJK (2017a), OJK menindaklanjuti 15 Penyimpangan Ketentuan Perbankan (PKP) yang diduga *fraud* pada 7 kantor bank yang merupakan *carry over* dari periode sebelumnya dan OJK melakukan investigasi pada 6 PKP yang terjadi di 2 kantor Bank Umum dan 1 kantor BPR. OJK juga menangani 75% dugaan tindak pidana kredit dan 25% pengadaan aset. Berikut adalah jumlah pelaku yang diduga melakukan Tipibank.

Tabel 2.6

Pelaku Fraud yang Diduga Tipibank	Jumlah
Direksi	6
Pejabat Eksekutif	4
Karyawan	4
TOTAL	14

Pelaku *Fraud* yang Diduga Tipibank Triwulan I Tahun 2017

Sumber : Laporan Triwulanan I OJK (2017)

Selama periode laporan Triwulan II tahun 2017, OJK melakukan pemeriksaan umum terhadap 1.007 bank dengan 948

kantor BPR dan BPRS serta 59 adalah kantor BUK dan UUS, sebanyak 991 adalah kantor pusat dan 230 adalah kantor cabang.

Selain pemeriksaan umum juga dilakukan pemeriksaan khusus secara insidental. Selama periode laporan Triwulan II Tahun 2017, OJK melakukan pemeriksaan khusus pada 191 bank terhadap BUK dan BPR.

Tabel 2.7
Pemeriksaan Khusus Bank Triwulan II Tahun 2017

Subjek Pemeriksaan	Triwulan II-2017
Setoran Modal	67
Aktivitas Operasional	88
<i>Joint Audit</i>	3
GCG	1
Teknologi dan Informasi	5
<i>Fraud</i>	8
Penetapan Pencabutan	1
Lainnya	18
TOTAL	191

Sumber : Laporan Triwulanan II OJK (2017)

Menurut Laporan Triwulanan II OJK (2017b), OJK menindaklanjuti 11 Penyimpangan Ketentuan Perbankan (PKP) yang diduga *fraud* dan OJK melakukan investigasi pada 3 PKP yang terjadi di kantor BPR.

Selama periode laporan Triwulan III tahun 2017, OJK melakukan pemeriksaan umum terhadap 2.101 bank dengan 1.532 kantor BPR dan BPRS serta 569 adalah kantor Bank Umum, sebanyak 1.618 adalah kantor pusat dan 483 adalah kantor cabang.

Selain pemeriksaan umum juga dilakukan pemeriksaan khusus secara insidental. Selama periode laporan Triwulan III Tahun 2017, OJK melakukan pemeriksaan khusus pada 302 bank terhadap Bank Umum.

Tabel 2.8
Pemeriksaan Khusus Bank Triwulan III Tahun 2017

Subjek Pemeriksaan	Triwulan III-2017
Setoran Modal	105
Aktivitas Operasional	132
<i>Joint Audit</i>	2
GCG	2
Teknologi dan Informasi	11
<i>Fraud</i>	19
Penetapan Pencabutan	1
Suku Bunga	-
Aktivitas Treasuri	-
Pemeriksaan Kesiapan Rencana Bank	-
Devisa	-
Lainnya	30
TOTAL	302

Sumber : Laporan Triwulanan III OJK (2017)

Menurut Laporan Triwulanan III OJK (2017c) OJK menindaklanjuti 12 Penyimpangan Ketentuan Perbankan (PKP) yang diduga *fraud* dan OJK melakukan investigasi pada 9 PKP yang terjadi di 5 kantor Bank.

Selama periode laporan Triwulan IV tahun 2017, OJK melakukan pemeriksaan umum terhadap 2.498 bank dengan 1.972 kantor BPR dan BPRS serta 526 adalah kantor Bank Umum, sebanyak 2.007 adalah kantor pusat dan 491 adalah kantor cabang.

Selain pemeriksaan umum juga dilakukan pemeriksaan khusus secara insidental. Selama periode laporan Triwulan IV Tahun 2017, OJK melakukan pemeriksaan khusus pada 488 bank terhadap Bank Umum.

Tabel 2.9
Pemeriksaan Khusus Bank Triwulan IV Tahun 2017

Subjek Pemeriksaan	Triwulan IV-2017
Setoran Modal	134
Aktivitas Operasional	230
<i>Joint Audit</i>	4
GCG	2
Teknologi dan Informasi	23
<i>Fraud</i>	28
Penetapan Pencabutan	2
Suku Bunga	-
Aktivitas Treasuri	1
Pemeriksaan Kesiapan Rencana Bank	-
Devisa	-
Lainnya	64
TOTAL	488

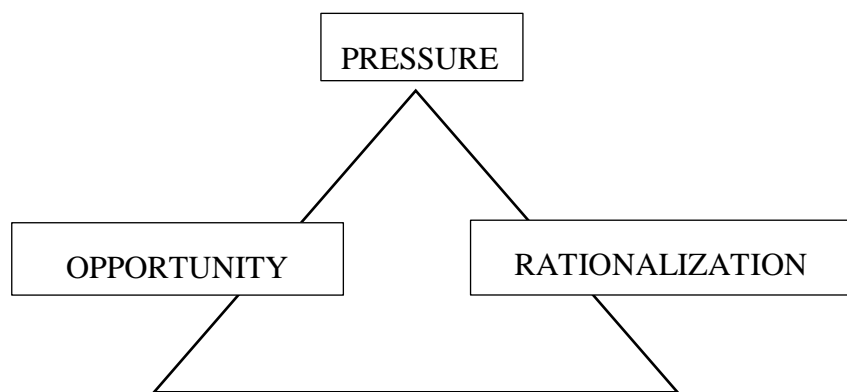
Sumber : Laporan Triwulanan IV OJK (2017)

Menurut Laporan Triwulanan IV OJK (2017d), OJK menindaklanjuti 11 Penyimpangan Ketentuan Perbankan (PKP) yang diduga *fraud* dan OJK melakukan investigasi pada 3 PKP yang terjadi di 1 kantor BPR.

2.2.1.4 *Fraud Triangle*

Teori *fraud triangle* merupakan suatu gagasan tentang penyebab terjadinya kecurangan yang dikemukakan oleh kriminolog Donald Cressey pada tahun 1953. Cressey menyatakan bahwa disetiap kecurangan yang dilakukan setiap orang terdapat tiga faktor yang mendorong dapat terwujudnya suatu tindak kecurangan. Dalam Cressey (1953), penelitian dilakukan dengan mewawancarai 250 pelaku kriminal dalam jangka waktu 5 bulan dan menghasilkan tiga faktor penyebab suatu kecurangan dapat terjadi. Ketiga faktor tersebut adalah Tekanan, Kesempatan, dan Rasionalisasi.

Gambar 2.1
Fraud Triangle



Sumber : Cressey (1953)

1. *Pressure* (Tekanan)

Sebagian besar pelaku kecurangan akan dipicu oleh tekanan yang dirasakan dan memotivasi pelaku melakukan kecurangan untuk kepentingan mereka sendiri. Tekanan yang dirasakan meliputi tuntutan perekonomian, gaya hidup, kebutuhan, pekerjaan dan tekanan lainnya berupa keuangan maupun non-keuangan. Dalam Buchholz (2012) berdasarkan SAS No.99, *pressure* dikategorikan kedalam empat kelompok, yaitu: (1) *financial stability*, kondisi dimana stabilitas keuangan perusahaan dipengaruhi keadaan ekonomi perusahaan, (2) *external pressure*, keadaan dimana manajemen perusahaan membutuhkan sumber pembiayaan dari pihak eksternal demi keberlangsungan entitasnya. Utang merupakan sumber pembiayaannya, (3) *personal financial need*, merupakan kondisi dimana para eksekutif mempengaruhi secara signifikan keuangan perusahaan sebagai pemilik saham dan jika terjadi kebutuhan keuangan pribadi, maka akan memberikan tekanan kepada para eksekutif untuk melakukan kecurangan, dan (4) *financial target*, yaitu target keuangan dari direksi yang harus dicapai manajemen dalam satu periode.

2. *Opportunity* (Kesempatan)

Peluang yang ada dalam organisasi memiliki dampak yang besar pada keputusan individu untuk melakukan *fraud*. Unsur

kesempatan yang paling mungkin untuk terjadi adalah ketika *fraud* memiliki kesempatan kecil untuk terdeteksi. Sesuai dengan Dalam Buchholz (2012) berdasarkan SAS No. 99, kesempatan meliputi: (1) *nature of industry*, atau operasi entitas yang memberikan kesempatan untuk terlibat dalam kecurangan pelaporan keuangan, dan (2) *ineffective monitoring*, atau pemantauan yang tidak efektif dari dewan komisaris, struktur organisasi yang tidak stabil, dan komponen pengendalian internal yang kurang efisien.

Pelaku kecurangan pasti pintar melihat kesempatan dan menemukan caranya sendiri serta yakin kecurangan yang dilakukan tidak terdeteksi oleh organisasi. Jika pelaku merupakan jajaran atas organisasi, mereka melihat kesempatan sesuai jabatannya bahwa merubah kebijakan atas pengendalian akan mempermudah kesempatan melakukan kecurangan serta dapat menyembunyikan tindakan kecurangan yang dilakukan, kecurangan ini termasuk penyalahgunaan posisi atau otoritas.

3. *Rationalization* (Rasionalisasi)

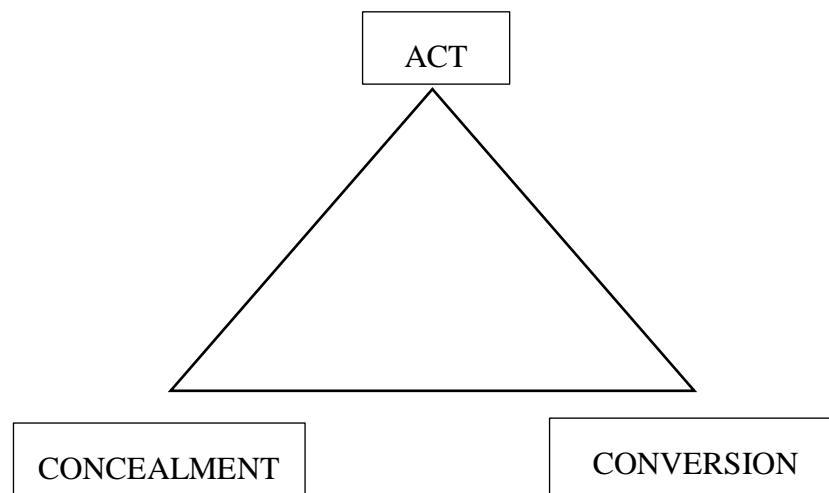
Rasionalisasi (*rationalization*) adalah sikap dimana pelaku *fraud* membenarkan tindakan yang mereka lakukan karena kuatnya tekanan yang dirasakan, sehingga pelaku tidak menghiraukan bahwa tindakan mereka tidak etis (Dorminey *et al.*, 2010). Dengan kata lain, rasionalisasi memungkinkan penipu

untuk melihat tindakan ilegal sebagai hal yang dapat diterima. Contohnya: “Saya hanya meminjam,” “Aku pantas mendapatkan bonus dan kenaikan gaji,” “Semua orang kaya, jadi mengapa aku tidak?” dan “Tidak ada yang dirugikan”. Pelaku kecurangan selalu membohongi dirinya sendiri bahwa apa yang dilakukannya benar supaya tidak merasa bersalah (Zikmund, 2008).

2.2.1.5 *Fraud Element Triangle*

Salah satu tujuan yang mengharuskan seorang auditor melakukan investigasi *fraud* adalah membongkar *fraud* tersebut. Dugaan atas tindakan *fraud* memerlukan bukti yang logis, dan dalam melakukan investigasi *fraud*, tidak boleh dilakukan jika tidak ada dugaan sebelumnya. Investigasi *fraud* dilakukan untuk memastikan dan menentukan *fraud* benar – benar terjadi dan apakah indikasi *fraud* yang ditemukan benar merupakan *fraud* atau hanya merupakan kesalahan yang tidak disengaja. Dasar yang mendasari adanya investigasi *fraud* menurut Albrecht *et al.* (2006) berfokus pada tindakan pencurian, penyembunyian dan konversi tindakan pencurian.

Gambar 2.2
Fraud Element Triangle



Sumber : Albrecht et al. (2006)

1. *Act* (Tindakan Pencurian)

Metode investigasi pada tindakan pencurian melibatkan usaha untuk menangkap pelaku tindak pencurian atau untuk mengumpulkan informasi terkait tindakan pencurian yang benar – benar terjadi.

2. *Concealment* (Penyembunyian)

Metode investigasi pada penyembunyian *fraud* akan berfokus pada berbagai bukti fisik berupa dokumen, catatan, program Teknologi Informasi, server komputer, Bank, maupun tempat – tempat yang sangat dimungkinkan untuk menyembunyikan tindakan *fraud* oleh pelaku. Penyembunyian merupakan tindakan

yang dilakukan untuk menyembunyikan hasil *fraud* agar tidak diketahui orang lain.

3. *Conversion* (Konversi)

Metode investigasi pada tindakan konversi melibatkan penemuan cara – cara yang dilakukan pelaku dalam menggunakan atau menjual bahkan jika dimungkinkan mengubah bentuk aset yang mereka curi. Konversi atas aset yang dicuri merupakan salah satu cara untuk menyembunyikan bukti dan dilakukan agar pelaku langsung menerima manfaat atas barang yang dicuri untuk kepentingan pribadi.

2.2.2 Strategi Anti *Fraud*

Dalam Lampiran Surat Edaran Bank Indonesia, Nomor 13/28/DPNP Tanggal 9 Desember 2011, Perihal Penerapan Strategi Anti *Fraud* Bagi Bank Umum, mencakup kegiatan bank secara konvensional maupun dengan prinsip syariah. Dalam melaksanakan proses pengendalian *fraud*, maka penerapan strategi anti *fraud* adalah sebuah wujud kebijakan untuk mengendalikan *fraud*, memperkuat pengendalian intern bank, meningkatkan pencegahan serta pendeteksian *fraud* dan proses investigasi agar dapat menjadi budaya anti *fraud* dalam seluruh aspek organisasi baik oleh manajemen / “*tone at the top*” maupun oleh karyawan. Hal itu tentu saja dikarenakan sebelum dikeluarkannya peraturan penerapan strategi anti *fraud*, Bank sudah

menerapkan Manajemen Risiko, Sistem Pengendalian Intern, dan Pelaksanaan Tata Kelola yang Baik, namun untuk menjadi prioritas dalam organisasi, maka diperlukan penerapan strategi anti *fraud*.

Selain itu, dalam proses mengendalikan risiko terjadinya *fraud*, Bank diwajibkan untuk menetapkan Manajemen Risiko, hal ini dilakukan agar memperkuat proses pengendalian risiko *fraud*. Manajemen Risiko cakupannya meliputi :

1. Pengawasan Aktif Manajemen

Penerapan strategi anti *fraud* keberhasilannya sangat tergantung kepada kebijakan “*tone at the top*” . Jajaran Dewan Komisaris dan Direksi merupakan sumber terciptanya kepedulian anti *fraud* dan pelopor terciptanya budaya anti *fraud*. Tanpa dukungan dan contoh yang baik dari “*tone at the top*” atau manajemen, akan sulit menumbuhkan kepedulian dan kesadaran dalam organisasi.

Tanggung jawab tersebut meliputi :

- a. Mengembangkan budaya anti *fraud* dan mengkomunikasikan kepada seluruh jajaran organisasi apa saja perilaku yang termasuk *fraud*.
- b. Menyusun dan mengawasi kode etik terhadap pencegahan *fraud* dan penerapan strategi anti *fraud*.
- c. Mengembangkan SDM terkait *fraud awareness*.
- d. Memantau, mengevaluasi dan menindaklanjuti tindakan *fraud*.

- e. Melakukan perbaikan komunikasi antar jajaran organisasi dalam kebijakan pengendalian *fraud* agar manajemen maupun pegawai mematuhi kebijakan yang ada.

2. Struktur Organisasi dan Pertanggungjawaban

Agar penerapan strategi anti *fraud* lebih efektif, Bank wajib membentuk unit atau fungsi yang bertugas mengawasi dan menangani penerapan strategi anti *fraud* di dalam struktur organisasi. Unit atau fungsi ini memiliki koordinasi dan pelaporan langsung terhadap Dewan Komisaris dan memiliki tanggung jawab langsung kepada Direktur Utama. Untuk membentuk unit atau fungsi tersebut perlu diperhatikan beberapa hal :

- a. Sesuai dengan kompleksitas dan karakteristik Bank
- b. Memiliki tugas dan tanggungjawab yang jelas
- c. Dilakukan oleh SDM yang berintegritas, kompeten dan independen

3. Pengendalian dan Pemantauan

Kedua hal ini sangat penting dalam menjaga efektivitas penerapan strategi anti *fraud*. Dengan adanya pemantauan menggunakan sistem teknologi informasi yang memadai, maka proses pengendalian risiko terjadinya *fraud* dapat dilaksanakan secara efisien. Pengendalian dan pemantauan yang dapat dilakukan berupa :

- a. Dilakukannya kajian ulang oleh manajemen dan kajian ulang operasional oleh SKAI atas pelaksanaan strategi anti *fraud*.
- b. Menetapkan kebijakan dan prosedur untuk mengendalikan *fraud* terkait SDM seperti rotasi posisi, kebijakan mutasi, adanya wajib cuti, dan pertanggungjawaban sosial atau *gathering*.
- c. Melakukan pemisahan tugas dan fungsi dalam semua proses aktivitas untuk seluruh jenjang organisasi, agar tidak timbul celah untuk melakukan *fraud* dan menyembunyikan tindakan *fraud*.
- d. Membuat sistem informasi untuk mengamankan data berupa dokumentasi maupun fisik dalam proses pengolahan dan penyimpanan serta menjamin data tetap akurat dan terpercaya dalam pelaporan keuangan bank seperti verifikasi dan rekonsiliasi.

2.2.2.1 Pencegahan

1. Anti Fraud Awareness

Sesuai dengan diterapkannya manajemen risiko melalui pengawasan aktif manajemen, maka manajemen atau pimpinan harus mengawali upaya kesadaran adanya anti *fraud*. Jika pemimpin mampu menciptakan anti *fraud awareness* melalui kebijakan yang di terapkan, maka semua unsur organisasi dalam

bank akan menciptakan budaya anti *fraud*. Hal ini dapat terwujud dengan adanya:

a. Sosialisasi tentang susunan Anti *Fraud Statement* atau *zero tolerance* terhadap *fraud*.

b. Program *employee awareness*

Bertujuan menumbuhkan kesadaran pegawai akan jenis – jenis *fraud* maupun tindak lanjut terhadap *fraud* melalui seminar, pelatihan, diskusi dan pemahaman pentingnya anti *fraud*.

c. Program *customer awareness*

Menumbuhkan kesadaran nasabah melalui sosialisasi melewati media cetak maupun media elektronik disekitar lingkungan Bank agar paham, peduli dan waspada terhadap *fraud*.

2. Identifikasi Kerawanan

Proses ini juga termasuk dalam proses manajemen risiko dalam melakukan identifikasi, analisis dan menilai potensi risiko munculnya *fraud*. Risiko yang dilakukan manajemen risiko berbentuk risiko melekat pada setiap proses aktivitas dalam bank yang berpotensi merugikan secara signifikan atau tinggi. Hasil proses identifikasi, analisis dan penilaian tersebut harus didokumentasikan dan diinformasikan langsung kepada pihak yang berkepentingan atas bank.

3. *Know Your Employee*

Mencegah terjadinya *fraud* yang dilakukan oleh orang internal atau pegawai membuat bank lebih berhati – hati dalam mengendalikan SDM yang ada di dalam bank. Hal tersebut dapat dilakukan sejak perekrutan SDM dengan mengenali proses pengenalan, perilaku, gaya hidup dan karakter nya. Yang terpenting adalah terlebih dahulu menetapkan sistem perekrutan yang efektif dan melakukan proses *screening* jejak rekam calon pegawai. Sistem seleksi juga harus mengedepankan kualifikasi, transparansi dan bersifat obyektif terhadap calon pegawai dengan prosedur mutasi maupun promosi. Hal ini ditekankan khususnya pada posisi yang berisiko tinggi terhadap *fraud*.

2.2.2.2 Deteksi

Bertindak sebagai perangkat untuk mengidentifikasi dan menemukan *fraud*. Pilar deteksi berisikan :

1. Kebijakan dan Mekanisme *Whistleblowing*

Whistleblowing system merupakan layanan pengaduan *fraud* dimana pengadu atau *whistleblower* diberikan perlindungan kerahasiaan identitasnya. Layanan ini merupakan sarana mengungkapkan temuan *fraud* dimana sebagai pendorong organisasi untuk ikut melaksanakan budaya anti *fraud* dan menumbuhkan kesadaran pegawai maupun pejabat bank untuk

melaporkan perilaku tidak etis yang menyimpang dan merugikan bank. Kebijakan ini tentu saja meliputi :

- a. Perlindungan kepada *Whistleblower*
- b. Regulasi Pengaduan *Fraud*

Diharapkan pengaduan *fraud* menaati ketentuan internal yang mengacu kepada peraturan perundang – undangan.

- c. Mekanisme Pelaporan dan Tindak Lanjut atas Laporan *Fraud*

Kejelasan atas mekanisme pelaporan mulai dari sarana pelaporan melalui layanan via sms atau *hotline*, tata cara pelaporan dan pihak yang bertanggung jawab untuk menindaklanjuti hasil laporan wajib diterapkan dan diharapkan konsisten serta transparan diketahui oleh seluruh aspek organisasi. Hal ini agar menjamin independensi dan kerahasiaan serta menimbulkan kepercayaan sehingga para *whistleblower* tidak perlu takut untuk mengadu.

2. *Surprise Audit*

Pelaksanaan *surprise audit* ini perlu dilaksanakan secara berhati – hati dan penting dilakukan pada unit bisnis yang berisiko *fraud* tinggi. Bisa dilakukan saat puncak penjualan atau disaat organisasi sedang beroperasi sangat sibuk.

3. *Surveillance System*

Surveillance system dilakukan oleh pihak – pihak yang dijamin independensinya didalam internal bank. Tentu saja proses ini adalah proses pemeriksaan dan pengujian terhadap efektifitas diterapkannya kebijakan anti *fraud*.

2.2.2.3 Investigasi, Pelaporan dan Sanksi

Bertindak sebagai perangkat untuk mendalami laporan aduan *fraud*, sistem pelaporan dan sanksi yang dikenakan atas *fraud* yang benar – benar terjadi atau dilakukan.

1. Investigasi

Investigasi merupakan pokok terpenting dalam menggali informasi lebih lanjut dan menguji keandalan informasi adanya tindakan *fraud* terhadap pihak – pihak terkait. Dengan kata lain, proses ini berguna untuk mengumpulkan bukti – bukti yang dianggap sebagai bagian dalam *fraud*. Bank harus memiliki standar investigasi yaitu :

- a. Menentukan pihak investigator yang independen dan berkompeten
- b. Mekanisme menindaklanjuti hasil pendeteksian *fraud* dengan tetap menjaga kerahasiaan informasi.

2. Pelaporan

Setiap bank wajib memiliki mekanisme pelaporan atas hasil investigasi *fraud* yang dilakukan secara sistematis dan efektif kepada pihak manajemen maupun Bank Indonesia.

3. Pengenaan Sanksi

Pengenaan sanksi ini dilakukan agar para pelaku *fraud* jera. Sanksi diberikan harus sesuai kebijakan setiap bank atas hasil investigasi yang dilakukan sebelumnya. Kebijakan berisikan :

- a. Mekanisme dalam mengenakan sanksi
- b. Pihak yang bertanggung jawab dalam pengenaan sanksi

2.2.2.4 Pemantauan, Evaluasi, dan Tindak Lanjut

Bertindak sebagai perangkat untuk menindaklanjuti hasil pemantauan dan evaluasi pelaporan *fraud*.

1. Pemantauan

Memantau hasil pelaporan *fraud* merupakan bagian penting dalam mengendalikan *fraud* karena untuk menindaklanjuti *fraud* tidak bisa semata – mata dilakukan tanpa proses pemantauan terlebih dahulu.

2. Evaluasi

Hasil pelaporan *fraud* akan di dokumentasikan dan dokumen tersebut akan sangat berguna untuk membantu pada proses evaluasi. Dokumen tersebut berisikan data – data kejadian *fraud* yang memiliki informasi kurang lebih:

- a. Jenis *fraud*, seperti kecurangan, *fraud*, penggelapan aset, pembocoran informasi dan tindak pidana bank.
- b. Tanggal terjadinya *fraud*
- c. Pihak yang diindikasikan terlibat, jika lebih dari 1 orang bisa dijelaskan masing – masing perannya dalam *fraud*
- d. Jabatan
- e. Perkiraan kerugian

- f. Tindakan bank terhadap pelaku *fraud* maupun pihak yang dirugikan atas kejadian *fraud*
- g. Penyebab terjadinya *fraud*
- h. Tindak lanjut dan perbaikan yang dilakukan atas penyebab *fraud*

3. Tindak Lanjut

Hasil evaluasi *fraud* kemudian perlu dilakukan tindak lanjut yang sangat berguna untuk memperkuat sistem pengendalian internal agar hal – hal penyebab *fraud* yang merupakan kelemahan dalam pengendalian internal dapat dilakukan perbaikan. Hal ini berguna agar tidak terulang kembali *fraud* yang disebabkan oleh lemahnya sistem pengendalian internal.

2.2.3 Pencegahan *Fraud*

2.2.3.1 Mengembangkan Budaya *Zero Tolerance* pada *Fraud*

Budaya organisasi atau korporat mengacu pada cara unik setiap organisasi menjalankan bisnisnya. Budaya perusahaan mencakup nilai, norma, kepercayaan, dan praktik etika bersama yang membentuk karakter organisasi. Manajemen puncak perlu menekankan pentingnya manajemen risiko *fraud* sebagai cara untuk menambah nilai bagi Bank dan untuk tata kelola yang efektif dari Bank. Kebijakan Bank yang mencakup etika bisnis dan *fraud* harus dikomunikasikan dan didukung sepenuhnya di seluruh organisasi.

Individu yang tepat perlu ditentukan dan diberi peran dan tanggung jawab untuk menerapkan strategi manajemen risiko *fraud* (Kimani, 2011).

Menurut Rubasundram (2015), mekanisme tata kelola dan kontrol yang baik dapat menyesatkan. Contohnya, Enron memiliki semua mekanisme sistem tata kelola dan pengendalian yang baik, namun karena budaya dan keputusan manajemen, kegiatan *fraud* tetap terjadi. Budaya perusahaan juga menjadi salah satu faktor risiko utama penyebab integritas dan kepatuhan di perusahaan diselewengkan. Jika terjadi *management override*, maka akan sangat mempengaruhi komitmen karyawan dalam menjaga integritasnya. Demi mencegah adanya aktivitas *fraud*, maka faktor paling kuat adalah jika *tone from the top* kuat dalam mematuhi kontrol internal. Tanpa dukungan dari Direktur dan manajemen, keberhasilan pelaksanaan tata kelola dan kontrol yang baik mungkin tidak dilakukan.

Dalam Hassmiller (2015), terdapat beberapa tips menciptakan budaya Anti-*Fraud*, yaitu :

1. *Set The Tone At The Top*

Menciptakan budaya anti *fraud* merupakan bagian dari tata kelola yang baik dan harus dimulai dengan komitmen yang jelas untuk mengatasi *fraud* dan korupsi yang dipimpin oleh dewan eksekutif. Toleransi nol terhadap kecurangan idealnya

merupakan bagian dari 'pernyataan misi etis' organisasi atau dokumen strategi, dan meningkatkan profil agenda anti *fraud*.

2. Memprioritaskan Risiko *Fraud* (Membentuk Tim Khusus)

Ketika organisasi mampu mendeteksi risiko *fraud*, maka penting dilakukan langkah menekan risiko dengan membentuk tim khusus untuk pencegahan *fraud* dalam setiap proses bisnis dalam organisasi.

3. *Scan the Horizon*

Sangat penting untuk suatu organisasi agar selalu *update* terhadap ancaman dan risiko terbaru dan bagaimana mengatasinya. Tim anti *fraud* yang berkualitas bisa memastikan jika mereka mencurigai sesuatu, tim tahu ke mana harus menindaklanjuti dan tahu rantai kecurangan akan terhubung ke jaringan lain yang mana.

4. *Build Fraud Awareness*

Menciptakan budaya anti *fraud* di mulai dari memobilisasi keseluruhan organisasi dalam memerangi kecurangan. Dapat dilakukan menggunakan *e-learning*, *briefing staf*, poster atau peringatan internal, atau kombinasi dari semua ini.

5. Memastikan Kebijakan dan Prosedur

Setiap organisasi harus memastikan kebijakan dan prosedur dalam melawan *fraud*. Seperti kebijakan *whistleblowing*, kebijakan ini harus mencakup panduan tentang apa yang harus

dilakukan saat kecurigaan kecurangan muncul, rencana tindak lanjut berikutnya, dan rincian daftar pihak dalam organisasi yang terhubung satu sama lain dalam *fraud*.

6. Buat Tim Anti *Fraud* yang Berdedikasi

Spesialis tim anti *fraud* idealnya berfungsi secara independen dari tim lain. Hal ini untuk memastikan objektivitas dan akses tak terbatas terhadap informasi dan sumber daya yang di butuhkan. Ini termasuk akses ke layanan spesialis, termasuk dukungan forensik dan sumber daya rahasia dan aman untuk menyimpan bukti.

7. Mengambil Tindakan

Tim anti *fraud* sepenuhnya harus dilatih dalam melakukan investigasi dan menindaklanjuti kasus hingga ke pengadilan dengan memberikan bukti – bukti atas hasil investigasi nya.

8. *Never Take Your Eye Off The Ball*

Fraud adalah ancaman yang terus berkembang dan tidak dapat dihindarkan, sebaiknya strategi organisasi dirancang untuk dapat melawannya. Jangan pernah lengah untuk tidak melakukan tindakan pencegahan.

2.2.3.2 Pengendalian Internal

Menurut Albrecht *et al.* (2006), mencegah kecurangan dapat dilakukan melalui Lingkungan Pengendalian, Penilaian Risiko, dan Aktivitas Pengendalian.

Esensi organisasi yang dikendalikan secara efektif terletak pada perilaku pihak manajemen mereka. Jika manajemen puncak percaya bahwa pengendalian penting, pihak lain dalam organisasi akan merespons dengan benar-benar memperhatikan pengendalian yang ada. Berikut adalah komponen paling penting dalam lingkungan pengendalian :

1. Integritas dan Nilai Etika
2. Partisipasi Dewan Direksi dan Komite Audit
3. Filosofi dan Gaya Operasional Manajemen
4. Kebijakan dan Praktik Sumber Daya Manusia

Aktivitas Pengendalian sendiri adalah kebijakan dan prosedur yang diperlukan untuk mencegah adanya tindakan yang menyebabkan terjadinya kecurangan. Seperti pada umumnya, terdapat lima tipe sebagai berikut :

1. Pemisahan Tugas
2. Otorisasi yang Sesuai atas Transaksi dan Aktivitas

Termasuk pengendalian adanya kata sandi, tanda tangan digital, dan teknologi biometrik (pola iris dan retina mata, sidik jari, pita suara, struktur wajah, dan bentuk tulisan tangan).

3. Dokumentasi dan Kegiatan Pencatatan yang Memadai

Adanya enkripsi yang melindungi informasi rahasia atau sensitif dari upaya pencurian.

4. Pengendalian Fisik dan Pencatatan atas Aset

5. Pengecekan yang Independen atas Kinerja

Menurut Albrecht *et al.* (2006), organisasi dapat membuat lingkungan dengan tingkat kecurangan yang rendah dan tingkat kecurangan yang tinggi. Faktor dasar yang termasuk lingkungan dengan tingkat kecurangan yang rendah adalah menciptakan budaya kejujuran, transparan dan mendukung proses mengurangi kesempatan terjadinya kecurangan.

2.2.3.3 Pengamanan dengan Teknologi

Pada tahun 2010, sebagian besar kasus *fraud* terjadi melalui sistem elektronik *banking*, sehingga mencerminkan kelemahan dalam sistem pengendalian internal (Sanusi, 2010). Hal ini menyebabkan perusahaan jasa keuangan dan organisasi mengalami kerugian besar atas terjadinya *fraud* dalam *online Banking*, *cheque* dan *card fraud*. Hal ini mengharuskan kebutuhan akan perbaikan terus menerus harus dilakukan guna mencegah *fraud*.

Menurut Benjamin (2011), jenis kecurangan yang biasa dialami oleh lembaga keuangan meliputi *sales fraud*, *purchase fraud*, *cheque payment fraud* dan *ATM fraud*. Strategi lain yang digunakan termasuk berkolaborasi dengan agen keamanan dan pejabat bank serta jaringan lokal dan internasional (Usman and Shah, 2013). Hal ini menunjukkan bahwa karyawan internal bank telah bekerjasama dengan penipu. Ini menghadirkan ancaman nyata karena karyawan internal memiliki

akses langsung ke sistem perbankan dan akses terhadap informasi pribadi nasabah dan catatan nasabah. Benjamin (2011) menemukan bahwa ketidaksetaraan yang dirasakan dan ketidakpastian kerja yang dirasakan karyawan berpengaruh signifikan terhadap niat curang karyawan.

Dalam penelitian yang dilakukan Usman and Shah (2013), cara tradisional penggunaan *e-banking* melalui *username* dan *passwords* masih belum cukup mencegah adanya pencurian data informasi akun pribadi nasabah. Terdapat pengamanan yang lebih canggih lagi melalui teknologi, yaitu dinamakan *biometric technology*.

Tabel 2.10
Metode Pencegahan *Fraud*

No.	Metode Pencegahan <i>Fraud</i>
1.	Otentikasi Biometrik
2.	Perangkat Lunak Pencegahan Penipuan
3.	<i>One Time Passwords</i> (OTP)
4.	Otentikasi <i>Smart Card</i>
5.	<i>Passwords</i>
6.	<i>Multi Layer Passwords</i>

Sumber : Usman and Shah (2013)

Tabel di atas merangkum beberapa tindakan pencegahan kecurangan mengacu kepada teknologi biometrik. Otentikasi biometrik mendukung aspek identifikasi dan otentikasi. Oleh karena

itu, jenis teknologi ini berpotensi memainkan peran penting dalam meminimalkan kecurangan *e-banking*. Teknologi biometrik dipandang sebagai solusi karena setiap fitur unik untuk setiap individu yaitu dapat digunakan untuk identifikasi. Meskipun kemajuan teknologi biometrik seperti sidik jari, pendeteksi suara, dan iris mata tampak menjanjikan, diperlukan juga otentikasi yang aman secara teknologi dan layak secara ekonomi. Penelitian oleh Usman and Shah (2013), telah membuktikan bahwa teknologi biometrik dapat secara signifikan mengurangi kecurangan *e-banking* dan telah diterapkan di beberapa bank seperti ATM biometrik oleh *First Bank* di Nigeria.

Murdoch and Anderson (2010) menekankan bahwa solusi otentikasi perlu dilakukan secara teknologis dan ekonomis, karena biaya untuk menerapkan teknologi semacam itu tidak kecil. Teknologi sidik jari bukanlah satu-satunya teknologi biometrik, beberapa bank ada yang memilih menggunakan *Keystroke Dynamics*. *Keystroke Dynamics* adalah proses menganalisis cara pengguna mengetik di terminal dengan memantau input keyboard ribuan kali per detik, dan mencoba untuk mengidentifikasi mereka berdasarkan pola irama kebiasaan seperti yang mereka ketik. *Bank Ekuador* dan *Bank of Utah* memilih pola *keystroke* karena kemudahan dan kemampuannya untuk meningkatkan keamanan perbankan online. Selain itu, biaya yang digunakan rendah.

Dukungan *Top Management* sangat berpengaruh dalam pencegahan *fraud* e-banking. Hal ini karena untuk mengamankan layanan *e-banking*, berbagai langkah pengamanan seperti enkripsi, password dan *One Time Passwords* (OTPs) digunakan dan hal ini tidak akan mungkin terjadi tanpa dukungan dari manajemen puncak.

2.2.3.4 Manajemen Sumber Daya Manusia (SDM)

Menurut Hadiyatno (2012), keunggulan kompetitif akan tercapai apabila pihak manajemen dapat mengelola sumber daya manusianya secara benar dan tepat. Pada dasarnya pegawai merupakan komponen penting bagi perusahaan untuk menciptakan daya saing yang memberikan kualitas lebih bagi pemegang saham dan pelanggan. Maka keberhasilan suatu organisasi dalam mewujudkan tujuannya sangat tergantung pada sumber daya manusia yang dimilikinya. sumber daya manusia mempunyai peran penting dalam pertumbuhan dan pengembangan organisasi, karena potensi yang ada dalam diri manusia seperti bakat, kreativitas, keinginan dan aktivitas kerja merupakan nilai tersendiri untuk SDM yang tidak dapat digantikan oleh mesin sekalipun. Manajemen SDM melalui proses seleksi SDM dengan prioritas SDM yang kompeten, hingga diberikannya sertifikasi maupun pelatihan serta rotasi pegawai merupakan cara yang perlu dilakukan perusahaan.

1. Proses Rekrutmen

Menurut Widjaja (2005:33), dalam upaya membangun lingkungan kerja yang positif, penerimaan pegawai merupakan langkah pertama untuk memperkerjakan orang – orang yang jujur. Melalui proses seleksi yang ketat, efektif dan memenuhi syarat tertentu diharapkan dapat menghindari terpilihnya calon pegawai yang memiliki tingkat kejujuran rendah. Kebijakan seperti itu mencakup pengecekan latar belakang orang – orang yang akan dipertimbangkan atau dipromosikan untuk menempati jabatan yang penting. Pengecekan latar belakang dilakukan dengan :

- a. Verifikasi pendidikan
- b. Riwayat pekerjaan
- c. Referensi pribadi calon karyawan
- d. Referensi karakter
- e. Referensi integritas

2. Sertifikasi

Menurut Gaffney and Essex (2014), untuk meningkatkan program pelatihan anti *fraud* dalam organisasi, maka perlu diberikan sertifikasi anti *fraud* yang ditetapkan oleh *Association of Certified Fraud Examiner (ACFE)*. ACFE sendiri mengharuskan unit khusus atau unit anti *fraud* memiliki sertifikat sebagai *Certified Fraud Examiner (CFE)*. Peningkatan dan pengembangan secara terus menerus yang dilakukan oleh

tim anti *fraud* melalui program pelatihan akan menambah kompetensi pengetahuan SDM dalam melakukan investigasi *fraud*. Seperti yang sudah dijelaskan sebelumnya dalam *fraud element triangle*, investigasi *fraud* dilakukan untuk memastikan dan menentukan *fraud* benar – benar terjadi dan apakah indikasi *fraud* yang ditemukan benar merupakan *fraud* atau hanya merupakan kesalahan yang tidak disengaja. Sehingga untuk mencegah adanya tindakan *fraud* di dalam organisasi, maka diperlukan SDM yang memiliki kompetensi sebagai *Fraud Examiner*. Untuk dapat mendapatkan sertifikasi sebagai *Fraud Examiner*, maka ACFE memiliki standar minimum pengetahuan yang harus dikuasai SDM yang akan menjadi agen khusus di dalam perusahaan. Dalam ujian sertifikasi yang diadakan ACFE, maka SDM minimal akan mempelajari kompetensi sebagai berikut :

Tabel 2.11

ACFE Fraud Knowledge Competency

ACFE FRAUD KNOWLEDGE COMPETENCY	
Section 1	Financial Transactions & Fraud Schemes
Subsection 1.1	Financial Transactions
Subsection 1.2	Occupational Fraud Schemes
Subsection 1.3	Other Fraud Schemes
Section 2	Law
Subsection 2.1	Pverview
Subsection 2.2	Punishing Offenders
Subsection 2.3	Practice & Procedure
Section 3	Investigation
Subsection 3.1	Investigation Procedures

Subsection 3.2	Interviewing
Subsection 3.3	Gathering Information
Subsection 3.4	Analyzing Evidence
Section 4	Fraud Prevention & Deterrence
Subsection 4.1	Understanding Crime
Subsection 4.2	Fraud Prevention
Subsection 4.3	Ethics & Responsibilities

Sumber : Gaffney and Essex (2014)

Secara keseluruhan, model kompetensi pengetahuan ACFE mencakup 45 kompetensi dengan 4 seksi yang sama, hanya saja subseksi yang lebih terperinci, tabel 2.11 berisikan kompetensi minimal yang diperlukan oleh tim khusus anti *fraud*.

3. Rotasi dan Cuti Pegawai

Menurut Parimita, Pambudi dan Aminah (2017) dikatakan bahwa pegawai yang memiliki kepuasan kerja yang baik dicerminkan dengan adanya prestasi kerja dan disiplin kerja yang baik.

Kepuasan kerja didapatkan ketika persepsi pegawai atas pekerjaannya adalah pekerjaan yang menyenangkan. Ketidakpuasan kerja akan berdampak kepada ketidakhadiran, rendahnya produktivitas dan keluarnya pegawai dari suatu organisasi. Ketidakpuasan kerja dipengaruhi oleh pengembangan karir yang dimiliki pegawai tersebut. Pengembangan karir untuk mendapat jabatan yang lebih tinggi harus didapatkan pegawai tanpa harus menunggu para senior

menghabiskan waktu yang lama pada posisi jabatannya, namun semua itu tergantung dari prestasi kerja setiap pegawai. Pengembangan karir merupakan proses berkelanjutan untuk pegawai di dalam perusahaan dalam mengisi jabatan perusahaan di masa mendatang.

Rotasi karyawan perlu dilakukan sehingga karyawan yang kurang menyukai posisi pekerjaannya yang sekarang dapat pindah ke posisi yang dianggapnya cocok sehingga pegawai akan mendapatkan kepuasan kerja.

Menurut Pusklatwas BPKP (2008), perlu dikembangkan metode kepekaan terhadap *fraud* dalam rangka upaya pencegahan *fraud* yang terintegrasi. Metode ini berisikan :

- a. Kualifikasi calon pegawai harus diperhatikan secara khusus, jika dimungkinkan terdapat referensi dari pihak – pihak yang sudah pernah melakukan kerjasama
- b. Setiap pegawai diperingatkan untuk melaporkan segala transaksi mencurigakan yang dilakukan pegawai lainnya. Rasa curiga tersebut harus dapat dipertanggungjawabkan.
- c. Para pegawai sebaiknya tidak diperbolehkan lembur secara rutin tanpa adanya pengawasan. Bahkan beberapa perusahaan di Amerika Serikat menganggap lembur

adalah bentuk ketidakefisienan kerja, dan hal tersebut harus dihindari, karena jika pegawai mampu manajemen waktu maka semua pekerjaan dapat diselesaikan tepat pada jam – jam kerja yang seharusnya.

- d. Karyawan wajib mengambil cuti setiap tahunnya. Jika seorang pegawai melakukan *fraud*, maka pegawai tersebut akan melakukan berbagai cara untuk menutupi perbuatannya. Kecurangan tersebut dapat diungkap hanya jika pada saat pegawai tersebut mengambil cuti dan tugas – tugasnya digantikan oleh pegawai lain. Hal yang mungkin dilakukan juga adalah dengan rotasi pegawai secara periodik dengan tujuan yang sama (Pusdiklatwas BPKP, 2008).

4. *Reward* atau Kompensasi

Kompensasi diberikan oleh perusahaan kepada pegawainya dengan harapan bahwa kesesuaian antara keinginan pegawai dan kompensasi yang diberikan itu sesuai. Dengan sesuainya kompensasi, maka diharapkan tercapai tujuan yaitu mencegah terjadinya kecurangan oleh pegawai.

Menurut Gibson (2003), kompensasi atau *reward* terbagi dalam dua kategori yaitu *reward* intrinsik dan ekstrinsik, berikut adalah penjelasannya :

a. *Reward* Intrinsik merupakan *reward* yang melekat pada pekerjaan itu sendiri. Contohnya :

1) *Completion*, yaitu *reward* yang diberikan bagi pegawai yang berhasil menyelesaikan suatu tugas.

2) *Achievement*, yaitu *reward* akan diri sendiri yang diberikan bagi pegawai karena mampu menyelesaikan suatu pekerjaan yang menantang.

3) *Autonomy*, yaitu pemberian kebebasan dalam pengambilan keputusan untuk pegawai terkait dengan cara menyelesaikan pekerjaan itu sendiri.

4) *Personal Growth*, yaitu meningkatnya kemampuan, ketrampilan atau keahlian dari yang sudah dimilikinya sekarang.

b. *Reward* Ekstrinsik

1) Keuangan, yaitu *reward* yang diberikan bagi pegawai dalam bentuk peningkatan upah / gaji.

2) *Interpersonal*, yaitu *reward* yang diberikan bagi pegawai yang berupa status dan *recognition*.

- 3) Promosi, yaitu *reward* yang diberikan bagi pegawai atas prestasi yang telah dicapai dalam bentuk jenjang karir.

2.2.4 Pendeteksian Fraud

2.2.4.1 *Whistleblowing System*

1. Kebijakan *Whistleblowing System*

Menurut Elias (2008), *whistleblowing* mencakup *whistleblowing* dari internal dan eksternal. Internal *whistleblowing* terjadi jika pegawai yang mengetahui kecurangan yang dilakukan di dalam organisasi maka akan melaporkan kecurangan tersebut kepada atasannya. Eksternal *whistleblowing* terjadi jika pegawai yang mengetahui kecurangan yang dilakukan di dalam organisasi maka akan melaporkan kecurangan tersebut kepada masyarakat dikarenakan kecurangan tersebut merugikan masyarakat.

Internal *whistleblowing system* yang baik berfungsi mendeteksi tindakan *fraud* secara tepat waktu, sehingga memungkinkan untuk perusahaan memperbaiki kesalahan yang terjadi dan mampu menekan biaya yang dibebankan atas *fraud* yang terjadi (Chung, Monroe and Thome, 2004).

Berdasarkan Haryanto *et al.* (2005), *whistleblowing* adalah salah satu kontrol yang berhubungan dengan kontrol manajemen. Dengan adanya *whistleblowing system*, diharapkan

kontrol manajemen dapat berjalan optimal dan dapat mencapai tujuan perusahaan. Dalam mendukung adanya *whistleblowing system*, observasi dan *surveillance system* (pengawasan) dapat menjadi pendukung adanya *whistleblowing system*. *Whistleblowing* bagi sebagian manajer akan dianggap sebagai ancaman, namun pada era globalisasi, manajer harus melihat dari sisi lain bahwa jika pegawai mengungkap fakta akan menjadi sumber yang berharga bagi manajemen. Jika pegawai memiliki komitmen yang tinggi untuk memberikan informasi yang berharga pada organisasi dan dapat menjadi pemecahan masalah di tempat dia bekerja, maka manajer harus mengambil tindakan untuk memfasilitasi pegawai dengan cara yang bermanfaat bagi perusahaan.

2. Mekanisme pelaporan pada *Whistleblowing System*

Penerapan *whistleblowing system* mengadopsi prinsip bahwa semua laporan dari pegawai akan ditindaklanjuti oleh bagian tertentu di dalam organisasi dan akan langsung dilaporkan ke CEO. Dengan demikian, perusahaan dapat mengetahui laporan mana yang hanya memfitnah perusahaan dan mana yang benar – benar harus ditindaklanjuti. CEO merupakan jajaran manajemen tingkat atas, sehingga keterlibatan manajemen atas secara langsung dapat menghindari konflik kepentingan dan memastikan keterlibatan langsung

kepemimpinan, hal ini menunjukkan bahwa organisasi menjaga komitmennya dalam mengurangi potensi terjadinya *fraud*. Dapat dikatakan bahwa penerapan *whistleblowing system* harus dimulai dari komitmen yang kuat dari jajaran organisasi tingkat atas (Haryanto *et al.*, 2005).

Whistleblowing system merupakan mekanisme yang efektif di dalam organisasi dalam melawan tindakan *fraud*. Salah satu langkah yang tepat untuk organisasi dalam mendeteksi tindakan menyimpang adalah memfasilitasi pegawai dengan fasilitas *hotline* (layanan) aduan *whistleblowing*. *Whistleblowing system* sangat penting karena dengan tidak adanya sistem yang efektif maka akan meminimalkan pelaporan kecurangan yang sebenarnya diketahui pegawai. Untuk memperkuat komitmen organisasi dalam mendeteksi *fraud*, maka penerapan *whistleblowing system* diperlukan layanan khusus atau *hotline* yang akan meningkatkan kredibilitas pelaporan tindakan menyimpang. Hal ini agar pelaporan kecurangan lebih independen dan tidak dilakukan langsung kepada atasan dalam divisi terkait, namun dapat ditangani langsung oleh unit independen di dalam organisasi, dimana nantinya tetap akan dilaporkan pada manajemen tingkat atas (Lee and Fargher, 2013).

Menurut Lee and Fargher (2013), menerapkan *whistleblowing system* yang efektif tidak hanya menerapkan kebijakan *whistleblowing system* yang baik, tetapi juga dalam pelaksanaan dan pemantauan *whistleblowing system* itu sendiri. Menurut survey yang dilakukan ACFE (2010) dalam Lee and Fargher (2013), kontrol anti *fraud* dengan adanya *hotline* pelaporan kecurangan mampu mengurangi kerugian yang disebabkan oleh tindakan *fraud* dalam persentase yang besar. Hal ini karena layanan *hotline* dapat berfungsi selama 24 jam penuh, sehingga memungkinkan karyawan untuk melaporkan tindakan kecurangan secara rahasia dan kapan saja. *Hotline* yang baik juga dapat diakses pegawai walaupun pegawai sedang berada diluar lingkungan geografis perusahaan. Adanya *hotline* tersebut juga membantu mengurangi perilaku yang tidak etis di tempat kerja meskipun diluar kantor pusat.

3. Perlindungan pada *Whistleblower*

Melindungi *whistleblower* atau pelapor indikasi kecurangan sangat lah penting untuk dilakukan, karena jika pelaku atau orang – orang di dalam organisasi mendengar nama pelapor tersebut maka tidak semua orang dapat berpikir jernih atas niat baik pelapor. Perlindungan secara hukum untuk pelapor dan keluarganya adalah langkah yang penting untuk meyakinkan para pegawai untuk tidak menghindari adanya pelaporan

tindakan *fraud* di dalam organisasi. Perlindungan tersebut dilakukan salah satunya jaminan perlindungan oleh kepolisian negara walaupun kasus yang dilaporkan belum naik ke meja hukum. (Lee and Fargher, 2013).

4. *Reward* kepada *Whistleblower*

Hasil penelitian dari BPPK (2014) dikatakan bahwa sebagian besar pegawai memilih penghargaan atau *reward* atas pelaporannya pada *whistleblowing system* yaitu berupa mutasi atau rotasi. Selain itu, pegawai juga memilih diberikannya promosi khusus dan pelatihan atau kursus secara singkat. Hadiah atau *reward* berupa uang menjadi pilihan terakhir. Tentu saja motif *reward* dalam penempatan posisi pada jabatan tertentu di dalam organisasi perlu dipastikan bahwa hal tersebut pantas dan tetap meningkatkan perbaikan lingkungan organisasi dalam kinerja pegawai.

Menurut Villena and Villena (2009), tingginya insentif atas *reward* yang diberikan pada para *whistleblower* dapat mendorong adanya agen korupsi atau pengungkap korup, dimana pencapaian atas *reward* akan disalahgunakan untuk mendapatkan keuntungan pribadi saja

2.2.4.2 Red Flags

Mendeteksi *fraud* cukup dini membantu meminimalkan kerugian dan meningkatkan kemungkinan mengatasi kecurangan yang

telah diidentifikasi. Pendeteksian dapat dianggap sebagai pencegah, mencegah kecurangan potensial untuk dilakukan dan membuat organisasi lebih tahan terhadap kecurangan. Melatih dan mendorong karyawan untuk mengenali, merespons, dan melaporkan *red flags* adalah dua cara yang efisien dan efektif untuk mendeteksi kecurangan. Saat melatih karyawan untuk mendeteksi kecurangan, mereka harus diberi tahu bahwa tidak semua orang di dalam atau di luar organisasi jujur dan dapat dipercaya. Terlepas dari kenyataan bahwa sulit untuk menetapkan siapa yang jujur atau tidak hanya dengan melihat mereka, beberapa *red flags* yang dapat membantu mendeteksi kecurangan atau menimbulkan kecurigaan telah ditetapkan. *Red flags* ini dikategorikan sebagai perilaku, transaksional, sistem atau perusahaan (Kimani, 2011).

1. *Red flags* perilaku; Tujuan dan subyektif

Tujuan *red flags* perilaku dapat diukur dan mencakup hal-hal seperti kekayaan berlebihan atau pengeluaran berlebih, hutang yang meningkat, tidak adanya pekerjaan atau kegagalan untuk cuti, perubahan pola kerja, lama tinggal di kantor setelah jam kerja normal dan penggantian berulang prosedur pengendalian normal.

Subyektif *red flags* perilaku biasanya bergantung pada pengetahuan manajer tentang karyawan tersebut. Ini mencakup masalah dengan perjudian atau penggunaan narkoba,

perubahan suasana hati yang berlebihan, agresi, penghindaran, jawaban yang salah dan penolakan untuk menjawab pertanyaan audit atau pertanyaan rutin.

2. *Red flags* transaksional

Informasi yang tersimpan pada sistem komputer, dokumen kertas dan laporan dapat berisi *red flags* transaksional di Bank. Karyawan yang bekerja di area risiko seperti pengadaan atau penggajian harus menerima pelatihan khusus untuk mengenali *red flags* transaksional. Beberapa jenis yang khas meliputi:

- a. *Ghost business partner* yang tidak harus ada tapi menjadi salah satu penyebab utama untuk kegiatan *fraud*
- b. Kurangnya tender yang kompetitif
- c. Pembayaran dilakukan ke akun eksekutif dan akun yang dikendalikan oleh karyawan
- d. Menyembunyikan kepemilikan pihak yang berkepentingan pada pelanggan dan mitra bisnis dengan menggunakan kaskade perusahaan lepas pantai untuk menyamarkan kepemilikan
- e. Pengiriman instruksi yang tidak biasa, misalnya melalui surat atau kurir dengan permintaan pemrosesan yang mendesak
- f. Fotokopi dokumen atau lampiran

- g. Kata atau penjelasan yang tidak perlu pada instruksi untuk membuatnya membuatnya lebih sah
- h. Nama penerima, alamat atau nomor rekening yang salah
- i. Dokumen yang mencurigakan, seperti ID, kartu pembayaran dan paspor; misalnya, foto pada dokumen tidak cocok dengan orang yang hadir dokumen

3. Sistem *red flags*

Bagian IT Bank dapat memainkan peran penting dalam memantau *red flags* di komputer dan sistem komunikasi. Semua karyawan perlu diberi tahu bahwa sistem terus dipantau, namun pemantauan harus dilakukan hanya oleh tim sistem.

Indikator perilaku tidak teratur yang mungkin termasuk sistem *red flags* :

- a. Kontrol atau audit log yang sengaja dimatikan
- b. Seseorang masuk ke sistem dengan menggunakan identifikasi pengguna dan kata sandi sebuah karyawan yang sedang cuti
- c. Jumlah login yang gagal lebih tinggi dari rata-rata
- d. Login pada waktu yang tidak biasa dalam sehari

- e. Mendownload atau bahkan mengirim file berukuran besar informasi perusahaan, terutama ke penerima tidak diketahui.

4. *Red flags* perusahaan

Potensi *red flags* perusahaan yang secara teratur menyebabkan jatuhnya organisasi meliputi:

- a. Keputusan manajemen otokratis seputar hubungan bisnis, seperti penolakan untuk mengubah pemasok utama
- b. Kerugian dan penurunan margin penjualan
- c. Hambatan buatan disiapkan oleh direksi untuk menghindari menjawab pertanyaan
- d. Mengesampingkan kontrol anggaran
- e. Catatan tidak lengkap
- f. Transaksi manual dan penyesuaian yang tidak biasa

Red flags perusahaan bisa dibilang merupakan kelompok tersulit untuk membangun program pendeteksian karena sulit untuk ditafsirkan. Pengalaman dan pelatihan spesialis tim anti *fraud* mungkin diperlukan. Dalam kasus karyawan melihat sesuatu yang mencurigakan, mereka harus melaporkan masalah biasanya melalui manajer lini mereka atau, jika melibatkan manajer lini mereka, melalui prosedur whistleblowing. Begitu kekhawatiran dilaporkan, harus ditindaklanjuti. Jika seorang karyawan disingkirkan oleh

seorang manajer pada saat pertama kali mereka mencoba mengemukakan masalah semacam itu, mungkin saja ini adalah saat terakhir mereka menimbulkan masalah. Setelah sebuah kejadian dilaporkan, bukti harus diperoleh dengan memeriksa rinciannya. Tes deteksi kecurangan harus menganalisis data dan transaksi komputer, indikator yang terkait dengan individu, dokumen dan informasi yang berkaitan dengan pihak ketiga seperti pelanggan, pemasok dan mitra bisnis.

2.3 Penelitian Terdahulu

Dalam penelitian ini, penulis menjelaskan beberapa penelitian terdahulu yang berkaitan terhadap penelitian yang akan dibuat kedepannya. Adapun beberapa penelitian yang berkaitan langsung maupun tidak langsung dengan penelitian yang akan dibahas. Dengan demikian, penulis dapat membandingkan penelitian terdahulu dengan penelitian yang akan ditulis.

Kimani (2011) dalam "*Fraud Risk Assessment Plan for Barclays Bank of Kenya*" menyatakan bahwa sebagian besar kecurangan terdeteksi melalui tip yang dilaporkan oleh karyawan, vendor atau *whistleblower*. Organisasi yang menerapkan pelatihan kesadaran kecurangan di seluruh perusahaan mampu mengurangi kecurangan hingga 52%. Barclays Bank of Kenya, adalah salah satu bank terkemuka di negara ini dan telah beroperasi di Kenya selama hampir 100 tahun. Bank ini sangat dihormati karena kinerjanya yang luar biasa dan citra keseluruhannya. Namun, bank

terus menghadapi kecurangan yang dilakukan oleh karyawannya dan atau pihak ketiga yang tidak dapat dihindarkan. Penilaian risiko *fraud* membantu untuk mengetahui melalui mana kecurangan dilakukan, mencegah kegiatan *fraud* lebih lanjut untuk tidak terjadi dan memberikan panduan penanganan kecurangan untuk melakukan tindakan terhadap pelaku. Jenis kecurangan utama yang diidentifikasi oleh Bank meliputi: pencurian identitas dan penggunaan dokumen hilang atau dicuri, penggunaan kartu palsu, penyuaipan dan benturan kepentingan, pencurian informasi rahasia, *fraud* cek dan transfer dana, dan pencucian uang. Agar Barclays Bank of Kenya dapat mencegah dan mengurangi kecurangan ini seminimal mungkin, tim penilai risiko *fraud* Bank harus mengikuti strategi penilaian risiko *fraud*.

Pada tahap penilaian kecurangan sangat penting untuk mengembangkan budaya anti-*fraud*, dan dapat terlaksana jika mendapat dukungan penuh dari direksi dan manajemen puncak. Semua karyawan Bank harus memahami sepenuhnya dampak yang terjadi akibat adanya kecurangan. Melalui deteksi, banyak *fraud* dapat dicegah. Karyawan dan manajer sama-sama perlu dilatih untuk lebih waspada dalam pekerjaan dan aktivitas mereka. Begitu *red flags* terdeteksi, karyawan perlu segera melaporkannya ke atasan mereka. *Whistleblower* harus dilindungi untuk melindungi identitas dan pekerjaan mereka.

Ermawati (2015) dalam “*Analisa Penerapan Fraud Early Warning System (FEWS) pada Bank ‘X’ di Surabaya*” menyatakan bahwa penyebab

fraud adalah lemahnya sistem pengendalian dan tidak diterapkannya tata kelola perusahaan yang baik. Surat Edaran Bank Indonesia, Nomor 13/28/DPNP Tanggal 9 Desember 2011, Perihal Penerapan Strategi Anti *Fraud* Bagi Bank Umum merupakan upaya untuk sistem peringatan dini atas kasus *fraud* pada industri perbankan. Dalam penerapan FEWS dan sesuai dengan penerapan strategi anti *fraud*, maka sosialisai *e-banking* dapat dilakukan peningkatan dengan sosialisasi melalui media televisi, *monitoring* pegawai melalui program khusus yang diadakan Sistem Kepegawaian dan SDM dapat ditingkatkan dengan adanya *family gathering* yang dikemas dalam bentuk *outbond* sekaligus dapat terlaksananya program *know your employee* dengan mengenal karakter dan cara berpikir pegawai, pengelolaan IT untuk menanggulangi *hacker* dapat ditingkatkan dengan bekerjasama dengan provider dari luar Bank ‘X’, identifikasi kerawanan ditingkatkan dengan adanya pemantauan khusus pada aktivitas yang rawan *fraud*, dan budaya *zero tolerancy for fraud* digalakkan lebih kuat dengan publikasi melalui website Bank ‘X’ maupun adanya mading – mading pada setiap kantor cabang.

BPPK (2014) dalam “*Employee Perceptions of Whistleblowing System, Ethics Code and Values : Empirical Evidence from The Directorate General of Taxes*” mengatakan bahwa adanya *whistleblowing system* pada Direktorat Jendral Pajak (DJP) didukung dengan adanya buku manual kode etik yang menyatakan dengan jelas regulasi persyaratan minimum untuk membenarkan tindakan ilegal atau menyimpang, serta

dengan adanya nilai – nilai kementrian keuangan yang diterjemahan ke dalam peraturan yang jelas. Agar pegawai tidak ragu untuk melaporkan tindakan indikasi kecurangan maka diperlukan pembuatan pernyataan yang jelas untuk para *whistleblower* bahwa adanya perlindungan keamanan seperti dijaga kerahasiaan identitas *whistleblower* dan perlindungan yang memadai dari Kepolisian Negara kepada *whistleblower* beserta keluarganya. Perlindungan terhadap *whistleblower* juga dapat dilakukan dengan membuat saluran komunikasi yang efektif dan hanya dapat diakses oleh pihak independen saja. Untuk meningkatkan independensi *whistleblower system*, maka diperlukan kerjasama dengan agen institusional khusus selain dari karyawan di dalam lingkungan organisasi. Dalam memberikan *reward* kepada para *whistleblower* yang melaporkan tindakan menyimpang di dalam perusahaan, DJP harus berhati – hati karena pegawai lain yang memiliki niat tidak baik pada pelapor dapat saja mengetahui siapa pelapor dan membahayakan keselamatan pelapor. Karena berdasarkan hasil penelitian, *reward* yang diinginkan *whistleblower* yang paling disukai adaah mutasi atau rotasi, lalu promosi khusus, lalu pelatihan atau *short course*, dan opsi terakhir adalah berupa uang.

Baihaque (2016) dalam “*Analisis Peranan Audit Internal dalam Upaya Penerapan Strategi Anti Fraud Bank BPD DIY Yogyakarta*” menemukan bahwa SPI merupakan fungsi yang bertanggung jawab dalam mengawali penerapan strategi anti *fraud* pada Bank BPD DIY Yogyakarta.

Namun dalam penerapannya masih terdapat beberapa hambatan seperti *whistleblowing system* yang belum berjalan optimal dan belum berjalannya upaya *customer awareness*. Hal ini karena banyak pegawai yang belum mengetahui *whistleblowing system* dan hanya melaporkan ke atasannya saja atau bahkan enggan untuk melaporkan.

Dalam Butcovan (2015), yang berjudul “*Banking Security In the Context of International Relations*” menyatakan bahwa, kejahatan dalam sistem perbankan tidak bisa dihentikan. Masalah ini tidak ada habisnya, karena, selama bertahun-tahun fenomena dan metode *fraud* ini telah berevolusi, namun selalu ada. Penelitian ini mengatakan bahwa reputasi dan kemampuan Bank bertahan dalam dunia perekonomian sangat dipengaruhi dengan kemampuan Bank untuk menghadapi dampak adanya kejahatan yang biasa terjadi seperti pencucian uang, pembiayaan terorisme, korupsi atau *fraud*. Hal tersebut dihadapi melalui keamanan sistem perbankan yang ditingkatkan dengan membangun dan meningkatkan kolaborasi antara institusi perbankan, pemerintah dan institusi yang khusus. Salah satu hal penting selanjutnya adalah Bank mengadopsi strategi keamanan nasional. Dapat dikatakan bahwa reputasi dan kemampuan bank untuk tetap berdiri tergantung dari kemampuannya untuk mengatasi tindak kriminal yang melibatkan bank.

Suhartono (2016) dalam “*Komite Anti Fraud: Solusi Menuju Zero Fraud*” menemukan bahwa adanya bahaya *fraud* yang sangat potensial dalam perusahaan, maka sudah menjadi kebutuhan yang sangat mendesak

bagi perusahaan-perusahaan dalam menerapkan strategi anti *Fraud* di lingkungan perusahaan dengan membentuk Komite Anti *Fraud*. Komite Anti *Fraud* diharapkan tercapainya zero *fraud* dalam perusahaan, sehingga kinerja perusahaan akan semakin meningkat dan nilai perusahaan dapat tercapai. Pengetahuan dan pemahaman manajemen risiko yang dimiliki oleh Komite Anti *Fraud* akan sangat dibutuhkan dalam menjalankan tugas dan tanggung jawabnya. Komite Anti *Fraud* harus mampu mengidentifikasi, menilai, dan mengevaluasi risiko-risiko potensial yang dapat muncul dan menjadi gangguan bagi perusahaan, baik akibat faktor internal maupun eksternal. Anggota Komite Anti *Fraud* juga harus memiliki softskill berupa kemampuan komunikasi dan kepemimpinan yang kuat.

Rubasundram (2015) dalam “*Perceived ‘Tone from the Top’ During a Fraud Risk Assessment*” mengatakan bahwa kasus penipuan baru – baru ini mencerminkan bersumber dari *tone from the top*. Tanpa adanya dukungan manajemen puncak dalam menerapkan budaya organisasi untuk mengatasi risiko *fraud*, maka pelaksanaan internal kontrol tidak dapat berjalan efektif. Hal tersebut karena komitmen karyawan akan dijaga hanya jika sikap manajemen puncak kuat untuk memegang komitmennya mencegah tindakan *fraud* dan mematuhi semua kontrol yang ada atau tidak melakukan *management override*, yaitu dengan sengaja tidak mematuhi kontrol internal yang ada. *Fraud Risk Assessment & Management Team* (FRAM) menitikberatkan bahwa tanpa dukungan Direksi atau manajemen

puncak maka keberhasilan implementasi pencegahan *fraud* melalui *whistleblowing* tidak akan berjalan efektif dan pihak Eksekutif hanya akan melakukan *override*.

Usman and Shah (2013) menyatakan dalam “*Critical Success Factors for Preventing e-Banking Fraud*” bahwa masalah keamanan merupakan hambatan utama dalam aktivitas internet banking dan e-commerce, kecurangan disorot sebagai risiko penting yang terkait dengan sistem pembayaran. Keberhasilan langkah-langkah pencegahan *fraud* e-banking memerlukan cara efektif yaitu mengendalikan risiko keamanan. Kurangnya pelatihan yang memadai, komunikasi yang tidak memadai, dan gaya kepemimpinan lemah dari supervisor dan manajer merupakan penyebab kecurangan. Di Inggris, perbankan online telah mengalami 32% penurunan dalam kecurangan dan ini disebabkan oleh peningkatan kesadaran pelanggan dan perangkat lunak deteksi kecurangan di bank. Oleh karena itu menunjukkan bahwa di luar aspek teknologi, kesadaran pelanggan sangat berpengaruh terhadap kecurangan.

Graffney (2014) dalam “*Training for Success : A Comparison of anti-fraud Knowledge Competencies*” mengatakan bahwa *The United States Air Force* (USAF) menemukan bahwa dalam proses pengadaan beragam persenjataan dalam skala besar ketika ditemukan kecurangan maka tim *Air Force Office of Special Investigations* (AFOSI) sebagai lembaga utama yang bertanggungjawab untuk menyelidiki kasus *fraud* melakukan sejumlah program dan pelatihan khusus yang berfokus untuk

pendidikan anti-*fraud* dan kejahatan keuangan yang diselenggarakan oleh *Association of Certified Fraud Examiners (ACFE)*. Program dan pelatihan khusus ini dilakukan dengan menyesuaikan kompetensi pengetahuan minimal yang disyaratkan ACFE dengan kompetensi investigasi AFOSI, sehingga dapat dilakukan proses untuk mendapatkan sertifikasi secara maksimal. Sertifikasi ini bertujuan untuk meningkatkan kompetensi AFOSI dalam menerapkan anti-*fraud* dan membantu proses investigasi kecurangan pengadaan.

Wibisono (2015) dalam "*Pengaruh Reward and Punishment dan Job Rotation terhadap Fraud*" mengatakan bahwa *Reward and Punishment* akan memotivasi pegawai untuk memilih tidak melakukan tindakan *fraud*, karena pegawai lebih memilih memerangi *fraud* dan mendukung kebijakan perusahaan sehingga tidak mendapatkan *punishment* (hukuman). Pemberian *reward* juga sangat penting untuk menghindari tindakan *wrongdoing* yang dilakukan pegawai karena disebabkan ekspektasi pegawai bahwa kurangnya apresiasi dari *top management*. Nilai *reward* yang diberikan tentu saja memiliki manfaat lebih besar dibandingkan jika pegawai melakukan *fraud*. *Job rotation* memberikan pengaruh besar terhadap pegawai untuk tidak melakukan *fraud*, karena pegawai mengetahui bahwa posisi mereka akan digantikan oleh rekan kerja mereka, sehingga dimungkinkan jika pegawai bersangkutan melakukan tindakan *fraud* maka akan diketahui karyawan yang menggantikan.

Beberapa penelitian terdahulu membahas mengenai cara menekan risiko kecurangan dengan mengutamakan tindakan pencegahan dan pendeteksian, dimulai dengan menciptakan budaya anti *fraud*, memperhatikan munculnya *red flags* dan segera melaporkannya melalui sistem *whistleblowing*, kerjasama antara institusi bank, pemerintah dan institusi yang khusus memerangi fenomena kriminal agar mampu menciptakan keamanan sistem perbankan, peningkatan kesadaran potensi kecurangan dan perangkat lunak (teknologi) deteksi kecurangan di bank, meningkatkan komunikasi di dalam organisasi atas kesadaran dampak adanya kecurangan dimulai dari *tone at the top*, adanya pelatihan dan sertifikasi untuk meningkatkan kompetensi agen anti-*fraud*, memberikan *reward*, *punishment* dan *job rotation*, dan bekerjasama dengan IT diluar organisasi dalam penerapan *whistleblowing system*.

Namun, penemuan pada penelitian terdahulu lebih fokus pada Bank yang berada di luar Indonesia sehingga kasus yang diteliti merupakan kasus *fraud* yang terjadi di bank di luar Indonesia, sedangkan untuk kasus di Indonesia yang sesuai dengan regulasi Bank Indonesia membahas mengenai peran Unit Anti *Fraud* terhadap penerapan Strategi Anti *Fraud*. Berdasarkan penelitian terdahulu, penulis ingin meneliti lebih lanjut sejauh mana strategi pengembangan unit anti *fraud* melalui pelatihan, penugasan dan pola rekrutmen SDM dalam proses peningkatan kinerja mendeteksi dan mencegah tindakan *fraud* mampu meminimalkan *fraud*. Serta seperti apa hubungan timbal balik antar SDM yang terjalin dengan SDM

Manajemen Risiko untuk meningkatkan kualitas pendeteksian dan pencegahan *fraud* pada PT Bank BPD DIY.

BAB III

METODOLOGI PENELITIAN

3.1 Pengenalan Bab

Dalam bab ini, peneliti akan menjabarkan metode penelitian yang digunakan dalam penelitian mengenai strategi pengembangan unit anti *fraud* dalam meminimalkan *fraud* yang ada. Pembahasan dalam bab ini akan berhubungan dengan bab selanjutnya, karena bab ini akan menjadi dasar proses penelitian untuk menjawab rumusan masalah yang sudah ditetapkan pada bagian pembahasan. Bab ini menjabarkan mengenai jenis penelitian, instrumen penelitian, fokus penelitian, sistematika penelitian, sumber dan jenis data, pemilihan responden, objek penelitian, teknik pengumpulan data, teknik pengujian keabsahan data dan teknik analisis data dalam penelitian ini.

3.2 Jenis Penelitian

Terdapat dua macam jenis penelitian yang sering digunakan, yaitu penelitian kuantitatif dan penelitian kualitatif. Menurut Sekaran and Bougie (2017) menyebutkan bahwa data kualitatif bersumber dari data primer dan/atau data sekunder, data primer berasal dari wawancara dengan individu. Dengan penelitian kualitatif, peneliti terlibat banyak interaksi secara langsung dengan sumber data sehingga dapat melihat fakta di lapangan. Menurut

Afrizal (2014) dalam penelitian kualitatif akan dilakukan analisis data hasil wawancara berupa kata – kata lisan maupun tulisan serta tingkah perbuatan dari objek penelitian tersebut. Peneliti tidak melakukan analisis terhadap angka sebagai data utama seperti dalam penelitian kuantitatif, namun tetap masih akan diperlukan analisis data berupa angka sebagai penguat argumen atas jawaban rumusan masalah.

Metode kualitatif akan dipilih ketika penelitian bertujuan untuk memahami lebih mendalam atas proses atau pengalaman dimana pemahaman lebih mengenai suatu informasi dibutuhkan dalam menentukan batasan – batasan atau karakteristik masalah yang diteliti atau hanya tersedia informasi berupa non-numerik (seperti, teks atau visual) (Bazeley dan Jackson, 2013). Metode yang digunakan pada penelitian ini adalah metode studi kasus.

Menurut Yin (1981:109) studi kasus adalah :

“...approach permitted a test and comparison of existing theories of knowledge utilization. And, the research was able to extend these theories. Thus, one study created some puzzlement regarding the structural and functional differences among the interorganizational arrangements; only after the case studies were completed was it realized that some of the interorganizational functions had to do with knowledge utilization, but others had to do with intergovernmental affairs.”

Pengertian studi kasus menurut Yin dapat diartikan bahwa pendekatan studi kasus memungkinkan tes dan perbandingan teori – teori yang ada dari pemanfaatan pengetahuan. Dan dengan penelitian mampu memperluas teori – teori ini. Dengan demikian, satu studi menciptakan beberapa konflik

mengenai perbedaan struktural dan fungsional diantara pengaturan antar organisasi; hanya setelah studi kasus selesai akan disadari bahwa beberapa fungsi antar organisasi harus dilakukan pemanfaatan pengetahuan, tetapi yang lainnya harus berhadapan dengan urusan antar pemerintah.

Menurut Creswell, Ivankova and Stick (2006) studi kasus adalah :

“...an exploration of a bounded system or a case over time through detailed, in-depth data collection involving multiple sources of information and rich in context (Merriam 1998). A multiple case study design includes more than one case, and the analysis is performed at two levels: within each case and across the cases (Stake 1995; Yin 2003).”

Pengertian studi kasus menurut Creswell, Ivankova dan Stick dapat diartikan bahwa studi kasus adalah eksplorasi sistem yang dibatasi atau kasus dari waktu ke waktu melalui pengumpulan data mendalam yang melibatkan banyak sumber informasi dan kaya akan konteks. Desain studi kasus yang banyak termasuk lebih dari satu studi kasus dan analisis dilakukan pada dua tingkatan : dengan setiap kasus dan pada seluruh kasus.

Menurut Leavy (2014:456) studi kasus adalah :

“...the methodology we found ourselves exploring, in order to understand how the projects were being implemented, why they had positive effects in some regions of the country and not others, and what the outcomes meant in different socio-political and cultural contexts.”

Pengertian studi kasus menurut Leavy dapat diartikan bahwa studi kasus merupakan metodologi yang membutuhkan eksplorasi lebih mendalam

dengan tujuan memahami bagaimana aktivitas penelitian dilaksanakan, mengapa aktivitas penelitian tersebut memiliki dampak positif di beberapa wilayah negara dan apa hasilnya dalam konteks sosio-politik dan budaya yang berbeda.

Penelitian studi kasus berarti mengidentifikasi topik yang membawa penelitian untuk mengumpulkan dan menganalisis informasi dari berbagai sumber informasi seperti wawancara, observasi dan dokumen, sehingga peneliti dalam penelitian studi kasus biasanya mencari tema atau kategori dari perilaku dan kejadian dibandingkan dengan membuktikan hubungan dengan hipotesis. Peneliti dalam penelitian studi kasus terkadang diperlukan untuk lebih memanfaatkan waktunya dalam lingkungan tempat peneliti melakukan wawancara ataupun observasi (Hancock and Algozzine, 2006).

Berdasarkan penjelasan tersebut, peneliti akan menggunakan metode kualitatif dikarenakan peneliti akan meneliti mengenai strategi pengembangan Unit Anti *Fraud* pada PT Bank BPD DIY. Kemudian, dalam penelitian ini, peneliti membandingkan peraturan yang dikeluarkan oleh Bank Indonesia mengenai Strategi Anti *Fraud* untuk bank umum khususnya pada pilar Pencegahan dan Pendeteksian, dan mengetahui bagaimana peraturan tersebut diterapkan oleh PT Bank BPD DIY. Selain itu, peneliti juga mencari tahu kekurangan dalam penerapan Strategi Anti *Fraud* yang disebabkan kendala yang dihadapi oleh Unit Anti *Fraud* PT Bank BPD DIY dalam menerapkan strategi anti *fraud*, serta memberikan saran peningkatan yang bisa dilakukan oleh Unit Anti *Fraud* dalam membantu meminimalkan *fraud*.

3.3 Instrumen Penelitian

Dalam penelitian kualitatif, instrumen utama yang membantu penelitian adalah peneliti itu sendiri. Peneliti akan melakukan wawancara secara langsung guna memperoleh informasi data yang dibutuhkan. Instrumen pendukung wawancara berupa alat perekam berupa *tape recorder* maupun telepon selular sebagai alat perekam dan alat pengambilan gambar / foto, daftar pertanyaan umum sekaligus mendalam dan dokumen yang diperlukan (Sekaran and Bougie, 2017).

Menurut Leavy (2014), peneliti dianggap instrumen yang paling berpengaruh dalam penelitian kualitatif dan objek penelitian diposisikan sebagai pembawa pengetahuan dan pendukung suatu penciptaan baru. Subjektivitas peneliti serta observasi dan perekaman oleh peneliti atas semua kejadian di lapangan merupakan instrumen pendukung dalam dilakukannya penelitian. Menurut Huberman and Miles (2010) mengatakan bahwa peneliti dalam metode penelitian kualitatif dapat digunakan sebagai instrumen utama.

Menurut Hancock and Algozzine (2006:8) peneliti adalah instrumen utama untuk mengumpulkan data dan menganalisis dalam penelitian kualitatif, peneliti harus menghabiskan waktu di dalam lingkungan yang diteliti.

3.4 Fokus Penelitian

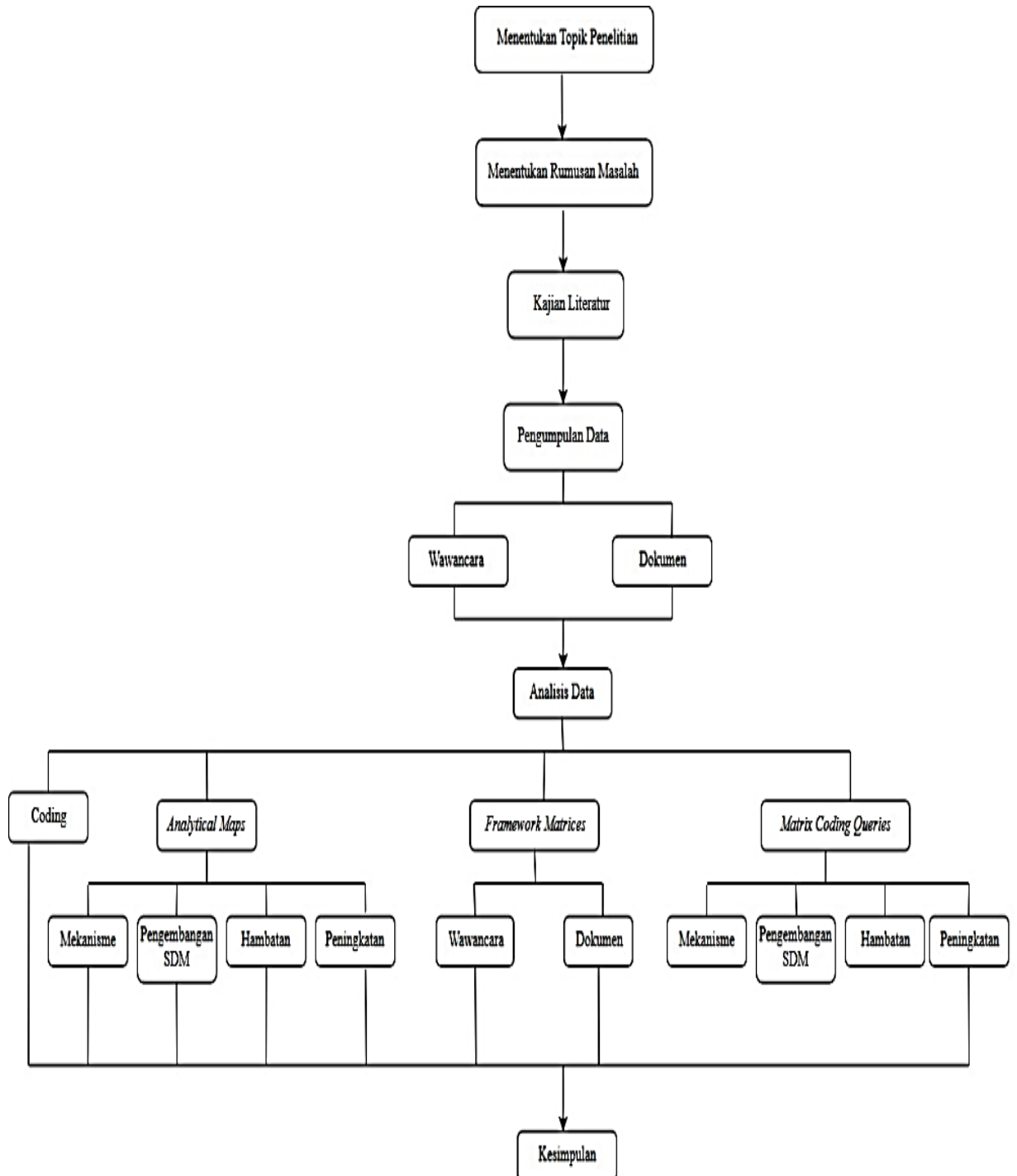
Fokus penelitian ini disusun dalam tujuan membatasi penelitian yang dilakukan agar sesuai dengan tujuan serta rumusan masalah penelitian yang telah ditetapkan. Fokus penelitian kali ini adalah sebagai berikut :

1. Mekanisme penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY pada Desember 2017 hingga April 2018.
2. Pengembangan SDM Unit Anti *Fraud* pada PT Bank BPD DIY dalam mendeteksi dan mencegah adanya tindakan *fraud* sejak Desember 2017 hingga April 2018.
3. Hambatan yang dihadapi Unit Anti *Fraud* pada PT Bank BPD DIY dalam meminimalkan *fraud* sejak Desember 2017 hingga April 2018.
4. Peningkatan yang dapat dilakukan oleh Unit Anti Fraud PT Bank BPD DIY dalam meminimalkan *fraud* untuk tahun 2018 dan kedepannya.

3.5 Sistematika Penelitian

Sistematika penelitian dalam penelitian kualitatif merupakan langkah – langkah penelitian yang dilakukan sejak awal penelitian hingga dapat ditarik kesimpulan. Untuk setiap penelitian yang dilakukan akan memiliki sistematika penelitian yang berbeda dan tidak akan sama sesuai dengan topik masing – masing penelitian. Berikut adalah langkah – langkah penelitian yang dilakukan peneliti :

Gambar 3.1
Sistematika Penelitian



3.5.1 Menentukan Topik Penelitian

Pada langkah pertama penelitian, peneliti mencari topik penelitian dengan cara mengamati berita yang berkaitan dengan Peraturan Bank Indonesia, kemudian peneliti mengamati penelitian terdahulu. Setelah mengamati lebih lanjut objek penelitian yang sesuai kriteria penelitian yaitu Bank yang sudah menerapkan Strategi Anti *Fraud* serta memiliki Unit yang memiliki tanggung jawab penerapan Strategi Anti *Fraud*, kemudian setelah mendapatkan beberapa topik alternatif akhirnya peneliti memutuskan untuk mengangkat topik mengenai penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY.

3.5.2 Menentukan Rumusan Masalah

Kemudian setelah topik telah ditentukan, peneliti menyusun rumusan masalah. Dalam penyusunan rumusan masalah, rumusan masalah haruslah memiliki keterkaitan satu dengan yang lainnya, sehingga rumusan masalah pertama merupakan dasar pembuatan rumusan masalah berikutnya, begitu pun selanjutnya. Peneliti memilih untuk membahas di dalam penelitiannya yaitu mekanisme penerapan Strategi Anti *Fraud*, pengembangan SDM Unit Anti *Fraud*, hambatan yang dihadapi dan peningkatan yang dapat dilakukan dalam meminimalkan *fraud*. Penelitian ini mengacu pada Peraturan Bank Indonesia No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum.

3.5.3 Kajian Literatur

Setelah peneliti menentukan rumusan masalah, peneliti melakukan kajian literatur yang mendasari dilakukannya penelitian ini. Kajian literatur sudah dibahas sebelumnya di dalam BAB II.

3.5.4 Pengumpulan Data

Langkah selanjutnya, peneliti mengumpulkan data, baik berupa data primer maupun data sekunder. Data primer dilakukan dengan melakukan wawancara pada pihak – pihak yang berkaitan dengan penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY. Wawancara adalah bentuk pengumpulan data yang sangat umum dilakukan dalam penelitian studi kasus (Hancock and Algozzine, 2006).

Data sekunder didapatkan melalui dokumen – dokumen yang berisikan kebijakan dan prosedur penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY, namun dokumen ini didapatkan dengan terbatas karena hanya dapat diperoleh dengan cara pengambilan gambar / foto. Hasil wawancara yang didapatkan, lalu peneliti melakukan transkrip berupa rekaman audio dari wawancara yang dilakukan menjadi berbentuk dokumen. Analisis dari dokumen – dokumen adalah metode yang sangat umum digunakan dalam penelitian studi kasus (Hancock and Algozzine, 2006).

3.5.5 Analisis Data

Data – data yang sudah terkumpul kemudian dilakukan analisis untuk menjawab rumusan masalah yang sudah disusun. Selama proses analisis data, jika diperlukan tambahan data untuk menghindari hasil wawancara yang bersifat subjektif maka peneliti kembali melakukan wawancara dengan menambah narasumber, hal ini dilakukan untuk memperkuat validitas data yang telah didapatkan sebelumnya. Analisis data diolah melalui *software* NVivo 11. NVivo membantu peneliti menganalisis data kualitatif seperti gambar, diagram, audio, halaman *website*, dan sumber dokumen lainnya (Bazeley and Jackson, 2013).

Menurut Corbin (2015), dalam penelitian kualitatif memiliki tiga unsur, yaitu data bersumber dari subjek penelitian, analisis data dan interpretasi untuk melakukan *coding*, serta pencatatan ulang transkrip wawancara dan dokumen – dokumen tertulis yang akan melengkapi pembuatan laporan. NVivo banyak digunakan oleh peneliti kualitatif, dimana cara kerjanya memudahkan dalam mengimport teks atau transkrip wawancara, rekaman wawancara dan teks dari kajian pustaka terkait untuk memudahkan membentuk pola hubungan dari semua sumber data kualitatif tersebut. Hal ini karena NVivo sangat memudahkan peneliti menganalisis data kualitatif dengan cara otomatis mencari kata – kata yang mirip dari hasil wawancara dengan teori yang tepat. Namun, untuk pembahasan dan penarikan kesimpulan, semua itu kembali lagi dari kemampuan peneliti itu sendiri

3.5.5.1 *Coding*

Tahap pertama dalam analisis data menggunakan NVivo adalah memasukkan data sebagai *internal sources* berupa dokumen dan audio hasil dari wawancara, peraturan Bank Indonesia, Laporan Tahunan PT Bank BPD DIY dan sumber yang terkait lainnya.

Tahapan ini memuat proses memilih data, mengkode data dan kategorisasi data. Data yang diperoleh dalam penelitian kualitatif akan menghasilkan data yang sangat banyak, sehingga sangat diperlukan reduksi data melalui pengkodean (*coding*) dan kategorisasi (Huberman and Miles, 2010).

Coding adalah proses mengumpulkan seluruh data untuk diolah menjadi data dan diintegrasikan ke dalam sebuah kategori. Kode adalah label atas teks yang akan dikelompokkan ke dalam suatu kategori.. Sebelum membuat *coding*, harus diperhatikan unsur – unsur nya yaitu seperti kata, kalimat, tema bahkan paragraf. Unsur yang sering dipakai adalah tema, hal ini karena ide sebuah tema akan memuat banyak kategori bahkan subkategori didalamnya.

Kategorisasi adalah proses selanjutnya dalam mengolah, menyusun dan klasifikasi hasil dari *coding*. Proses kategorisasi ini sudah dapat membantu peneliti menemukan pola hubungan antar data. Daftar kategori dan subkategori dapat berubah selama proses analisis

data, karena proses analisis data harus dilakukan secara berulang hingga menghasilkan kesimpulan yang valid.

NVivo membantu peneliti mengolah data yang sudah dilakukan *coding* menjadi suatu ide yang mendukung dalam mengatur dan menyediakan akses cepat dalam membuat kategori.

Dalam melakukan proses *coding*, peneliti menggunakan semua *sources* yang ada ke dalam *nodes* sesuai dengan klasifikasi yang dibutuhkan sebagai referensi untuk setiap *nodes*. *Nodes* yang dibuat mengacu pada ke empat rumusan masalah di dalam penelitian ini. *Nodes* merupakan tempat untuk menyimpan semua sumber data yang dijadikan referensi, sehingga peneliti dapat melihat kembali konsep, topik, ide, kasus dan hubungan yang berbeda untuk setiap *nodes* (Bazeley dan Jackson, 2013).

Selain membuat *nodes*, peneliti juga membuat node dalam bentuk *case*. *Case nodes* ini berguna untuk menyimpan seluruh data hasil wawancara dari setiap narasumber yang berbeda, dan setiap *case nodes* diberi nama sesuai nama narasumber. Lalu peneliti membuat *case classifications* yang berisikan informasi terkait narasumber pada setiap *case nodes* yang telah dibuat. *Case classifications* ini berisikan jenis kelamin, umur, pendidikan, jabatan dan masa kerja.

Dan yang terakhir peneliti membuat *relationships* yang menghubungkan setiap *nodes* rumusan masalah sehingga

menunjukkan adanya hubungan antar *nodes*. Dari hasil *relationship*, peneliti bertujuan menunjukkan hubungan antara *nodes* kekurangan yang terjadi dalam penelitian terhadap *nodes* setiap rumusan masalah.

3.5.5.2 *Analytical Maps*

Menyajikan data adalah tahapan lanjutan setelah dilakukan reduksi data melalui proses *coding*. Penyajian data harus dilakukan secara singkat dan terorganisir. Menyajikan data perlu dibuat sedemikian rupa agar memudahkan penarikan kesimpulan, sehingga dapat dilakukan dengan membuat matriks / bagan / grafik, sehingga akan mudah dilihat konsep pola yang berhubungan (Huberman and Miles, 2010). Peneliti membuat *analytical maps*, *matrix coding query*, dan *framework matrices* yang merupakan hasil olahan dari NVivo sebagai bentuk penyajian data.

Kemudian tahap kedua, hasil dari dilakukannya *coding* maka peneliti akan membuat *analytical maps* untuk menggambarkan model penelitian terhadap setiap rumusan masalah yang disusun. Di dalam *maps*, akan dimunculkan *nodes*, *case nodes* dan *relationships* antar *nodes*. Peneliti membuat empat *analytical maps* terkait dengan mekanisme penerapan Strategi Anti *Fraud*, pengembangan SDM Unit Anti *Fraud*, hambatan yang dihadapi Unit Anti *Fraud*, serta peningkatan yang dapat dilakukan Unit Anti *Fraud*. Untuk *maps* yang pertama peneliti memunculkan hubungan dalam penerapan Strategi Anti *Fraud* dengan kekurangan dalam penerapan Strategi Anti *Fraud*.

Untuk *maps* yang kedua peneliti memunculkan hubungan antara pengembangan SDM Unit Anti *Fraud* dengan kekurangan dalam penerapan Strategi Anti *Fraud*. Untuk *maps* yang ketiga peneliti memunculkan hubungan antara kekurangan dalam penerapan Strategi Anti *Fraud* dengan kendala dalam penerapan Strategi Anti *Fraud* yang menyebabkan kekurangan itu muncul. Dan untuk *maps* yang keempat, peneliti memunculkan hubungan antara kendala yang dihadapi dengan peningkatan yang dapat dilakukan oleh Unit Anti *Fraud* atas kendala yang dihadapi Unit Anti *Fraud* tersebut.

3.5.5.3 *Framework Matrices*

Tahap ketiga setelah pembuatan *coding* maka hasil proses *coding* akan disajikan dalam *framework matrices*. Terdapat dua kelompok *framework matrices*, yaitu *framework matrix* wawancara dan *framework matrix* dokumen. *Framework matrix* ini berisikan tabel yang menunjukkan hasil proses *coding* dari semua *internal sources* yang dipakai untuk referensi, dan dikelompokkan menurut hasil wawancara atau dokumen.

3.5.5.4 *Matrix Coding Queries*

Tahap yang terakhir setelah membuat *framework matrices* adalah pembuatan *queries*. Terdapat beberapa pilihan dalam pembuatan *queries*, untuk mendukung penjelasan analisis data yang dilakukan peneliti, maka peneliti menggunakan *matrix coding queries*. Bazeley and Jackson (2013) mengatakan bahwa *matrix coding query*

menghasilkan informasi dalam bentuk tabel untuk menemukan atribut yang di *coding* pada dua atau lebih pada *nodes* yang sama. Tabel tersebut terdiri atas, *row* dan *coloumn*. Peneliti menggunakan *row* berupa dokumen dan hasil wawancara yang digunakan sebagai atribut, serta *coloumn* berupa *nodes*. Nilai yang dimunculkan di dalam tabel harus lebih dari 1, hal tersebut untuk memastikan bahwa atribut berupa *sources* yang di *coding* valid, karena jika nilainya lebih dari 1 maka tidak subjektif. Peneliti membuat empat *matrix coding query* terkait dengan mekanisme penerapan Strategi Anti *Fraud*, pengembangan SDM Unit Anti *Fraud*, hambatan yang dihadapi Unit Anti *Fraud*, serta peningkatan yang dapat dilakukan Unit Anti *Fraud*.

3.5.6 Kesimpulan

Kemudian tahap terakhir dalam sistematika penelitian, peneliti akan menyusun kesimpulan berdasarkan semua data yang sudah didapat dan dianalisis selama penelitian. Kesimpulan ini ditarik setelah menyusun bab pembahasan, kesimpulan berfungsi untuk melihat hasil pembahasan secara garis besar.

Penarikan kesimpulan adalah tahap akhir dalam analisis data. Penarikan kesimpulan ini merupakan proses menjawab rumusan masalah di dalam penelitian, proses ini memerlukan interpretasi pola hubungan dalam *coding* dan membandingkan antar pola hubungan. Penarikan kesimpulan harus diperoleh dari data – data yang dapat dipercaya,

reliabel dan valid. Data yang reliabel atau reliabilitas data itu sangat penting dalam penarikan kesimpulan (Huberman and Miles, 2010).

3.6 Sumber dan Jenis Data

Afrizal (2014) menyebutkan bahwa data yang dipakai dalam penelitian kualitatif contohnya berupa pembicaraan lisan, tulisan dalam notulen rapat, tulisan dalam media, kebijakan pemerintah dan aktivitas yang dilakukan oleh orang. Sumber yang digunakan dalam penelitian kualitatif adalah sumber data primer. Sumber data ini bersumber dari wawancara, observasi dan dokumentasi ke bagian yang bersangkutan dengan topik yang peneliti tentukan.

3.6.1 Sumber Data Primer

3.6.1.1 Wawancara

Dalam penelitian kuantitatif, peneliti sangat membutuhkan teknik pengumpulan data yang mampu menghasilkan data sebanyak-banyaknya. Kemudian peneliti akan melakukan wawancara dan pengumpulan dokumen. Dalam melakukan wawancara secara mendalam, peneliti akan membuat pertanyaan secara umum yang akan dikembangkan sedetail mungkin menjadi pertanyaan berikutnya ketika sedang wawancara maupun setelah wawancara selesai untuk tahapan wawancara berikutnya. Pertanyaan secara umum tersebut akan menjadi pedoman wawancara dan peneliti akan mendapatkan

lebih banyak data karena melakukan wawancara dengan pertanyaan terbuka (Afrizal, 2014).

Moleong (2014) mengatakan bahwa wawancara adalah proses tanya jawab yang mempunyai maksud tertentu antara pewawancara dan orang yang di wawancara.

3.6.2 Sumber Data Sekunder

Sumber data sekunder berasal dari laporan tahunan perusahaan, publikasi peraturan, peraturan pemerintah, artikel jurnal, acara konferensi dan internet. Sumber data sekunder berguna sebagai penguat sumber data primer.

3.6.2.1 Dokumen

Dokumen dapat berupa notulen rapat, peraturan Bank Indonesia, dan Peraturan Perusahaan. Pengumpulan dokumen ini berguna sebagai proses pencocokan kebenaran informasi yang didapat secara lisan serta memiliki tingkat akurasi yang lebih tinggi didukung dengan adanya peraturan, tanggal serta angka di dalam dokumen. Silverman (2013) mengatakan bahwa dokumentasi adalah metode pengumpulan data dengan mempelajari arsip atau dokumen tertulis baik bersumber dari internal maupun eksternal, dapat berupa tulisan, gambar atau karya monumental seseorang.

Peneliti menggunakan dokumen antara lain :

1. Buku Pedoman Perusahaan tentang Strategi Anti *Fraud*

2. Laporan tahunan PT Bank BPD DIY tahun 2016
3. Surat Edaran Bank Indonesia No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum
4. Surat Edaran BI No.9/30/DPNP tanggal 12 Desember 2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum

3.7 Pemilihan Responden

Penelitian ini dalam menentukan sampel menggunakan metode *purposive sampling*. Menurut Leavy (2014) dalam penelitian kualitatif menggunakan sampel bertujuan atau *purposive sample* dimana peneliti secara hati – hati dan berpengetahuan memilih orang yang akan di wawancara. Dalam metode ini peneliti akan menetapkan kriteria subjek penelitiannya sebelum melakukan wawancara, sehingga peneliti akan mendapatkan informasi yang tepat dan *valid*.

Dalam penelitian ini, responden yang diwawancara peneliti berjumlah 8 orang dan memiliki pengetahuan dan pemahaman penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY. Berikut narasumber dalam penelitian ini adalah :

1. Bapak Suwasono Adi selaku Pimpinan Unit Anti *Fraud* bertugas untuk memastikan jalannya seluruh Strategi Anti *Fraud* sesuai Peraturan Bank Indonesia..

2. Bapak Zukhroni Ariffin selaku Staff Unit Anti *Fraud* bertugas untuk melaksanakan tanggung jawab yaitu memastikan seluruh jajaran organisasi mendukung pelaksanaannya Strategi Anti *Fraud*.
3. Ibu Nur Aeni selaku Kepala Risiko Kredit Divisi Manajemen Risiko dan Kepatuhan bertugas untuk memastikan jalannya manajemen risiko dalam upaya pelaksanaan Strategi Anti *Fraud*.
4. Bapak Daryoko selaku Analis Kepatuhan Divisi Manajemen Risiko dan Kepatuhan bertugas untuk melakukan analisis dijalankannya fungsi kepatuhan dalam organisasi.
5. Bapak Andrianto Dwi P. selaku Officer Junior Kepatuhan Divisi Manajemen Risiko dan Kepatuhan bertugas untuk melaksanakan tugas yang diberikan oleh Bapak Daryoko dalam pelaksanaan fungsi kepatuhan.
6. Bapak Muhammad Agus Salam S. selaku Analis Kredit Divisi Manajemen Risiko dan Kepatuhan bertugas untuk melakukan tugas yang diberikan Ibu Nur Aeni dalam memastikan jalannya manajemen risiko dalam upaya pelaksanaan Strategi Anti *Fraud* khususnya analisis kredit.
7. Bapak Pandu Kuncoro selaku Analis Junior Kredit Divisi Manajemen Risiko dan Kepatuhan bertugas membantu jalannya analisis kredit bersama Bapak Muhammad Agus Salam S.
8. Bapak Ivan Nugroho selaku Officer Divisi Manajemen Risiko dan Kepatuhan bertugas untuk melaksanakan tugas yang diberikan oleh

Kepala Divisi Manajemen Risiko dan Kepatuhan untuk memastikan jalannya manajemen risiko dalam upaya pelaksanaan Strategi Anti *Fraud*.

Tabel 3.1
Profil Narasumber

Narasumber	Jabatan	Jenis Kelamin	Masa Kerja	Pendidikan	Umur
Bapak Suwasono Adi Kurniawan	Pimpinan Unit Anti Fraud	Laki - Laki	14 Tahun	S1	41
Bapak Zukhroni Ariffin	Staff Unit Anti Fraud	Laki - Laki	13 Tahun	S1	39
Ibu Nur Aeni	Kepala Risiko Kredit Divisi Manajemen Risiko dan Kepatuhan	Perempuan	27 Tahun	S2	52
Bapak Daryoko	Analisis Kepatuhan Divisi Manajemen Risiko dan Kepatuhan	Laki - Laki	14 Tahun	S1	40
Bapak Andrianto Dwi P.	Officer Junior Kepatuhan Divisi Manajemen Risiko dan Kepatuhan	Laki - Laki	7 Tahun	S1	32
Bapak Muhammad Agus Salam S.	Analisis Kredit Divisi Manajemen Risiko dan Kepatuhan	Laki - Laki	12 Tahun	S1	37
Bapak Pandu Kuncoro	Analisis Junior Kredit Divisi Manajemen Risiko dan Kepatuhan	Laki - Laki	10 Tahun	S1	33
Bapak Ivan Nugroho	Officer Divisi Manajemen Risiko dan Kepatuhan	Laki - Laki	15 Tahun	S1	36

Sumber : PT Bank BPD DIY

3.8 Objek Penelitian

Objek dalam penelitian ini adalah PT Bank BPD DIY, khususnya Unit Anti *Fraud* dan Divisi Manajemen Risiko. Obyek penelitian ini dipilih karena sesuai dengan topik yang dipilih serta berguna untuk memenuhi pertanyaan atas rumusan masalah yang diajukan. Adapun rumusan masalah yang akan diajukan yaitu, bagaimanakah mekanisme penerapan strategi anti *fraud* di Bank BPD DIY, bagaimanakah pengembangan SDM Unit Anti *Fraud* Bank BPD DIY dalam mendeteksi dan mencegah adanya tindakan *fraud* apakah mampu meminimalkan *fraud*, bagaimana kendala apa yang dihadapi dan bagaimana peningkatan yang dapat dilakukan.

3.9 Teknik Pengumpulan Data

Teknik pengumpulan data dengan wawancara dan dokumentasi dapat dilakukan secara individual atau bahkan bersama – sama. Data berupa dokumen akan sangat membantu kelengkapan data yang diambil, karena dokumen adalah bukti fisik dari wawancara yang dilakukan. Teknik pengumpulan data yang dilakukan peneliti adaah sebagai berikut :

1. Untuk memenuhi data mengenai mekanisme penerapan Strategi Anti *Fraud* yang ada di PT Bank BPD DIY maka peneliti melakukan wawancara dengan narasumber yang menjabat sebagai Pimpinan dan Staff Unit Anti *Fraud*.

2. Untuk menghindari data yang subjektif, peneliti juga melakukan wawancara dengan beberapa narasumber yang menjabat di dalam Divisi Manajemen Risiko dan Kepatuhan.
3. Untuk mendukung sumber data primer berupa hasil wawancara, maka peneliti juga memperoleh dokumen yang berkaitan dengan penerapan Strategi Anti *Fraud* yang ada di PT Bank BPD DIY.

3.10 Teknik Pengujian Keabsahan Data

Menurut Guba and Lincoln (1994), penelitian kualitatif melakukan empat kriteria dalam mengevaluasi penelitian kualitatif, yaitu kepercayaan (*credibility*), keteralihan (*transferability*), kebergantungan (*dependability*), dan kepastian (*confirmability*) terhadap pendekatan keabsahan tradisional yaitu *internal validity*, *external validity*, *reliability and objectivity*. Penjelasannya sebagai berikut :

1. Kepercayaan (*credibility*)

Kepercayaan (*credibility*) merupakan elemen yang memungkinkan orang lain untuk mengenali pengalaman yang terkandung dalam penelitian melalui interpretasi pengalaman peneliti, memeriksa keterwakilan data secara keseluruhan, pemeriksaan anggota yang melibatkan kembali peneliti untuk memastikan bahwa interpretasi peneliti adalah representasi akurat dari pengalaman penelitian. Aspek ini untuk menggantikan aspek pada pendekatan tradisional yang sebelumnya sering dipakai untuk uji keabsahan pada penelitian kualitatif, yaitu aspek *internal validity* (validitas internal).

Dalam penelitian ini, peneliti melakukan wawancara kepada narasumber yang benar-benar bertanggung jawab dalam penerapan Strategi Anti *Fraud* yaitu Pemimpin dan Staff Unit Anti *Fraud*. Hal ini dilakukan agar dapat menghasilkan data yang akurat dan *valid*. Narasumber pun tidak hanya dari satu narasumber, sehingga tidak terdapat data yang subjektif.

2. Keteralihan (*Transferability*)

Keteralihan merupakan kemampuan untuk mentransfer hasil penelitian dari satu kelompok ke kelompok lain, deskripsi yang lengkap digunakan untuk memberikan informasi yang terperinci kepada pembaca. Aspek ini menggantikan aspek *external validity* (validitas eksternal) pada pendekatan tradisional.

Pada penelitian ini, peneliti memberikan fasilitas dengan teliti melalui adanya *analytical maps* yang menggambarkan hubungan antar permasalahan yang diteliti dan menjabarkan proses sistematisa penelitian hingga dicapai kesimpulan.

3. Kebergantungan (*Dependability*)

Kebergantungan dapat tercapai ketika peneliti memiliki rekan-rekan peneliti yang berpartisipasi dalam proses analisis. Aspek ini setara dengan aspek *reability* (reliabilitas) pada pendekatan tradisional.

Pada penelitian ini, peneliti mendapatkan evaluasi oleh pembimbing atas proses penelitian yang dilakukan peneliti secara rutin. Peneliti juga melakukan konsultasi dengan beberapa narasumber dalam kaitannya layak atau tidak peneliti mengutarakan suatu saran peningkatan atas kendala yang ada dalam penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY.

4. Kepastian (*Cornfimability*)

Elemen kepastian merupakan sikap kritis terhadap diri sendiri pada bagian dari penelitian tentang bagaimana prasangka sendiri dapat mempengaruhi penelitian. Aspek yang digantikan pada pendekatan tradisional, yaitu aspek *objectivity* (objektivitas).

Pada penelitian ini, peneliti melakukan wawancara tidak hanya kepada satu orang ke divisi yang terkait dengan penerapan strategi anti *fraud*. Hal ini dikarenakan peneliti menghindari adanya jawaban yang subjektif. Selain itu, peneliti juga melibatkan dosen pembimbing sebagai pihak yang memiliki pengetahuan dan pengalaman untuk dilakukannya evaluasi selama proses penelitian agar hasil dari penelitian ini dapat diterima.

Selain itu, untuk memperkuat keabsahan data, peneliti menggunakan teknik triangulasi data. Menurut Moleong (2014) triangulasi adalah teknik pengujian keabsahan data yang memanfaatkan informasi diluar data dan digunakan sebagai

pembandingan terhadap data tersebut. Teknik ini sangat membantu dalam mendapatkan informasi yang valid dikarenakan proses pengumpulan data tidak bias dalam sebuah kelompok namun memperkuat informasi yang didapat. Dalam penelitian kali ini, peneliti menggunakan teknik triangulasi. Triangulasi yang digunakan peneliti adalah triangulasi sumber dan teknik. Teknik tersebut dijelaskan sebagai berikut :

1. Triangulasi Sumber

Triangulasi sumber merupakan cara menguji kredibilitas data dengan memperoleh data dari berbagai sumber. Dalam penelitian ini, untuk mengetahui bagaimana mekanisme Strategi Anti Fraud yang diterapkan PT Bank BPD DIY, peneliti melakukan wawancara kepada beberapa sumber yang ada di dalam subjek penelitian.

2. Triangulasi Teknik

Triangulasi teknik merupakan cara menguji kredibilitas data yang dilakukan dengan cara mengecek data kepada sumber yang sama namun dengan teknik yang berbeda. Dalam penelitian ini, peneliti melakukan wawancara, observasi dan pengecekan dokumen yang dilakukan untuk setiap divisi dan atau tim yang dijadikan objek penelitian, seperti Buku Pedoman Perusahaan tentang Strategi Anti *Fraud*.

Selain digunakan teknik triangulasi, peneliti juga memakai *software* Nvivo dalam melakukan uji keabsahan data. *Software* Nvivo memiliki keunggulan dibanding dengan *software* analisis data kuantitatif lainnya yang membantu peneliti dalam mencari dan menghubungkan sumber *sources* maupun hasil *coding* dengan *nodes*.

1. *Matrix Coding Queries*

Langkah pertama yang dilakukan yaitu peneliti melakukan *matrix coding queries*. *Matrix coding query* berfungsi untuk menemukan kombinasi *item* (biasanya *node* dan atribut) dan menampilkan hasil dalam tabel. Tabel tersebut terdiri atas, *row* dan *coloumn*. Peneliti menggunakan *row* berupa dokumen dan hasil wawancara yang digunakan sebagai atribut, serta *coloumn* berupa *nodes*. Nilai yang dimunculkan di dalam tabel harus lebih dari 1, hal tersebut untuk memastikan bahwa atribut berupa *sources* yang di *coding* valid, karena jika nilainya lebih dari 1 maka tidak subjektif. Peneliti membuat empat *matrix coding query* terkait dengan mekanisme penerapan Strategi Anti *Fraud*, pengembangan SDM Unit Anti *Fraud*, hambatan yang dihadapi Unit Anti *Fraud*, serta peningkatan yang dapat dilakukan Unit Anti *Fraud*. Hasil dari *matrix coding queries* tercantum dalam Lampiran 20 hingga Lampiran 23.

2. *Framework Matrices*

Setelah melakukan *matrix coding query*, peneliti membuat *Framework Matrices* atau kerangka kerja *matrix* berfungsi untuk memetakan apa yang sudah peneliti *coding* di tahap awal. *Framework matrices* dapat mempermudah peneliti dalam membuktikan validitas bahwa apa yang peneliti tulis itu ada datanya. Hasil dari *framework matrices* ini berupa tabel, baris pada tabel sebagai *case node* dan kolom pada tabel sebagai tema dari *node*. Pada penelitian ini, peneliti membuat *framework matrices* yang berisi sumber data wawancara dan narasumbernya. Pada baris tabel berisi narasumber, sedangkan kolom tabel berisi *node* hasil dari proses *coding*. Tabel *framework matrices* yang dibuat peneliti adalah *framework matrix* wawancara dan *framework matrix* dokumen. Hasil dari *framework matrices* tercantum dalam Lampiran 16 hingga Lampiran 19.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pengenalan Bab

Dalam bab ini, peneliti akan menjabarkan hasil penelitian yang dilakukan di PT Bank BPD DIY mengenai strategi pengembangan unit anti *fraud* dalam meminimalkan *fraud* yang ada. Bagian awal bab ini akan menjelaskan profil PT Bank BPD DIY. Selanjutnya peneliti akan menjabarkan jawaban atas rumusan masalah yang telah ditetapkan berdasarkan data yang diperoleh selama penelitian dilakukan. Dan di bagian akhir akan diberikan rekomendasi peningkatan atas jawaban rumusan masalah beserta lampiran transkrip wawancara sebagai sumber data diolah atas jawaban rumusan masalah.

4.2 Profil Objek Penelitian PT Bank BPD DIY

4.2.1 Sejarah Berdirinya PT Bank BPD DIY

Bank BPD DIY didirikan sebagai bank BUMD pada tanggal 15 Desember 1961 dengan nama Bank Pembangunan Daerah Daerah Istimewa Yogyakarta dengan dikeluarkannya keputusan DPRD Provinsi DIY Nomor 11/K/DPRD/1961 kepada Kepala Daerah Provinsi DIY untuk mengusahakan modal sebesar Rp 2.500.000, dan berdasarkan akta notaris Nomor 11, Notaris R.M. Soerjanto Partaningrat, para pihak yang menghadap ke notaris saat pendirian bank adalah Sri Sultan

Hamengkubuwono IX selaku Gubernur DIY dan Sri Paduka Pakualam VIII selaku Wakil Gubernur DIY.

Bank BPD DIY memperoleh surat izin usaha dengan Surat Keputusan Menteri Keuangan Nomor BUM 9/1/27/II Tanggal 5 Maret 1962. Modal dasar Bank BPD DIY sebesar Rp 20.000.000 yang terdiri dari 500 lembar saham prioritas dengan nilai Rp 10.000 dan 1500 lembar saham biasa dengan nilai Rp 10.000. Ketika didirikan ditanam 400 lembar saham prioritas dan 1 lembar saham biasa dengan jumlah uang sebanyak Rp 4.010.000 dan sebesar 62,5% atau sejumlah Rp 2.506.250 telah dibayar tunai dan menjadi modal awal operasional Bank BPD DIY.

Dengan dikeluarkannya Peraturan Daerah, UU Nomor 3 Tahun 1976 tentang Bank Pembangunan Daerah Provinsi DIY, maka Bank BPD DIY ditetapkan sebagai Perusahaan Daerah. Dalam peraturan daerah tersebut diatur bahwa Bank BPD DIY adalah milik pemerintah daerah tingkat I. Pernyataan ini tidak berarti pemerintah daerah tingkat II tidak dapat menyetorkan modalnya. Sebagaimana tercantum pada ketentuan tentang modal, ditetapkan bahwa modal dasar bank sebesar Rp. 500.000.000,- yang terdiri dari penyertaan pemerintah daerah tingkat I dan pemerintah daerah tingkat II.

Namun, dengan dikeluarkannya Peraturan Daerah Nomor 9 Tahun 1985 Bank BPD DIY yang statusnya milik BUMD tingkat I ditiadakan, dan modal dasar bank ditetapkan sebesar Rp 5.000.000.000 (5 miliar). Akhirnya pada tahun 1986 Bank BPD DIY menambah jangkauannya

hingga tingkat kabupaten, dengan membuka Kantor Cabang Wates, Kulonprogo dan Gunungkidul. Lalu pada tahun 1988 Bank BPD DIY membuka Kantor Cabang Bantul dan pada tahun 1990 membuka Kantor Cabang Pembantu Senopati dan Sleman.

Pada tahun 1989 Bank BPD DIY mulai mengembangkan sistem pengolahan data berbasis komputer. Dan pada tahun 1990 kantor cabang telah terkoneksi secara *online* dalam jaringan komputer. Serta pola rekrutmen pegawai mulai diubah dengan seleksi yang ketat serta diadakan pelatihan dasar – dasar perbankan bagi pegawai baru. Pada tahun 2002, Bank BPD DIY menerbitkan kartu ATM yang tergabung dalam jaringan ATM Bersama.

Pada tahun 2012 Bank BPD DIY meningkatkan kualitas pelayanan kepada nasabah untuk mendukung pengembangan ekspor bagi produk – produk kerajinan dan industri kreatif di DIY dengan mengembangkan diri menjadi Bank Devisa. Hal ini dilakukan dengan merubah bentuk badan hukum yang semula perusahaan daerah menjadi perseroan terbatas (PT) seiring dengan dikeluarkannya Peraturan Daerah Nomor 11 Tanggal 26 Desember Tahun 2012. Perubahan ini ditungkan dalam akta pendirian Nomor 2 Tanggal 5 April 2013 yang dibuat didepan Notaris Muhammad Agus Hanafi, S.H melalui Surat Keputusan No.AHU-0044251. AH.01.09 tahun 2013 tanggal 14 Mei 2013 dan diumumkan dalam Tambahan Berita Negara Republik Indonesia tanggal 10 September 2013 No.73. Persetujuan prinsip perubahan bentuk hukum dari Bank Indonesia

berdasarkan surat No.15/1/GBI/ DPIP tanggal 4 September 2013 yang kemudian mendapatkan ijin operasi berdasarkan Keputusan Gubernur Bank Indonesia No.15/121a/KEP.GBI/2013 tanggal 4 Desember 2013, tentang persetujuan pengalihan izin usaha dari Bank Pembangunan Daerah Propinsi Daerah Istimewa Yogyakarta menjadi PT Bank Pembangunan Daerah Daerah Istimewa Yogyakarta.

PT Bank BPD DIY berdasarkan Akta Perubahan Pendirian yang terakhir No 2 Tanggal 5 April 2013 yang disahkan oleh Notaris Muhammad Agus Hanafi, S.H maka komposisi kepemilikan saham adalah sebagai berikut :

Tabel 4.1
Komposisi Kepemilikan Saham Modal Awal
 (*dalam ribuan)

<i>Sum ber : Lap ora n Tah una n PT Ban k BP D</i>	No	Pemilik Saham	Persentase Kepemilikan Saham	Lembar Saham	Nominal
	1	Pemerintah Daerah DIY	38,54%	510*	Rp510.000.000*
	2	Pemerintah Kota Yogyakarta	15,90%	98*	Rp98.000.000*
	3	Pemerintah Kabupaten Sleman	20,15%	98*	Rp98.000.000*
	4	Pemerintah Kabupaten Bantul	11,98%	98*	Rp98.000.000*
	5	Pemerintah Kabupaten Kulonprogo	6,31%	98*	Rp98.000.000*
	6	Pemerintah Kabupaten Gunungkidul	7,11%	98*	Rp98.000.000*
	TOTAL		100%	1000*	Rp1.000.000.000*

DIY Tahun 2016

Sampai dengan akhir tahun 2016 jumlah modal yang telah disetor dan disahkan RUPS adalah sebesar Rp 735.631.000.000 dengan rincian sebagai berikut :

Tabel 4.2
Komposisi Kepemilikan Saham Modal Disetor
 (*dalam ribuan)

No	Pemilik Saham	Persentase Kepemilikan Saham	Lembar Saham	Nominal
1	Pemerintah Daerah DIY	38,54%	283,5	Rp283.500.000
2	Pemerintah Kota Yogyakarta	15,90%	117	Rp117.000.000
3	Pemerintah Kabupaten Sleman	20,15%	148,2	Rp148.200.000
4	Pemerintah Kabupaten Bantul	11,98%	88,155	Rp88.155.000
5	Pemerintah Kabupaten Kulonprogo	6,31%	46,438	Rp46.438.000
6	Pemerintah Kabupaten Gunungkidul	7,11%	52,338	Rp52.338.000
TOTAL		100%	735,631	Rp735.631.000

Sumber : Laporan Tahunan PT Bank BPD DIY Tahun 2016

Dengan komposisi Manajemen PT Bank BPD DIY adalah sebagai berikut

:

Tabel 4.3
Susunan Manajemen

Sumber : Laporan Tahunan PT Bank BPD DIY Tahun 2016

4.2.2 Produk dan Layanan

Dalam menjalankan proses bisnisnya, menurut Laporan Tahunan

Nama	Jabatan
Dewan Komisaris	
Ainun Na'im	Komisaris Utama
Djoko Susanto	Komisaris Independen
Bambang Wisnu Handoyo	Komisaris
Direksi	
Bambang Setiawan	Direktur Utama
Bambang Ghiri Dwi Kuncoro	Direktur Pemasaran dan Usaha Syariah
Cahya Widi	Direktur Umum
Santoso Rohmad	Direktur Kepatuhan
Dewan Pengawas Syariah	
H.M. Thoha Abdurrahman	Ketua
Syafaruddin Alwy	Anggota
Pemimpin Divisi/SPI/UUS/Pemimpin Desk	
Widodo	Divisi Perencanaan dan Pengembangan
Erna Wukiratun	Divisi Trisuri
Nur Iswantoro	Divisi Perkreditan
R. Hangkoso	Divisi Teknologi Informasi
Gamal Kristiyanto	Divisi Sumber Daya Manusia dan Umum
Kustianti	Divisi Manajemen Risiko dan Kepatuhan
Arief Yulianto	Satuan Pengawasan Intern
Muhammad Afnan	Unit Usaha Syariah
CH. Dwiani Surastrati Ati	Pemimpin Desk Administrasi dan Keuangan
Pemimpin Cabang	
Kwartono A. Rachmadi	Cabang Utama
R. Wahyu Wijonarko	Cabang Senopati
R. Agus Trimurjanto	Cabang Sleman
Dian Ariani	Cabang Bantul
Riani Ernastuti	Cabang Wates
Plati Soulistyanti	Cabang Wonosari
Supriyanto	Cabang Syariah

Tahun 2016, PT Bank BPD DIY memiliki beberapa produk Tabungan, Dana, Kredit dan Jasa Layanan.

Produk Tabungan terdiri dari Tabungan Simpeda, Tabungan Sutera, Tabungan Sutera Emas, Tabungan Sutera Istimewa, Tabungan Tunas, Tabungan Shafa, Tabungan Simpel dan Tabungan “Tabunganku”.

Produk Dana terdiri dari GIRO, Simpanan Berjangka, dan Deposito Berjangka Kapitalisasi.

Produk Kredit terdiri dari Kredit Swaguna, Kredit Sindikasi, Kredit Modal Kerja Transaksional/Kelayakan, Kredit Mikro Ekonomi Produktif (KMEP), Kredit Umum Konsumsi, Kredit Pundi, Kredit Multi Usaha, Kredit Mikro Makarya, Kredit Usaha Rakyat (KUR), Kredit Kepemilikan Rumah (KPR), Kredit Ketahanan Pangan dan Energi (KPP-E), Kredit Kepada Masyarakat Koperasi (KRIDAMAS-KOP), Kredit Purnakarya, Kredit SUP-005, Kredit Angkringan (Angsuran Kredit Ringan) dan Kredit Usaha Pembibitan Sapi (KUPS).

Untuk Jasa Layanan, terdapat fasilitas Kartu ATM, Kartu *Flazz*, *Safe Deposit Box* (SDB), E-Samsat & E-POSTI, Bank Garansi, Bancassurance, Pasar Lelang PT Bank BPD DIY, UKM Center PT Bank BPD DIY dan Referensi Bank.

Sesuai komitmennya, hingga tahun 2016, PT Bank BPD DIY memiliki 961 Karyawan, 6 Kantor Cabang, 1 Kantor Cabang Syariah,

31 Kantor Cabang Pembantu, 79 Kantor Kas, 26 *Payment Point*, 6 Kas Mobil, 31 Layanan Syariah dan 109 Terminal ATM.

4.2.3 Struktur Organisasi PT Bank BPD DIY

Struktur Organisasi PT Bank BPD DIY disusun berdasarkan Peraturan Bank Indonesia Nomor 8/4/PBI/2006 tentang Pelaksanaan *Good Corporate Governance* bagi Bank Umum yang diperbarui dengan Peraturan Otoritas Jasa Keuangan (POJK) nomor 55/POJK.03/2016 tanggal 7 Desember 2016 tentang Penerapan Tata Kelola Bagi Bank Umum. Struktur Organisasi PT Bank BPD DIY dalam menjalankan kegiatan operasionalnya memiliki bentuk vertikal. Hal tersebut berarti wewenang mengalir dimulai dari atas kebawah. Sehingga pegawai bertanggungjawab langsung kepada atasannya.

Berdasarkan struktur organisasi, organ tertinggi perusahaan berada pada RUPS (Rapat Umum Pemegang Saham), yang berfungsi sebagai forum bagi para pemegang saham untuk menggunakan haknya, mengemukakan pendapat dan memberikan suara dalam proses pengambilan keputusan yang berkaitan dengan perusahaan. RUPS memiliki kewenangan eksklusif yang tidak diberikan kepada Direksi dan Dewan Komisaris.

Dewan Komisaris adalah organ perusahaan yang bertugas mengawasi dan memberikan nasihat atas kebijakan Direksi dalam menjalankan perusahaan sesuai tujuan perusahaan. Dalam rangka mendukung efektivitas pelaksanaan tugas dan tanggung jawabnya,

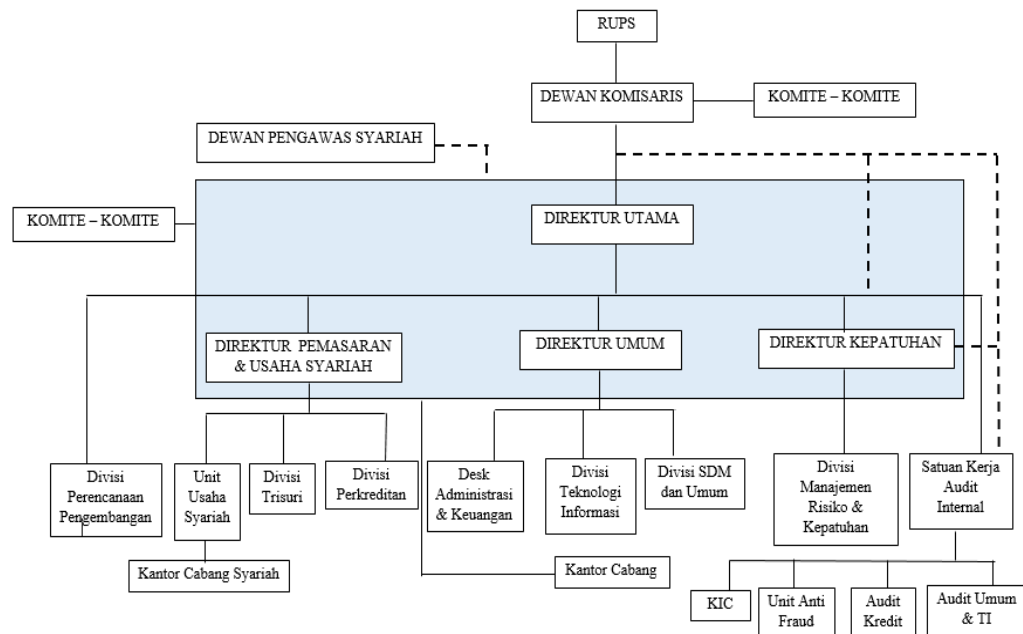
Dewan Komisaris juga membentuk Komite – Komite, terdiri dari Komite Audit, Komite Pemantau Risiko dan Komite Remunerasi dan Nominasi. Komite-Komite merupakan pihak independen yang membantu dan memberi masukan Dewan Komisaris serta memantau dan mengevaluasi kinerja seluruh Direksi.

Direksi merupakan organ perusahaan penting yang bertugas melaksanakan kepengurusan sesuai dengan kepentingan dan tujuan perusahaan termasuk menyiapkan rencana kerja pelaksanaan usaha dan kegiatan Bank yang nantinya dilaporkan ke Dewan Komisaris. Direksi memiliki jumlah anggota 3 orang, terdiri dari Direktur Kepatuhan, Direktur Umum dan Direktur Pemasaran & Unit Syariah. Direksi dipimpin oleh Direktur Utama. Dalam kegiatan operasional, Direksi dibantu oleh Direktur Kepatuhan yang membawahi Divisi Manajemen Risiko & Kepatuhan, lalu Direktur Umum yang membawahi Divisi SDM dan Umum, Divisi Teknologi Informasi, dan Desk Administrasi & Keuangan, serta Direktur Pemasaran & Unit Syariah yang membawahi Divisi Perkreditan, Divisi Trisuri, dan Unit Usaha Syariah.

Garis putus – putus memiliki arti bahwa Direktur Kepatuhan dan Satuan Kerja Audit Intern (SKAI) memiliki hubungan komunikasi dan pelaporan langsung kepada Dewan Komisaris. SKAI dan Divisi Perencanaan dan Pengembangan bertanggung jawab langsung kepada Direktur Utama, dan SKAI merupakan organ perusahaan yang independen.

Gambar 4.1

Struktur Organisasi PT Bank BPD DIY



Sumber : Laporan Tahunan PT Bank BPD DIY Tahun 2016

4.3 Struktur dan Mekanisme Penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY

4.3.1 Gambaran Umum *Fraud* yang Dihadapi PT Bank BPD DIY

PT Bank BPD DIY menurut Aeni (2018), mempersiapkan pencegahan dan pendeteksian *fraud* secara dini didukung dengan adanya Standar Operasional Prosedur (SOP), Pengendalian Internal dan disempurnakan melalui ditetapkannya Strategi Anti *Fraud*.

Dalam adanya jenis *fraud* internal dan eksternal maka dapat digolongkan berdasarkan *fraud* yang dimungkinkan dihadapi sebagai berikut :

1. *Internal Fraud*

Dalam dilakukannya perjalanan dinas atau adanya serifikasi maupun pelatihan keluar kota, maka semua proses mulai dari menghubungi pihak ketiga, pembelian tiket pesawat, hingga *booking* hotel akan dilakukan oleh pihak SDM. Bahkan untuk menghindari *refund* tiket maka setiap pegawai akan diminta menyetorkan nomer *boarding passed* (Kurniawan, 2018).

Dalam pengamanan teknologi semua dilakukan oleh tim Teknologi Informasi PT Bank BPD DIY, seperti tidak bisa di aksesnya *flashdisk* jika dimasukkan ke *laptop*, tidak bisanya penggunaan *wifi* dari luar dan termasuk pembuatan serta pengamanan *whistleblowing system*. Hal ini untuk kedepannya dapat dimungkinkan beberapa karyawan Teknologi Informasi mengakses informasi rahasia untuk kepentingan pribadi Kurniawan, 2018).

Untuk pengamanan aset perusahaan, Kontrol *Intern* Cabang (KIC) melakukan *surprise audit* kepada cabang tidak hanya berupa uang namun juga inventaris seperti HVS, alat tulis, buku tabungan, surat berharga dan materai (Kurniawan, 2018).

Untuk pemalsuan cek, konflik kepentingan, pemalsuan slip gaji dan kecurangan yang dilakukan oleh *teller*, selama ini tidak pernah terjadi karena sudah dilaksanakannya SPI secara benar (Kurniawan, 2018; Aeni, 2018).

2. *External Fraud*

PT Bank BPD DIY menurut Aeni (2018), mengalami salah satu tindakan merugikan bank yang mengindikasikan *fraud* yaitu adanya pemberian data palsu yang diberikan oleh nasabah dalam salah satu transaksi kredit.

Nasabah juga pernah memiliki pengaduan kepada PT Bank BPD DIY yaitu berkurangnya saldo tabungannya, namun setelah ditelusuri menggunakan rekaman CCTV ditemukan bahwa pihak yang melakukan penarikan uang tersebut adalah anggota keluarganya sendiri (Aeni, 2018).

Dalam kasus *skimming* yang baru – baru ini dihadapi oleh beberapa Bank, PT Bank BPD DIY juga menjadi korban, *skimming* ini dipasang bukan di ATM PT Bank BPD DIY namun ketika nasabah PT Bank BPD DIY melakukan transaksi menggunakan ATM Bersama pada ATM Bank lain (Aeni, 2018).

Untuk adanya *money laundering*, menurut Bapak Kurniawan (2018), pernah didatangi pihak KPK untuk memastikan apakah terdapat daftar nasabah yang terkena kasus *money laundering* memiliki rekening di PT Bank BPD DIY, tetapi penanganan untuk *money laundering* akan dilaksanakan oleh fungsi kepatuhan dengan prinsip Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU & PPT).

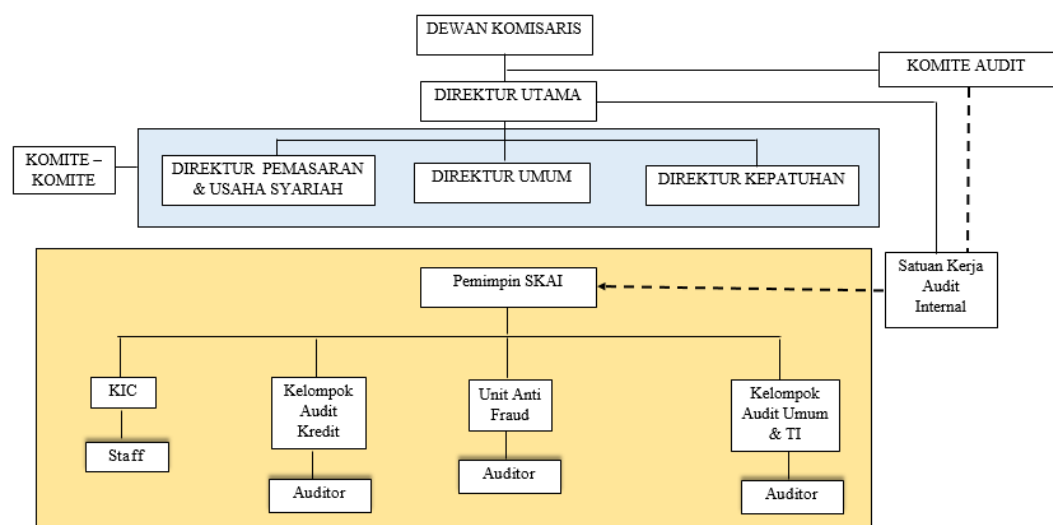
4.3.2 Struktur Organisasi Unit Anti *Fraud* PT Bank BPD DIY

Dalam meningkatkan efektivitas pelaksanaan strategi anti *fraud*, menurut Surat Edaran BI No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum, maka Bank wajib membentuk unit atau fungsi di dalam struktur organisasi Bank yang bertugas menangani penerapan strategi anti *fraud*. Pembentukan unit atau fungsi ini disertai wewenang dan tanggung jawab yang jelas dan langsung bertanggung jawab kepada Direktur Utama serta memiliki hubungan komunikasi dan pelaporan langsung kepada Dewan Komisaris. Berdasarkan hasil wawancara dengan narasumber, PT Bank BPD DIY telah membentuk unit kerja khusus yang bernama Unit Anti *Fraud*. Dikemukakan oleh Bapak Suwasono Adi Kurniawan (2018) bahwa pembentukan Unit Anti *Fraud* sudah direncanakan dibentuk pada tahun 2016 dan pada awal tahun 2017 sudah mulai melakukan tugasnya, di dalam organisasi. Unit Anti *Fraud* berada dibawah SKAI dengan Bapak Suwasono Adi Kurniawan sebagai Pemimpin Unit Anti *Fraud* dan Bapak Zukhroni Ariffin sebagai staff Unit Anti *Fraud*.

SKAI melalui Pemimpin SKAI diawasi dan memiliki hubungan komunikasi langsung dengan Komite Audit dan Dewan Komisaris, serta memiliki tanggung jawab langsung kepada Direktur Utama. SKAI dalam menjalankan tugasnya membawahi 4 unit yaitu Kelompok Audit Umum & Teknologi Informasi, Kelompok Audit Kredit, Unit Anti *Fraud* dan Kontrol Intern Cabang (KIC). KIC

bertugas seperti SKAI tetapi di kantor cabang, KIC terdapat di setiap kantor cabang, dan untuk kantor cabang besar akan terdiri dari 2 orang staff. Ke empat unit dibawah SKAI memiliki tanggung jawab langsung kepada Pemimpin SKAI.

Gambar 4.2
Struktur Organisasi Unit Anti *Fraud* PT Bank BPD DIY



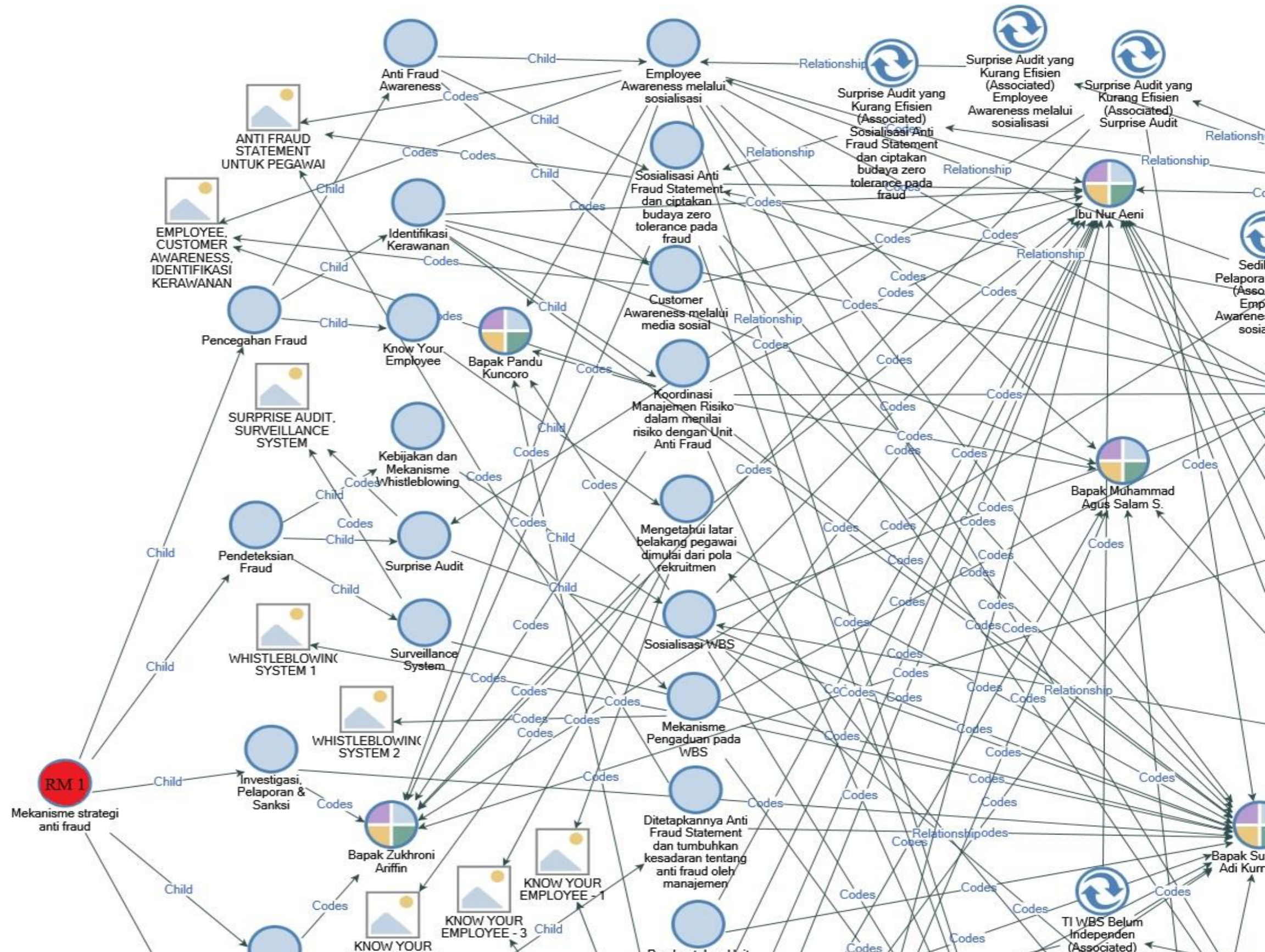
Sumber : Dokumen Unit Anti Fraud PT Bank BPD DIY

4.3.3 Analisis Mekanisme Penerapan Strategi Anti *Fraud* PT Bank BPD DIY

Penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY memiliki 4 pilar yaitu Pencegahan, Deteksi, Investigasi, Pelaporan, dan Sanksi serta Pemantauan, Evaluasi, dan Tindak Lanjut. Hal tersebut sesuai dengan Surat Edaran BI No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum. Mekanisme penerapan strategi anti *fraud* pada PT Bank BPD DIY akan dijelaskan menggunakan peta hasil olahan dari aplikasi NVivo seperti gambar dibawah ini :

Gambar 4.3

Analytical Maps Mekanisme Penerapan Strategi Anti Fraud PT Bank BPD DIY



Dalam menjalankan Strategi Anti *Fraud*, PT Bank BPD DIY telah memiliki Buku Pedoman Perusahaan yang menjadi acuan dalam mekanisme penerapan Strategi Anti *Fraud*. Berdasarkan kebijakan dan mekanisme penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY, mekanisme penerapan strategi anti *fraud* dimulai dari proses pencegahan *fraud*. Pilar pencegahan *fraud* mencakup 3 proses untuk mengurangi potensi terjadinya *fraud* yaitu ; *Anti Fraud Awareness*, Identifikasi Kerawanan dan *Know Your Employee* (KYE). Pilar kedua adalah Deteksi *fraud*. Proses deteksi *fraud* mencakup 3 proses yaitu Kebijakan dan Mekanisme *Whistleblowing system*, *Surprise Audit* dan *Surveillance System*. Pilar ketiga adalah Investigasi, Pelaporan, dan Sanksi. Dan pilar yang terakhir adalah Pemantauan, Evaluasi dan Tindak Lanjut.

Penerapan Strategi Anti *Fraud* merupakan bagian dari pelaksanaan Manajemen Risiko. Oleh karena itu, di dalam penerapan Strategi Anti *Fraud* sudah pasti terdapat penerapan manajemen risiko yang merupakan pendukung dan penguat dalam proses mengendalikan *fraud*. Cakupan dalam Manajemen Risiko yang dibutuhkan dalam penerapan Strategi Anti *Fraud* yaitu ; Pengawasan Aktif Manajemen, Struktur Organisasi dan Pertanggungjawaban, serta Pengendalian dan Pemantauan.

Untuk mekanisme penerapannya secara umum sendiri peneliti menemukan kekurangan yang terdapat dalam proses penerapan

mekanisme tersebut. Kekurangan yang berhubungan dengan pilar pencegahan terdapat pada proses *Anti Fraud Awareness* dan *Know Your Employee*. Kekurangan yang berhubungan dengan pilar deteksi terdapat pada proses Kebijakan dan Mekanisme *Whistleblowing system* dan *Surprise Audit*. Dan untuk pelaksanaan Manajemen Risiko terdapat kekurangan yang berhubungan terhadap proses Pengendalian dan Pemantauan. Peneliti akan menjelaskan lebih rinci mengenai mekanisme penerapan Strategi Anti *Fraud* pada setiap pilar termasuk penerapan Manajemen Risiko.

4.3.3.1 Pilar Pencegahan pada Analisis Mekanisme Penerapan Strategi Anti *Fraud* PT Bank BPD DIY

1. *Anti Fraud Awareness*

Menurut Kurniawan (2018) pencegahan *fraud* yang pertama dimulai dari dalam organisasi, yaitu menumbuhkan *anti fraud awareness*. *Anti fraud awareness* tumbuh melalui sosialisasi budaya *anti fraud*. Sosialisasi tersebut selain untuk semua pegawai juga oleh dikenalkan kepada para nasabah. Pernyataan mengenai *Anti Fraud Awareness* terkait *Employee Awareness* dan *Customer Awareness* juga terdapat pada Lampiran 12.

a. *Employee Awareness*

Daryoko (2018) mengatakan proses *Employee Awareness* dilakukan melalui sosialisasi rutin setiap 3 bulan

sekali terhitung setelah adanya pegawai baru yang masuk. Sosialisasi dilakukan melalui pendidikan yang diisi oleh Unit Anti *Fraud*, pendidikan yang dilakukan terlebih dahulu untuk semua pimpinan, lalu untuk seluruh pegawai. Selain melalui pendidikan, sosialisasi juga dilakukan dengan diwajibkannya setiap pegawai menampilkan pada *desktop* komputer maupun laptop mereka berupa gambar yang berisikan konten mengenai anti *fraud* (Kurniawan, 2018) . Jika pegawai tidak menerapkan kesadaran untuk memerangi adanya *fraud* di dalam perusahaan maka akan menimbulkan dampak berupa kekurangan penerapan strategi anti *fraud*, yaitu berhubungan dengan sedikitnya pelaporan indikasi *fraud* ke *Whistleblowing system* (WBS) serta pelaksanaan *Surprise Audit* yang kurang efisien, karena jika antar teman dari kantor pusat dan kantor cabang saling kenal lalu memberitahu temannya bahwa unit bersangkutan akan dilakukan *surprise audit*, maka unit itu akan mempersiapkan diri dan kemungkinan ditemukan aktivitas yang tidak wajar lebih kecil, dan hal tersebut adalah wujud dari kurangnya kesadaran pegawai dalam menjaga konsistensinya terhadap *zero tolerance* atas *fraud*.

- b. Sosialisasi Anti *Fraud Statement* dan Ciptakan Budaya *Zero Tolerance* pada *Fraud*

Proses Sosialisasi *Anti Fraud Statement* dan Ciptakan Budaya *Zero Tolerance* pada *Fraud* dilakukan oleh Unit *Anti Fraud* melalui kampanye sosialisasi budaya anti *fraud*, kampanye ini artinya adalah keliling setiap cabang, dimulai dari cabang pembantu hingga kantor kas (Kurniawan, 2018). Materi sosialisasi melalui kampanye dan pendidikan kurang lebih sama yaitu memberikan ilmu setiap aktivitas dimana letak paling rawan terjadinya *fraud*, penyebab *fraud* secara teori maupun hasil survey. Sosialisasi *Anti Fraud Statement* dilakukan karena hal ini merupakan kebijakan baru dimana pegawai seluruh jajaran organisasi menandatangani *Anti Fraud Statement*. Jika seluruh jajaran organisasi juga tidak menerapkan secara sungguh – sungguh dengan niat yang baik atas *Anti Fraud Statement* yang ditandatangani nya, maka akan menimbulkan dampak berupa kekurangan penerapan strategi anti *fraud*, yaitu berhubungan dengan sedikitnya pelaporan ke *Whistleblowing system* (WBS) serta pelaksanaan *Surprise Audit* yang kurang efisien. Jika pegawai tidak menjaga komitmennya dalam melaksanakan semua kewajibannya yang sudah tertuang dalam *Anti Fraud Statement*, maka kedua hal tersebut dapat terjadi.

c. *Customer Awareness*

Customer Awareness melalui Media Sosial dilakukan melalui website di www.bpddiy.co.id serta diadakan *gathering* untuk nasabah – nasabah dan nanti didalamnya akan diberikan materi mengenai pelaksanaan strategi anti *fraud* yang dilakukan bank serta memperingatkan customer untuk selalu waspada saat menarik uang di ATM, dengan tidak memberikan pin ATM bahkan kepada anak sendiri serta sebelum melakukan transaksi perlu dilakukan pengecekan apakah ada *skimmer* atau tidak (Aeni, 2018).

2. Identifikasi Kerawanan

a. Koordinasi Manajemen Risiko dalam Menilai Risiko dengan Unit Anti *Fraud*

Proses yang kedua adalah Identifikasi Kerawanan yang merupakan proses manajemen risiko. Proses ini juga dilakukan dengan melakukan koordinasi dengan pihak Manajemen Risiko dalam melakukan tugasnya menilai risiko dengan Unit Anti *Fraud*. Untuk identifikasi kerawanan sendiri pada dasarnya sudah diterapkan didalam SOP setiap aktivitas bank, dimana terdapat mitigasi risiko apa saja yang memerlukan perhatian (Salam, 2018). Ketika melakukan audit juga dilakukan *risk based audit*, sehingga titik rawan setiap aktivitas yang menimbulkan risiko tertinggi juga sebagai perhatian. Unit Anti *Fraud* melakukan identifikasi kerawanan

dengan melihat mitigasi pada setiap Standar Operasional Prosedur (SOP) pada setiap aktivitas bank.

Proses manajemen risiko untuk mengidentifikasi, menganalisa dan menilai proses potensi risiko terjadinya fraud dilakukan terhadap seluruh aktivitas yang menimbulkan risiko. Dilakukan oleh masing – masing unit kerja, seperti unit pelayanan, unit kredit, dan administrasi kredit (Kurniawan, 2018). Contohnya seperti ini :

Pada risiko operasional dimungkinkan internal fraud :

- 1) Penerbitan kartu debit palsu oleh karyawan
- 2) Menerbitkan kartu ATM tanpa persetujuan pejabat yang berwenang
- 3) Pencurian informasi kartu ATM oleh karyawan
- 4) Penarikan dana oleh karyawan dengan kartu ATM palsu

Mitigasi nya :

- 1) Sosialisasi budaya risiko pada karyawan
- 2) Sosialisasi nilai perusahaan
- 3) dst

Eksternal fraud :

- 1) Pemalsuan kartu / *hacking*
- 2) Penarikan dana ATM
- 3) *Skimming*

Mitigasi nya :

- 1) Edukasi terhadap nasabah

- 2) Memberikan pengetahuan yang cukup kepada nasabah saat membuka rekening
- 3) Pengamanan mesin ATM
- 4) Asuransi terhadap mesin ATM
- 5) Pengamanan sistem

Menurut Aeni (2018), Unit Anti *Fraud* sangat terbantu dengan melihat laporan hasil analisis penilaian risiko oleh Manajemen Risiko setiap triwulan yang diperlukan identifikasi lebih jauh, biasanya setelah dilakukan penilaian risiko oleh manajemen risiko maka manajemen risiko akan meminta SKAI untuk melanjutkan proses audit pada risiko yang diperlukan, lalu jika memang temuan indikasi *fraud* perlu ditindaklanjuti, maka SKAI akan membuat surat tugas ke Unit Anti *Fraud* (Daryoko, 2018).

Manajemen Risiko memberikan format penilaian risiko yang perlu menjadi perhatian kepada tiap divisi di pusat maupun kantor cabang untuk diberikan kepada manajemen risiko sehingga terdapat komunikasi dua arah dan memperkuat keabsahan analisis manajemen risiko (Kuncoro, 2018). Format tersebut dinamakan kuisisioner kerawanan, namun dalam pembuatannya Unit Anti *Fraud* juga ikut membuat. Berikut isi dari kuisisioner kerawanan :

- 1) Apakah ada pemberian kepercayaan berlebih kepada karyawan tanpa pemberian kerja yang efektif

- 2) Apakah unit terkait memiliki pengalaman kejadian *fraud* di masa lalu

Untuk mendeteksi penyebab karyawan melakukan *fraud*, maka akan berpedoman pada teori *fraud triangle*, yaitu *pressure, opportunity, rationalization*. Berikut isinya :

- 1) Apakah ada karyawan yang bekerja dibawah tekanan, *stress*, mengalami krisis keuangan, hutang atau masalah pernikahan dan siapa
- 2) Apakah ada karyawan yang membutuhkan uang yang besar karena sakit parah, suka mabuk, dsb
- 3) Apakah ada karyawan yang suka mengeluh atau *complain*
- 4) Apakah ada *conflict of interest* sesama rekan
- 5) Apakah ada *critical issue* yang meresahkan tentang pengurangan karyawan atau tidak akan bagi THR, padahal sebenarnya baik – baik saja, hanya membuat keresahan
- 6) Apakah ada karyawan yang kurang atau tidak patuh terhadap kode etik
- 7) Apakah ada perubahan kepribadian karyawan yang mencolok
- 8) Apakah ada karyawan yang kampanye

Penilaian dilakukan periodik setahun sekali. Kepala unit kerja di pusat dan cabang yang akan melakukannya, dan hal ini ini bersifat rahasia dan terbatas. Pengisian kuisioner ini menggunakan *scoring*, skor 0 – 6 dianggap *low*, skor 25 -30 dianggap *high*, sehingga dapat diketahui potensi terjadinya fraud atas masing – masing kerawanan akan masuk ke dalam kelompok apa.

Menurut Kurniawan (2018) proses identifikasi ini dikenal dengan *three line of defense*, jadi menghadapi risiko yang pertama dimulai dari *front office* saat berhadapan dengan nasabah. Yang kedua yang mengawasi mereka itu adalah manajemen risiko. Lalu yang ketiga itu setelah dilakuksn audit oleh SKAI, lalu Unit Anti *Fraud* menindaklanjuti apa yang menjadi laporan SKAI. SKAI akan membuat rencana audit dalam setahun kedepan itu dasarnya adalah penilaian risiko dari manajemen risiko, dinamakan *business plan*. Jika memang tidak ada indikasi *fraud* yang signifikan, maka SKAI tidak akan meminta Unit Anti *Fraud* menindaklanjuti temuan, hanya akan ada audit operasional oleh SKAI saja.

3. *Know Your Employee (KYE)*

Proses yang ketiga adalah *Know Your Employee (KYE)* yang dilakukan dengan mengetahui latar belakang pegawai mulai dari proses rekrutmen. Kebijakan dan prosedur mengenai KYE sudah

tercantum di dalam BPP Anti *Fraud*, yang melakukan *know your employee* itu adalah divisi SDM (Kurniawan, 2018). Hasil pelaksanaannya dilaporkan kepada Direktur Utama lalu ditembuskan ke Unit Anti *Fraud* dan Manajemen Risiko. Proses rekrutmen dalam menilai setiap calon pegawai memiliki standar minimal mencakup kompetensi, psikologis, dan sebagainya. Menurut Kurniawan (2018) kebijakan penilaian calon pegawai juga melalui penilaian karakter pegawai melalui *asesment*. Seperti pendidikan, pelatihan yang pernah diikuti, pengalaman bekerja atau lamanya bekerja di pekerjaan sebelumnya, kepribadian pegawai, penghargaan yang pernah diterima, sanksi yang pernah diterima, informasi terkait anggota keluarga, rekening pegawai yang dimiliki di Bank BPD DIY, hubungan kekerabatan pegawai dengan pegawai lainnya seperti anak, bapak, ibu, suami dan istri, jika terdapat hal yang melanggar ketentuan maka akan menjadi perhatian khusus. Hasil *asesment* ini berguna sebagai profil pegawai. Aeni (2018) mengatakan proses KYE juga melalui proses berupa informasi debitur (*indeb*) pegawai yang disediakan oleh OJK dan akan dilakukan saat seleksi penerimaan. SDM menelusur apakah calon pegawai tersebut mempunyai kredit macet atau tidak. Untuk proses *Know Your Employee* yang dilakukan Unit Anti *Fraud* sendiri dilakukan dengan menganalisis adanya laporan dari setiap pimpinan divisi untuk melaporkan setiap tindakan menyimpang bawahannya.

Kekurangannya adalah belum adanya rekrutmen untuk Unit Anti *Fraud*, hal ini tentu saja dikarenakan unit tersebut baru terbentuk di awal tahun 2017. Hubungannya dengan proses KYE adalah jika akan melakukan rekrutmen, diperlukan persyaratan dengan kualifikasi bersertifikasi Anti *Fraud* Examiner akan dipertimbangkan, hal ini bertujuan agar SDM Unit Anti *Fraud* dapat diatasi dengan segera menambah personil yang kompeten. Pernyataan mengenai *Know Your Employee* juga terdapat pada Lampiran 13.

4.3.3.2 Pilar Deteksi pada Analisis Mekanisme Penerapan Strategi Anti *Fraud* PT Bank BPD DIY

1. Kebijakan dan Mekanisme *Whistleblowing system* (WBS)

Pilar deteksi *fraud* dilakukan pertama kali melalui proses Kebijakan dan Mekanisme *Whistleblowing system* (WBS). Kebijakan WBS sendiri mencakup diadakannya Sosialisasi WBS kepada para pegawai serta terdapat Mekanisme tersendiri dalam penerapan WBS.

a. Mekanisme Pengaduan pada *Whistleblowing system* (WBS)

Untuk proses Mekanisme Pengaduan pada WBS sendiri semua diatur di dalam Buku Pedoman Perusahaan tentang Strategi Anti *Fraud*, dan sudah dilakukan sebelum Unit Anti *Fraud* terbentuk yaitu sejak tahun 2012 melalui Surat Keputusan

Direksi Nomor 001/KPTS/DP/2012 (PT Bank BPD DIY, 2016). Kurniawan (2018) mengatakan bahwa *whistleblowing system* difasilitasi oleh jaringan intranet di dalam bank yang hanya dapat di akses oleh pegawai saja. Untuk mengakses nya dapat membuka wbs.intranet.co.id, antar cabang juga tentu saja dapat membukanya. Untuk sekarang yang bertanggung jawab adalah Direktur Utama serta yang diperbolehkan membuka akses hanya Pimpinan SKAI dan Pimpinan Manajemen Risiko. Setelah kedua *key user* tersebut menganalisis laporan yang ada dalam WBS, maka mereka akan membuat laporan yang diteruskan ke Unit Anti *Fraud* hanya jika terdapat kejadian tidak wajar yang perlu ditindaklanjuti. Untuk para pelapor ke WBS, akan dijamin kerahasiaan identitasnya, sehingga Unit Anti *Fraud* juga tidak tahu siapa pihak yang melaporkan. WBS ini hanya berlaku untuk pihak *internal*, untuk pihak eksternal hanya difasilitasi adanya layanan pengaduan nasabah serta melalui surat kaleng (Aeni, 2018). Untuk tindakan yang dapat dilaporkan itu yang memenuhi beberapa atau satu kriteria yaitu :

- 1) Termasuk kategori pelanggaran, pelanggaran hukum, perbuatan tidak etis di dalam lingkungan PT Bank BPD DIY
- 2) Laporan terjadi paling lama 2 tahun sejak tanggal pelaporan

b. Sosialisasi *Whistleblowing system* (WBS)

Proses Sosialisasi WBS sendiri bertujuan menumbuhkan kesadaran pegawai pentingnya menjaga kesehatan bank dengan ikut berpartisipasi melaporkan tindak kecurangan maupun tindak tidak etis yang ada di dalam lingkungan bank. Proses sosialisasi yang diperlukan untuk seluruh jajaran organisasi adalah cara mengakses WBS, kriteria dan jenis *fraud* yang dilaporkan, serta dampak yang terjadi baik bagi perusahaan maupun tiap pegawai jika membiarkan tindak *fraud* tidak diatasi (Daryoko, 2018). Sosialisasi ini dilakukan sama halnya dengan sosialisasi *fraud awareness* yaitu 3 bulan sekali (Aeni, 2018). Namun, tetap terdapat kekurangan dalam proses sosialisasi WBS, yaitu Sedikitnya Pelaporan ke WBS. Hal ini masih menjadi bahan kajian Unit Anti *Fraud*. Untuk sosialisasi WBS memang belum mendapat perhatian para pegawai dapat dimungkinkan hal tersebut yang menjadi alasan sedikitnya partisipasi WBS.

2. *Surprise Audit*

Proses *Surprise Audit* dilakukan baik di kantor pusat maupun di kantor cabang. Kurniawan (2018) mengatakan bahwa Kontrol Intern Cabang (KIC) merupakan kaki tangan SKAI yang ada di setiap cabang. Mereka dapat membantu proses *surprise audit* yang sekarang menjadi tanggung jawab Unit Anti *Fraud*. KIC dapat melakukan *surprise audit* kapan saja dan KIC merupakan pihak independen di

kantor cabang. Pada dasarnya KIC adalah pegawai kantor pusat, dengan gaji seperti pegawai kantor pusat namun ditempatkan di cabang – cabang. KIC juga merupakan seorang auditor, namun tidak melakukan aktivitas operasional cabang. KIC akan melaporkan hasil *surprise audit* nya langsung kepada SKAI dan Unit Anti *Fraud* di kantor pusat. Unit Anti *Fraud* sendiri juga pasti melakukan *surprise audit*, namun tidak seperti KIC yang dapat setiap saat dilakukan. Pelaksanaan *Surprise Audit* harus diperhatikan dengan benar, terkadang jika melakukan sesuai prosedur maka *surprise audit* kurang efisien, karena jika antar teman dari kantor pusat dan kantor cabang saling kenal lalu memberitahu temannya bahwa unit bersangkutan akan dilakukan *surprise audit*, maka unit itu akan mempersiapkan diri dan kemungkinan ditemukan aktivitas yang tidak wajar lebih kecil (Ariffin, 2018). Pernyataan mengenai *Surprise Audit* juga terdapat pada Lampiran 14.

3. Surveillance System

Proses *Surveillance System* di PT Bank BPD DIY dilakukan untuk memantau SKAI dan setelah Unit Anti *Fraud* terbentuk, karena berada dibawah pimpinan SKAI maka Unit Anti *Fraud* juga akan dipantau dan diperiksa efektivitas kerjanya oleh badan yang independen seperti KAP dan BPKP. Setiap 3 tahun BPKP akan melakukan tugasnya untuk mengevaluasi apakah ada kode etik yang dilanggar serta apakah kinerja SKAI maupun Unit Anti *Fraud* sesuai

Peraturan Bank Indonesia atau tidak (Kurniawan, 2018). BPKP juga akan melakukan survei ke lapangan seperti ke cabang seperti apa kinerja auditor. BPKP akan melaporkan hasil evaluasinya kepada OJK. Pernyataan mengenai *Surveillance System* juga terdapat pada Lampiran 14.

4.3.3.3 Pilar Investigasi, Pelaporan dan Sanksi pada Analisis Mekanisme Penerapan Strategi Anti *Fraud* PT Bank BPD DIY

Pilar Investigasi, Pelaporan dan Sanksi dapat dipastikan termasuk di dalamnya terdapat 3 proses yaitu Investigasi, Pelaporan dan Sanksi.

Hasil Unit Anti *Fraud* melakukan investigasi akan dilaporkan Direktur Utama dan ke OJK berupa Laporan Penerapan Strategi Anti *Fraud*. Pelaporan ini dilakukan tiap semesteran maksimal tanggal 10 setelah bulan pelaporan. Format laporan sudah ada di Lampiran Surat Edaran BI No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum.

Menurut Ariffin (2018), proses pengenaan Sanksi dilakukan oleh Komite Kepegawaian (KMK), karena Unit Anti *Fraud* sudah tidak berwenang dalam pengenaan sanksi. Unit Anti *Fraud* hanya melaporkan bahwa hasil investigasi *fraud*

akan berdampak apa saja. Sanksi yang dibebankan oleh KMK kepada pelaku sesuai tingkat *fraud* yang dilakukan, sesuai kebijakan adalah downgrade, tidak diberikan THR 100%, pemberhentian tanpa predikat dan yang terparah adalah PHK. Pemberhentian tanpa predikat disini artinya adalah pelaku harus melunasi terlebih dahulu kewajiban yang masih belum diselesaikannya, untuk PHK maka akan lunas atas semua kewajibannya. Untuk mengatasi hal itu maka jika pegawai melakukan pinjaman dalam jumlah yang besar wajib diberikan jaminan atas pinjamannya.

Pilar Investigasi, Pelaporan dan Sanksi tidak memiliki hubungan dan tidak menimbulkan kekurangan dalam penerapan strategi anti *fraud*.

4.3.3.4 Pilar Pemantauan, Evaluasi dan Tindak Lanjut pada Analisis Mekanisme Penerapan Strategi Anti *Fraud* PT Bank BPD DIY

Pilar Pemantauan, Evaluasi & Tindak Lanjut dapat dipastikan terdiri dari proses Pemantauan, Evaluasi dan Tindak Lanjut.

Untuk proses pemantauan dan evaluasi Unit Anti *Fraud* juga membuat laporan. Untuk proses tindak lanjut, Unit Anti *Fraud* akan memberi usulan pihak dirugikan untuk melakukan

hal – hal pencegahan, hal itu hanya jika Direksi menyetujui usulan Unit Anti *Fraud* (Ariffin, 2018).

Pilar Pemantauan, Evaluasi & Tindak Lanjut tidak memiliki hubungan dan tidak menimbulkan kekurangan dalam penerapan strategi anti *fraud*.

4.3.3.5 Manajemen Risiko pada Analisis Mekanisme Penerapan Strategi Anti *Fraud* PT Bank BPD DIY

Manajemen Risiko bersamaan dengan sudah diterapkannya adanya pengendalian *internal* dan tata kelola yang baik (*Good Corporate Governance*) pada dasarnya merupakan dasar pencegahan *fraud*, penerapan strategi anti *fraud* adalah suatu upaya peningkatan dengan menjadikan pencegahan *fraud* menjadi fokus perhatian dan budaya di Bank baik untuk manajemen maupun untuk pegawai. Penerapan strategi anti *fraud* tidak dapat terlepas dari penerapan manajemen risiko, sehingga peneliti menganalisis adanya penerapan manajemen risiko di dalam mekanisme penerapan strategi anti *fraud*. Pilar Manajemen Risiko meliputi 3 proses yaitu ; Pengawasan Aktif Manajemen, Struktur Organisasi & Pertanggungjawaban, serta Pengendalian & Pemantauan.

1. Pengawasan Aktif Manajemen

- a. Ditetapkannya Anti *Fraud Statement* dan Tumbuhkan Kesadaran tentang Anti *Fraud* oleh Manajemen

Proses Pengawasan Aktif Manajemen meliputi proses – proses yang menjadi tanggung jawab Dewan Komisaris maupun Direksi dalam membuat kebijakan yang memastikan pengendalian *fraud* dijalankan. Berdasarkan wawancara yang dilakukan dengan Bapak Kurniawan (2018) pada PT Bank BPD

DIY, sejak tahun 2012 sudah ditetapkan pakta integritas. Hal tersebut wajib dilaksanakan seluruh manajemen dan pegawai. Setelah Unit Anti *Fraud* terbentuk, Unit Anti *Fraud* mengusulkan ke Direktur Utama mengenai ditetapkannya *Anti Fraud Statement* dan tumbuhkan kesadaran tentang Anti *Fraud* oleh manajemen sebagai penyempurna pakta integritas yang dibuat untuk Dewan Komisaris dan Direksi serta untuk seluruh pegawai, berikut isinya:

- 1) Dewan Komisaris dan Direksi bertanggung jawab atas terlaksananya strategi anti *fraud*.
- 2) Dewan Komisaris sepenuhnya mendukung dan senantiasa mengawasi langkah – langkah yang diambil dalam penerapan strategi anti *fraud*.
- 3) Bahwa dalam rangka mewujudkan budaya anti *fraud* Direksi akan bertanggungjawab menerapkan strategi anti *fraud* pada semua tingkatan organisasi.
- 4) Bahwa dalam rangka melaksanakan strategi anti *fraud* SKAI bertanggungjawab dalam pengelolaan pelaksanaannya.
- 5) Bahwa dalam rangka antisipasi terjadinya *fraud* Dewan Komisaris dan Direksi bersama dengan pegawai bank

berkewajiban melaporkan fakta penyimpangan yang terjadi yang berpotensi *fraud* kepada OJK

6) Bahwa dalam rangka antisipasi terjadinya *fraud* Direksi dan Dewan Komisaris berkomitmen untuk melindungi pelapor kecurangan dalam bentuk kerahasiaan

7) Bahwa dalam rangka antisipasi terjadinya *fraud* Direksi dan Dewan Komisaris tidak mentolerir (*zero tolerance*) terhadap setiap tindakan *fraud*

Ini ditandatangani Dewan Komisaris, Komisaris Utama, Direktur Utama, Direktur Pemasaran & Unit Usaha Syariah, Direktur Umum, dan Direktur Kepatuhan.

Untuk pegawai terdapat format tersendiri yaitu :

Saya yang bertanda tangan dibawah ini :

Nama :

Nomor Induk Pegawai :

Pangkat / Jabatan :

Unit Kerja :

Menyatakan persetujuan untuk melaksanakan strategi anti *fraud* yang dikemukakan dalam Buku Pedoman Strategi Anti *Fraud* dan memahami bahwa bank tidak akan mentolerir setiap

tindakan *fraud* yang dilakukan dan akan menerapkan sanksi tegas terhadap pelaku *fraud*. Nilai – nilai inti yang disepakati adalah sebagai berikut:

- 1) Setiap insan bank sebelum melaksanakan kegiatan, selalu diawali dengan niat baik dan semata – mata bekerja untuk kepentingan bank serta tidak merugikan orang lain, yang dilandasi keikhlasan dan tulus sehingga dapat memuaskan *stakeholders*.
- 2) Setiap insan bank berkewajiban menghindari perbuatan-perbuatan penyimpangan yang dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah atau pihak lain menderita kerugian dan/atau pelaku *fraud* memperoleh keuntungan.
- 3) Setiap insan bank berkewajiban melaporkan setiap fakta penyimpangan yang dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah atau pihak lain menderita kerugian.

- 4) Setiap insan bank tidak diperbolehkan memberi dan/atau menerima hadiah/cinderamata/gratifikasi dalam bentuk apapun yang berhubungan dengan jabatan dan pekerjaannya sehingga menimbulkan konflik kepentingan.

Sehingga pernyataan ini dinyatakan dengan penuh kesadaran serta memahami ketentuan ini merupakan komitmen saya dalam penerapan strategi anti *fraud* dan merupakan hal penting untuk dijaga dan meningkatkan efektivitasnya. Pernyataan ini juga terdapat pada Lampiran 10 dan Lampiran 11.

2. Struktur Organisasi dan Pertanggungjawaban

Proses Struktur Organisasi & Pertanggungjawaban tercipta saat dibentuknya Unit Anti *Fraud*. PT Bank BPD DIY sendiri sudah menerapkan strategi anti *fraud* dengan terlebih dahulu menerapkan *Whistleblowing system* (WBS) yang disahkan dengan dikeluarkannya Surat Keputusan Direksi Nomor 001/KPTS/DP/2012 tentang Penerapan Kebijakan Strategi Anti *Fraud*. Saat itu WBS dikelola oleh Satuan Kerja Audit Intern (SKAI) dalam menerima laporan maupun menindaklanjuti.

a. Pembentukan Unit Anti *Fraud*

Unit Anti *Fraud* secara organisasi berada dibawah SKAI dan terdiri dari 2 personil. Unit Anti *Fraud* di dalam organisasi memang dapat berdiri sendiri atau dibawah naungan SKAI, hal

tersebut ditentukan dari tingkat efektivitas atas dasar *firm size* Bank bersangkutan. Untuk PT Bank BPD DIY karena hanya mencakup wilayah DIY saja maka Unit Anti *Fraud* berada dibawah naungan SKAI (Kurniawan, 2018).

3. Pengendalian dan Pemantauan

a. Penggunaan Teknologi Informasi untuk Mengendalikan *Fraud*

Proses Pengendalian & Pemantauan dimulai dari Penggunaan Teknologi Informasi untuk Mengendalikan *Fraud*. Berdasarkan wawancara yang dilakukan dengan Bapak Kurniawan (2018) pada PT Bank BPD DIY, sistem keamanan yang dilakukan dikembangkan oleh Divisi Teknologi Informasi. Setiap laptop maupun komputer yang dipakai untuk operasional perusahaan dirancang agar tidak dapat dimasukkan *flashdisk*, sehingga hanya *flashdisk* khusus milik pegawai saja yang dapat. Penggunaan *wifi* selain dari *hotspot* yang disediakan disetiap ruangan juga tidak diperbolehkan, hal tersebut agar terpantau layanan internet yang disediakan dipakai setiap pegawai untuk mengakses apa saja. Dan setiap laptop maupun komputer dirancang memiliki *username* dan *password*, sehingga selain pemilik tidak dapat membuka data – data yang ada di dalamnya. Jika ingin meminjam laptop maupun komputer milik teman maka dapat *log in* menggunakan *username* dan *password*

sendiri, dan otomatis tampilan yang keluar serta data – data yang dimunculkan adalah milik pemegang *username* tersebut.

Pengamanan Teknologi Informasi dilakukan dengan adanya server cadangan seluruh pusat data di Kantor Cabang Wates. Hal tersebut untuk mengantisipasi jika terjadi bencana alam ataupun pencurian data oleh pelaku *fraud*, data – data masih aman karena ada *backup* data. Sama halnya dengan WBS, hanya Direktur Utama serta Pimpinan SKAI dan Pimpinan Manajemen Risiko saja yang diberikan akses membuka WBS. Kekurangannya adalah Teknologi Informasi yang diterapkan khususnya untuk *Whistleblowing system* belum independen, karena PT Bank BPD DIY tidak memakai Teknologi Informasi dari penyedia jasa yang sesuai kebutuhan kompleksitas Bank.

Sesuai dengan Surat Edaran BI No.9/30/DPNP tanggal 12 Desember 2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum bahwa Bank tidak dapat menyelenggarakan sendiri Teknologi Informasi yang digunakan untuk efisiensi dalam kegiatan operasional juga yang digunakan untuk meningkatkan pelayanan kepada nasabah. PBI tersebut disempurnakan dalam peraturan OJK yaitu POJK No 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, bahwa Bank wajib menerapkan proses manajemen

risiko dalam penggunaan Teknologi Informasi jika penggunaan masih belum memakai jasa pihak ketiga maupun sudah memakai pihak ketiga.

b. Pengendalian *Internal*

Untuk proses Pengendalian *Internal*, berdasarkan wawancara yang dilakukan dengan Ibu Aeni (2018) SKAI yang bertanggung jawab memastikan bahwa Sistem Pengendalian *Internal* (SPI) dijalankan pada setiap kegiatan operasional oleh setiap pegawai. Dimulai dari teller, dan kemudian untuk seluruh bagian, terdapat Standar Operasional Prosedur (SOP) yang berisikan pemisahan fungsi dan tanggung jawab untuk setiap bagian dan diwajibkannya otorisasi oleh pimpinan divisi atau pihak yang berwenang. Sebagai contoh SPI pada cek, tandatangan *speciment* pada cek yang akan dicairkan apakah sama dengan pemilik cek atau tidak. Hal itu termasuk salah satu pengendalian yaitu mencocokkan. Lalu untuk mencairkan akan diminta kartu identitas seperti KTP, barulah dicocokkan dengan data dalam program komputer. Pada saat pencairan jika pencair ingin mencairkan melebihi nominal maksimal setiap pencairan maka *teller* tetap hanya bisa mengeluarkan sesuai ketentuan saja. Dan juga saat bank mengeluarkan cek itu pasti ada nomer seri nya dan sudah di *input* di sistem, kertas bahan untuk cek pun berbeda, dibuat seperti percetakan uang dan tidak akan ada

yang sama dengan percetakan di luar sana. Dapat disimpulkan untuk satu aktivitas saja sudah mencakup pengendalian yaitu keabsahan *speciment* tanda tangan, nomer seri pada cek dan otorisasi oleh pihak yang bertanggung jawab.

c. Kebijakan Rotasi dan Cuti Pegawai

Proses yang terakhir yaitu Kebijakan Rotasi dan Cuti Pegawai. Pada PT Bank BPD DIY rotasi jabatan dilakukan setiap 4 tahun sekali (Salam, 2018). Rotasi jabatan dilakukan dalam beberapa jenis, dapat dilakukan rotasi untuk level yang sama dengan berbeda Divisi, atau dalam Divisi yang sama namun dipindahkan dari kantor pusat ke cabang atau dari cabang ke kantor pusat, atau dapat di level yang sama tetapi berbeda divisi dan dipindahkan antar cabang. Selain rotasi juga dilakukan mutasi jabatan, promosi atau bahkan delusi (turun jabatan).

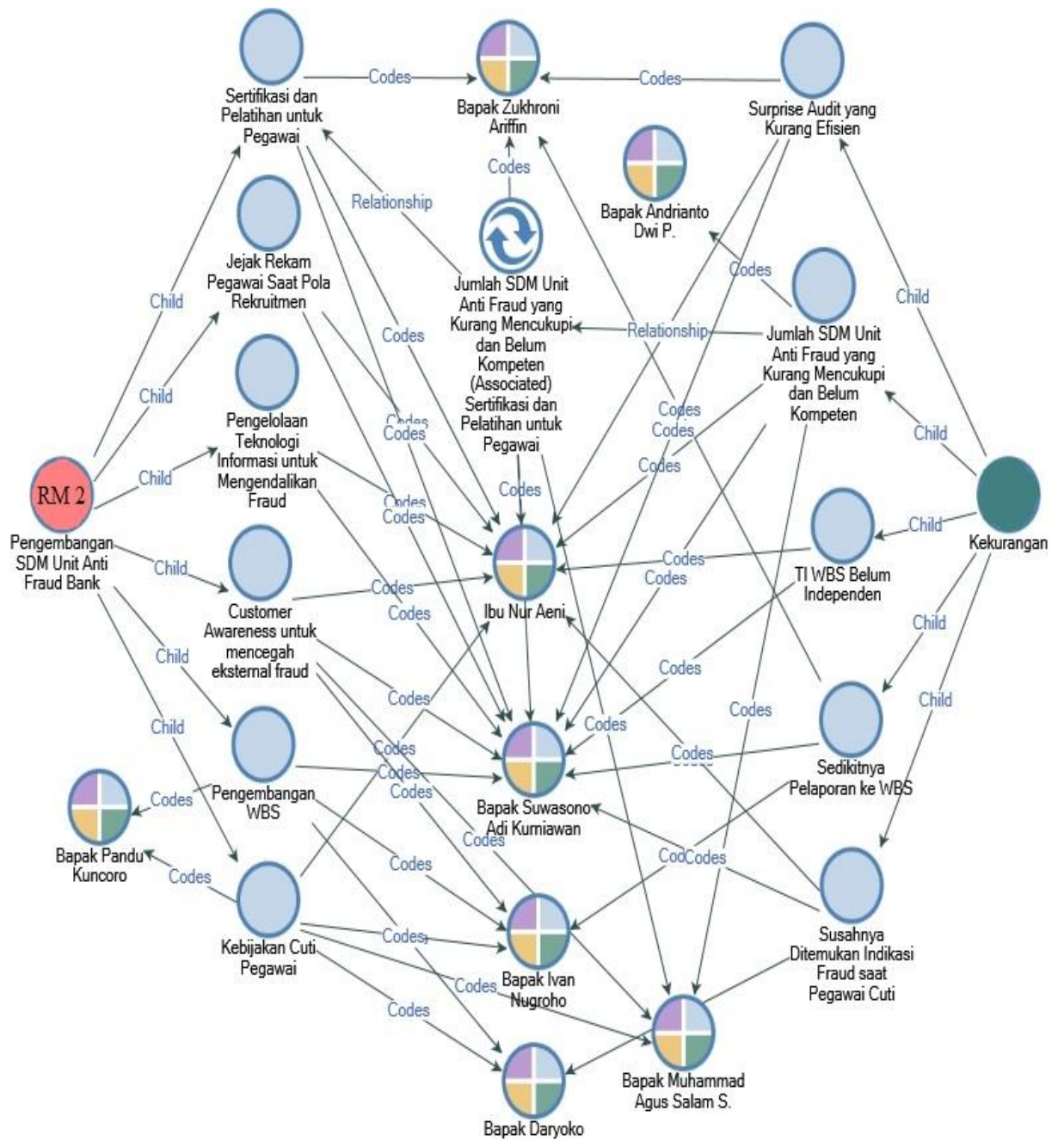
Berdasarkan wawancara yang dilakukan dengan Bapak Kurniawan (2018) cuti pegawai pada PT Bank BPD DIY diberikan jatah 12 hari dalam satu tahun. Setelah Unit Anti *Fraud* terbentuk, jatah cuti 12 hari ini tidak termasuk cuti bersama atau pun hari libur nasional. Jatah cuti tersebut dapat diambil kapan saja dan dalam kurun waktu sesuai kebutuhan. Kekurangannya adalah Susahnya Ditemukan Indikasi *Fraud* saat Pegawai Cuti. Hal ini karena saat semua pegawai

mengambil jatah cuti pada hari dimana semua pegawai juga libur maka tidak ada yang dapat menggantikan sehubungan dengan SDM yang tidak mencukupi, maka akan susah kemungkinan ditemukannya hal yang tidak wajar (Aeni, 2018).

4.4 Analisis Pengembangan SDM Unit Anti *Fraud* PT Bank BPD DIY

Pengembangan SDM Unit Anti *Fraud* beserta analisis atas kekurangan mekanisme penerapan Strategi Anti *Fraud* akan dijelaskan melalui peta hasil olahan dari aplikasi NVivo 11 dibawah ini:

Gambar 4.4
Analytical Maps Pengembangan SDM Unit Anti Fraud PT Bank BPD DIY



Sumber : Data Diolah dari NVivo 11

Pengembangan SDM Unit Anti *Fraud* pada PT Bank BPD DIY dilakukan melalui 4 proses, yaitu ; Sertifikasi dan Pelatihan untuk Pegawai, Jejak Rekam Saat Pola Rekrutmen, Pengelolaan Teknologi Informasi untuk Mengendalikan *Fraud*, Customer Awareness untuk Mencegah *Fraud*, serta Pengembangan WBS dan Kebijakan Cuti Pegawai.

4.4.1 Sertifikasi dan Pelatihan untuk Pegawai

Proses yang pertama adalah Sertifikasi dan Pelatihan untuk Pegawai yang dilakukan rutin untuk pegawai, setiap pegawai diberikan minimal 2 kali untuk mengikuti sertifikasi dan pelatihan. Semua biaya yang dikeluarkan untuk mengikuti sertifikasi dan pelatihan akan dibiayai oleh PT Bank BPD DIY. Di awal tahun juga setiap divisi wajib membuat *training list analyst*. Sehingga setahun kedepan divisi itu akan mengikuti pelatihan di bidang apa saja dan diberikan kepada SDM. SDM akan mengolah, dan ketika pihak ketiga melakukan penawaran ke SDM dan sesuai dengan *training list analyst* divisi – divisi yang mengajukan maka seluruh biaya pengeluaran seperti pendaftaran, pesawat, hotel, uang saku dan makan akan dilakukan oleh bagian SDM. Ini juga merupakan salah satu tindakan pencegahan *fraud* (Kurniawan, 2018).

Untuk sertifikasi, Bank mempunyai syarat minimal pegawai memiliki sertifikasi level 1 dari 5 level sesuai dengan jabatannya, untuk staff minimal level 1 (Aeni, 2018). Setiap level, Bank akan memberikan kesempatan dibiayai bank maksimal 2 kali, hal tersebut

untuk mengantisipasi jika tidak lulus sertifikasi. Untuk sertifikasi dan pelatihan yang sudah ditempuh pegawai selama tahun 2016, semua dicantumkan pada Laporan Tahunan PT Bank BPD DIY untuk Tahun 2016. Di tahun 2018 ini, salah satu contoh pengajuan sertifikasi untuk SKAI di PT Talents Indonesia yang berlokasi di Tangerang adalah *Refreshment Sertifikasi Audit Internal Bank*, karena sertifikat akan hangus jika melebihi waktu 3 tahun apabila tidak dilakukan *refreshment*. Sertifikasi tersebut diadakan untuk 2 gelombang, masing – masing gelombang diikuti 10 orang terdiri dari KIC, Unit Anti *Fraud* dan personil auditor SKAI, brosur pelatihan dicantumkan dalam Lampiran. Namun, untuk Unit Anti *Fraud*, karena terbentuk di tahun 2017, maka SDM nya belum memiliki sertifikasi khusus untuk *fraud examiner*. Pada dasarnya SDM Unit Anti *Fraud* berasal dari SKAI, maka mereka hanya sudah bersertifikasi *internal auditor* (Ariffin, 2018). Kekurangannya adalah Unit Anti *Fraud* hanya terdiri dari 2 orang, sedangkan penerapan Strategi Anti *Fraud* mencakup 4 pilar. Dan kompetensi SDM Unit Anti *Fraud* belum sesuai dengan divisinya.

4.4.2 Jejak Rekam Pegawai saat Pola Rekrutmen

Proses yang kedua adalah Jejak Rekam Saat Pola Rekrutmen dengan adanya kerjasama antara Unit Anti *Fraud* dengan Divisi SDM. Hal tersebut dilakukan saat proses *Know Your Employee* dimulai pada saat rekrutmen. Proses KYE bertujuan agar PT Bank BPD DIY

memilih calon pegawai yang kompeten, terhindar dari masalah hukum serta memiliki kepribadian dan etika yang mampu mendukung danya budaya anti *fraud* dalam organisasi. Mengetahui profil calon pegawai juga sangat penting untuk menghindari *conflict of interest* (Kurniawan, 2018).

4.4.3 Pengelolaan Teknologi Informasi untuk Mengendalikan Fraud

Proses yang ketiga adalah Pengelolaan Teknologi Informasi untuk Mengendalikan *Fraud*. Informasi didapat dari semua data yang dimiliki Bank, semua data yang ada di dalam PT Bank BPD DIY tentu saja sangat penting untuk dilakukan pengamanan. Tidak hanya data yang berhubungan dengan operasional perusahaan saja, tetapi juga data yang berhubungan dengan nasabah. Informasi yang berhubungan dengan nasabah untuk menghindari adanya penyalahgunaan maka PT Bank BPD DIY sudah menerapkan adanya pengecekan rutin setiap di setiap mulut ATM ada atau tidak alat *skimmer*. Salah satu cara mencegah adanya penyalahgunaan yang dilakukan PT Bank BPD DIY adalah dengan membuka layanan ATM di setiap kantor cabang maupun kantor pusat. Jika ATM melekat pada kantor maka pelaku kecurangan akan berpikir dua kali, dan juga jika terjadi skimming akan dapat segera ditindaklanjuti dan dapat segera dilacak. Menurut Ibu Aeni (2018) pada dasarnya kecurangan Teknologi pada ATM dapat dikurangi dengan tidak membuka layanan ATM di tempat yang jauh dari keramaian selain dipasangnya CCTV.

4.4.4 Customer Awareness untuk Mencegah Fraud

Proses yang keempat adalah Customer Awareness untuk Mencegah *Fraud*. Unit Anti *Fraud* sendiri sudah membuat rencana kedepan untuk menumbuhkan *customer awareness* dengan dibuatnya brosur yang berisikan strategi anti *fraud* supaya nasabah tidak dirugikan, dan dibagikan untuk setiap nasabah yang selesai melakukan transaksi. Serta akan ditayangkan pada Televisi yang ada di kantor pusat maupun cabang, untuk menayangkan konten mengenai pentingnya kesadaran menjaga informasi pribadi yang berhubungan dengan Bank kepada siapapun termasuk anak sendiri (Kurniawan, 2018).

4.4.5 Pengembangan Whistleblowing system (WBS)

Selanjutnya yaitu proses yang kelima adalah Pengembangan WBS. Seperti yang dikatakan oleh Bapak Kurniawan (2018) Unit Anti *Fraud* sudah merencanakan strategi untuk menyempurnakan *whistleblowing system* PT Bank BPD DIY. Tampilan WBS akan diperbarui dan digantikan dengan kata “Surat kepada Direktur Utama”. Hal ini dilakukan dalam upaya meingkatkan partisipasi pegawai. Dan juga akan dilakukan perluasan jangkauan WBS untuk dapat diakses melalui *smart kit* BPD DIY berupa BPD DIY *Mobile*, karena selama ini hanya digunakan pegawai untuk melihat katalog

produk saja. Hal ini dilakukan agar pegawai dapat melaporkan tindakan yang sesuai kategori pelanggaran yang dilakukan orang di dalam organisasi langsung saat itu juga, untuk menghindari gangguan secara emosional seperti jika esok hari bertemu di kantor dan mengurungkan niat untuk melaporkan dikarenakan pelaku sangat baik kepada pelapor. Pernyataan mengenai pengembangan *whistleblowing system* terdapat pada Lampiran 15.

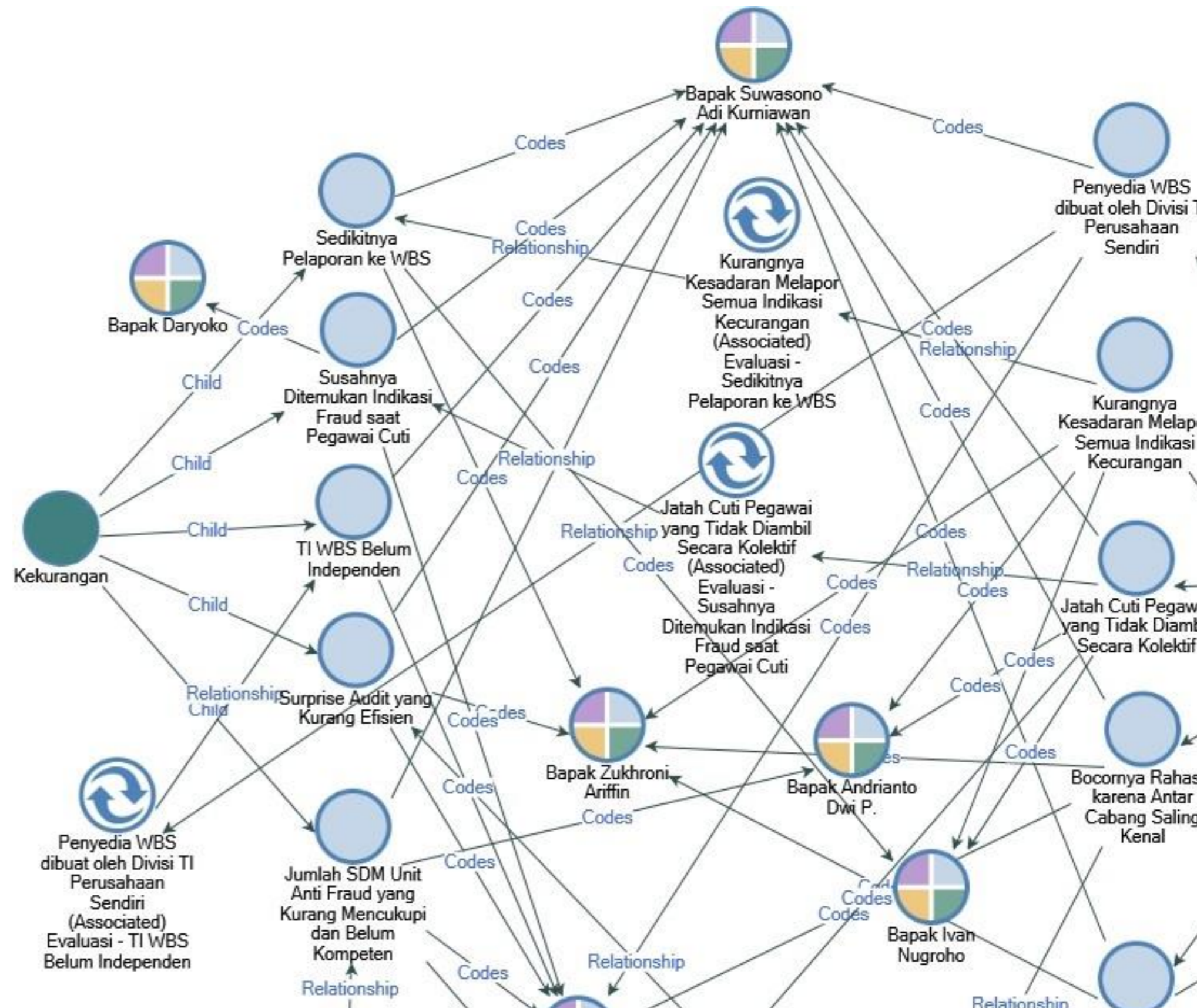
4.4.6 Kebijakan Cuti Pegawai

Untuk proses yang terakhir yaitu Kebijakan Cuti Pegawai yang akan segera diterapkan Unit Anti *Fraud* dengan pegawai wajib untuk mengambil jatah cuti secara kolektif minimal 2 hari. Hal ini dilakukan agar saat pegawai yang bersangkutan digantikan temannya maka kemungkinan ditemukan hal yang tidak wajar menjadi lebih besar, serta jatah cuti yang tidak diambil tidak dapat digantikan dengan gaji.

4.5 Analisis Kendala yang Dihadapi oleh Unit Anti *Fraud* PT Bank BPD DIY

Analisis kekurangan yang disebabkan kendala yang terjadi dalam mekanisme penerapan Strategi Anti *Fraud* akan dijelaskan melalui peta hasil olahan dari aplikasi NVivo 11 dibawah ini :

Gambar 4.5
Analytical Maps Kendala yang Dihadapi oleh Unit Anti Fraud PT Bank BPD DIY



Berdasarkan kekurangan penerapan Strategi Anti *Fraud* maka peneliti menemukan hubungan antara kekurangan dengan kendala yang menyebabkan kekurangan tersebut.

4.5.1 Penyedia *Whistleblowing system* (WBS) Dibuat oleh Divisi Teknolgi Informasi (TI) Perusahaan Sendiri

Kekurangan yang ketiga adalah Teknologi Informasi WBS Belum Independen. Kendala yang menyebabkan ini terjadi adalah menurut Aeni (2018) Penyedia WBS dibuat oleh Divisi Teknologi Informasi Perusahaan Sendiri. Tentu saja setiap perusahaan akan mempertimbangkan jika mengeluarkan biaya investasi pada Teknologi Informasi nya maka seberapa besar manfaat yang dapat kembali, jika melebihi pengorbanan biaya yang dikeluarkan maka akan menguntungkan perusahaan, namun jika sebaliknya maka akan lebih baik tidak melakukannya. PT Bank BPD DIY memiliki pertimbangan khusus untuk tidak memakai penyedia jasa dari pihak ketiga dikarenakan alasan tersebut (Kurniawan, 2018).

4.5.2 Kurangnya Kesadaran Melapor Semua Indikasi Kecurangan

Kekurangan yang pertama adalah Sedikitnya Pelaporan ke WBS. Kendala yang terjadi di dalam organisasi adalah Kurangnya Kesadaran Melapor Semua Indikasi Kecurangan. Kurangnya kesadaran tersebut terjadi bukan tanpa sebab, beberapa hal yang dimungkinkan menjadi penyebabnya adalah tampilan *Whistleblowing*

system yang tidak menarik (Nugroho, 2018), pegawai merasa tidak ada *feedback* secara langsung jika melapor, merasa tidak ada yang perlu dilaporkan karena belum memahami secara jelas apa saja yang perlu dilaporkan (Dwi P., 2018), jika terjadi di cabang maka lebih memilih melapor pada KIC dan KIC tidak segera melaporkan ke Unit Anti *Fraud* karena akan mempengaruhi penilaian terhadap cabang tersebut, dan bahkan karena belum tumbuhnya rasa loyalitas dalam bekerja sehingga tidak menganggap kerugian yang dihadapi Bank akan berpengaruh pada kemakmuran pegawai (Ariffin, 2018).

4.5.3 Jatah Cuti Pegawai yang Tidak Diambil Secara Kolektif

Kekurangan yang kedua adalah Susahnya Ditemukan Indikasi *Fraud* saat Pegawai Cuti. Penyebabnya adalah terkait dengan kendala Jatah Cuti Pegawai yang Tidak Diambil Secara Kolektif. Tentu saja para pegawai akan mengambil jatah cuti sesuai dengan kebutuhan mereka. Namun banyak yang sengaja tidak mengambil semua jatah karena merasa pekerjaan kantor sangat menyita waktu dan lebih sering jika pegawai hanya mengambil satu atau dua hari setiap bulan (Dwi P., 2018). Oleh karena itu jika digantikan oleh pegawai lain, tidak cukup banyak waktu yang dapat dimanfaatkan untuk menemukan kejadian tidak wajar oleh pegawai yang mengambil cuti tersebut.

4.5.4 Bocornya Rahasia karena Antar Cabang Saling Kenal

Kekurangan yang keempat adalah *Surprise* Audit yang Kurang Efisien. Hal ini disebabkan kendala yaitu Bocornya Rahasia karena antar Cabang Saling Mengenal. Sebenarnya adalah jika Unit Anti *Fraud* akan melakukan *surprise* audit maka mereka akan meminjam kendaraan dari divisi lain, dan bukan tidak mungkin salah satu dari divisi tersebut tidak mempunyai teman di cabang yang akan dilakukan *surprise* audit, dimungkinkan karena orang tersebut sebelumnya bekerja di cabang tersebut atau benar – benar hanya teman karena satu DIY merupakan wilayah yang tidak seluas jika pegawai di Jakarta yang dapat berasal dari berbagai kota bahkan pulau, namun untuk membocorkan informasi seperti itu mereka tidak ragu (Ariffin, 2018). Para pegawai yang belum memiliki kesadaran bahwa organisasi yang sehat adalah organisasi yang tidak menutupi atau bahkan melindungi adanya tindak kecurangan di dalam organisasi tentu saja mampu melakukan hal ini. karena dengan mereka sengaja memberitahu teman sesama pegawai.

4.5.5 Belum Adanya Rekrutmen dan Sertifikasi untuk Unit Anti *Fraud*

Kekurangan yang terakhir adalah Jumlah SDM Unit Anti *Fraud* yang Kurang Mencukupi dan Belum Kompeten. Hal ini disebabkan oleh Belum adanya Rekrutmen dan Sertifikasi untuk Unit Anti *Fraud*. Seperti yang dikatakan Bapak Salam (2018) bahwa Unit Anti

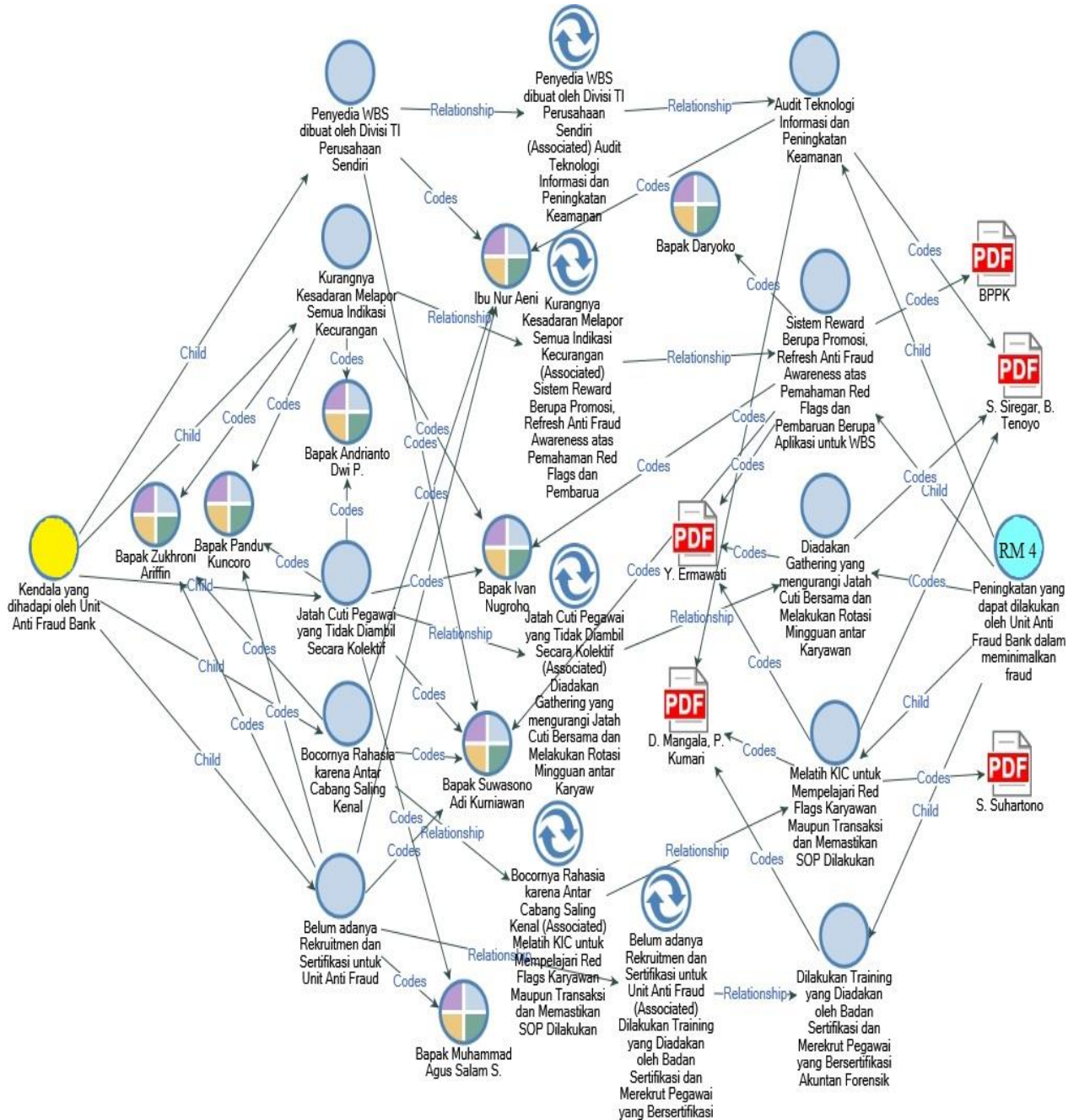
Fraud hanya berjumlah 2 orang, sedangkan strategi anti *fraud* memiliki 4 pilar dimana setiap pilar terdiri dari beberapa proses. Sehingga belum adanya rekrutmen sangat berpengaruh dalam menjalankan ke empat pilar tersebut. Untuk dapat menjalankan strategi anti *fraud* akan lebih membantu PT Bank BPD DIY jika Unit Anti *Fraud* dapat menambah tingkat kualitas selain bersertifikasi *internal auditor* juga memiliki sertifikasi sebagai *fraud examiner* (Kuncoro, 2018).

4.6 Analisis Peningkatan yang Dilakukan Unit Anti *Fraud* dalam Meminimalkan *Fraud* PT Bank BPD DIY

Kendala yang dihadapi Unit Anti *Fraud* dalam penerapan Strategi Anti *Fraud* beserta peningkatan yang perlu dilakukan akan dijelaskan melalui peta hasil olahan dari aplikasi NVivo 11 dibawah ini:

Gambar 4.6

Analytical Maps Peningkatan yang Dilakukan Unit Anti Fraud dalam Meminimalkan Fraud PT Bank BPD DIY



Sumber : Data Diolah dari NVivo 11

Berdasarkan kekurangan dan kendala yang telah dijelaskan sebelumnya, maka terdapat beberapa peningkatan yang dapat dilakukan oleh PT Bank BPD DIY dalam penerapan Strategi Anti *Fraud*. Peningkatan yang dapat dilakukan berdasarkan peraturan yang terkait dengan penerapan Strategi Anti *Fraud* serta analisis yang dilakukan peneliti setelah melakukan wawancara dengan pihak yang berkaitan dengan pelaksanaannya Strategi Anti *Fraud* di PT Bank BPD DIY.

4.6.1 Audit Teknologi Informasi dan Peningkatan Keamanan

Peningkatan pertama yang dapat dilakukan adalah dilakukannya audit serta peningkatan keamanan Teknologi Informasi untuk pelaksanaan *Whistleblowing system*. Menurut Siregar and Tenoyo (2015), perusahaan yang bergerak di bidang industri keuangan sangat penting untuk melakukan manajemen risiko atas penggunaan Teknologi Informasi dan menerapkan proses tambahan untuk mencegah dan mendeteksi *fraud* dengan adanya audit Teknologi Informasi. Hal ini dilakukan karena *whistleblowing system* masih memakai Teknologi Informasi yang dibuat oleh perusahaan. Dalam wawancara yang dilakukan dengan Kurniawan (2018) PT Bank BPD DIY memiliki pertimbangan khusus untuk tidak memakai penyedia jasa dari pihak ketiga dikarenakan perlu dilakukannya analisis apakah biaya yang dikorbankan untuk investasi memiliki pengembalian yang melebihi biaya yang dikorbankan. Peningkatan keamanan dapat dilakukan selain dengan adanya username dan password yang hanya

diberikan akses kepada Pemimpin SKAI dan Manajemen Risiko, Divisi Teknologi Informasi juga dilakukan pencegahan agar tidak dapat membuka *whistleblowing system* dengan adanya *multi layer passwords* yang dibuat dan hanya diketahui oleh Pemimpin SKAI dan Manajemen Risiko.

4.6.2 Sistem Reward Berupa Promosi, Refresh Anti *Fraud Awareness* atas Pemahaman *Red Flags* dan Pembaruan Berupa Aplikasi untuk WBS

Peningkatan kedua yang dapat dilakukan adalah diterapkannya sistem *reward* berupa promosi atas partisipasinya yang dengan sungguh – sungguh berkomitmen menjaga budaya anti *fraud* di dalam perusahaan. Dengan syarat untuk pegawai yang melaporkan indikasi maupun tindakan kecurangan hanya jika pegawai tersebut aktif melaporkan minimal 5 kali pelaporan selama masa jabatan 1 tahun dengan tingkat akurasi informasi yang dilaporkan dapat menyelamatkan aset perusahaan dalam jumlah yang signifikan (BPPK, 2014). Dapat dilakukan juga *refreshment* atas pemahaman anti *fraud awareness* mengenai *red flags* yang mengarah pada tindakan *fraud*, karena tidak semua pegawai memahami hal itu. Serta untuk pembaruan aplikasi untuk *whistleblowing system*, sesuai dengan analisis peneliti terhadap wawancara dengan Bapak Kurniawan (2018) maka perlu dilakukan perubahan tampilan menjadi “Surat kepada Direktur Utama”, lalu akan dilakukan perluasan jangkauan WBS

untuk dapat diakses melalui *smart kit* BPD DIY berupa BPD DIY Mobile. Hal ini dapat mengatasi kendala kurangnya kesadaran pegawai dalam melaporkan inikasi kecurangan.

4.6.3 Diadakan *Gathering* yang Mengurangi Jatah Cuti Bersama dan Melakukan Rotasi Mingguan antar Karyawan

Peningkatan ketiga yang dapat dilakukan adalah diadakannya *gathering* yang mengurangi jatah cuti bersama selama 3 hari dengan peserta bukan berasal dari Divisi yang sama dan hanya beberapa orang saja secara bergilir sehingga semua dapat mengikuti namun dalam waktu pelaksanaan yang berbeda. Hal ini selain meningkatkan keakraban antar pegawai juga berguna agar saat beberapa orang sedang tidak ada di kantor maka dapat digantikan oleh pegawai lain, sehingga kemungkinan ditemukannya *fraud* atau hal yang tidak wajar akan lebih besar (Ermawati, 2015). Bapak Kurniawan (2018) mengatakan bahwa setelah dibentuknya Unit Anti *Fraud*, akan dilakukan perubahan kebijakan dengan mewajibkan pegawai wajib mengambil cuti secara berurutan minimal 3 hari bahkan akan diusahakan 5 hari, hal ini merupakan salah satu bentuk pendeteksian *fraud*. Namun dapat juga dilakukan adanya rotasi setiap satu minggu secara mendadak dengan pegawai satu divisi. Hal ini dilakukan untuk mengantisipasi jatah cuti pegawai yang tidak diambil secara kolektif.

4.6.4 Melatih KIC untuk Mempelajari *Red Flags* Karyawan maupun Transaksi dan Memastikan SOP Dilakukan

Peningkatan keempat yang dapat dilakukan adalah dengan melatih Kontrol Intern Cabang (KIC) untuk memahami *red flags* karyawan, karena menurut Suhartono (2016), banyak pelaku *fraud* menunjukkan ciri – ciri perilaku menyimpang (*red flags*) yang dapat digunakan sebagai indikasi dilakukannya *fraud*. Menurut Kurniawan (2018), perlu dilakukan pemantauan pada setiap pegawai atas gejala yang mengindikasikan perilaku penyebab seseorang melakukan *fraud* yaitu atas dasar *pressure*, *oppurtunity* dan *rationalization*. Pentingnya KIC untuk mempelajari *red flags* karena jika *Surprise Audit* kurang efisien disebabkan oleh bocornya rahasia jika akan dilakukan *surprise audit* maka jika KIC juga dapat memberikan laporan kepada Unit Anti *Fraud*, sehingga saat dilakukan *surprise audit* Unit Anti *Fraud* tahu kemana arah mereka untuk fokus terhadap pegawai yang mengindikasikan perilaku tidak wajar.

4.6.5 Dilakukan *Training* yang Diadakan oleh Badan Bersertifikasi dan Merekrut Pegawai yang Bersertifikasi Akuntan Forensik

Peningkatan kelima dapat dilakukan dengan diberikan training oleh badan bersertifikasi secara rutin agar ketika personil Unit Anti *Fraud* dapat segera lulus saat mengikuti sertifikasi. Hal ini selain mengurangi biaya kegagalan sertifikasi juga dapat menambah wawasan Unit Anti *Fraud*. Setelah itu sangat penting diperhatikan

untuk menambah personil Unit Anti *Fraud* yang sudah memiliki sertifikasi Akuntan Forensik, sehingga pelaksanaan ke empat pilar strategi anti *fraud* dapat berjalan dengan maksimal. Menurut Mangala and Kumari (2015), peningkatan kemampuan auditor dalam mendeteksi dan mencegah *fraud* dipengaruhi dengan peningkatan adanya Akuntan Forensik di dalam perusahaan.

4.7 Kesimpulan Bab

Berdasarkan hasil dan pembahasan yang diperoleh terkait dengan penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY dapat disimpulkan bahwa Unit Anti *Fraud* dalam melaksanakan Strategi Anti *Fraud* sudah sesuai dengan Surat Edaran BI No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum, namun belum sesuai dengan Surat Edaran BI No.9/30/DPNP tanggal 12 Desember 2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

PT Bank BPD DIY sudah melakukan ke empat pilar Strategi Anti *Fraud*, namun masih terdapat beberapa kendala dan kekurangan. Kendala yang timbul dalam penerapan Strategi Anti *Fraud* adalah *whistleblowing system* masih dibuat oleh Divisi Teknologi Informasi perusahaan sehingga menyebabkan kekurangan yaitu Teknologi Informasi *whistleblowing system* belum independen. Kendala yang kedua adalah kurangnya kesadaran melaporkan semua indikasi kecurangan sehingga menyebabkan kekurangan yaitu sedikitnya pelaporan ke *whistleblowing*

system. Kendala yang ketiga adalah jatah cuti pegawai yang tidak diambil secara kolektif sehingga menyebabkan kekurangan yaitu susahny ditemukan indikasi fraud saat pegawai cuti. Kendala yang keempat adalah bocornya rahasia karena antar cabang saling mengenal sehingga menyebabkan kekurangan yaitu *surprise audit* yang kurang efisien. Kendala yang terakhir adalah belum adanya rekrutmen dan sertifikasi untuk Unit Anti *Fraud* sehingga menyebabkan kekurangan yaitu jumlah SDM Unit Anti *Fraud* yang kurang mencukupi dan belum kompeten karena hanya bersertifikasi Internal Audit dan belum bersertifikasi khusus anti-*fraud* serta Unit ini baru terbentuk secara independen di dalam struktur organisasi di awal tahun 2017 dan SDM Unit Anti *Fraud* baru terdiri dari 2 orang. Agar Unit Anti *Fraud* mampu memiliki kompetensi yang lebih dari sebelumnya maka diperlukan merekrut anggota Unit Anti *Fraud* yang baru dengan diharapkan sudah memiliki sertifikasi akuntan forensik, sehingga masing - masing pilar Strategi Anti *Fraud* dapat dilakukan secara maksimal dalam meminimalkan *fraud*.

BAB V

PENUTUP

5.7 Pengenalan Bab

Dalam bab ini peneliti akan membahas mengenai kesimpulan atas penelitian yang telah dilakukan. Kesimpulan didapatkan berdasarkan analisa yang telah dilakukan dari hasil wawancara dan dokumen-dokumen yang digunakan untuk menjawab rumusan masalah. Dalam bab ini juga disampaikan mengenai keterbatasan penelitian dan saran yang peneliti berikan untuk penelitian selanjutnya.

5.2 Kesimpulan Penelitian

Berdasarkan hasil pembahasan dan analisis yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut :

1. Mekanisme penerapan Strategi Anti *Fraud* pada PT Bank BPD DIY sudah sesuai dengan Surat Edaran BI No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti *Fraud* bagi Bank Umum, namun masih terdapat kekurangan dalam penerapannya. PT Bank BPD DIY sudah melakukan ke empat pilar Strategi Anti *Fraud*, namun ditemukan kekuarangan yaitu Surprise Audit yang kurang efisien, sedikitnya pelaporan ke *whistleblowing system*, jumlah SDM

Unit Anti *Fraud* yang kurang mencukupi dan belum kompeten (belum sertifikasi anti-*fraud*), dan Teknologi Informasi belum independen.

2. Pengembangan SDM Unit Anti *Fraud* sudah memiliki penugasan sesuai dengan peraturan Bank Indonesia Nomor 13 Tahun 2017, yaitu sudah adanya pengelolaan teknologi informasi untuk mengendalikan *fraud*, sudah dilaksanakan dan akan dikembangkan *customer awareness* untuk mencegah eksternal *fraud*, akan dilakukannya pengembangan *whistleblowing system*, dan akan ditegaskan kembali kebijakan cuti pegawai. Untuk pola rekrutmen SDM dilakukan untuk seluruh pegawai dengan menerapkan jejak rekam pegawai saat pola rekrutmen. Untuk hubungan timbal balik dengan Manajemen Risiko dan Kepatuhan sudah dilakukan dan terbukti dalam pelaksanaan pilar pencegahan mencakup proses identifikasi kerawanan, SDM Unit Anti *Fraud* melakukan koordinasi dengan SDM Manajemen Risiko dan Kepatuhan.
3. Kendala yang dihadapi Unit Anti *Fraud* akan menyebabkan kekukurangan dalam pelaksanaan Strategi Anti *Fraud*, kendala yang ditemukan pertama adalah penyedia *whistleblowing system* yang dibuat oleh Divisi Teknologi Informasi perusahaan sendiri, kedua adalah kurangnya kesadaran pegawai untuk melaporkan semua indikasi kecurangan, ketiga adalah jatah cuti pegawai yang tidak diambil secara kolektif, keempat adalah bocornya rahasia surprise audit karena antar cabang saling kenal, dan yang kelima adalah belum

adanya sertifikasi dan rekrutmen untuk Unit Anti *Fraud* sehingga menyebabkan kurangnya SDM Unit Anti *Fraud* dan SDM Unit Anti *Fraud* belum kompeten. Untuk hubungan timbal balik dengan Manajemen Risiko dan Kepatuhan tidak ditemukan adanya kendala.

4. Untuk mengatasi kendala yang dihadapi oleh Unit Anti *Fraud*, maka terdapat beberapa peningkatan yang dapat dilakukan yaitu pertama adalah dilakukannya audit Teknologi Informasi dan peningkatan keamanan. Kedua adalah diberikan *reward* berupa promosi bagi pegawai yang aktif melaporkan ke *whistleblowing system* dengan ketentuan dapat menyelamatkan aset perusahaan serta dilakukan *refresh* pemahaman anti *fraud awareness* maupun *red flags* yang mengindikasikan terjadinya *fraud* dan pembaruan aplikasi untuk *whistleblowing system* sehingga dapat mengatasi kurangnya kesadaran melapor semua indikasi kecurangan ke *whistleblowing system*. Ketiga adalah diadakannya *gathering* berupa *outbond* yang dapat mengurangi jatah cuti bersama yang tidak diambil secara kolektif serta dilakukan rotasi jabatan secara mingguan. Keempat adalah dilakukan pelatihan pada Kontrol Intern Cabang (KIC) untuk mempelajari *red flags* karyawan dan transaksi serta memastikan seluruh SOP dilaksanakan, kelima adalah dilakukannya training oleh badan bersertifikasi seperti ACFE untuk Unit Anti *Fraud*.

5.3 Keterbatasan Penelitian

Dalam melaksanakan penelitian, peneliti masih menemukan beberapa keterbatasan sebagai berikut :

1. Laporan tahunan yang digunakan adalah tahun 2016, hal itu dikarenakan laporan tahunan tahun 2017 belum dikeluarkan.
2. Dalam melakukan konfirmasi mengenai pelaksanaan Strategi Anti *Fraud* hanya dilakukan oleh beberapa bagian di dalam Divisi Manajemen Risiko dan Kepatuhan.

5.4 Saran Penelitian

Berdasarkan penelitian yang telah dilakukan, terdapat saran yang ditujukan kepada PT Bank BPD DIY peneliti selanjutnya, dan masyarakat umum meliputi :

1. Agar pelaksanaan Strategi Anti *Fraud* dalam meminimalkan *fraud* dapat berjalan maksimal maka pengemban tanggung jawab yaitu Unit Anti *Fraud* dapat segera dilakukan rekrutmen dan sertifikasi, sehingga dapat dilaksanakan pembagian tugas dan wewenang.
2. Bagi peneliti selanjutnya dan mahasiswa yang akan melakukan penelitian, dapat menambah responden dari divisi lain untuk menghindari jawaban yang subjektif.
3. Untuk masyarakat umum diharapkan dapat lebih waspada terhadap kemungkinan kecurangan di dalam lingkungan Bank dengan lebih melaksanakan prinsip kehati – hatian, sehingga tidak mengakibatkan kerugian baik untuk diri sendiri maupun pihak PT Bank BPD DIY.

DAFTAR PUSTAKA

(ACFE), A. O. C. F. E. 2016. 'Report To The Nations On Occupational Fraud and Abuse'. <http://www.acfe.com/rtnn/docs/2014-report-to-nations>.

Aeni, Nur. 2018. Interview dengan Nur Aeni, diinterview oleh Dewi Kilisuci A.P., 8 Maret, Yogyakarta.

Afrizal. 2014. *Metode Penelitian Kualitatif, Sebuah Upaya Mendukung Penggunaan Penelitian Kualitatif Dalam Berbagai Disiplin Ilmu*. 1st edn. Jakarta: Rajawali Pers.

Albrecht, C. C., Albrecht, W. S., Albrecht, C. O. and Zimbelman, M. F. 2006. *Forensic Accounting*. 4th edn. Singapore: South Western-Cengage.

Ariffin, Zukhroni. 2018. Interview dengan Zukhroni Ariffin, diinterview oleh Dewi Kilisuci A.P., 16 Maret, Yogyakarta.

Baihaque, M. R. 2016. 'Analisis Peranan Audit Internal dalam Upaya Penerapan Strategi Anti Fraud Bank BPD DIY Yogyakarta'. Universitas Islam Indonesia.

Bank Indonesia. 2011. Surat Edaran Bank Indonesia No.13/28/DPNP tanggal 9 Desember 2011 tentang Penerapan Strategi Anti Fraud bagi Bank Umum, <http://www.bi.go.id>.

Bazeley, P. and Jackson, K. 2013. *Qualitative Data Analysis with NVivo*.

Second. Great Britain: SAGE Publications Ltd.

Benjamin, O. A. and Samson, B. S. 2011. 'Effect of Perceived Inequality and Perceived Job Insecurity on Fraudulent Intent of Bank Employees in Nigeria', *Europe's Journal of Psychology*, 7(1), pp. 99–111. doi: 10.5964/ejop.v7i1.107.

BPPK. 2014. 'Employee Perceptions of Whistleblowing System , Ethics Code and Values : Empirical Evidence from the Directorate General of Taxes', 7, pp. 75–89.

Buchholz, A. K. 2012. 'SAS 99: Deconstructing The Fraud Triangle and Some Classroom Suggestions', *Journal of Leadership, Accountability and Ethics*, 9(2), pp. 109–118.

Butcovan, A. 2015. 'Banking Security In The Context Of International Relations', (July), pp. 7–14.

Chung, J., Monroe, G. . and Thome, L. 2004. 'An Examination of Factors Affecting External and Internal Whistleblowing by Auditors'. Toronto.

Corbin, J. and Strauss, A. 2015. *Dasar - Dasar Penelitian Kualitatif, Tatalangkah dan Teknik - Teknik Teorisasi Data*. Edited by Kamdani. Yogyakarta: Pustaka Pelajar.

Cressey, D. 1953. 'The Internal Auditor as Fraud Buster', *Managerial Auditing Journal*.

Creswell, J. W., Ivankova, N. V. and Stick, S. L. 2006. 'Using Mixed-

Methods Sequential Explanatory Design: From Theory to Practice', *Field Methods*, 18(1), pp. 3–20. doi: 10.1177/1525822X05282260.

Daryoko. 2018. Interview dengan Daryoko, diinterview oleh Dewi Kilisuci A.P., 16 Maret, Yogyakarta.

Dorminey, J. W., Fleming, A. S., Kranacher, M.-J. and Riley, Jr, R. A. 2010. 'Beyond the Fraud Triangle', *The CPA Journal*, (July).

Dwi P., Andrianto. 2018. Interview dengan Andrianto Dwi P., diinterview oleh Dewi Kilisuci A.P., 16 Maret, Yogyakarta.

Elias, R. 2008. 'Auditing Student Professional Commitment and Anticipatory Socialization and Their Relationship to Whistleblowing', in, pp. 283–294.

Ermawati, Y. 2015. 'Analisa Penerapan Fraud Early Warning System (FEWS) pada Bank 'X' di Surabaya'. Universitas Wijaya Surabaya.

Gaffney, M. M. and Essex, N. R. 2014. 'Training for Success : A Comparison of Anti-Fraud Knowledge Competencies'.

Gibson, J. . 2003. *Struktur Organisasi dan Manajemen*. Jakarta: Erlangga.

Grosse, R. E. 2001. *Drugs and Money : Laundering Latin America's Cocaine Dollars*. London: Greenwood Publishing Group.

Guba, E. G. and Lincoln, Y. S. 1994. *Competing Paradigms in Qualitative Research*. Beverly Hills: Sage Publication Inc.

Hadiyatno, D. 2012. 'Effect of Competence , Compensation , and Job Satisfaction of Employee Performance at PT. Ciomas Adisatwa Balikpapan'. Universitas Balikpapan.

Hancock, D. R. and Algozzine, B. 2006. *Doing Case Study Research*. New York: Teachers College Press.

Haryanto, J. O., Halim, R. E., Manansang, R. E. and Kus, J. N. A. 2005. *Whistleblowing system and Organization 's Performance*. 13–68.

Hassmiller, S. B. 2015. 'How to Create an Anti-Fraud Culture', *AJN, American Journal of Nursing*, 112(3), pp. 61–66. doi: 10.1097/01.NAJ.0000412641.93516.99.

Huberman, A. M. and Miles, M. 2010. *The Qualitative Researcher 's Companion. Understanding and Validity in Qualitative Research, The Qualitative Researcher 's Companion*. Thousand Oaks: SAGE Publication Inc.

Isa, Y. M., Sanusi, Z. M., Haniff, M. N. and Barnes, P. A. 2015. 'Money Laundering Risk: From The Bankers' and Regulators Perspectives', *Procedia Economics and Finance*. Elsevier B.V., 28(April), pp. 7–13. doi: 10.1016/S2212-5671(15)01075-8.

Kimani, J. 2011. 'Fraud Risk Assessment Plan for Barclays Bank of Kenya.' Tampere University of Applied Sciences.

Kuncoro, Pandu. 2018. Interview dengan Pandu Kuncoro, diinterview oleh

Dewi Kilisuci A.P., 15 Maret, Yogyakarta.

Kurniawan, S. A. 2018. Interview dengan Suwasono Adi Kurniawan, diinterview oleh Dewi Kilisuci A.P., 9 Maret, Yogyakarta.

Leavy, P. 2014. *The Oxford Handbook of Qualitative Research*. Oxford University Press.

Lee, G. and Fargher, N. 2013. ‘Companies’ Use of Whistle-Blowing to Detect Fraud: An Examination of Corporate Whistle-Blowing Policies’, *Journal of Business Ethics*, 114(2), pp. 283–295. doi: 10.1007/s10551-012-1348-9.

Mangala, D. and Kumari, P. 2015. ‘Corporate Fraud Prevention and Detection’, *Journal of Commerce & Accounting Research*, 4(1), pp. 51–62. <http://www.publishingindia.com>.

McLaughlin, J. and Pavelka, D. 2009. ‘Anti-Money Laundering Initiatives : A Briefing for Busness Educators’, in *Business, Society & Governmenr Consortium*. Chicago, pp. 92–113.

Moleong, L. 2014. *Metodologi Penelitian Kualitatif : Edisi Revisi*. Bandung: PT Remaja Rosdakarya.

Murdoch, S. J. and Anderson, R. 2010. ‘Verified by Visa and MasterCard SecureCode: Or, How not to Design Authentication’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6052 LNCS, pp. 336–342. doi: 10.1007/978-3-642-

14577-3_27.

Nugroho, Ivan. 2018. Interview dengan Ivan Nugroho, diinterview oleh Dewi Kilisuci A.P., 16 Maret, Yogyakarta.

Otoritas Jasa Keuangan. 2015. Laporan Tahunan Perbankan 2015. Jakarta.
<http://www.ojk.go.id>.

Otoritas Jasa Keuangan. 2017a. Laporan Triwulanan I OJK. Jakarta.
<http://www.ojk.go.id>.

Otoritas Jasa Keuangan. 2017b. Laporan Triwulanan II OJK. Jakarta.
<http://www.ojk.go.id>.

Otoritas Jasa Keuangan. 2017c. Laporan Triwulanan III OJK.
<http://www.ojk.go.id>.

Otoritas Jasa Keuangan. 2017d. Laporan Triwulanan IV OJK. Jakarta. A
<http://www.ojk.go.id>.

Parimita, W., Pambudi, W. S. and Aminah, H. 2017. 'The Impact of Career Development and Workload Toward Employee Job Satisfaction at PT Askrindo', *Jurnal Riset Manajemen Sains Indonesia (JRMSI)*, 8(1), pp. 39–57. doi: doi.org/10.21009/JRMSI.008.1.03.

PT. Bank BPD DIY. 2016. Laporan Tahunan 2016 'Sustainably Growing. Yogyakarta. <http://www.bpddiy.co.id>.

- Pusdiklatwas BPKP. 2008. *Kode Etik dan Standar Audit*. Kelima. Bogor: Pusat Pendidikan dan Pelatihan Pengawasan BPKP.
- Ruankaew, T. 2016. 'Beyond the Fraud Diamond', *International Journal of Business Management and Economic Research (IJBMER)*, 7(1), pp. 474–476.
- Rubasundram, G. A. 2015. 'Perceived "Tone From the Top" During A Fraud Risk Assessment', *Procedia Economics and Finance*. Elsevier B.V., 28(April), pp. 102–106. doi: 10.1016/S2212-5671(15)01087-4.
- Salam, M. A. 2018. Interview dengan Muhammad Agus Salam S., diinterview oleh Dewi Kilisuci A.P., 15 Maret, Yogyakarta.
- Sanusi, S. L. 2010. 'Growth Prospects for The Nigerian economy', *Research Department of the Central Bank of Nigeria*, (November), pp. 1–18.
- Sekaran, U. and Bougie, R. 2017. *Metode Penelitian untuk Bisnis, Pendekatan Pengembangan Keahlian*. 6th edn. Edited by A. N. Hanifah. Jakarta: Salemba Empat.
- Siregar, S. V. and Tenoyo, B. 2015. 'Fraud Awareness Survey of Private Sector in Indonesia', *Journal of Financial Crime*, 22(3), pp. 329–346. doi: 10.1108/JFC-03-2014-0016.
- Suhartono, S. 2016. 'Komite Anti Fraud: Solusi Menuju Zero Fraud', 5(1), pp. 90–104. doi: ISSN : 2089-7219.
- Usman, A. K. and Shah, M. H. 2013. 'Critical Success Factors for Preventing

e-Banking Fraud', *Journal of Internet Banking and Commerce*, 15(1), pp. 1–11.

doi: 10.1007/978-3-531-92534-9_12.

Villena, M. G. and Villena, M. J. 2009. *On The Economics of Whistle-blowing behavior : The Role of Incentive*. Chile. <https://mpra.ub.uni-muenchen.de/36310/>.

Wibisono, P. W. 2015. 'Pengaruh Reward and Punishment dan Job Rotation Terhadap Fraud'. Universitas Negeri Yogyakarta.

Widjaja, A. T. 2005. *Pokok - Pokok Audit Kecurangan*. Jakarta: Harvarindo.

Yin, R. K. 1981. 'The Case Study as a Serious Research Strategy', *Science Communication*, 3(1), pp. 97–114. doi: 10.1177/107554708100300106.

Zikmund, P. E. 2008. 'Reducing The Expectation GAP', *The CPA Journal*.

LAMPIRAN

LAMPIRAN 1**TRANSKRIP WAWANCARA 1**

Narasumber : Ibu Nur Aeni

Tanggal Wawancara : 8 Maret 2018

Jabatan : Pemimpin Divisi Manajemen Risiko dan
Kepatuhan

P : Pewawancara

N : Narasumber

P : Bagaimana koordinasi antara tugas Manajemen Risiko dan SKAI?

N : SKAI dalam melakukan audit nya akan membuat rencana audit dalam satu tahun kedepan itu dasarnya adalah penilaian risiko dari manajemen risiko. Jadi ini adalah dua divisi yang terpisah, SKAI sama manajemen risiko. Kita akan mendapatkan penilaian manajemen risiko masing – masing cabang itu kita lihat, misalnya ada disini 7 cabang, dari 7 cabang itu ternyata hanya 5 ini yang memiliki risiko operasional tertinggi, makannya di 5 cabang ini SKAI akan melakukan audit operasional yang lebih dalam. Mungkin yang 2 enggak, disini bukan risiko operasional tapi risiko hukum, bisa jadi kan. Memang SKAI dan manajemen risiko itu terkait. Pada saat manajemen risiko membuat laporan, SKAI akan membuat sebuah rencana *business plan* pada satu tahun kedepan,

apa – apa saja yang akan dilakukan audit. Nah kalo bicara mengenai anti fraud, itu akan berjalan pada saat kita melakukan audit operasional. Kemudian sebagai audit operasional itu kita lihat, kayaknya ada praduga tidak bersalah ni, ada fraud. Itu nanti anti fraud akan masuk. Jadi anti fraud kalau tidak ada fraud dia tidak akan bergerak, dia hanya bergerak sebagai audit biasa. Tapi dalam hasil audit biasa itu ada praduga tidak bersalah, atau ada gejala menuju fraud, lalu SKAI akan membuat surat tugas sendiri. Jadi awalnya surat tugas audit secara umum, secara umum itu bisa operasional, bisa audit khusus kredit, audit khusus kepagawaian.

P : Jadi nanti jika ada risiko signifikan misal dibagian kredit, yang maju tim anti fraud nya?

N : Jadi itu nanti akan ada surat tugas baru. Saat audit umum kita melihat sepertinya di satu titik ini akan ada masalah yang signifikan, dan ada kemungkinan cenderung ke fraud. Nah baru anti fraud ini mengambil tindakan memperdalam.

P : Kalau orang – orang tim anti fraud itu nanti yang ada di dalam SKAI juga?

N : Iya. Karena anti fraud itu ada di bawah SKAI. Jadi SKAI itu ada 3 tiga bagian, audit kredit, audit operasional, anti fraud. Jadi itu ada PBI nya. Jadi anti fraud bank itu ada yang berdiri sendiri dan ada yang di dalam (SKAI), nah ini tergantung dari *size* bank nya. Karena BPD ini hanya satu wilayah DIY

saja, sehingga anti fraud ini dibawah SKAI. Dan juga ditahun 2017 ini kan *zero fraud*, ya kalo bisa memang selalu *zero fraud*. Jadi kalau misalnya adapun tetap dibawah naungan SKAI.

P : Kalau untuk penerapan strategi anti fraud itu SKAI juga atau anti fraud?

N : Anti fraud. Jadi jika sudah bicara ke fraud ya anti fraud. Strategi apa yang harus dia buat. Jadi misalnya didalam pekerjaan rutin dia (SKAI) itu kayak anti fraud. Tapi jika ada fraud ya dia akan melakukan audit fraud. Tapi dia akan berusaha *zero fraud*, sehingga dia (SKAI) akan sosialisasi ke cabang. Dijelaskan jika melakukan fraud akan berdampak seperti pegawai tersebut dikeluarkan. Nah selain itu dia akan mengelola *Whistleblowing*. Misalnya ada gak masukan. Bisa dari internal bisa dari eksternal.

P : Jadi kalau aduan seperti itu melalui *website* atau sms?

N : Hanya kalau di kita internal. Kalau bicara eksternal biasanya lewat surat kaleng. Kalau bicara di sistem itu *website*. Jadi khusus untuk internal melalui *website*. WBS yang mengelola ya tim anti fraud.

P : Jadi kalau menemukan aduan yang signifikan untuk diperdalam akan lapor ke SKAI dulu?

N : Iya. Nanti otomatis SKAI akan meminta dibuatkan surat tugas dari direktur utama.

P : Jadi SKAI juga bisa langsung ke direktur utama ya bu?

N : Jadi manajemen risiko dan SKAI itu dua hal yang sejajar ya. Tapi SKAI itu bisa langsung ke direktur utama.

P : Kalau manajemen risiko ke kepatuhan ya?

N : Iya. Sudah punya struktur organisasinya BPD ya?

P : Sudah bu, sudah saya print

N : Memang anti fraud itu baru. Tapi sudah dibuat PBI nya kan itu tentang anti fraud yang setiap bank harus punya unit, sehingga dibuat anti fraud.

P : Berarti manajemen risiko itu koordinasi sama SKAI itu hanya saat SKAI mau membuat strategi ya?

N : Iya.

P : Jadi bukan saat SKAI membuat laporan trisemester, nanti manajemen risiko akan memberitahu untuk ke cabang – cabang yang memiliki risiko signifikan untuk dilakukan audit khusus?

N : Jadi manajemen risiko ini setiap triwulan atau semester akan membuat laporan dimana dia akan turun ke semua unit kantor pusat dan kantor cabang. Dilihat risiko mana yang ada, berapa nilainya dan risiko mana yang tinggi. Saya lupa laporannya triwulan atau semesteran, tapi SKAI ini harus nempel terus ke manajemen risiko. Jadi setiap hasil dari manajemen risiko akan dipakai dasar bagi SKAI untuk dipakai audit.

P : Jadi manajemen risiko akan melakukan penilaian risiko dulu baru SKAI akan bertindak ya bu?

N : Iyaa...

P: Jadi SKAI itu kan ada sitem pengendalian internal ya, nanti ada hubungannya dengan manajemen risiko tidak bu?

N : Tidak ada. Jadi gini, ini manajemen risiko, dasarnya akan dilaksanakan audit, nah dengan adanya audit ini kan akan mengecilkan risiko. Sehingga keduanya seperti lingkaran yang tidak terpisahkan. Dan hasil audit ini yang akan masuk manajemen risiko. Hasil audit apa saja tahun sebelumnya yang masih belum sesuai ketentuan atau SOP. Kan orang kalau bekerja jika ada yang mengawasi artinya risiko nya kecil, kesalahan *human error* nya kecil, dia akan merasa “aku harus hati – hati” karena diawasi. Nah akhirnya risiko operasionalnya turun. Nah jadi akan saling terkait, dimana hasil manajemen risiko akan menjadi dasar untuk melakukan audit, tetapi apa yang dilakukan audit akan mengecilkan risiko untuk kedepannya.

P: Jadi manajemen risiko itu tidak terjun langsung membantu berlangsungnya strategi anti fraud ya bu? Tetapi nanti dalam bentuk laporan akan dilaporkan ke SKAI, baru SKAI menindaklanjuti?

N : Iya, jadi kalau bicara anti fraud itu pencegahannya itu satu, dia akan melakukan sosialisasi. Risiko – risiko nya jika melakukan fraud itu seperti apa, bisa dikeluarkan, bisa ditangkap polisi.

P : Kalau sosialisasi itu nanti lewat apa bu dalam internal?

N : Seperti mas adi (Unit Anti Fraud), dia melakukan sosialisasi ke cabang – cabang. Jadi menilai risiko di kantor pusat dan cabang, audit pun di kantor pusat dan cabang.

P : Tapi SDM nya semua di kantor pusat atau ada yang di cabang?

N : Kalau untuk SKAI itu juga ada di cabang. Jadi nanti SKAI akan mendapat laporan dari SKAI yang ada di cabang.

P : Kalau manajemen risiko di pusat semua ya bu?

N : Iyaa..

P : Kalau sosialisasi itu seminar atau bagaimana?

N : Bukan, jadi dikumpulkan kayak pendidikan. Jadi dijelaskan WBS itu bagaimana, jika ada teman yang melakukan pelanggaran dan merasa tidak enak ya lewat WBS. Kan WBS lebih tidak diketahui yang melapor.

P : Jadi WBS di sosialisasikan ke semua jajaran organisasi atau ke pimpinan saja?

N : Tidak tidak, ke semua jajaran organisasi. Sosialisasi ini paling tiga bulan sekali. SKAI melihat ada indikasi fraud selain dari laporan audit juga dari laporan – laporan lain.

P : WBS kalau untuk eksternal bagaimana?

N : Kalau untuk yang sistem WBS hanya internal, kita belum berani ke eksternal. Kalau eksternal kan kadang ada laporan yang hanya buat – buat saja. Jadi lebih ke surat kaleng begitu.

P : Kalau semisal ada nasabah yang mengeluh tabungannya berkurang padahal dia tidak melakukan transaksi itu nanti dia akan mengeluh ke bagian apa?

N : Ooh jadi nanti itu lain. Kalau di bank, PBI nya lain. Itu masuk ke unit pengaduan. Nanti laporan otomatis ke kantor cabang, nah dari kantor cabang diteruskan dikantor pusat ada unit namanya unit perencanaan dan pengembangan. Jadi khusus WBS untuk internal. Kalau eksternal seperti itu bisa lewat surat – surat ataupun laporan lisan. Kalau dari PBI sendiri itu ada aturannya maksimal 3 hari kerja aduan itu sudah selesai. Jadi nasabah maksimal sudah dapat jawaban penyebabnya dan selesai masalahnya. Kecuali jika unit perencanaan itu melihat ada gejala fraud, nah itu nanti akan terjadi lintas divisi, artinya unit perencanaan koordinasi ke SKAI untuk dilakukan audit lanjutan.

P : Kalau untuk transaksi seperti kredit, apa pernah nasabah berusaha menipu bank? Seperti memberikan data palsu?

N : Sebenarnya seperti itu banyak, makannya bank itu ada *prudence* / kehati – hatian. Kembali lagi ke analis, saat penerimaan dikroscek slip gajinya, benar tidak dai pegawai situ.

P : Kalau semisal ditemukan seperti itu tindakan yang dilakukan ke nasabah bagaimana?

N : Kan kita ada agunannya. Di kita ada 2 kredit yang menggunakan agunan atau potong gaji. Kalau potong gaji itu tidak ada masalah. Tapi kembali lagi

kalau ada debitor nakal seperti tadi itu ya kita eksekusi jaminannya. Kan ada *second without nya*.

P : Siapa yang membuat WBS?

N : WBS itu dibuat oleh TI kita, tapi untuk pengelolaannya dilakukan SKAI yang sekarang ada Unit Anti Fraud.

P : Apa ada rotasi pegawai bu?

N : Iya ada. Biasanya 4 tahun sekali. Dulu saya di SKAI, sekarang di Manajemen Risiko. Nah seperti rotasi pegawai itu merupakan salah satu mitigasi kepada karyawan untuk tidak berbuat fraud. Lalu untuk mitigasi karyawan tidak berbuat fraud itu dibuat namanya cuti. Cuti itu harus di ambil. Pada saat dia cuti kan digantikan sama teman lain yang satu unit. Bisa jadi kan dia (temennya) menemukan.

P : Untuk jatah cuti itu bagaimana sistemnya bu?

N : Satu tahun 12 hari, boleh diambil kapan saja dan wajib diambil. Biasanya pegawai hanya ambil satu dua hari, kalau seperti itu susah digantikan pegawai lain, karena kan jika digantikan teman dan waktunya cukup lama, kemungkinan ditemukan hal yang tidak wajar jadi lebih besar.

P : Kalau jatah cuti tidak diambil boleh diganti gaji?

N : Nggak boleh.

P : Kalau SKAI pengendalian internal nya sudah dilakukan darimana bu?

N : Pengendalian internal teller misalnya dari slip. Pada saat selesai jam kantor itu harus nol, tidak boleh selisih. Itu transaksinya, kalau pengendaliannya itu kan teller ada atasannya, nah atasannya itu harus mengoreksi setiap transaksi yang terjadi per hari.

P : Jadi tidak mungkin ya bu cek di palsukan?

N : Jadi kalau bicara cek dipalsukan, cuman kan tinggal pengendalian internalnya gimana. Jadi kalau semisal ada yang meneliti, kan harus jelas, tandatangan *speciment* ini sama gak seperti si pemilik cek ini. Itu termasuk salah satu pengendalian mencocokkan. Terus dimintai ktp si pencair. Sebenarnya setiap bank itu kan ada SOP (Standar Operasional Prosedur), kalau semua itu dijalankan maka akan sangat minimal bahkan tidak ada namanya fraud. Tapi bisa jadi ada orang kehilangan cek dan jatuh, cuma kembali lagi *speciment* (tandatangan) nya akan dicocokkan *speciment* pemilik. Pada saat pencairan pun kalau melebihi kewenangan itu kan tetep yang harus mengotorisasi kan atasannya, jadi teller itu hanya bisa mengeluarkan 10 juta, tapi ceknya itu 25 juta. Teller tetap tidak bisa mengeluarkan, walaupun warkat sah, *speciment* sama, nomer PG nya sama. Jadi satu cek itu pengendaliannya banyak. Saat bank mengeluarkan cek itu pasti ada nomer seri nya, nah nomer seri itu sudah di input di sistem. Jadi kalau semisal orang buat cek di percetakan, otomatis nomer seri nya tidak ada. Nah itu udah pengendalian awal, pengendalian kedua dilihat *speciment* nya, pengendalian ketiga ada untuk diotorisasi atasannya.

P : Kalau seperti phishing, skimming atau pengambilan data nasabah oleh orang luar itu ada tidak?

N : Ada, baru saja terjadi, semua bank kena. Itu *skimmer* nya dipasang di ATM. Nah pengendalian internal yang kita lakukan pada ATM kita itu pada saat kita rutin melihat di mulut ATM. Jadi kalau kamu punya kartu ATM, sebelumnya kalau di mulut ATM ada yang mencurigakan itu jangan kamu masukkan. Jadi ATM kan bisa dilakukan lintas bank, seperti ATM Bersama, nah makannya kena di ATM lain karena terpasang *skimmer*. Karena itu pengendalian internal itu di kita, setiap hari mulut ATM kita periksa.

P : Jadi di BPD ini setiap hari dicek oleh siapa bu?

N : Iya, itu dilakukan di bagian pelayanan. Kan ATM kita kebanyakan di kantor kita. Jadi bukan di mall, ya pokoknya yang jauh dari kantor bank. Yang sering terpasang justru ATM – ATM yang jauh, atau tertutup. Kan kalau di mall terbuka, terkadang kalau mau pasang bisa terlihat. Biasanya ATM – ATM yang dikotak – kotaki cuma ada satu.

P : Kalau seperti itu kan merugikan nasabah dan menurunkan citra bank, itu nasabahnya diberikan sosialisasi tidak?

N : Jadi sosialisasi itu tugasnya semua bank. Itu kalau di kita yang membuat divisi perencanaan sebelum tim fraud ada. Nanti akan mengundang nasabah - nasabah kita, nanti kita bentuk seperti *gathering*. Kita beri sosialisasi bahwa saat akan memakai ATM diperiksa dahulu ada *skimmer* tidak, dan pin itu hanya punya kita pribadi jangan dikasihkan orang lain. Itu ada PBI nya juga.

Namanya orang juga kan gak semua bisa karena udah tua, cuman minta tolong orang waktu di ATM dan kebetulan dapat orang yang tidak baik. Jika ada laporan juga kita buka ni kapan transaksinya, jam berapa, di terminal mana, kan ada CCTV nya disetiap ATM kita buka. Nanti kita tunjukkan ke nasabah, kenal tidak, ada itu kejadian ternyata anaknya sendiri. Ibu nya pernah tidak memberikan pin ke anaknya? Biasanya pernah karena minta diambilkan, mungkin karena usianya sudah lanjut dan tidak memungkinkan, atau diminta tolong ambilkan pensiunan. Kadang kan tergantung, kalo anaknya tidak baik atau diri kita yang lupa. Karena ada itu ternyata kesalahan nasabah sendiri.

P : Kalau semisal nasabah berupa perusahaan gitu apakah pernah bu mereka terlibat seperti money laundering?

N : Kalau selama ini di BPD gak ada, tapi mungkin di bank lain ada. Jadi sebenarnya yang sulit itu kita harus melaporkan ke PPATK tentang setoran tunai. Ada nasabah menyetorkan uang tunai 1 Milyar. Nah sulitnya mengidentifikasi nilai uang yang mencurigakan, karena walaupun hanya 100 ribu juga bisa dianggap mencurigakan. Tapi ini pun sudah kita antisipasi. Jadi ada APU, Anti Pencucian Uang. Jadi di kita di sistem, misalnya ni saya, misal gaji saya sebulan 10 juta, apabila di rekening saya terjadi transaksi melebihi 5 kali gaji saya, itu akan ada *warning* di sistem kita, dianggap transaksi mencurigakan. Akan dilihat darimana asal uang. Misal ternyata saya mendapatkan transferan itu dari hasil penjualan tanah, yasudah tidak ditindaklanjuti.

penjualan tanah, yasudah tidak ditindaklanjuti.

P : Apakah pernah dilakukan surprise audit oleh Unit Anti Fraud?

N : Pernah mbak. Tapi karena dulu strategi anti fraud masih SKAI yang menjalankan jadi dilakukan sekalian dengan audit umum. Tapi kalau sekarang mereka biasanya jika akan surprise audit ke cabang gitu ya susahnya saat informasi bocor, jadi pihak cabang kayak misal Wates, itu sudah siap - siap dahulu.

P : Kalau surprise audit kan ada di tim anti fraud kan ada, di manajemen risiko ada?

N : Ooh tidak ada.

P : Kalau perekrutan SDM itu bagian yang merekrut ada kualifikasi bahwa SDM nya kompeten?

N : Kita ada, standar itu ada. Kita bisa buka informasi debitur, dari OJK namanya indeb (identitas debitur). Kalau kita mau merekrut itu nanti kita ambilkan indeb. Misal ternyata dia ini punya kredit macet di bank lain, kenapa bisa macet? Apa karena ngemplang atau tidak punya i'tikad yang baik, kemudian kita minta SKCK, tidak menggunakan narkoba. Kalau masalah kompeten pendidikan kita kan kerjasama sama UGM untuk rekrutmen.

P : Kalau sertifikasi atau pendidikan itu disediakan untuk pegawai atau tidak?

N : Oh iya, jadi bank itu ada sertifikasi 5 level, semua harus punya. Minimal sekali punya 1 level, tergantung jenjang jabatannya. Untuk staff harus level 1.

P : Kalau akan dipromosikan naik itu harus naik ke level berikutnya?

N : Iya.

P : Apakah itu semua dibiayai bank?

N : Iya, jadi di kita itu semisal kamu ambil sertifikasi ni sekali gak lulus, coba lagi kedua gak lulus, nah baru yang ketiga kamu biayai sendiri. Jadi jatahnya 2 kali. Tapi masing – masing bank punya kebijakan sendiri.

P : Kalau pegawai itu sekali saja lulus, tapi masih ingin ambil sertifikasi tingkat atasnya lagi, itu masih bisa dibiayai lagi?

N : Iya semua dibiayai. Jadi level 1 dibiayai, level 2 dibiayai, seterusnya sampai level 5 dan masing – masing jatahnya 2 kali.

P : Apakah untuk Unit Anti Fraud sudah semua bersertifikasi?

N : Setahu saya karena mereka baru dan hanya terdiri dari dua orang, mereka untuk sertifikasi khusus belum ada, hanya baru sertifikasi untuk internal audit.

P : Pernah tidak bu terjadi *management override*?

N : Nggak ada mba itu...

P : Kalau rekrut pegawai ada syarat harus sertifikasi tidak bu?

N : Ooh tidak ada.. Tapi kalau dia udah punya sendiri tidak masalah.

LAMPIRAN 2**TRANSKRIP WAWANCARA 2**

Narasumber : Bapak Suwasono Adi Kurniawan

Tanggal Wawancara : 9 Maret 2018

Jabatan : Pemimpin Unit Anti Fraud

P : Pewawancara

N : Narasumber

P : Bagaimana peran masing – masing bagian di dalam struktur organisasi mengenai penerapan strategi anti fraud?

N : Di kita, BPD DIY, untuk tim sendiri, di kita unit anti fraud baru ada sejak 2017, namun untuk penerapan strategi anti fraud sudah sejak 2012. Karena sesuai dengan PBI, PBI mewajibkan di tahun 2011 itu dan tahun 2012 kita langsung menerapkan, isinya kurang lebih sama, cuman waktu itu dia masih yang mengelola di SKAI, jadi belum ada tim khususnya. Isinya sama dengan yang ada disini (menunjuk BPP Strategi Anti Fraud) cuman memang tidak ada yang membidangi secara terpusat. Karena kan di setiap perusahaan itu kan kalau mau ada perubahan organisasi harus ada perencanaan lalu diputuskan dalam RUPS dan sebagainya. Di tahun 2016 sudah direncanakan dan definitif ada di awal tahun 2017. Jadi baru tahun kemarin ada unit

khusus, unit anti fraud namanya. Secara organisasi berada dibawah Satuan Kerja Audit Internal. Dengan personilnya ada 2, saya dan mas Zukhron tadi, dan saya yang jadi pemimpin unit anti fraud nya, dan mas Zukhron sebagai staff.

N : Kalau untuk peran masing – masing bagian itu maksudnya seluruh organisasi?

P :Iya pak kan saya lihat tidak ada di struktur organisasi di laporan tahunan 2016, jadi saya kira semua bagian di struktur organisasi ikut berperan.

N : Nah iya karena di tahun 2017 kita sudah ada, bisa di copy struktur organisasi kita tahun 2017, karena kita sudah ada unit anti fraud.

P :Apakah Unit Anti Fraud akan ditambah lagi personilnya?

N : Rencana untuk kesitu belum ada, tapi mungkin akan segera kami lakukan. Karena kan ini unit nya baru terbentuk juga.

P :Bagaimana mekanisme penerapan strategi anti fraud pada kantor cabang?

N : Kita setelah ada unit, kita kan selain SKAI yang di kantor pusat, juga ada namanya Kontrol Intern Cabang, ada 1 orang KIC dengan 1 staff, untuk kantor cabang besar seperti sleman, kita ada 2 orang staff, itu adalah tim SKAI kita yang ada di cabang. Di cabang dia bertanggung jawab langsung terhadap pemimpin SKAI. Di cabang dia Cuma nebeng ruangan, semua

peralatan dari kita, komputer, printer dan gaji ikut pusat. Mereka benar – benar nebeng dan tidak ikut melakukan kegiatan operasional cabang.

P :KIC melakukan tugasnya setiap kapan saja?

N : Sehari – hari, jadi dia lebih memantau pengendalian internalnya berjalan. Mulai dari verifikasi, kadang juga surprise audit untuk teller, diminta untuk langsung cek jumlah uang, karena dia auditor juga jadi bisa melakukan itu. Kalau di perusahaan lain mungkin namanya *residence auditor*. Nah dari kantor cabang ada *report* berkala langsung ke sini (kantor pusat), kalau ada audit dari kantor pusat juga nanti dia (KIC) juga akan ikut tim kita. Dari temen – temen cabang sendiri juga kita bekali terutama supervisor atau pemimpin cabang yaitu indikasi fraud begitu.

P :Kalau untuk *red flags* sendiri bagaimana pak?

N : Kami bekali juga untuk hal – hal seperti itu, walaupun tidak khusus memantau karena job nya banyak. Indikasi fraud apa saja, mereka membantu memantau staff – staffnya yang agak aneh seperti pergantian pola hidup seperti itu. Kalau tidak *report* kesini bisa ke KIC. Semua memang dari kantor – kantor cabang, termasuk semua itu membuat pemetaan titik – titik kerawanan. Misalnya proses pembukaan tabungan, itu titik rawannya dimana. Kalau di *risk based audit* itu nanti kan kita harus memperhatikan mana yang menimbulkan risiko tertinggi.

P :Apakah ada kerjasama dengan manajemen risiko?

N : Kalau untuk kerjasama jelas ada, tapi di kita bahkan mungkin tempat lain, jadi gini, manajemen risiko itu lebih ke pra kejadian jadi untuk pencegahan. Nah SKAI itu setelah kejadian. Jadi di kita itu dikenal dengan *three line of defense*. Jadi menghadapi risiko yang pertama itu yang di *front office*, yang di cabang berhadapan dengan nasabah. Yang kedua yang mengawasi mereka itu manajemen risiko. Nah yang ketiga itu setelah kejadian untuk SKAI sendiri, itu kita mengaudit apa yang telah terjadi, sedangkan manajemen risiko tidak. Ketika mau melangkah konsultasi ke manajemen risiko seperti ini ini nah bisa jadi tidak jadi mengaudit lanjutan itu bisa. Misalnya untuk kredit, saat diajukan itu dinilai. Tapi saat sudah cair nanti kita turun (SKAI).

P : Bagaimana perbedaan SKAI dan Unit Anti Fraud?

N : Kalau anti fraud itu nanti jika hanya sudah ada indikasi adanya fraud, kita memastikan, mencari bukti. Namun jika tidak ada fraud kita juga punya peran juga untuk mendeteksi dan pencegahan. Jadi di Anti Fraud itu kita ada 4, pencegahan, pendeteksian, investigasi dan pelaporan, sama seperti di kuliah kan. Nanti kalau pencegahan kita melalui sosialisasi, kalau untuk pegawai nanti di desktop semua komputer akan berganti *background* dengan konten – konten berhubungan dengan anti fraud, dan akan ada kampanye juga tentang anti fraud ke kantor – kantor cabang.

P : Kalau untuk kampanye sosialisasi budaya anti fraud itu bagaimana pak?

N : Jadi itu kita keliling ke kantor – kantor cabang untuk sosialisasi anti fraud. Kemarin sudah keliling ke cabang sleman, dari kantor cabang pembantu sampai ke kantor kas, itu kita kumpulkan seharian, kita sosialisasikan, yang rawan dimana, indikasi – indikasinya, penyebab fraud secara teori seperti ini dan kalau hasil survey seperti ini. Sudah dimulai sebelum 2017, tapi dulu kan belum ada unit anti fraud, jadi saat audit begitu sekalian. Kalau sekarang kan bisa jalan sendiri – sendiri, jadi ada tim yang audit dan juga kita (unit anti fraud) jalan sendiri.

P :Seperti apa penerapan anti *fraud awareness*?

N : Kita baru akan melakukan, tapi sudah siap materinya. Selama ini sudah ada pakta integritas, di awal tahun semua pegawai akan dapat. Nah setelah ada unit ini, ada tambahan lagi, kalau pakta integritas kan semua manajemen dan pegawai, kalau ini yang dari unit anti fraud, namanya *Anti Fraud Statement*. Ini tapi belum kita jalankan, baru sosialisasi dulu ke semua cabang. Ini tambahan untuk pengurus yaitu Direksi dan Dewan Komisaris juga tanda tangan.

P :Jadi dengan tanda tangan ini dari awal mereka sudah berstatement untuk melakukan ini?

N : Iya.. (membacakan isinya)

- 1) Dewan Komisaris dan Direksi bertanggung jawab atas terlaksananya strategi anti fraud.

- 2) Dewan Komisaris sepenuhnya mendukung dan senantiasa mengawasi langkah – langkah yang diambil dalam penerapan strategi anti fraud.
- 3) Bahwa dalam rangka mewujudkan budaya anti fraud Direksi akan bertanggungjawab menerapkan strategi anti fraud pada semua tingkatan organisasi.
- 4) Bahwa dalam rangka melaksanakan strategi anti fraud SKAI bertanggungjawab dalam pengelolaan pelaksanaannya.
- 5) Bahwa dalam rangkaantisipasi terjadinya fraud Dewan Komisaris dan Direksi bersama dengan pegawai bank berkewajiban melaporkan fakta penyimpangan yang terjadi yang berpotensi fraud kepada OJK
- 6) Bahwa dalam rangkaantisipasi terjadinya fraud Direksi dan Dewan Komisaris berkomitmen untuk melindungi pelapor kecurangan dalam bentuk kerahasiaan

P : Melindungi pelapor itu bagaimana pak?

N : Dalam bentuk kerahasiaan ya, kalau perilaku seperti undang – undang kan kita susah. Harus dijaga rumahnya, kan kita gak punya wewenang kesitu

- 7) Bahwa dalam rangkaantisipasi terjadinya fraud Direksi dan Dewan Komisaris tidak mentolerir (*zero tolerance*) terhadap setiap tindakan fraud

Ini ditandatangani Dewan Komisaris, Komisaris Utama, Direktur Utama, Pemasaran, Umum, Kepatuhan

Nah ini yang pegawai.

Saya yang bertanda tangan dibawah ini :

Nama :

Nomor Induk Pegawai :

Pangkat / Jabatan :

Unit Kerja :

Menyatakan persetujuan untuk melaksanakan strategi anti *fraud* yang dikemukakan dalam Buku Pedoman Strategi Anti *Fraud* dan memahami bahwa bank tidak akan mentolerir setiap tindakan *fraud* yang dilakukan dan akan menerapkan sanksi tegas terhadap pelaku *fraud*. Nilai – nilai inti yang disepakati adalah sebagai berikut:

- 1) Setiap insan bank sebelum melaksanakan kegiatan, selalu diawali dengan niat baik dan semata – mata bekerja untuk kepentingan bank serta tidak merugikan orang lain, yang dilandasi keikhlasan dan tulus sehingga dapat memuaskan *stakeholders*.
- 2) Setiap insan bank berkewajiban menghindari perbuatan-perbuatan penyimpangan yang dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah atau pihak lain menderita kerugian dan/atau pelaku *fraud* memperoleh keuntungan.
- 3) Setiap insan bank berkewajiban melaporkan setiap fakta penyimpangan yang dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain yang terjadi di

lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah atau pihak lain menderita kerugian.

- 4) Setiap insan bank tidak diperbolehkan memberi dan/atau menerima hadiah/cinderamata/gratifikasi dalam bentuk apapun yang berhubungan dengan jabatan dan pekerjaannya sehingga menimbulkan konflik kepentingan.

Sehingga pernyataan ini dinyatakan dengan penuh kesadaran serta memahami ketentuan ini merupakan komitmen saya dalam penerapan strategi anti *fraud* dan merupakan hal penting untuk dijaga dan meningkatkan efektivitasnya.

Nah ini yang termasuk *fraud awareness*, selain sosialisasi aturan ini juga ada. Kita juga melakukan sosialisasi secara lisan setiap kesempatan kepada seluruh pegawai.

P : Bagaimana cara menumbuhkan budaya untuk melaporkan tindakan *fraud*?

N : Kalau orang Jawa kan ewuh-pekewuh, kita mencoba mengedukasi itu dengan kita sediakan saluran *whistleblowing*. Kalau tidak enak untuk mengatakannya kepada atasan jika teman satu divisi yang melakukannya kan bisa langsung ke sistem itu, kita jamin kerahasiaannya. Yang bisa membuka *whistleblowing* itu sementara ini tim SKAI. Kita sedang dalam proses mau merombak juga tampilannya agar terlihat lebih familiar karena kan sudah ada unit anti *fraud*.

P : Apakah banyak yang berpartisipasi dalam WBS?

N : Nah itu yang menjadi permasalahan, karena untuk tahun ini yang saya lihat dari laporan hasil pengaduan hanya sedikit sekali yang melaporkan. Entah karena tampilan WBS tidak menarik yang sedang kami usulkan ke Direktur, atau juga karena merasa bahwa tidak semua indikasi penting untuk dilaporkan.

P : *Whistleblowing system* ini melalui internet atau sms pak?

N : Melalui intranet. Jadi di kantor kita ini semua terhubung satu jaringan untuk internal saja. Sementara kita untuk internal dulu, kalau untuk eksternal sudah ada di website kita untuk aduan, kritik & saran. Sementara ini juga sering informasi masuk dari situ.

P : Bagaimana pelaksanaan *customer awareness*?

N : Ini kita melakukannya hanya semacam sosialisasi dengan bantuan kantor cabang untuk sosialisasi ke instansi mana, nah itu kita selipkan materi tentang strategi anti *fraud*. Kita juga sudah mempersiapkan brosur, selain kita membuat brosur tentang produk kita, kita juga akan membuat brosur tentang pelaksanaan strategi anti fraud. Tapi ini masih dalam proses karena kan unit anti *fraud* masih baru. Dan nantinya kan tayangan tv yang ada di bawah yang langsung terlihat oleh *customer* biasanya hanya informasi tentang *rate*, nilai kurs dan produk kita, nantinya akan kita munculkan materi tentang strategi anti fraud.

P : Seperti apa identifikasi kerawanan dalam proses penilaian risiko?

N : Nah ini kan jelas manajemen risiko punya sendiri, tapi kan kita juga berusaha juga untuk punya sendiri. Kita kan SKAI independen, jadi kalau

pakai penilaian risiko ya berusaha pakai penilaian kita sendiri. Kerawanan risiko itu seperti ini (menunjuk buku).

Proses manajemen risiko untuk mengidentifikasi, menganalisa dan menilai proses potensi risiko terjadinya fraud dilakukan terhadap seluruh aktivitas yang menimbulkan risiko. Dilakukan oleh masing – masing unit kerja, unit pelayanan membuat sendiri, unit kredit membuat sendiri, administrasi kredit membuat sendiri. Minimal isinya :

Nama produk : deposito atau tabungan

Aktivitas : pembukaan deposito atau pembukaan tabungan

Misalnya juga divisi *treasury* mengeluarkan produk baru, nanti kan mengeluarkan SOP, nah nanti akan tercantum risiko – risiko yang melekat. Kita sudah ada semua. Proses bisnis yang berpotensi sekiranya menimbulkan *fraud* juga. Ada juga kajian mengenai identifikasi risiko, nah kajian itu bisa di mitigasi dengan langkahnya ini dan ini.

Ini SOP ATM BPD DIY (memegang buku), semua prosedur tentang ATM ada disini semua. Kalau ATM rusak dan harus dimusnahkan langkahnya apa, *maintanance system* nya bagaimana, lengkap semua. Nah dibagian akhir selalu ada kebijakan manajemen risiko. Contohnya ini, risiko operasional, internal fraud :

- 1) Penerbitan kartu debit palsu oleh karyawan
- 2) Menerbitkan kartu ATM tanpa persetujuan pejabat yang berwenang
- 3) Pencurian informasi kartu ATM oleh karyawan
- 4) Penarikan dana oleh karyawan dengan kartu ATM palsu

Mitigasi nya :

- 1) Sosialisasi budaya risiko pada karyawan
- 2) Sosialisasi nilai perusahaan
- 3) dst

Jadi memang di setiap produk kita itu sudah ada identifikasi kerawanan / mitigasi nya.

Eksternal fraud :

- 1) Pemalsuan kartu / *hacking*
- 2) Penarikan dana ATM
- 3) *Skimming*

Mitigasi nya :

- 1) Edukasi terhadap nasabah
- 2) Memberikan pengetahuan yang cukup kepada nasabah saat membuka rekening
- 3) Pengamanan mesin ATM
- 4) Asuransi terhadap mesin ATM
- 5) Pengamanan sistem

P : Bagaimana proses *know your employee* dilakukan sejak perekrutan pegawai?

N : Sudah berlangsung tapi di kita adalah hal baru, karena kita unit baru. PBI nomer berapa saya lupa tapi kita sudah melaksanakannya, di SDM. Di Anti *Fraud* kita sudah melaksanakan tapi tidak sebesar di SDM. Semua

dilaksanakan mulai dari proses perekrutan sampai sudah jadi pegawai. Kalau saat perekrutan kita mengawasi, kan wewenangnya SDM. Harus diumumkan di koran, kalau tidak kan nanti bisa jadi hanya orang – orang tertentu saja yang akses. Kalau seperti itu nanti ya kita sempit. Rotasi, mutasi, promosi dan delusi (turun jabatan) harus jelas. Rotasi itu ketika digeser ke level yang sama, atau dipindah ke beda cabang tapi di level yang sama. Seperti *front officer* ya tetap di *front officer* tapi beda cabang, karena kan salah satu mitigasi fraud ya rotasi itu. Kita rata – rata 4 tahun sekali. Seperti yang ada disini (BPP Anti *Fraud*) yang melakukan *know your employee* itu dilaksanakan oleh divisi SDM. Hasil pelaksanaannya dilaporkan ke Direktur Utama lalu ditembuskan ke kita (Anti *Fraud*) dan Manajemen Risiko. Proses rekrutmen misalnya menilai setiap calon pegawai dengan standar minimal mencakup kompetensi, psikologis, dan sebagainya. Kebijakan penilaian calon pegawai juga melalui penilaian karakter pegawai, jadi melalui *asesment*. Seperti pendidikannya apa, pelatihan yang pernah diikuti, pengalaman bekerja atau lamanya bekerja di kita atau di sebelumnya, kepribadian pegawai, penghargaan yang pernah diterima, sanksi yang pernah diterima, informasi terkait anggota keluarga, mengenai rekening pegawai nah kalau ini cuma yang sebatas di rekening kita, hubungan kekerabatan pegawai dengan pegawai lainnya seperti anak, bapak, ibu, suami dan istri, jika selain itu maka akan menjadi perhatian khusus. Perhatian khusus itu seperti proses masuknya sesuai prosedur atau tidak, melalui pendaftaran, jika saat sudah diterima benar

atau tidak dalam pekerjaannya. Hasil *asesment* ini berguna sebagai masukan *initial* profil pegawai.

Ini yang belum terlaksana, jadi jujur saja ya, karena ini di kita itu sangat sibuk, cuti itu tidak semua diambil jadi sisa. Kita ini jatahnya 12 hari, tapi dulu itu dipotong cuti bersama 4 hari seperti natal, tahun baru, lebaran jadi sisa 8 hari. Nah tapi setelah ada unit baru ini, itu nggak masuk potongan, dan sudah berlaku sejak tahun kemarin bahwa cuti tetap utuh tanpa dipotong cuti bersama dan kita mewajibkan setelah ada unit itu cuti itu wajib diambil yang secara berurutan ada minimal 3 hari. Saat dia ada pengganti maka kemungkinan akan ditemukan hal – hal menyimpang saat dia bekerja, hal ini merupakan salah satu bentuk pendeteksian *fraud*. Mungkin kedepan kita arahnya 5 hari, karena SDM juga terbatas kan kasian juga yang menggantikan. Nanti juga ada kuisisioner *asesment* nya. SDM juga punya bukunya dan lebih detail, mereka juga mengajak kita kok dalam menyusunnya. Kuisisioner kerawanan isinya :

- 1) Apakah ada pemberian kepercayaan berlebih kepada karyawan tanpa pemberian kerja yang efektif

Ini nanti yang mengisi atasan, nanti atasannya lagi ngisi untuk bawahannya

- 2) Apakah unit terkait memiliki pengalaman kejadian *fraud* di masa lalu

Sekarang bagian *pressure*, kan penyebab melakukannya ada *pressure*, *oppurtunity*, *rationalization*.

- 1) Apakah ada karyawan yang bekerja dibawah tekanan, *stress*, mengalami krisis keuangan, hutang atau masalah pernikahan dan siapa
- 2) Apakah ada karyawan yang membutuhkan uang yang besar karena sakit parah, suka mabuk, dsb
- 3) Apakah ada karyawan yang suka mengeluh atau *complain*
- 4) Apakah ada *conflict of interest* sesama rekan
- 5) Apakah ada *critical issue* yang meresahkan tentang pengurangan karyawan atau tidak akan bagi THR, padahal sebenarnya baik – baik saja, hanya membuat keresahan
- 6) Apakah ada karyawan yang kurang atau tidak patuh terhadap kode etik
- 7) Apakah ada perubahan kepribadian karyawan yang mencolok
- 8) Apakah ada karyawan yang kampanye

Karena yang pertama tahu pasti orang – orang terdekatnya, pasti atasannya langsung.

Penilaian dilakukan periodik setahun sekali. Kepala unit kerja di pusat dan cabang semua, ini bersifat rahasia dan terbatas. Ini nanti kita scoring, 0 – 6 dianggap Low, 25 -30 dianggap high, jadi potensi terjadinya fraud tinggi.

Ini memang baru kita awali ya, jadi apakah angka - angka ini dapat mewakili, memotret gitu, karena kan range nya terlalu jauh, jadi seiring waktu nanti kita perbaiki.

Ini pedoman penerapan strategi anti *fraud* tahun 2012 (memegang buku), isinya kurang lebih sama hanya awal diterapkan. Kalau tidak segera diterapkan

kan kita ini satu – satunya perusahaan yang pengawasnya banyak. Ada auditor, KAP, BPK, BPKP, PPATK, ada BI, ada OJK, semua meriksa kita dan KPK kadang, setahun pasti masuk. Kalau dulu awal diterapkan SKAI semua yang bertanggung jawab, sekarang sudah disahkan unit anti fraud baru.

P : Bagaimana mekanisme penerapan deteksi fraud melalui *whistleblowing system*?

N : Ini kita masih pakai yang lama karena kan sudah berlaku sejak 2012.

Surat edaran petunjuk pelaksanaan penyampaian pelaporan pengakuan indikasi tindak pelanggaran beserta pelanggarnya (menunjuk buku mekanisme penerapan *whistleblowing system*) jadi lewat sini semua, langkah – langkahnya ada.

Asas WBS :

1) Kerahasaan, tidak diskriminatif, perlindungan

Yang bisa dilaporkan itu yang memenuhi beberapa atau satu kriteria :

1) Termasuk kategori pelanggaran

2) Laporan terjadi paling lama 2 tahun sejak tanggal pelaporan

Ini websitenya, wbs.intranet.co.id, ini yang bisa buka hanya 1 orang 2 orang. Ini yang lama, untuk aturan baru hanya kita ulangi. Yang bertanggung jawab atas WBS itu direktur utama. Yang bisa diberi kewenangan untuk membuka ada laporan atau tidak itu SKAI. Nah untuk unit anti fraud belum tahu, kita bisa membuka atau hanya sekedar diberi laporan, ini ada kejadian disana silahkan ditindaklanjuti tanpa tahu siapa yang melaporkan. Karena

beberapa perusahaan itu WBS dikelola oleh pihak ketiga. Tahu kan misalnya E&Y, Deloitte itu mereka menyediakan jasa itu, jadi laporan yang masuk ke web mereka. Mereka sudah membuatkan web misalnya *uii.whistleblowingsystem*, nanti laporan yang masuk ke mereka dibaca ini layak atau tidak, memenuhi syarat atau tidak, di verifikasi OK, lalu UII cuma dapetnya ini ada pelanggaran di fakultas mana silahkan tindak lanjuti, tidak tahu pelapornya siapa, jadi kerahasiaan lebih terjamin. Sehingga karyawan itu percaya laporan yang masuk. PERTAMINA itu pakai ini. Jadi KAP itu bukan sekedar memberikan opini wajar tidak wajar saja, ada *whistleblowing*, investigasi jadi kayak detektif swasta gitu. Nanti sekiranya ada kecurangan di bagian pengadaan gitu ya diturunkan tim forensik, alatnya lengkap karena kan standarnya amerika jadi bisa diungkap.

Jadi dikita *whistleblowing system* itu ada, sedang dalam proses penyempurnaan oleh kita. Jadi namanya tadi itukan WBS atau *whistleblowing system*, besok rencananya kita buat “Surat kepada Direktur Utama” , jadi kita buat tidak menakutkan. Sekarang hanya bisa diakses dengan komputer melalui intranet, besok kita coba dapat diakses melalui *gadget*. Karena kalau yang di mobile itu kan kita punya BPD DIY Mobile untuk transaksi, yang khusus karyawan kita itu ada BPD DIY Smart itu isinya katalog produk kita. Jadi untuk yang kita tidak tahu langkah – langkahnya dengan produk begitu bisa buka lewat situ, jadi seperti *smart kit* nya BPD DIY. Kita juga ada BPD DIY KU / Kawan Usaha, jadi jika ingin mengajukan kredit usaha gitu bisa lewat *mobile*. Ini nanti langsung masuk bagian marketing, nanti kan tekoneksi

GPS jadi bisa tahu juga cabang terdekat dimana. Kita juga bisa tahu untuk program yang sedang ada terbaru apa. Tapi kan kalau di bank tidak sama dengan perusahaan lainnya yang produksi bisa langsung di launch, kalau kita harus izin dulu dan sebagainya untuk bisa *launch*, tapi memang untuk izin sudah bisa semua tinggal *launch*. Jadi mungkin kedepan BPD DIY Smart itu bisa juga untuk layanan pengaduan. Fungsinya ya semisal ada orang melihat pegawai BPD misalnya masuk ke tempat yang tidak senonoh, nah itu nanti bisa langsung dilaporkan. Misal itu hari sabtu gitu jadi tidak usah menunggu senin keburu lupa, atau malah senin ketemu orang nya terus ditaraktir gitu jadi nggak jadi ngelaporkan, jangan sampe, jadi bisa langsung saat itu juga melaporkannya.

P : Siapa yang bertanggung jawab dalam mengelola pengaduan melalui *whistleblowing system*?

N : Nah untuk *whistleblowing system* yang bertanggung jawab untuk saat ini Direktur Utama, nah yang ditunjuk oleh Direktur Utama untuk membuka laporan itu karena tidak semua diperbolehkan itu pemimpin SKAI dan pemimpin Manajemen Risiko. Jadi password nya cuma di 2 orang itu.

P : Bagaimana pengamanan yang tersedia pada portal pengaduan *whistleblowing system* untuk melindungi *whistleblower*?

N : Di kita *whistleblowing system* membangun sendiri ya, jadi tidak ambil dari luar. Kalo di bank lain kan dari vendor. Jadi di BPD DIY ini kita punya tim sendiri yang membangun, jadi memang kelemahannya mungkin tim – tim IT bisa membuka. Pengamanannya ada tim IT kita yang ruangnya ada di

lantai 4 situ, kita juga ada server di lantai 5 ini, cadangan server kita juga ada di Cabang Wates. Jadi kalau semisal ada bencana disini ambruk kita masih tetap bisa berjalan karena ada cadangan di tempat lain.

P : Bagaimana penerapan *whistleblowing system* di kantor cabang?

N : Sama. Ini kan online.

P : Bagaimana mekanisme pengaduan yang disampaikan oleh nasabah?

Apakah juga melalui *whistleblowing system*?

N : Nasabah tidak melalui WBS tetapi lewat form. Kalau ini yang mengelola divisi perencanaan dan pengembangan. Jadi di divisi perencanaan ini ada yang namanya unit pembinaan cabang. Jadi jika ada pengaduan oleh nasabah, cabang terkait yang akan turun. Form nya secara tertulis maupun di *website* juga ada. Jadi kotak saran dan pengaduan beserta formnya itu wajib ada di semua kantor cabang, jika nggak ada itu termasuk pelanggaran. Termasuk ada *register* ini masuk tanggal berapa dan wajib diselesaikan sekian hari ada aturannya.

P : Apakah *surprise audit* dilakukan di semua kantor cabang?

N : Ya, *surprise audit* dilakukan di semuanya tanpa pandang bulu, cuman kan tidak setiap saat dapat dilakukan, hari ini dicabang sini besok dicabang sana kan tidak valid. Nanti KIC bisa, unit anti fraud juga bisa. Tapi tidak semua melulu tentang uang. Bisa inventaris dicek kertas HVS atau alat tulis yang tersedia tinggal berapa, buku tabungan, surat berharga, materai.

P : Jadi mungkin atau tidak pak pegawai memalsukan cek?

N : Kalau memalsukan cek kemungkinannya sangat kecil. Karena cek itu percetakannya sama seperti uang, cek kita itu produksinya per *week*. Secara bahan juga susah dipalsukan.

P : Siapakah pihak independen yang bertanggungjawab dalam *surveillance system*?

N : Kalau di kita *surveillance system* itu tindakan melakukan audit secara diam – diam tanpa diketahui orangnya. Nah itu ada 2, ada yang dilakukan oleh kita, jika ada laporan misal di kantor cabang sana jadi kita secara diam – diam ke kantor, dokumen – dokumennya kita minta melalui KIC, dan melalui *mobile banking* itu juga kita cek. Namun ada juga *surveillance system* yang dilakukan untuk memantau kinerja nya SKAI itu sendiri. Pihak SKAI dinilai efektivitasnya. Yang memeriksa nanti pihak luar, bisa KAP bisa BPKP. Disamping itu 3 tahun sekali SKAI itu wajib di review oleh pihak ketiga. Kita terakhir itu tahun 2017 kemarin oleh BPKP, jadi kode etik kita ada yang dilanggar tidak, cara kerja kita sudah sesuai PBI nggak itu nanti di review. Mereka juga akan survei ke lapangan – lapangan mengenai kinerja auditor – auditor terkait. Misal bisa jadi ada laporan oh auditor yang itu tidak menguasai, kemarin mengaudit tanpa mengirim konfirmasi tiba – tiba dijadikan temuan padahal kejadiannya tidak seperti itu. Lapornya itu nanti langsung disampaikan ke OJK. Kita biasanya selama ini pakai BPKP, karena selain milik negara juga gratis.

P : Bagaimana tindakan yang dilakukan jika terjadi *management override*?

N : Ini kita di PPAT (Program Periksa Audit Tahunan) salah satu program audit yang dijadwalkan adalah audit manajemen dan kantor pusat. Walaupun tidak seperti yang di kantor cabang ya karena kan ada batasan – batasannya. Misalnya, Direksi itu kalau pergi SPJ nya sekian hari, jadi kalau lebih ya kita sempit dan harus nuker kelebihannya, seperti itu. Tapi terkait kebijakan itu kita nggak ikut, karena SKAI itu mengurus bagian operasional. Jadi kalau berhubungan kebijakan – kebijakan Direksi atau Surat Keputusan Direksi itu nanti Manajemen Risiko yang mengurusnya, karena MR kan sebelum, kalau kita sesudah yaitu saat pelaksanaannya atau operasionalnya. Misalnya, Direksi membuat keputusan *platform* kredit maksimal sekian, nominal diatasnya masuk kolektif kolegal. Kalau nanti dilanggar ya kita menindaklanjuti.

P : Jadi nanti Manajemen Risiko itu menganalisis, lalu laporan tahun lalu yang menurut Manajemen Risiko perlu ditindaklanjuti SKAI nanti akan diberikan ke SKAI itu bisa?

N : Iya seperti itu juga benar. Jadi kita kan *risk based audit*. Cuman kalau hanya dari Manajemen Risiko kadang kurang mantep, bener atau tidak ini semua, kan auditor kan seringnya bersikap *skeptis*, jangan – jangan ini sudah direkayasa. Jadi selain memakai itu, kita juga membuat profil risiko sendiri.

P : Apakah kecurangan dari eksternal seperti *phising*, *skimming*, *money laundering*, penggunaan kartu palsu, pencurian informasi bank pernah terjadi?

N : Ini semuanya bisa terjadi di kita, kalau sering relatif tidak. Khusus yang eksternal seperti *money laundering* ini kan kita tidak bisa mengontrol asalnya darimana. Biasanya kita hanya tahu ada tim PPATK, mereka akan minta keterangan apakah nasabah ini mempunyai rekening disini atau tidak. Biasanya nama – nama pejabat yang ditanyakan. KPK juga biasanya begitu. Karena kan kalau *money laundering* pasti melibatkan lebih dari 1 bank.

Jadi pernah kita alami dulu ada anak SMA buka deposito sebesar 100 juta, itu kan besar sekali dan tidak sesuai profil, nah itu harus kita pantau. Jadi MR itu rutin melaporkan transaksi – transaksi yang mencurigakan setiap bulan wajib ke PPATK. Kalau kita cukup mendalami dilihat dari form yang diisi, ini uang darimana. Nah itu ternyata bapaknya jual tanah dan membukakan deposito atas nama anaknya untuk tabungan masa depan. Jadi sudah *clear*.

Kalau kartu palsu kan otomatis kita tahunya dari aduan nasabah, uang saya kok berkurang.

P : Apakah kecurangan dari internal seperti pemalsuan cek, konflik kepentingan dan slip gaji pegawai palsu pernah terjadi?

N : Kalau pemalsuan cek itu belum pernah ada, konflik kepentingan juga belum pernah ada, kalau slip gaji pegawai palsu juga tidak pernah terjadi.

P : Bagaimana program pendidikan karir, profesi, ketrampilan, pelatihan dan seminar yang diadakan manajemen dalam pengembangan SDM Unit Anti Fraud?

N : Walaupun ini unit baru, kita ikut pelatihan ada 2 yang jadi rujukan kita, Lembaga Pengembangan Anti Fraud (LPAF). Itu lembaga yang ditunjuk untuk mengadakan pelatihan, dan pelatihan itu terintegrasi dengan ACFE. Jadi lembaga itu yang membantu nanti untuk ujian. Itu untuk internasional. Kalau yang nasional itu ada CRFA, *Certified Forensic Audit*. Itu nanti semua wajib ikut yang baru maupun pegawai baru, karena ada dalam Peraturan BI bahwa 5% dari biaya tenaga kerja itu adalah wajib untuk pendidikan. Jadi di kita itu pegawai minimal 2 kali mengikuti pendidikan. Itu semua dibiayai bank. Pendaftaran, transportasi, uang saku dan hotel dibiayai kita. Jadi untuk Anti Fraud itu terprogram, karena kan arahnya sertifikasi. Ini ada contohnya (memegang brosur) lembaga LPAF, ini lembaga bimbingan persiapan ujian CFE, biaya bimbingan per bulan 10 juta, untuk sertifikasinya USD1150. Selain itu kita juga sertifikasi internal audit bank. Tanggal 15 besok kita juga akan ada *refreshment* karena sertifikat akan hangus bulan maret ini, hanya berlaku 3 tahun. Dan kalau untuk sertifikasi Anti Fraud kita berdua sendiri memang belum tapi memang menuju ke arah sana. Karena kan kemarin SKAI yang sertifikasi internal audit yang sudah. Sebenarnya sama saja, tetapi kalau sudah sertifikasi Anti Fraud itu bedanya kita sudah bisa menjadi saksi ahli di pengadilan nanti dan ini diakui di luar negeri. Kalau sertifikasi yang ini modelnya seperti pemeliharaan, jadi harus mengikuti *workshop* nya. Kemarin konferensi internasional nya ada di jogja.

P : Kalau untuk Laporan Anti Fraud itu mekanismenya bagaimana?

N : Jadi laporan anti fraud itu tiap semester dilaporkan ke OJK. Ini yang rutin ya Laporan Penerapan Strategi Anti Fraud. Kalau yang tidak rutin ya jika ada indikasi fraud atau sudah terjadi fraud yang kerugiannya itu bisa mempengaruhi kondisi perekonomian perusahaan wajib dilaporkan maksimal 3 hari setelah tanggal kejadian. Kalau laporan ke intern, itu ada Laporan Hasil Audit dan Laporan Hasil Investigasi. Jadi kita itu saat mem PHK orang disuratnya menyebutkan kejahatan yang dilakukan.

P : Jadi kalau untuk SKAI yang sudah bersertifikasi itu sertifikasi apa?

N : Yang itu tadi Auditor Internal Bank. Sama juga sertifikasi Manajemen Risiko itu semua dari negara. Seperti saya ini sudah bersertifikasi itu.

P : Bagaimana hambatan yang dihadapi Tim Anti Fraud?

N : Perusahaan BPD DIY itu kan tidak besar, jadi kita itu kan saling kenal. Beda sama perusahaan nasional, tim audit datang takut semua tidak ada yang kenal. Karena ini perusahaannya lokal jadi harus mengesampingkan rasa tidak enak, bisa jadi karena tetangga atau teman dari kecil. Kalau perusahaan di Jakarta itu kan rekrutmen ya langsung di posisikan di audit, kalau contohnya seperti saya begitu kan sempat di cabang dulu. Otomatis banyak kenal dan kedekatan dengan pegawai lain itu ada, apalagi ini semua wilayah di Jogja. Dan seperti itu sebenarnya kendala. Jadi terasa terhadap pelaporan *whistleblowing system* nya, walaupun saya baru melihat setelah saya disini dan juga saya tidak punya akses, tapi saya diberi laporannya, itu partisipasi pelaporannya masih rendah. Apakah benar rendah itu karena tidak ada yang dilaporkan atau karena tidak berani bahkan tidak enak saja. Kita sedang susur

penyebabnya. Dan pak Direktur Utama sudah minta dibahas oleh kita. Kita sudah menyampaikan ke Direktur Utama untuk judul *whistleblowing system* itu kita ganti menjadi Surat Kepada Direktur Utama, lalu jaringan intranetnya diubah tadinya “wbs” menjadi “skdu”. Dan untuk pelaporan melalui sms maupun Whatsapp masih perlu dikaji lagi, untuk penanggung jawabnya siapa. Penyempurnaan Mobile Banking semua tadi membuka kemungkinan kita bekerjasama dengan pihak ketiga, tapi dipertimbangkan lagi biaya yang dikeluarkan dengan biaya yang diselamatkan itu sebanding tidak. Tahun ini saja ada dua orang yang kita PHK atas sanksinya yang dilaporkan lewat *whistleblowing system*.

P : Bagaimana pengamanan teknologi yang ada di BPD DIY?

N : Pengamanan teknologi kita dikembangkan oleh tim IT kita, seperti flashdisk saja tidak bisa diakses jika masuk ke laptop atau komputer. Wifi umum tidak bisa walaupun internet juga kita disediakan layanan proxy dan itu pun terbatas. Kalau dikantor hotspot disediakan di setiap ruangan.

P : Saya lihat dilaporan tahunan ada pendidikan yang rutin diikuti pegawai itu bagaimana mekanismenya?

N : Nah contohnya ini (menunjukkan surat usulan mengikuti pendidikan), kita mengajukan 10 orang untuk gelombang 1. Ini tentang fraud kebetulan temanya:

- 1) Definisi dan disiplin fraud
- 2) Pengumpulan bukti dan pelaksanaan audit investigasi
- 3) Pengumpulan dan evaluasi bukti keuangan

- 4) Audit investigasi dan kasus produk dana
- 5) Audit investigasi dan kasus produk kredit
- 6) Psikologi dan kesiapan mental audit
- 7) Teknik interview
- 8) Pelaporan

Dirinci biaya nya sekian, peserta mengikuti selama 2 hari di Bandung. Ada 2 gelombang, yang gelombang 1 itu KIC agar mereka juga paham semua tentang fraud, gelombang 2 termasuk saya, sebenarnya saya sudah beberapa kali ikut, tapi karena ini tujuannya untuk *refreshment* jadi mau gak mau harus ikut.

Di awal tahun juga setiap divisi wajib membuat *training list analyst*. Jadi setahun kedepan itu mau pelatihan di bidang apa saja dan diberikan ke SDM. SDM akan mengolah, nah saat ada penawaran ke SDM dan sesuai dengan apa yang diminta divisi kemarin maka mulai dari kontak dinas, tiket pesawat akan dilakukan oleh bagian SDM. Ini juga merupakan salah satu tindakan pencegahan fraud, dan *boarding pass* nya juga harus kembali jadi tidak bisa di *refund*. Hotel juga biaya berapa pun jika memang pendidikan diadakan di hotel itu maka diusahakan menginap juga disitu.

P : Bagaimana pelaksanaan proses pemantauan, evaluasi dan tindak lanjut?

N : Evaluasi dilakukan setelah pemantauan dilakukan. Evaluasi dilakukan seiring dibuatnya laporan. Untuk evaluasi kita memberikan perbaikan yang

harus dilakukan pada bagian yang terlibat tindakan *fraud*. Tindak lanjut tidak bisa dilakukan oleh Unit Anti *Fraud*, itu dilakukan oleh Komite Kepegawaian atau KMK.

LAMPIRAN 3**TRANSKRIP WAWANCARA 3**

Narasumber : Bapak Zukhroni Ariffin

Tanggal Wawancara : 16 Maret 2018

Jabatan : Staff Unit Anti Fraud

P : Pewawancara

N : Narasumber

P : Bagaimana hambatan yang dirasakan dalam pelaksanaan strategi anti fraud?

N : Jadi kalau kita menemukan fraud di salah satu cabang, itu akan berpengaruh di penilaian cabang. Sehingga itu yang menyebabkan terkadang cabang itu menyelesaikan masalah itu lama memberi laporan ke kita (Unit Anti Fraud), kan disana kita juga ada KIC, jadi sudah ditangani mereka. Jadi terkadang kalau kita meminta laporan ya agak lama, karena itu tadi, berpengaruh ke score masing – masing cabang itu. Jadi ya prinsipnya waktunya saja yang lama untuk melaporkan ke kita.

P : Bagaimana mekanisme pelaksanaan investigasi, pelaporan dan sanksi?

N : Kalo pelaporan strategi anti fraud itu jelas, kita melaporkan tiap 6 bulan sekali. Kita melaporkan hasil investigasi kita. Kalau memang ada ya kita laporkan semua, kalau tidak ada ya tetap kita laporkan NIHIL. Jadi setiap 6 bulan, maksimal tanggal 10 setelah bulan pelaporan sudah saya laporkan ke OJK. Jadi laporan anti fraud setiap semesteran, nanti ada formatnya dari OJK.

Kalau hasil investigasi kita itu nanti kita laporkan ke atasan langsung dan Direktur Utama. Kalau sanksi dari investigasi itu bukan di ranah kita lagi, kita sebatas penyelidikan saja. Penyelidikan pun harus dikeluarkan surat tugas khusus dari Direktur Utama. Kalau sanksi mau seperti apa itu nanti KMK (Komite Kepegawaian) yang menentukan dari hasil fraud itu. Kita hanya melaporkan bahwa ditemukan fraud ini yang akan berdampak ini oleh ini. Nah selanjutnya KMK yang menentukan apa yang harus dilakukan untuk si pelaku fraud.

P : Bagaimana mekanisme pelaksanaan pemantauan, evaluasi dan tindak lanjut?

N : Untuk memantau dan evaluasi itu nanti kita tetap buat laporan, misalnya karena melibatkan kantor kas, maka tindak lanjutnya kita akan memberi usulan kantor kas untuk melakukan hal – hal pencegahan seperti ini. Itupun, setelah Direksi menyetujui usulan kami. Kalau untuk memvonis atau memberikan sanksi itu tetap KMK nanti yang melakukan.

P : Kalau untuk mencegah fraud yang sudah ditemukan untuk terjadi lagi itu bagaimana?

N : Kalau dari kami, sosialisasi sudah dilakukan, dari hasil laporan atas investigasi kita itu kita akan memberikan usulan ke direksi, nanti setelah usulan kami diterima barulah akan dibuat kebijakan baru. Itupun kita perumusan usulan juga mencantumkan, untuk mengatasi permasalahan seperti ini akan diperlukan penggunaan SOP yang seperti ini, sehingga kalau rekomendasi kami disetujui akan memungkinkan muncul SOP baru. Ini hampir sama dengan tindak lanjut hasil evaluasi.

P : Biasanya dari KMK sanksi terparah untuk pelaku itu apa pak?

N : Ya PHK. Downgrade atau turun adri jabatannya, bisa juga dia tidak diberikan hak – haknya selama beberapa tahun kedepan sesuai dengan tingkat fraud yang dilakukan, misalnya THR tidak akan diberikan 100%, atau pun pemberhentian tanpa predikat. Kalau untuk PHK dari segi pelaku fraud akan senang, karena akan lunas kewajibannya. Tapi kalau tanpa predikat berarti dia harus melunasi kewajiban itu dulu. Makannya di pihak intern kami pun kalau pengen punya pinjaman jangka panjang yang nominalnya besar, paling tidak ada jaminan atas pinjaman itu, jadi untuk mengantisipasi hal – hal terkait PHK itu.

P : Bagaimana hambatan yang dirasakan dalam pelaksanaan surprise audit?

N : Kebetulan di kantor cabang itu ada kepanjangan tangan kami namanya KIC. Nah jika kita akan ke kantor cabang, otomatis kita itu akan meminjam kendaraan yang otomatis dari divisi lain, sehingga kami harus konfirmasi ke

Divisi Umum mau pinjam kendaraan misal ke Wates. Tapi kalau kami ditanyai buat apa kesana ya kami tidak bisa menutupi itu. Jadi kalau dari Divisi Umum kebetulan dekat dengan orang di cabang lain pasti nanti akan telfon dan memberitahukan kalau kita akan kesana, ya gak jadi surprise audit. Tapi untuk mengatasi itu semua ya mau tidak mau kami berbohong. Dan jika memang harus sesuai prosedur ya pasti akan bocor.

P : Untuk Unit Anti Fraud sendiri sudah merencanakan apa pak untuk dilakukan rencana pelatihan atau sertifikasi?

N : Kalau untuk auditor sendiri ada syarat mengikuti sertifikasi auditor level 1 dan 2 untuk syarat supervisor. Kalau yang level 1 sebagian sudah dan sebagian belum. Kami juga sedang usulkan ke pimpinan untuk bisa mendapatkan sertifikasi yang oleh ACFE.

P : Apakah hambatan dalam pelaksanaan WBS?

N : Kalau bicara WBS itu sudah kita lakukan sejak 2012, sudah 5 tahun yang lalu. Dulu yang bisa mengakses membuka WBS hanya pimpinan SKAI dan pimpinan MR. Nah begitu kami terbentuk, maka kami sekarang juga diberikan hardcopy hasil dari WBS itu, itu 100% bisa diselesaikan. Tapi untuk WBS tidak bisa anonim, cuman memang pasti kami lindungi kerahasiaan data pelapor itu. Kalo sekarang kan WBS sebagai sarana keluhan, jadi kita sedang tahap merombak agar tidak hanya sebagai sarana menyampaikan keluhan seperti itu saja.

P : Bagaimana penilaian risiko dilakukan?

N : Kalau penilaian risiko itu semua divisi menilai risiko masing – masing. Tetapi tetap MR yang mengelola, nanti ada draft tersendiri. Nanti hasil temuan yang dikelola MR akan dikomunikasikan ke SKAI dan Anti Fraud juga. Celah dari risiko itu nanti jadi bahan untuk kami olah juga, karena kami juga akan mengaudit semua divisi di kantor pusat. Dan bahkan kami pun di audit oleh BPK.

P : Apakah dalam pelaksanaan know your employee itu dibantu juga oleh pimpinan setiap divisi?

N : Iya, itu tetep. Dan nanti pimpinan juga akan melaporkan kesini. Itu bukan hanya pimpinan yang melakukan, kita juga melakukan itu, tapi memang tanggung jawab pimpinan salah satunya membuat laporan *know your employee* itu.

P : Bagaimana sosialisasi yang dilakukan jika ada pegawai baru masuk?

N : Jadi jika ada pegawai baru masuk begitu pasti 3 bulan setelah itu ada pendidikan pertama untuk pegawai baru, dan disitu kami (Unit Anti Fraud) pasti ngisi. Setiap satu unit biasanya 1 hari. Kalau Unit Anti Fraud kan resmi berdiri baru Desember 2016, nah OJK mewajibkan setiap adanya untu baru harus mengeluarkan Buku Pedoman Perusahaan, cuma BPP atas unit baru baru direalisasikan Desember 2017 kemarin. Nah sebenarnya ini kita sedang adakan roadshow sosialisasi. Kemarin saya ke Jalan Senopati, Senin besok saya ke cabang Wonosari. Kalau yang sekarang ini baru semua pimpinan, kalau besok pertengahan April baru yang seluruh karyawan.

LAMPIRAN 4**TRANSKRIP WAWANCARA 4**

Narasumber : Bapak Pandu Kuncoro

Tanggal Wawancara : 15 Maret 2018

Jabatan : Analis Junior Kredit Divisi Manajemen Risiko dan
Kepatuhan

P : Pewawancara

N : Narasumber

**P :Apakah ada keluhan tentang pelaksanaan strategi anti fraud sebelum
Unit Anti fraud dibentuk?**

N : Keluhan sebenarnya tidak ada, karena kita juga *zero fraud* selama beberapa tahun ini. Mungkin Whistleblowing system nya bisa dilakukan perubahan sehingga pegawai akan lebih berpartisipasi.

**P :Adakah saran yang perlu dilakukan Unit Anti Fraud kedepannya
dalam melaksanakan strategi anti fraud?**

N : Selain WBS juga bisa menambah tingkat kualitas Unit Anti Fraud melalui sertifikasi atau pelatihan – pelatihan.

P : Biasanya kecurangan apa saja yang perlu dilaporkan melalui WBS?

N : Sebenarnya itu sudah terjawab dari sosialisasi yang diadakan pak suwasono ya.. Ya kesadaran kita melaporkan hal – hal yang memang mengarah penting untuk ditindaklanjuti, tidak hanya berupa keluhan.

P : Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?

N : Ya.. Ada itu mbak

P : Dalam penilaian risiko di cabang, apakah MR menyediakan draft tersendiri untuk SKAI ataupun divisi lain?

N : Selama ini iya. Jadi selain dari kita yang terjun langsung, tiap divisi kan pasti lebih tau apa saja risiko signifikan yang mereka hadapi dan perlu menjadi perhatian.

P : Seperti apa sosialisasi mengenai WBS yang didapatkan?

N : Mulai dari intranet yang diakses, apa saja aduan yang bisa dilaporkan, dampak jika kita tidak melaporkan tindakan kecurangan di dalam organisasi..

P : Apakah sudah pernah dilakukan rotasi jabatan?

N : Iya, biasanya empat tahun sekali.

P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?

N : Tidak bisa mba. Jadi memang harus kita ambil semua.

P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari?

N : Itu tergantung keadaan kita, kalau mau diambil kolektif saat momen – momen libur panjang diluar cuti bersama biasanya jatah cuti diambil.

LAMPIRAN 5**TRANSKRIP WAWANCARA 5**

Narasumber : Bapak Muhammad Agus Salam S.

Tanggal Wawancara : 15 Maret 2018

Jabatan : Analis Kredit Divisi Manajemen Risiko dan
Kepatuhan

P : Pewawancara

N : Narasumber

P :Manajemen risiko itu koordinasi sama SKAI itu hanya saat SKAI mau membuat strategi ya?

N : Iya, jadi MR itu seperti memberikan hasil analisis risiko di setiap cabang nah nanti SKAI memakai untuk dipakai sebagai dasar audit. Jika sudah mulai tercium indikasi fraud barulah unit anti fraud sekarang yang maju.

P :Jadi nanti jika ada risiko signifikan misal dibagian kredit, yang maju tim anti fraud nya?

N : Iya...

P :Jadi manajemen risiko akan melakukan penilaian risiko dulu baru SKAI akan bertindak ya pak?

N : Benar. Jadi ya memang kita ini berbeda divisi dan SKAI kan independen, tapi kita bisa saja koordinasi seperti itu.

P : Jadi manajemen risiko itu tidak terjun langsung membantu berlangsungnya strategi anti fraud ya pak? Tetapi nanti dalam bentuk laporan akan dilaporkan ke SKAI, baru SKAI menindaklanjuti?

N : Tidak. Kita MR itu tugasnya menilai risiko yang dapat berdampak signifikan terhadap organisasi. Jika ada temuan kita laporkan SKAI dan perlu diperdalam lagi kalau memang perlu oleh Anti Fraud.

P : Kalau untuk transaksi seperti kredit, apa pernah nasabah berusaha menipu bank? Seperti memberikan data palsu?

N : Bisa saja itu terjadi, tapi kita kan setiap divisi ada SOP nya. Dan disitu bisa dilihat mitigasi atas aktivitas terkait apa saja, jadi kemungkinan kecil sekali karena sudah dilakukan pencegahan terlebih dahulu.

P : Apakah sudah pernah dilakukan rotasi jabatan?

N : Pasti dilakukan kalau itu mbak. Kisaran 4 tahun jabatan maksimal.

P : Apakah bapak biasanya mengambil semua jatah cuti?

N : Tidak semua kadang, biasanya satu atau dua hari. Kalau berhari - hari ya nunggu momen liburan.

P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?

N : Selama ini sih tidak bisa.

P :Bagaimana cara menumbuhkan budaya untuk melaporkan tindakan *fraud*?

N : Semua dimulai dari budaya perusahaan kita, kalau budaya sudah baik pasti semua akan memiliki rasa kepedulian yang besar. Budaya perusahaan bisa tumbuh kalau sejak dini kita disadarkan dampak yang bisa terjadi jika kecurangan terus dipelihara, dan kerugian bagi kita (pegawai) akan seperti apa.

P :Apakah ada keluhan tentang pelaksanaan strategi anti fraud sebelum Unit Anti fraud dibentuk?

N : Mungkin lebih kepada sosialisasi ke nasabah ya mbak. Karena kan banyak ni kasus *skimming* yang merugikan nasabah dan reputasi bank itu sendiri.

P :Adakah saran yang perlu dilakukan Unit Anti Fraud kedepannya dalam melaksanakan strategi anti fraud?

N : Kalau setahu saya di Unit Anti Fraud hanya terdiri dari 2 orang ya, mungkin bisa ditambah personilnya. Bisa dicari yang memiliki dasar – dasar kualifikasi yang kompeten saat rekrutmen jadi segera bisa membantu kedua personil yang sekarang.

LAMPIRAN 6**TRANSKRIP WAWANCARA 6**

Narasumber : Bapak Daryoko

Tanggal Wawancara : 16 Maret 2018

Jabatan : Analis Kepatuhan Divisi Manajemen Risiko Dan
Kepatuhan

P : Pewawancara

N : Narasumber

P : Bagaimana koordinasi antara Manajemen Risiko dan SKAI?

N : Jadi gini, Manajemen Risiko itu bertugas membuat laporan hasil analisis penilaian risiko, nanti SKAI akan melanjutkan audit mendalam dengan membuat surat tugas ke Unit Anti Fraud karena sekarang sudah terbentuk Unit itu.

P : Dalam penilaian risiko apakah MR menyediakan draft tersendiri untuk SKAI ataupun divisi lain?

N : Ya.. Jadi selain kita (MR), tiap divisi juga mempunyai tugas untuk mengetahui risiko signifikannya yang perlu menjadi perhatian MR untuk dikelola lebih jauh.

P :Jadi nanti Manajemen Risiko itu menganalisis, lalu laporan tahun lalu yang menurut Manajemen Risiko perlu ditindaklanjuti SKAI nanti akan diberikan ke SKAI itu bisa?

N : Jadi gini. Saat MR sudah mendapatkan laporan dari setiap divisi tersebut, itu berguna sebagai penguat analisis risiko yang sudah dilakukan MR. Nanti MR akan membuat laporan yang akan menjadi dasar SKAI untuk mempertimbangkan perlu atau tidak dilakukan tindaklanjut. Jika perlu dan sudah mengarah ke fraud, maka nanti akan ditugaskan Unit Anti Fraud yang menindaklanjuti.

P :Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari?

N : Sesuai individunya mbak. Tapi akan lebih baik secara kolektif, karena disaat pegawai itu cuti dan digantikan pegawai lain, maka kemungkinan menemukan kecurangan yang dilakukan pegawai yang cuti tersebut bisa lebih besar.

P :Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?

N : Tidak bisa kalau itu.

P :Biasanya kecurangan apa saja yang perlu dilaporkan melalui WBS?

N : Semua tindak fraud mbak. Ada banyak sekali jenisnya, bisa yang dilakukan oleh sesama pegawai bahkan atasan kita sendiri pun harus kita laporkan. Sosialisasi yang dilakukan SKAI, Anti Fraud kalau sekarang, itu sudah mencakup semua itu.

P :Seperti apa sosialisasi mengenai WBS yang didapatkan?

N : Mencakup jenis - jenis tindakan fraud atau bentuk perilaku dan aktivitas mencurigakan yang mengindikasikan fraud, dampak jika kita enggan melaporkan sehingga untuk para pegawai pasti akan berpikir 2 kali jika akan melakukan kecurangan.

P :Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?

N : Ya.. Bagus itu, karena pesan tersampaikan tanpa harus susah – susah mengumpulkan semua pegawai, ya walaupun kita BPD DIY memang rutin 3 bulan sekali ada sosialisasi.

P :Apakah ada keluhan dan saran tentang pelaksanaan strategi anti fraud sebelum Unit Anti fraud dibentuk?

N : Sejauh ini menurut saya cukup baik ya, karena sebelumnya kan SKAI, mereka sudah cukup kompeten dalam melaksanakan *whistleblowing system* nya. Tapi mungkin perlu dilakukan namanya reward untuk pegawai yang aktif melaporkan ke WBS, jadi semua lebih aktif.

LAMPIRAN 7**TRANSKRIP WAWANCARA 7**

Narasumber : Bapak Andrianto Dwi P.

Tanggal Wawancara : 16 Maret 2018

Jabatan : Officer Junior Kepatuhan Divisi Manajemen
Risiko

dan Kepatuhan

P : Pewawancara

N : Narasumber

P :Apakah sudah pernah melaporkan indikasi fraud ke WBS? Mudah atau ribet dalam mengaksesnya?

N : Belum. Sebenarnya mudah, tetapi selama ini saya nggak menemukan hal – hal yang mengarah ke kecurangan dan merugikan ke organisasi secara signifikan.

P :Apakah sudah pernah dilakukan rotasi jabatan?

N : Sudah kalau itu.

P: Apa saja hambatan yang dirasakan dalam melaporkan indikasi kecurangan?

N : Kadang kalau kita merasa beberapa indikasi fraud itu tidak merugikan maka kita memilih tidak melaporkannya ke WBS.

P :Adakah saran yang perlu dilakukan Unit Anti Fraud kedepannya dalam melaksanakan strategi anti fraud?

N : Mungkin agar masing – masing strategi anti fraud dalam terlaksana secara maksimal, diperlukan SDM yang lebih banyak dari yang ada sekarang, sehingga setiap orang memiliki tanggungjawab di masing – masing strategi.

P :Kepada siapakah jika ingin melaporkan tindakan atau aktivitas yang tidak wajar dari sesama pegawai?

N : Tentu saja langsung ke WBS. Atau bisa ke atasan kita.

P :Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?

N : Ya, ada seperti itu. Karena menurut saya penyampaian maksud melalui visual akan lebih cepat diterima, apalagi jika setiap hari dapat dilihat.

P :Seperti apa sosialisasi mengenai WBS yang didapatkan?

N : Kami mendapatkannya lewat itu tadi konten di desktop atau pengumpulan karyawan setelah jam kantor selesai untuk diberikan materi – materi mengenai fraud dan strategi anti fraud itu sendiri.

P :Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari?

N : Lebih sering mengambil harian mbak. Kalau untuk kolektif juga bisa dan diambil di momen – momen libur panjang.

LAMPIRAN 8**TRANSKRIP WAWANCARA 8**

Narasumber : Bapak Ivan Nugroho

Tanggal Wawancara : 16 Maret 2018

Jabatan : Officer Divisi Manajemen Risiko dan Kepatuhan

P : Pewawancara

N : Narasumber

P : Bagaimana koordinasi antara Manajemen Risiko dan SKAI?

N : Untuk penilaian risiko dilakukan oleh Manajemen Risiko, tapi untuk menentukan risiko yang perlu di audit lebih lanjut itu nanti tergantung kebijakan SKAI. SKAI nanti akan membuat rencana audit dari hasil penilaian risiko MR. Jika memang nanti perlu dilakukan tindaklanjut atas indikasi fraud maka akan ditindaklanjuti Unit Anti Fraud kalau sekarang ya namanya.

P : Dalam penilaian risiko apakah MR menyediakan draft tersendiri untuk SKAI ataupun divisi lain?

N : Betul sekali, itu ada. Jadi hal itu merupakan salah satu strategi kita untuk melihat apakah penilaian MR dan permasalahan setiap divisi sudah sesuai atau belum.

P : Jadi nanti Manajemen Risiko itu menganalisis, lalu laporan tahun lalu yang menurut Manajemen Risiko perlu ditindaklanjuti SKAI nanti akan diberikan ke SKAI itu bisa?

N : Benar sekali. Itu tadi, kalau SKAI merasa perlu dipelajari lebih lanjut tentang indikasi fraud maka akan dilakukan oleh Unit Anti Fraud.

P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari?

N : Tidak pasti kalau itu, tapi untuk saat ini ada yang ambil satu dua hari, ada juga yang kolektif.

P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?

N : Tidak bisa.

P : Biasanya kecurangan apa saja yang perlu dilaporkan melalui WBS?

N : Kalau itu ya pasti hal – hal yang mengarah kepada indikasi fraud. Seperti transaksi tidak wajar atau pun aktivitas tidak wajar. Dan setiap divisi kan juga ada SOP nya, nah disitu bisa jadi acuan kita, tercantum juga untuk mitigasi nya atas aktivitas yang ada itu apa saja.

P : Seperti apa sosialisasi mengenai WBS yang didapatkan?

N : Menyadarkan pentingnya melaporkan tindakan kecurangan yang ada di dalam organisasi. Dan dijelaskan juga dampak kerugian yang kita (pegawai) dapatkan atas kerugian perusahaan. Sama cara mengakses nya sih lewat intranet.

P : Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?

N : Ya.. Selain BPD DIY memang rutin 3 bulan sekali ada sosialisasi, hal itu juga perlu.

P : Apakah sudah pernah melaporkan indikasi fraud ke WBS? Mudah atau ribet dalam mengaksesnya?

N : Sejauh ini belum. Mudah kok mbak, hanya saja kami melaporkan hanya untuk indikasi fraud yang benar – benar signifikan saja.

P : Apakah ada keluhan dan saran tentang pelaksanaan strategi anti fraud sebelum Unit Anti fraud dibentuk?

N : Mungkin sosialisasi bisa dilakukan untuk nasabah juga, karena kan banyak ditemukan sekarang pemasangan alat *skimmer* di ATM, agar nasabah juga bisa memprotect diri sendiri dahulu, juga ditekankan untuk tidak memberikan pin ATM bahkan ke anak sendiri. Dan WBS mungkin bisa dibuat lebih menarik untuk menarik para pegawai lebih aktif dalam melaporkan setiap tindakan yang mengindikasikan fraud.

LAMPIRAN 9

Surat Izin Penelitian



SURAT KETERANGAN

Nomor : 3209/ RB 0000

Yang bertandatangan di bawah ini :

Nama : GAMAL KRISTIYANTO
 Jabatan : Pemimpin Divisi SDM dan Umum
 PT. Bank Pembangunan Daerah
 Daerah Istimewa Yogyakarta
 Alamat : Jl. Tentara Pelajar No. 7 Yogyakarta

Dengan ini menerangkan bahwa :

Nama : DEWI KILISUCI ANISHA PURI
 Nomor Mahasiswa : 14312137
 Perguruan Tinggi : Universitas Islam Indonesia Yogyakarta
 Fakultas : Ekonomi
 Program Studi : Akuntansi

Telah mengadakan penelitian di Kantor Pusat PT. Bank Pembangunan Daerah Daerah Istimewa Yogyakarta dimulai tanggal 8 Maret – 15 April 2018 dengan judul penelitian : *“Strategi Pengembangan Unit Anti Fraud PT. Bank BPD DIY dalam Meminimalkan Fraud”*.

Demikian surat keterangan ini dibuat untuk dipergunakan sebagaimana mestinya.

Yogyakarta, 9 Mei 2018

Pemimpin Divisi SDM dan Umum,

GAMAL KRISTIYANTO

dvd

LAMPIRAN 10

Anti Fraud Statement

BAB III PENCEGAHAN FRAUD

Pilar pencegahan memuat perangkat-perangkat yang ditujukan untuk mengurangi potensi terjadinya *fraud*, mencakup anti *fraud awareness*, identifikasi kerawanan dan *know your employee*.

A. ANTI FRAUD AWARENESS

Anti fraud awareness adalah upaya untuk menumbuhkan kesadaran mengenai pentingnya pencegahan *fraud* oleh seluruh pihak terkait. Melalui kepemimpinan yang baik didukung dengan anti *fraud awareness* yang tinggi diharapkan tumbuh kepedulian semua unsur di Bank terhadap pengendalian *fraud*. Moral dan *awareness* dari pimpinan terhadap anti *fraud* harus menjiwai setiap kebijakan atau ketentuan yang ditetapkannya.

Kebijakan Anti *fraud awareness*

1. ANTI FRAUD STATEMENT

Bank tidak memberikan toleransi kepada pegawai dalam jabatan maupun kedudukan apapun yang melakukan *fraud* (*zero tolerance*). Pegawai yang terbukti melakukan tindakan *fraud*, diberikan sanksi sesuai ketentuan dan bertanggung jawab atas kerugian bank maupun kerugian nasabah

Anti Fraud Statement terdiri dari :

1. *Anti fraud statement* Direksi dan Komisaris(terlampir pada lampiran Formulir 01)
 2. *Anti fraud statement* pegawai(terlampir pada lampiran Formulir 02)
- Anti *fraud statement* ditandatangani oleh seluruh pegawai dan pengurus Bank.

LAMPIRAN 11

Anti Fraud Statement untuk Pegawai

Saya yang bertanda tangan dibawah ini :

Nama :
 Nomor Induk Pegawai :
 Pangkat/ Jabatan :
 Unit Kerja :

Menyatakan persetujuan untuk melaksanakan strategi anti *fraud* yang dikemukakan dalam buku Pedoman Penerapan Strategi Anti *Fraud* dan memahami bahwa Bank tidak akan mentolerir setiap tindakan *fraud* yang dilakukan dan akan menerapkan sanksi tegas terhadap pelaku *fraud*. Nilai-nilai inti yang disepakati adalah sebagai berikut:

1. Setiap Insan Bank sebelum melaksanakan kegiatan, selalu diawali dengan niat baik dan semata-mata bekerja untuk kepentingan bank serta tidak merugikan orang lain, yang dilandasi keikhlasan dan tulus sehingga dapat memuaskan *stake holders*.
2. Setiap Insan Bank berkewajiban menghindari perbuatan-perbuatan penyimpangan yang dilakukan untuk mengelabui, menipu atau memanipulasi Bank, nasabah, atau pihak lain, yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah, atau pihak lain menderita kerugian dan/atau pelaku *fraud* memperoleh keuntungan.
3. Setiap Insan Bank berkewajiban melaporkan setiap fakta penyimpangan yang dilakukan untuk mengelabui, menipu atau memanipulasi Bank, nasabah, atau pihak lain, yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah, atau pihak lain menderita kerugian.
4. Setiap Insan Bank tidak diperbolehkan memberi dan/atau menerima hadiah/cinderamata/gratifikasi dalam bentuk apapun yang berhubungan dengan jabatan dan pekerjaannya sehingga menimbulkan konflik kepentingan.

52

/s/

LAMPIRAN 12

Employee dan Customer Awareness

2. PROGRAM EMPLOYEE AWARENESS

Dalam rangka pemberdayaan sumber daya manusia agar terdapat pemahaman bentuk-bentuk *fraud* dan kepedulian untuk melakukan mitigasi sekaligus meningkatkan *sistem* pengendalian, maka dikembangkan pendidikan dan pelatihan, termasuk seminar atau diskusi terkait anti *fraud* kepada seluruh pegawai.

3. PROGRAM CUSTOMER AWARENESS

Untuk meningkatkan kepedulian dan kewaspadaan nasabah terhadap kemungkinan terjadinya *fraud*, maka dikembangkan program *customer awareness* melalui pembuatan brosur, penjelasan tertulis maupun melalui sarana lainnya untuk meningkatkan kepedulian dan kewaspadaan nasabah terhadap kemungkinan terjadinya *fraud*

B. IDENTIFIKASI KERAWANAN

1. KEBIJAKAN

- a. Identifikasi Kerawanan merupakan proses manajemen risiko untuk mengidentifikasi, menganalisa, dan menilai potensi risiko terjadinya *fraud*.
- b. Identifikasi kerawanan dilakukan terhadap seluruh aktivitas yang mengandung risiko *fraud* baik yang bersumber dari aktivitas konvensional maupun syariah.
- c. Identifikasi kerawanan dilakukan oleh masing-masing unit kerja terkait sesuai dengan pedoman yang berlaku.
- d. Identifikasi kerawanan sebagai mana dimaksud huruf C disampaikan kepada Direktur Kepatuhan dan ditembuskan ke Satuan Kerja Audit Internal.

LAMPIRAN 13

Know Your Employee

C. KNOW YOUR EMPLOYEE

Sebagai upaya pencegahan terjadinya *fraud*, kebijakan *know your employee* merupakan upaya pengendalian dari aspek SDM

- a. Pelaksanaan *Know Your Employee* dilakukan dalam bentuk :
 - 1) Proses rekrutmen pegawai yang selektif dan transparan
 - 2) Proses rotasi, mutasi, promosi atau demosi.
 - 3) Kebijakan mengenali pegawai.
 - 4) Penerapan cuti wajib (*mandatory vacation*).
- b. *Know Your Employee* dilaksanakan oleh Divisi SDM & Umum.
- c. Hasil pelaksanaan *Know Your Employee* disampaikan kepada Direktur Umum dan Direktur Kepatuhan dan ditembuskan kepada Satuan Kerja Audit Internal dan Divisi MR & Kepatuhan.
- d. Proses rekrutment pegawai yang selektif dilakukan dalam bentuk :
 - 1) Menilai setiap calon pegawai Bank dalam proses rekrutmen dengan standar penilaian minimal mencakup :
 1. Aspek kompetensi yang meliputi kompetensi dasar dan bidang ilmu yang dimiliki calon pegawai;
 2. Aspek psikologis calon pegawai meliputi sikap dan perilaku calon pegawai;

3. Aspek riwayat hidup dan pekerjaan calon pegawai meliputi latar belakang dari calon pegawai yang direkrut terutama informasi bahwa pegawai yang direkrut tidak pernah terlibat dan/atau melakukan *fraud* (*track record*).
- 2) Melaksanakan proses rekrutmen yang jelas minimal mencakup:
 1. Pihak pelaksana rekrutmen (pihak eksternal dan/atau pihak internal).
 2. Mekanisme koordinasi dengan unit kerja terkait.
 3. Pihak yang bertanggung jawab terhadap pelaksanaan rekrutmen.
 4. Dokumen-dokumen yang menjadi bukti pelaksanaan rekrutmen.
 5. Prosedur pemantauan dan evaluasi pelaksanaan rekrutmen serta wujud pemantauan dan evaluasi tersebut.
- e. Proses rotasi, mutasi, promosi dan demosi dilakukan dalam bentuk:
 - 1) Melakukan penilaian terhadap pegawai yang akan dirotasi, mutasi, promosi atau demosi, yang minimal mencakup :
 1. Dasar pertimbangan dilakukannya rotasi, mutasi, promosi dan demosi.
 2. Dasar pertimbangan penempatan pegawai (baik mutasi, promosi maupun rotasi) :
 - (1) Kemampuan dan pemahaman pegawai terhadap bidang tugas.
 - (1) Pemahaman pegawai terhadap risiko yang dihadapi dalam melaksanakan operasional bank termasuk pemahaman pegawai terhadap perilaku *fraud* .
 - (2) Catatan jejak (*track record*) dari pegawai yang menimbulkan peristiwa risiko.
-) Menetapkan batasan jangka waktu rotasi dan mutasi berdasarkan aktivitas yang dilakukan, contoh : Teller dirotasi minimal 1 (satu)

- tahun sekali, Petugas Kredit dirotasi minimal 4 (empat) tahun sekali.
 Analisis kredit dirotasi minimal 4 (empat) tahun sekali.
- 3) Mekanisme pelaksanaan rotasi, mutasi dan promosi minimal memuat:
 1. Unit kerja pelaksana rotasi dan mutasi.
 2. Pejabat yang bertanggung jawab dalam pelaksanaannya.
 3. Dokumen-dokumen yang menjadi bukti pelaksanaan rotasi dan mutasi.
 4. Prosedur pemantauan dan evaluasi pelaksanaan rotasi dan mutasi serta wujud pemantauan dan evaluasi tersebut.
- f. Kebijakan mengenai pegawai
- 1) Kebijakan mengenai pegawai dilakukan dalam bentuk pengenalan karakter pegawai, perilaku, dan gaya hidup pegawai melalui *assesment* terhadap pegawai yang minimal mencakup :
 1. Pendidikan
 2. Pelatihan yang pernah diikuti
 3. Pengalaman kerja/lama bekerja
 4. Penilaian kinerja
 5. Penilaian kepribadian pegawai
 6. Penghargaan (*reward*) dan sanksi (*punishment*) yang pernah diterima pegawai.
 7. Informasi terkait anggota keluarga pegawai
 8. Rekening pegawai dan keluarganya
 9. Hubungan kekerabatan antara pegawai dengan pegawai lainnya
 10. Dan catatan-catatan lain pegawai
 - 2) Hasil *assesment* sebagaimana dimaksud pada angka 1 (satu) diatas, digunakan sebagai bahan masukan dalam penyusunan profil pegawai.

- 3) Pelaksanaan "cuti wajib" (*mandatory vacation*) dilaksanakan dalam bentuk mewajibkan pegawai yang belum menjalankan hak cutinya dalam jangka waktu tertentu untuk segera melaksanakan cuti.
- 4) Pelaksanaan Evaluasi terhadap *Know Your Employee* dilakukan oleh Divisi SDM & Umum secara berkala dan disampaikan ke Direktur Umum dan ditembuskan ke Satuan Kerja Audit Internal, dan Divisi MR & Kepatuhan.
- 5) Laporan hasil evaluasi digunakan sebagai bahan masukan untuk memperbaiki program *Know Your Employee* selanjutnya.
- 6) Satuan Kerja Audit Internal bekerja sama dengan Divisi SDM & Umum mensosialisasikan kuisisioner *assesment* pegawai terkait dengan parameter risiko *fraud* sebagaimana lampiran 05 ke seluruh pimpinan unit kerja Bank, untuk melakukan *assessment* terhadap pegawai yang dipimpinnya.
- 7) Pimpinan unit kerja Bank harus meng-update kuisisioner minimal sekali dalam setahun menggunakan Kuisisioner Identifikasi Kerawanan dan *Know Your Employee*, dengan format kuisisioner Lampiran 05.
- 8) Pemimpin Satuan Kerja Audit Internal melakukan identifikasi unit kerja yang berada pada risiko *fraud* yang berpotensi *fraud*, untuk selanjutnya melakukan investigasi.

LAMPIRAN 14

Surprise Audit dan Surveillance System

B. SURPRISE AUDIT

Bagi unit kerja yang berisiko tinggi atau rawan terhadap terjadinya *fraud*, dilakukan pemeriksaan melalui *Suprise Audit* yakni audit yang dilakukan secara mendadak atau acak dan bersifat rahasia. Pelaksanaan *suprise audit* diputuskan oleh Pemimpin Satuan Kerja Audit Internal. *Suprise audit* dilakukan apabila :

- 1) Berdasarkan hasil identifikasi kerawanan, terdapat unit kerja/aktivitas yang memiliki nilai tingkat kerawanan yang tinggi dan berpotensi *fraud* ;
- 2) Berdasarkan hasil penilaian audit internal, aktivitas memiliki tingkat pelanggaran yang tinggi dan memiliki kecenderungan (*trend*) yang meningkat dan berpotensi *fraud* ; dan/atau
- 3) Berdasarkan rekomendasi dari unit kerja lain yang menyatakan adanya indikasi potensi *fraud* ;
- 4) Kriteria/kondisi lain yang mengharuskan dilaksanakannya *suprise audit*.

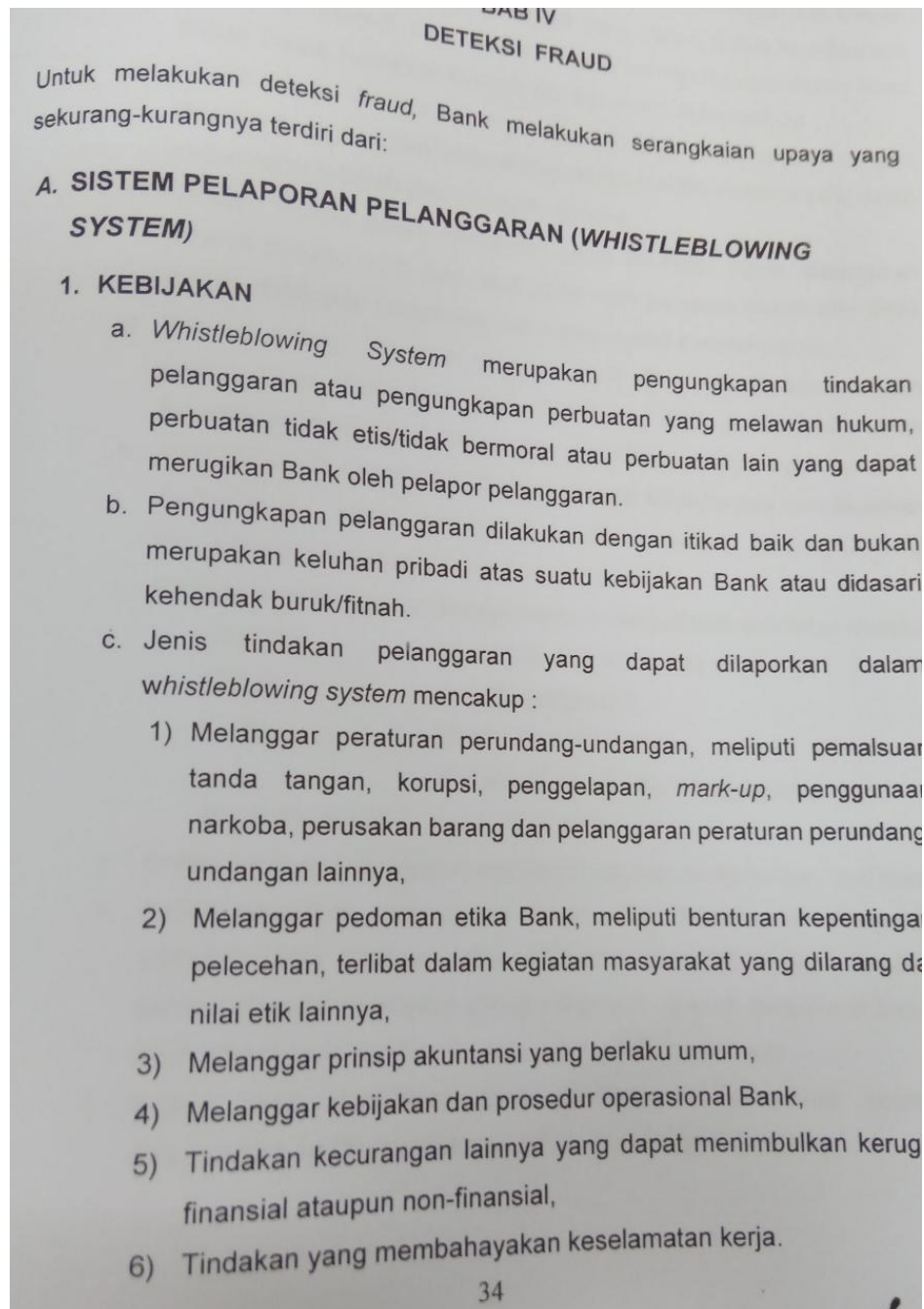
C. SURVEILLANCE SYSTEM

suatu tindakan pengujian atau pemeriksaan yang dilakukan tanpa diketahui atau disadari oleh pihak yang diuji atau diperiksa dalam rangka memperoleh keyakinan adanya dugaan penyimpangan/*fraud*. Pelaksanaan *Surveillance System* diputuskan oleh Pemimpin Satuan Kerja Audit Internal. *Surveillance System*, dilakukan berdasarkan:

- 1) Hasil identifikasi kerawanan, menunjukkan adanya unit kerja yang memiliki nilai kerawanan yang cenderung (*trend*) meningkat dan berpotensi *fraud* ;

LAMPIRAN 15

Whistleblowing System



- d. Pelapor pelanggaran adalah Insan Bank yaitu organ-organ dari Dewan Komisaris, Direksi, Komite, Pegawai tetap dalam status kepegawaian dan jabatan apapun, baik yang masih aktif bekerja maupun dalam Masa Bebas Tugas, karyawan kontrak dan karyawan *outsourcing*
- e. *Whistle blower* dalam mengungkapkan informasi *fraud* disertai dengan identitas yang jelas dan tidak menggunakan identitas lainnya yang dapat menyebabkan fitnah dan mengadu domba;
- f. *Whistle blower* dalam mengungkapkan informasi *fraud* diharapkan disertai dengan bukti dan fakta yang kuat sehingga membantu SKAI dalam melakukan investigasi dan mengungkap kebenarannya;
- g. *Whistle blower* bersedia sebagai saksi dan bekerja sama dalam mengungkap kebenaran jika diperlukan oleh SKAI baik untuk kepentingan investigasi internal dan penyidikan oleh penegak hukum;
- h. *Whistle blower* dalam kapasitasnya sebagai saksi berhak mendapatkan perlindungan saksi sebagaimana diatur dalam Undang-Undang Perlindungan Saksi dan Korban yang berlaku;
- i. Pelaporan pelanggaran sebagaimana dimaksud butir (c) diatas melalui:
- Website : <http://skdu.intranet.bpddiy.co.id>
 - Email : skdu@bpddiy.co.id
 - Surat : Direksi Bank BPD DIY
Jl. Tentara Pelajar No 7 Yogyakarta
- SMS/WhatsApp : 0811 25XX XXX
- j. Setiap pelapor pelanggaran mendapat jaminan perlindungan dari Bank
- k. Setiap pelaporan pelanggaran disampaikan kepada Tim Pengelola *Whistleblowing System* untuk dilakukan identifikasi awal, analisis, sampai dengan keputusan status pelaporan apakah berpotensi *fraud*, telah terjadi peristiwa *fraud*, atau tidak berdampak *fraud*.
- l. Setiap hasil identifikasi awal sebagaimana dimaksud huruf(k) disampaikan ke Direktur Utama untuk dimintakan keputusan.

LAMPIRAN 16
Framework Matrix Mekanisme Penerapan Strategi Anti Fraud

	A : Investigasi, Pelaporan & Sanksi	B : Manajemen Risiko	C : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen	D : Kebijakan Rotasi dan Cuti Pegawai	E : Pengendalian Internal
<p>1 : lampiran pelaporan penerapan strategi anti fraud</p>	<p>2 SURAT EDARAN BANK INDONESIA NOMOR 13/28/DPNP TANGGAL 9 DESEMBER 2011 PERIHAL PENERAPAN STRATEGI ANTI FRAUD BAGI BANK UMUM PT BANK LAPORAN PENERAPAN STRATEGI ANTI FRAUD SEMESTER I/II*) - TAHUN I. Perkembangan Pelaksanaan Penerapan Strategi Anti Fraud a) II. Inventarisasi Kejadian Fraud dan Tindak Lanjut Kejadian Fraud Jenis Fraud b) (1) Tanggal terjadi nya Fraud (2) Divisi/ Bagian terjadinya Fraud (3) Pihak yang terlibat c) (4) Jabatan (5) Kerugian d) (jutaan rupiah) (6) Tindakan Bank e) (7) Tindak Lanjut Kelemahan /penyebab terjadinya Fraud f) (8) Tindak lanjut/ perbaikan g) (9) (ttd) (.....</p>				

	A : Investigasi, Pelaporan & Sanksi	B : Manajemen Risiko	C : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen	D : Kebijakan Rotasi dan Cuti Pegawai	E : Pengendalian Internal
2 : lampiran strategi anti fraud	<p>Investigasi dilakukan untuk mengumpulkan bukti-bukti yang terkait dengan kejadian yang patut diduga merupakan tindakan Fraud. Standar investigasi yang dimiliki Bank paling kurang mencakup: 1) penentuan pihak yang berwenang melaksanakan investigasi dengan memperhatikan independensi dan kompetensi yang dibutuhkan mekanisme pelaksanaan investigasi dalam rangka menindaklanjuti hasil deteksi dengan tetap menjaga kerahasiaan informasi yang diperoleh Bank wajib memiliki mekanisme pelaporan yang efektif atas pelaksanaan investigasi dan kejadian Fraud yang ditemukan. Mekanisme pelaporan tersebut mencakup pelaporan secara internal kepada pihak manajemen Bank maupun kepada Bank Indonesia. Bank wajib memiliki kebijakan pengenaan sanksi secara internal yang efektif dalam rangka menindaklanjuti hasil investigasi agar menimbulkan efek jera bagi para pelaku Fraud. Kebijakan ini paling kurang memuat hal-hal berikut: 1) mekanisme pengenaan sanksi; dan 2) pihak yang berwenang mengenakan sanksi. Kebijakan pengenaan sanksi harus diterapkan secara transparan dan konsisten</p>	<p>pelaksanaan pencegahan Fraud telah dilaksanakan Bank, antara lain melalui penerapan Manajemen Risiko khususnya sistem pengendalian intern, dan pelaksanaan tata kelola yang baik. Namun demikian, agar penerapannya menjadi efektif masih diperlukan upaya peningkatan agar pencegahan Fraud tersebut benar-benar menjadi fokus perhatian dan budaya di Bank pada seluruh aspek organisasi, baik oleh manajemen maupun karyawan.</p> <p>Penerapan strategi anti Fraud sebagai bagian dari pelaksanaan penerapan Manajemen Risiko tidak dapat dipisahkan dari cakupan penerapan Manajemen Risiko secara umum. Oleh karena itu efektifitas penerapan strategi anti Fraud paling kurang perlu didukung dengan penguatan pada aspek-aspek Manajemen Risiko yang fokus pada pengendalian Fraud. Aspek-aspek tersebut paling kurang meliputi pengawasan aktif manajemen, struktur organisasi dan pertanggungjawaban, serta pengendalian dan pemantauan.</p>	<p>pengembangan budaya dan kepedulian terhadap anti Fraud pada seluruh jenjang organisasi, antara lain meliputi deklarasi anti fraud statement dan komunikasi yang memadai kepada seluruh jenjang organisasi tentang perilaku yang termasuk tindakan Fraud;</p> <p>pengembangan kualitas sumber daya manusia (SDM), khususnya yang terkait dengan peningkatan awareness dan pengendalian Fraud;</p> <p>pengembangan saluran komunikasi yang efektif di internal Bank agar seluruh pejabat/pegawai Bank memahami dan mematuhi kebijakan dan prosedur yang berlaku, termasuk kebijakan dalam rangka pengendalian Fraud.</p>	<p>pengendalian di bidang SDM yang ditujukan untuk peningkatan efektivitas pelaksanaan tugas dan pengendalian Fraud, misalnya kebijakan rotasi, kebijakan mutasi, cuti wajib, dan aktivitas sosial atau gathering;</p>	<p>penetapan kebijakan dan prosedur pengendalian yang khusus ditujukan untuk pengendalian Fraud; pengendalian melalui kaji ulang baik oleh manajemen (top level review) maupun kaji ulang operasional (functional review) oleh SKAI atas pelaksanaan strategi anti Fraud; penetapan pemisahan fungsi dalam pelaksanaan aktivitas Bank pada seluruh jenjang organisasi, misalnya penerapan four eyes principle dalam aktivitas perkreditan dengan tujuan agar setiap pihak yang terkait dalam aktivitas tersebut tidak memiliki peluang untuk melakukan dan menyembunyikan Fraud dalam pelaksanaan tugasnya</p>

--	--	--	--	--

A : Investigasi, Pelaporan & Sanksi	B : Manajemen Risiko	C : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen	D : Kebijakan Rotasi dan Cuti	E : Pengendalian Internal
--	----------------------	--	--	---------------------------------

			Pegawai	
3 : laporan_tahun an_bpddiy_20 16	<p>Laporan yang disusun pada tahun 2016, adalah: 1. Laporan Kinerja Satuan Pengawasan Intern Tahun 2016 2. Laporan Pokok-Pokok dan Hasil Audit Intern Semester I dan II Tahun 2016 yang disampaikan kepada OJK setiap semester dan juga kepada Dewan Komisaris.</p> <p>3. Laporan Anti-Fraud yang disampaikan kepada OJK setiap semester.</p>	<p>Penerapan melalui manajemen proses risiko Bank penerapan meliputi pengawasan aktif Dewan Komisaris dan Direksi; kecukupan kebijakan, prosedur, dan penetapan limit; kecukupan proses identifikasi, pengukuran, pemantauan, pengendalian risiko dan sistem informasi manajemen risiko; serta sistem pengendalian intern yang menyeluruh. Bank membangun kerangka dan sistem informasi manajemen risiko yang memadai dalam rangka mendukung keberhasilan penerapan manajemen risiko.</p> <p>Penerapan manajemen risiko mencakup 4 (empat) pilar, yaitu : 1. Pengawasan aktif Dewan Komisaris dan Direksi 2. Kecukupan kebijakan, prosedur, dan penetapan limit</p> <p>3. Kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian Sistem Informasi Manajemen Risiko</p> <p>4. Sistem pengendalian intern yang menyeluruh</p>	<p>1. Pengawasan aktif Dewan Komisaris dan Direksi</p> <p>a. Pengawasan aktif Dewan Komisaris dan Direksi dalam penerapan manajemen risiko dilakukan melalui, antara lain evaluasi terhadap Rencana Bisnis Bank (RBB), Laporan Penilaian Profil Risiko, Laporan Penilaian Tingkat Kesehatan Bank, serta Laporan Direktur Kepatuhan.</p> <p>b. Di samping pengawasan pasif (off-site), Direksi khususnya Direktur Kepatuhan dan Divisi Manajemen Risiko dan Kepatuhan melakukan kunjungan ke kantor cabang untuk melakukan sosialisasi manajemen risiko dengan tujuan memberikan pemahaman yang benar kepada pegawai dalam rangka meningkatkan awareness terhadap risiko yang melekat pada setiap individu dan aktivitas pekerjaan serta memastikan kepatuhan terhadap peraturanperaturan/ketentuan-ketentuan yang berlaku dari setiap aktivitas yang dilakukan berdasarkan prinsip kehati-hatian.</p>	

	A : Investigasi, Pelaporan & Sanksi	B : Manajemen Risiko	C : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen	D : Kebijakan Rotasi dan Cuti Pegawai	E : Pengendalian Internal
5 : strategi anti fraud, 2011	<p>Pilar investigasi, pelaporan, dan sanksi merupakan bagian dari sistem pengendalian Fraud yang paling kurang memuat langkah-langkah dalam rangka menggali (investigasi), sistem pelaporan, dan pengenaan sanksi atas Fraud dalam kegiatan usaha Bank. Dalam rangka memantau penerapan strategi anti Fraud, Bank wajib menyampaikan kepada Bank Indonesia, hal-hal sebagai berikut: a. Strategi anti Fraud sebagaimana dimaksud pada angka III, paling lambat 6 (enam) bulan sejak berlakunya Surat Edaran Bank Indonesia ini. b. Laporan penerapan strategi anti Fraud, setiap semester untuk posisi akhir bulan Juni dan Desember, paling lambat 10 (sepuluh) hari kerja setelah akhir bulan laporan, dengan format dan cakupan sebagaimana dimaksud dalam Lampiran 2. Laporan ini harus disampaikan terhitung sejak laporan posisi akhir bulan Juni 2012. c. Setiap Fraud yang diperkirakan berdampak negatif secara signifikan terhadap Bank dan/atau nasabah, termasuk yang berpotensi menjadi perhatian publik, paling lambat 3 (tiga) hari kerja setelah Bank mengetahui terjadinya Fraud.</p> <p>Laporan dimaksud paling kurang memuat nama pelaku, bentuk penyimpangan/jenis</p> <p>Fraud, tempat kejadian, informasi singkat mengenai modus, dan indikasi kerugian. Pelaporan tersebut tidak mengurangi kewajiban Bank untuk melakukan langkahlangkah sesuai dengan strategi anti Fraud yang dimiliki.</p>				

	A : Investigasi, Pelaporan & Sanksi	B : Manajemen Risiko	C : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen	D : Kebijakan Rotasi dan Cuti Pegawai	E : Pengendalian Internal
6 : D. Mangala, P. Kumari	<p>Forensic Accounting</p> <p>Nowadays continuously increasing fraud and inability of auditors to detect fraud has resulted in increasing demand of forensic accountants (Razaee & Burton, 1997). Forensic accountant improves auditor's ability to detect fraud and acts as a bridge to audit expectation gap (Okoye & Okaro, 2011). Emeh & Obi (2013) found that only presence of professionalised accountant will not reduce fraud but forensic accountant can reduce.</p> <p>Forensic accountants should be given participative role in preparation of audit plan rather than consultative role. They have ability to use the unique procedure in audit test</p> <p>Forensic accountant is in a better position to detect fraud (Okoye & Okaro, 2011) but is not the only available tool for fraud detection (Modugu & Anyaduba, 2013). Chi-Chi & Ebimobowei (2012) argued that if perpetrator fears of being caught by forensic accountant then they would never think of committing crime.</p>				
7 : S. Suhartono		Manajemen harus terus menerus menilai risiko fraud dan melakukan program pencegahan fraud yang disesuaikan dengan risikonya			
8 : S. Siregar, B. Tenoyo				Based on their responses, here are some suggestions they give regarding fraud prevention and detection:	

					Rotation of key account employees.
--	--	--	--	--	------------------------------------

	F : Penggunaan TI untuk mengendalikan fraud	G : Pembentukan Unit Anti Fraud	H : Pemantauan, Evaluasi & Tindak Lanjut	I : Customer Awareness melalui media sosial	J : Employee Awareness melalui sosialisasi
2 : lampiran strategi anti fraud	pengendalian sistem informasi yang mendukung pengolahan, penyimpanan, dan pengamanan data secara elektronik untuk mencegah potensi terjadinya Fraud	Untuk mendukung efektifitas penerapan strategi anti Fraud, Bank wajib memiliki unit atau fungsi yang menangani implementasi strategi anti Fraud pembentukan unit atau fungsi dalam struktur organisasi disesuaikan dengan karakteristik dan kompleksitas kegiatan usaha Bank; pertanggungjawaban unit atau fungsi tersebut langsung kepada Direktur Utama serta hubungan komunikasi dan pelaporan secara langsung kepada Dewan Komisaris	memantau tindak lanjut yang dilakukan terhadap kejadian-kejadian Fraud, baik sesuai ketentuan internal Bank maupun sesuai dengan ketentuan dan peraturan perundang-undangan yang berlaku. mendukung pelaksanaan evaluasi, Bank perlu memelihara data kejadian Fraud (Fraud profiling). Data kejadian tersebut dapat digunakan sebagai alat bantu evaluasi. Berdasarkan data kejadian Fraud dan hasil evaluasi tersebut dapat diidentifikasi kelemahan dan penyebab terjadinya Fraud serta ditentukan langkah-langkah perbaikan yang diperlukan, termasuk memperkuat sistem pengendalian intern. Bank wajib memiliki mekanisme tindak lanjut berdasarkan hasil evaluasi atas kejadian Fraud untuk memperbaiki kelemahan-kelemahan dan memperkuat sistem pengendalian intern agar dapat mencegah terulangnya kembali Fraud	3) Program customer awareness. Contohnya pembuatan brosur anti Fraud, penjelasan tertulis maupun melalui sarana lainnya untuk meningkatkan kepedulian dan kewaspadaan nasabah/deposan terhadap kemungkinan terjadinya Fraud.	2) Program employee awareness. Contohnya penyelenggaraan seminar atau diskusi terkait anti Fraud, training, dan publikasi mengenai pemahaman terhadap bentuk-bentuk Fraud, transparansi hasil investigasi, dan tindak lanjut terhadap Fraud yang dilakukan secara berkesinambungan.

		karena kelemahan yang serupa.	
--	--	-------------------------------	--

	F : Penggunaan TI untuk mengendalikan fraud	G : Pembentukan Unit Anti Fraud	H : Pemantauan, Evaluasi & Tindak Lanjut	I : Customer Awareness melalui media sosial	J : Employee Awareness melalui sosialisasi
5 : strategi anti fraud, 2011			Pilar pemantauan, evaluasi, dan tindak Lanjut merupakan bagian dari sistem pengendalian Fraud yang paling kurang memuat langkah-langkah dalam rangka memantau dan mengevaluasi Fraud, serta mekanisme tindak lanjut.		

7 : S. Suhartono				Pendeteksian dan pencegahan fraud baik dijalankan melalui program training bagi manajer dan karyawan, training ditujukan untuk meningkatkan kesadaran akan adanya risiko fraud.
------------------	--	--	--	---

<p>8 : S. Siregar, B. Tenoyo</p>	<p>information technology (IT) audit is not on the top list of tools/steps that have been implemented in respondents' companies to detect or prevent fraud. The IT auditor has an important role in fraud detection and prevention in today's business world, especially due to rapid changes in technology.</p>				
----------------------------------	--	--	--	--	--

<p>K : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud</p>	<p>L : Identifikasi Kerawanan</p>	<p>M : Koordinasi Manajemen Risiko dalam menilai risiko dengan Unit Anti Fraud</p>	<p>N : Mengetahui latar belakang pegawai dimulai dari pola rekrutmen</p>
---	-----------------------------------	--	--

<p>2 : lampiran strategi anti fraud</p>	<p>diperlukan pemahaman yang tepat dan menyeluruh tentang Fraud oleh manajemen agar dapat memberikan arahan dan menumbuhkan awareness untuk pengendalian risiko Fraud pada Bank. Anti Fraud awareness adalah upaya untuk menumbuhkan kesadaran mengenai pentingnya pencegahan Fraud oleh seluruh pihak terkait. Upaya untuk menumbuhkan anti Fraud awareness dilakukan antara lain melalui: 1) Penyusunan dan sosialisasi Anti Fraud Statement. Contohnya kebijakan zero tolerance terhadap Fraud.</p>	<p>Identifikasi kerawanan merupakan proses Manajemen Risiko untuk mengidentifikasi, menganalisis, dan menilai potensi risiko terjadinya Fraud. mengidentifikasi risiko terjadinya Fraud yang melekat pada setiap aktivitas yang berpotensi merugikan Bank. Bank wajib melakukan identifikasi kerawanan pada setiap aktivitas. Hasil identifikasi didokumentasikan dan diinformasikan kepada pihak berkepentingan dan selalu dikinikan terutama terhadap aktivitas yang dinilai berisiko tinggi untuk terjadinya Fraud.</p>	<p>Kebijakan know your employee yang dimiliki Bank paling kurang mencakup: 1) sistem dan prosedur rekrutmen yang efektif. Melalui sistem ini diharapkan dapat diperoleh gambaran mengenai rekam jejak calon karyawan (pre employee screening) secara lengkap dan akurat; 2) sistem seleksi yang dilengkapi kualifikasi yang tepat dengan mempertimbangkan risiko, serta ditetapkan secara obyektif dan transparan. Sistem tersebut harus menjangkau pelaksanaan promosi maupun mutasi, termasuk penempatan pada posisi yang memiliki risiko tinggi terhadap Fraud; dan 3) kebijakan “mengetali karyawan” (know your employee) antara lain mencakup pengenalan dan pemantauan karakter, perilaku, dan gaya hidup karyawan.</p>
---	--	--	---

<p>K : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud</p>	<p>L : Identifikasi Kerawanan</p>	<p>M : Koordinasi Manajemen Risiko dalam menilai risiko dengan Unit Anti Fraud</p>	<p>N : Mengetahui latar belakang pegawai dimulai dari pola rekrutmen</p>
---	-----------------------------------	--	--

<p>3 : laporan_tahunan _bpddiy_2016</p>			<p>Dalam pelaksanaan fungsi audit intern, PT Bank BPD DIY telah membentuk Satuan Pengawasan Intern (SPI) dan Kontrol Intern Cabang (KIC) yang masing-masing independen terhadap satuan kerja operasional. SPI bertanggung jawab langsung kepada Direktur Utama sedangkan KIC bertanggung jawab langsung kepada SPI. Sesuai dengan Surat Keputusan Direksi nomor 0307/OM 1006 tanggal 30 Desember 2016 tentang Buku Pedoman Perusahaan Bidang Organisasi PT. Bank Pembangunan Daerah Daerah Istimewa Yogyakarta, Satuan Pengawasan Intern (SPI) berubah penamaan menjadi Satuan Kerja Audit Intern (SKAI).</p>	<p>Selain hal tersebut diatas, manajemen telah melakukan sistem penerimaan pegawai yang sesuai dengan kompetensinya untuk memenuhi kebutuhan sumber daya manusia dari setiap unit kerja untuk pengelolaan risikonya.</p>
---	--	--	---	--

<p>K : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud</p>	<p>L : Identifikasi Kerawanan</p>	<p>M : Koordinasi Manajemen Risiko dalam menilai risiko dengan Unit Anti Fraud</p>	<p>N : Mengetahui latar belakang pegawai dimulai dari pola rekrutmen</p>
---	---	--	--

6 : D. Mangala, P. Kumari	Zero tolerance policy needs to be followed for any kind of fraudulent act committed by any person working at any level of organisation. Only setting up a policy is not enough but requires proper follow up. Proper guideline should be circulated and acceptable and unacceptable behaviour should be categorized (Ceonon, 2008). Further, there is need of strict and timely action in case any suspicion arises.			
7 : S. Suhartono	Untuk memberikan arahan dalam internalisasi budaya anti Fraud, peningkatan kewaspadaan maupun peningkatan kesadaran risiko Fraud pada tiap aktifitas kegiatan perusahaan.			

O : Kebijakan dan Mekanisme Whistleblowing	P : Sosialisasi WBS	Q : Surprise Audit	R : Surveillance System
--	---------------------	--------------------	-------------------------

<p>2 : lampiran strategi anti fraud</p>	<p>Kebijakan whistleblowing harus dirumuskan secara jelas, mudah dimengerti, dan dapat diimplementasikan secara efektif agar memberikan dorongan serta kesadaran kepada pegawai dan pejabat Bank untuk melaporkan Fraud yang terjadi. Untuk meningkatkan efektifitas penerapan kebijakan whistleblowing maka kebijakan tersebut paling kurang mencakup: 1) Perlindungan kepada Whistleblower Bank harus memiliki komitmen untuk memberikan dukungan dan perlindungan kepada setiap pelapor Fraud serta menjamin kerahasiaan identitas pelapor Fraud dan laporan Fraud yang disampaikan.</p> <p>2) Regulasi yang terkait dengan Pengaduan Fraud Bank perlu menyusun ketentuan internal terkait pengaduan Fraud dengan mengacu pada ketentuan dan perundang-undangan yang berlaku.</p> <p>3) Sistem Pelaporan dan Mekanisme Tindak Lanjut Laporan Fraud Bank perlu menyusun sistem pelaporan Fraud yang efektif yang memuat kejelasan proses pelaporan, antara lain mengenai tata cara pelaporan, sarana, dan pihak yang bertanggung jawab untuk menangani pelaporan. Sistem pelaporan harus didukung dengan adanya kejelasan mekanisme tindak lanjut terhadap kejadian Fraud yang dilaporkan.</p>		<p>Kebijakan dan mekanisme surprise audit perlu dilakukan terutama pada unit bisnis yang berisiko tinggi atau rawan terhadap terjadinya Fraud. Pelaksanaan surprise audit dapat meningkatkan kewaspadaan karyawan dalam melaksanakan tugasnya.</p>	<p>Surveillance system merupakan suatu tindakan pengujian atau pemeriksaan yang dilakukan tanpa diketahui atau disadari oleh pihak yang diuji atau diperiksa dalam rangka memantau dan menguji efektifitas kebijakan anti Fraud. Surveillance system dapat dilakukan oleh pihak independen dan/atau pihak internal Bank.</p>
---	--	--	--	--

<p>O : Kebijakan dan Mekanisme Whistleblowing</p>	<p>P : Sosialisasi WBS</p>	<p>Q : Surprise Audit</p>	<p>R : Surveillance System</p>
---	----------------------------	---------------------------	--------------------------------

<p>3 : laporan_tahun_bpddiy_2016</p>	<p>Whistleblowing System</p> <p>Sistem Pelaporan Pelanggaran (Whistleblowing System) adalah sistem yang mengelola pengaduan/ penyingkapan mengenai perilaku melawan hukum, perbuatan tidak etis/tidak semestinya secara rahasia, anonim dan mandiri yang digunakan untuk mengoptimalkan peran sertadan pihak lainnya dalam mengungkapkan pelanggaran yang terjadi di lingkungan PT Bank BPD DIY.</p> <p>PT Bank BPD DIY telah memiliki Whistleblowing System berdasarkan Surat Keputusan Direksi Nomor: 001/KPTS/DP/2012 tentang penerapan Kebijakan Strategi Anti Fraud.</p> <p>Pengelolaan Whistleblowing System</p> <p>Mekanisme pengelolaan Whistleblowing System yang sedang dikembangkan Bank BPD DIY yakni setiap pegawai atau siapa saja yang ingin melaporkan indikasi fraud, sedangkan jika merasa sungkan maka laporan dapat disampaikan melalui SMS atau e-mail dengan alamat khusus dengan menggunakan surat ditujukan kepada pengelola Whistleblowing System.</p>	<p>Sosialisasi Whistleblowing System</p> <p>Sosialisasi Whistleblowing System di internal Bank BPD DIY disampaikan melalui berbagai media seperti buletin internal, poster, sosialisasi etika maupun presentasi langsung kepada unit kerja terkait. Untuk eksternal, sosialisasi dilakukan melalui website Bank BPD DIY dan pengiriman surat edaran/memo.</p>		
--	---	---	--	--

	O : Kebijakan dan Mekanisme Whistleblowing	P : Sosialisasi WBS	Q : Surprise Audit	R : Surveillance System
6 : D. Mangala, P. Kumari	<p>Whistle blowing policies motivate them to report fraud. It is easiest and least expensive method (Deloitte, 2012). It helps to improve internal control and recover the embezzled funds (Waldron, 2012). Hotline is a common and efficient method to whistle blow (ACFE, 2014). For successful functioning of whistle blowing program proper channel of communication, protection to whistle blower, staff awareness and staff trust is very important (PwC, 2008). Miceli & Near (1984) found that one would not report a fraud through an unknown channel. Firstly, a person observes wrongdoing and its consequences. Then, with effect of personal and emotional characteristics, that person reports wrongdoing. Finally, organisation decides whether to act over report or not. Okoye & Okaro (2011) found significant agreement about inculcation of whistle blowing in organisation culture. Corrective actions taken on whistle blowing encourage whistle blowing and result in efficient organisational operation (Miceli & Near, 1984). Whistle blower may be external or internal but external whistleblowers are less fearful about its consequences.</p>			

	O : Kebijakan dan Mekanisme Whistleblowing	P : Sosialisasi WBS	Q : Surprise Audit	R : Surveillance System
7 : S. Suhartono	<p>Program anti-fraud yang ampuh adalah mempersenjatai individu dengan sarana yang memudahkan pelaporan mengenai aktivitas yang mencurigakan. Sarana bisa berupa hot-line yang menerima laporan baik dari pihak internal maupun eksternal. Pengirim laporan tidak perlu menyebutkan nama dan identitas lainnya agar kerahasiaan terjaga. Management perlu mendorong karyawan agar melapor jika ada hal-hal yang mencurigakan. Perusahaan yang memiliki program training melawan fraud bagi executives, manager dan karyawan ternyata mengalami kerugian fraud yang lebih sedikit dan lama fraud yang lebih singkat dibanding dengan yang tidak memiliki program seperti itu. Paling tidak staf harus di edukasi mengenai tindakan fraud, bagaimana fraud merugikan semua orang dalam perusahaan, dan agar melapor jika ada yang mencurigakan.</p>		<p>Indikator Fraud (red flag) adalah suatu bentuk sinyal terhadap adanya bukan kemungkinan Fraud. Perlu ditekankan bahwa indikator Fraud menunjukkan sudah pasti terjadi tindak Fraud, namun hanya merupakan sinyal peringatan untuk diketahui lebih lanjut.</p>	<p>Surveillance System adalah suatu tindakan pengamatan, pengujian atau pemeriksaan yang dilakukan tanpa diketahui atau disadari oleh pihak yang diuji</p>

8 : S. Siregar, B. Tenoyo	<p>We might recall the name of Sherron Watkins. She is the former vice president of Enron and known as the whistleblower who helped to uncover the Enron scandal in 2001. This is one of the evidence of the importance of whistle-blowing policy.</p>	<p>well-defined whistle-blowing policy is the second least important one that a good fraud risk management process should cover. Anonymous reporting of suspicions of fraud, corruption or misconduct should be another important system the company should put in place to prevent and detect fraud. Whistle-blowing policy is important, so people are encouraged to speak out if they are suspicious of frauds or encounter either corruption or misconduct.</p>		
---------------------------	--	---	--	--

	A : Investigasi, Pelaporan & Sanksi	B : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen
6 : Bapak Suwasono Adi Kurniawan	<p>P : Kalau untuk Laporan Anti Fraud itu mekanismenya bagaimana?</p> <p>N : Jadi laporan anti fraud itu tiap semester dilaporkan ke OJK. Ini yang rutin ya Laporan Penerapan Strategi Anti Fraud. Kalau yang tidak rutin ya jika ada indikasi fraud atau sudah terjadi fraud yang kerugiannya itu bisa mempengaruhi kondisi perekonomian perusahaan wajib dilaporkan maksimal 3 hari setelah tanggal kejadian.</p>	<p>Selama ini sudah ada pakta integritas, di awal tahun semua pegawai akan dapat. Nah setelah ada unit ini, ada tambahan lagi, kalau pakta integritas kan semua manajemen dan pegawai, kalau ini yang dari unit anti fraud, namanya Anti Fraud Statement. Ini tapi belum kita jalankan, baru sosialisasi dulu ke semua cabang. Ini tambahan untuk pengurus yaitu Direksi dan Dewan Komisaris juga tanda tangan.</p> <p>P : Jadi dengan tanda tangan ini dari awal mereka sudah berstatement untuk melakukan ini?</p> <p>N : Iya</p>
	A : Investigasi, Pelaporan & Sanksi	B : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen
7 : Bapak Zukhroni Ariffin	<p>P : Bagaimana mekanisme pelaksanaan investigasi, pelaporan dan sanksi?</p> <p>N : Kalo pelaporan strategi anti fraud itu jelas, kita melaporkan tiap 6 bulan sekali. Kita melaporkan hasil investigasi kita. Kalau memang ada ya kita laporkan semua, kalau tidak ada ya tetap kita laporkan NIHIL. Jadi setiap 6 bulan, maksimal tanggal 10 setelah bulan pelaporan sudah saya laporkan ke OJK. Jadi laporan anti fraud setiap semesteran, nanti ada formatnya dari OJK.</p> <p>Kalau hasil investigasi kita itu nanti kita laporkan ke atasan langsung dan Direktur Utama. Kalau sanksi dari investigasi itu bukan di ranah kita lagi, kita sebatas penyelidikan saja. Penyelidikan pun harus dikeluarkan surat tugas khusus dari Direktur Utama. Kalau sanksi mau seperti apa itu nanti KMK (Komite Kepegawaian) yang menentukan dari hasil fraud itu. Kita hanya melaporkan bahwa ditemukan fraud ini yang akan berdampak ini oleh ini. Nah selanjutnya KMK yang menentukan apa yang harus dilakukan untuk si pelaku fraud.</p> <p>P : Biasanya dari KMK sanksi terparah untuk pelaku itu apa pak?</p> <p>N : Ya PHK. Downgrade atau turun adri jabatannya, bisa juga dia tidak diberikan hak - haknya selama beberapa tahun kedepan sesuai dengan tingkat fraud yang dilakukan, misalnya THR tidak akan diberikan 100%, atau pun pemberhentian tanpa predikat. Kalau untuk PHK dari segi pelaku fraud akan senang, karena akan lunas kewajibannya. Tapi kalau tanpa predikat berarti dia harus melunasi kewajiban itu dulu. Makannya di pihak intern kami pun kalau pengen punya pinjaman jangka panjang yang nominalnya besar, paling tidak ada jaminan atas pinjaman itu, jadi untuk mengantisipasi hal - hal terkait PHK itu.</p>	

	C : Kebijakan Rotasi dan Cuti Pegawai		C : Kebijakan Rotasi dan Cuti Pegawai		C : Kebijakan Rotasi dan Cuti Pegawai		C : Kebijakan Rotasi dan Cuti Pegawai
1 : Bapak Andrianto Dwi P.	P : Apakah sudah pernah dilakukan rotasi jabatan? N : Sudah kalau itu.	2 : Bapak Daryoko	P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji? N : Tidak bisa kalau itu.	4 : Bapak Muhammad Agus Salam S.	P : Apakah sudah pernah dilakukan rotasi jabatan? N : Pasti dilakukan kalau itu mbak. Kisaran 4 tahun jabatan maksimal. P : Apakah bapak biasanya mengambil semua jatah cuti? N : Tidak semua kadang, biasanya satu atau dua hari. Kalau berhari - hari ya nunggu momen liburan. P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji? N : Selama ini sih tidak bisa.	8 : Ibu Nur Aeni	C : Apa ada rotasi pegawai bu? N : Iya ada. Biasanya 4 tahun sekali. Dulu saya di SKAI, sekarang di Manajemen Risiko. Cuti itu harus di ambil. Pada saat dia cuti kan digantikan sama teman lain yang satu unit. Bisa jadi kan dia (temennya) menemukan. P : Untuk jatah cuti itu bagaimana sistemnya bu? N : Satu tahun 12 hari, boleh diambil kapan saja dan wajib diambil. Biasanya pegawai hanya ambil satu dua hari, kalau seperti itu susah digantikan pegawai lain, karena kan jika digantikan teman dan waktunya cukup lama, kemungkinan ditemukan hal yang tidak wajar jadi lebih besar. P : Kalau jatah cuti tidak diambil boleh diganti gaji? N : Nggak boleh.

3 : Bapak Ivan Nugroho	P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji? N : Tidak bisa.	5 : Bapak Pandu Kuncoro	P : Apakah sudah pernah dilakukan rotasi jabatan? N : Iya, biasanya empat tahun sekali. P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji? N : Tidak bisa mba. Jadi memang harus kita ambil semua.	6 : Bapak Suwasono Adi Kurniawan	Rotasi itu ketika digeser ke level yang sama, atau dipindah ke beda cabang tapi di level yang sama. Seperti front officer ya tetap di front officer tapi beda cabang, karena kan salah satu mitigasi fraud ya rotasi itu. Kita rata - rata 4 tahun sekali. kita mewajibkan setelah ada unit itu cuti itu wajib diambil yang secara berurutan ada minimal 3 hari. Saat dia ada pengganti maka kemungkinan akan ditemukan hal - hal menyimpang saat dia bekerja, hal ini merupakan salah satu bentuk pendeteksian fraud. Mungkin kedepan kita arahnya 5 hari
------------------------	--	-------------------------	--	----------------------------------	--

D : Pengendalian Internal	E : Penggunaan TI untuk mengendalikan fraud	F : Pembentukan Unit Anti Fraud	G : Pemantauan, Evaluasi & Tindak Lanjut	H : Customer Awareness melalui media sosial
---------------------------	---	---------------------------------	--	---

<p>6 : Bapak Suwasono Adi Kurniawan</p>	<p>P : Jadi mungkin atau tidak pak pegawai memalsukan cek? N : Kalau memalsukan cek kemungkinannya sangat kecil. Karena cek itu percetakannya sama seperti uang, cek kita itu produksinya per week. Secara bahan juga susah dipalsukan.</p>	<p>P : Bagaimana pengamanan teknologi yang ada di BPD DIY? N : Pengamanan teknologi kita dikembangkan oleh tim IT kita, seperti flashdisk saja tidak bisa diakses jika masuk ke laptop atau komputer. Wifi umum tidak bisa walaupun internet juga kita disediakan layanan proxy dan itu pun terbatas. Kalau dikantor hotspot disediakan di setiap ruangan.</p>	<p>P : Bagaimana peran masing - masing bagian di dalam struktur organisasi mengenai penerapan strategi anti fraud? N : Di kita, BPD DIY, untuk tim sendiri, di kita unit anti fraud baru ada sejak 2017, namun untuk penerapan strategi anti fraud sudah sejak 2012. Karena sesuai dengan PBI, PBI mewajibkan di tahun 2011 itu dan tahun 2012 kita langsung menerapkan, isinya kurang lebih sama, cuman waktu itu dia masih yang mengelola di SKAI, jadi belum ada tim khususnya. Jadi baru tahun kemarin ada unit khusus, unit anti fraud namanya. Secara organisasi berada dibawah Satuan Kerja Audit Internal. Dengan personilnya ada 2, saya dan mas Zukhron tadi, dan saya yang jadi pemimpin unit anti fraud nya, dan mas Zukhron sebagai staff. P : Bagaimana perbedaan SKAI dan Unit Anti Fraud? N : Kalau anti fraud itu nanti jika hanya sudah ada indikasi adanya fraud, kita memastikan, mencari bukti. Namun jika tidak ada fraud kita juga punya peran juga untuk mendeteksi dan pencegahan.</p>	<p>P : Bagaimana pelaksanaan proses pemantauan, evaluasi dan tindak lanjut? N : Evaluasi dilakukan setelah pemantauan dilakukan. Evaluasi dilakukan seiring dibuatnya laporan. Untuk evaluasi kita memberikan perbaikan yang harus dilakukan pada bagian yang terlibat tindakan fraud. Tindak lanjut tidak bisa dilakukan oleh Unit Anti Fraud, itu dilakukan oleh Komite Kepegawaian atau KMK.</p>	<p>P : Bagaimana pelaksanaan customer awareness? N : Ini kita melakukannya hanya semacam sosialisasi dengan bantuan kantor cabang untuk sosialisasi ke instansi mana, nah itu kita selipkan materi tentang strategi anti fraud. Kita juga sudah mempersiapkan brosur, selain kita membuat brosur tentang produk kita, kita juga akan membuat brosur tentang pelaksanaan strategi anti fraud. Tapi ini masih dalam proses karena kan unit anti fraud masih baru. Dan nantinya kan tayangan tv yang ada di bawah yang langsung terlihat oleh customer biasanya hanya informasi tentang rate, nilai kurs dan produk kita, nantinya akan kita munculkan materi tentang strategi anti fraud.</p>
---	---	--	--	---	---

	D : Pengendalian Internal	E : Penggunaan TI untuk mengendalikan fraud	F : Pembentukan Unit Anti Fraud	H : Customer Awareness melalui media sosial
8 : Ibu Nur Aeni	<p>P : Kalau SKAI pengendalian internal nya sudah dilakukan darimana bu?</p> <p>N : Pengendalian internal teller misalnya dari slip. Pada saat selesai jam kantor itu harus nol, tidak boleh selisih. Itu transaksinya, kalau pengendaliannya itu kan teller ada atasannya, nah atasannya itu harus mengoreksi setiap transaksi yang terjadi per hari.</p> <p>P : Jadi tidak mungkin ya bu cek di palsukan?</p> <p>N : Jadi kalau bicara cek dipalsukan, cuman kan tinggal pengendalian internalnya gimana. Jadi kalau semisal ada yang meneliti, kan harus jelas, tandatangan speciment ini sama gak seperti si pemilik cek ini. Itu termasuk salah satu pengendalian mencocokkan. Terus dimintai ktp si pencair. Sebenarnya setiap bank itu kan ada SOP (Standar Operasional Prosedur), kalau semua itu dijalankan maka akan sangat minimal bahkan tidak ada namanya fraud. Tapi bisa jadi ada orang kehilangan cek dan jatuh, cuma kembali lagi speciment (tandatangan) nya akan dicocokkan speciment pemilik. Pada saat pencairan pun kalau melebihi kewenangan itu kan tetep yang harus mengotorisasi kan atasannya, jadi teller itu hanya bisa mengeluarkan 10 juta, tapi ceknya itu 25 juta. Teller tetap tidak bisa mengeluarkan, walaupun warkat sah, speciment sama, nomer PG nya sama. Jadi satu cek itu pengendaliannya banyak. Saat bank mengeluarkan cek itu pasti ada nomer serinya, nah nomer seri itu sudah di input di sistem. Jadi kalau semisal orang buat cek di percetakan, otomatis nomer serinya tidak ada. Nah itu udah pengendalian awal, pengendalian kedua dilihat speciment nya, pengendalian ketiga ada untuk diotorisasi atasannya.</p> <p>P : Kalau seperti phising, skimming atau pengambilan data nasabah oleh orang luar itu ada tidak?</p> <p>N : Ada, baru saja terjadi, semua bank kena. Itu skimmer nya dipasang di ATM. Nah pengendalian internal yang kita lakukan pada ATM kita itu pada saat kita rutin melihat di mulut ATM. Jadi kalau kamu punya kartu ATM, sebelumnya kalau di mulut ATM ada yang mencurigakan itu jangan kamu masukkan. Jadi ATM kan bisa dilakukan lintas bank, seperti ATM Bersama, nah makannya kena di ATM lain karena terpasang skimmer. Karena itu pengendalian internal itu di kita, setiap hari mulut ATM kita periksa.</p>	<p>P : Siapa yang membuat WBS?</p> <p>N : WBS itu dibuat oleh TI kita, tapi untuk pengelolaannya dilakukan SKAI yang sekarang ada Unit Anti Fraud.</p>	<p>P : Kalau orang - orang tim anti fraud itu nanti yang ada di dalam SKAI juga?</p> <p>Jadi SKAI itu ada 3 tiga bagian, audit kredit, audit operasional, anti fraud. Jadi itu ada PBI nya. Jadi anti fraud bank itu ada yang berdiri sendiri dan ada yang di dalam (SKAI), nah ini tergantung dari size bank nya. Karena BPD ini hanya satu wilayah DIY saja, sehingga anti fraud ini dibawah SKAI.</p> <p>P : Kalau untuk penerapan strategi anti fraud itu SKAI juga atau anti fraud?</p> <p>N : Anti fraud. Jadi jika sudah bicara ke fraud ya anti fraud. Strategi apa yang harus dia buat. Jadi misalnya didalam pekerjaan rutin dia (SKAI) itu kayak anti fraud.</p> <p>N : Memang anti fraud itu baru. Tapi sudah dibuat PBI nya kan itu tentang anti fraud yang setiap bank harus punya unit, sehingga dibuat anti fraud.</p>	<p>P : Kalau seperti itu kan merugikan nasabah dan menurunkan citra bank, itu nasabahnya diberikan sosialisasi tidak?</p> <p>Nanti akan mengundang nasabah - nasabah kita, nanti kita bentuk seperti gathering. Kita beri sosialisasi bahwa saat akan memakai ATM diperiksa dahulu ada skimmer tidak, dan pin itu hanya punya kita pribadi jangan dikasihkan orang lain.</p>

	I : Employee Awareness melalui sosialisasi	J : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud		I : Employee Awareness melalui sosialisasi	J : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud	L : Koordinasi Manajemen Risiko dalam menilai risiko dengan Unit Anti Fraud
2 : Bapak Daryoko	<p>P : Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?</p> <p>N : Ya.. Bagus itu, karena pesan tersampaikan tanpa harus susah - susah mengumpulkan semua pegawai, ya walaupun kita BPD DIY memang rutin 3 bulan sekali ada sosialisasi.</p>	<p>P : Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?</p> <p>N : Ya.. Bagus itu, karena pesan tersampaikan tanpa harus susah - susah mengumpulkan semua pegawai, ya walaupun kita BPD DIY memang rutin 3 bulan sekali ada sosialisasi.</p>	3 : Bapak Ivan Nugroho	<p>P : Seperti apa sosialisasi mengenai WBS yang didapatkan?</p> <p>N : Menyadarkan pentingnya melaporkan tindakan kecurangan yang ada di dalam organisasi. Dan dijelaskan juga dampak kerugian yang kita (pegawai) dapatkan atas kerugian perusahaan. Sama cara mengakses nya sih lewat intranet.</p> <p>P : Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?</p> <p>N : Ya.. Selain BPD DIY memang rutin 3 bulan sekali ada sosialisasi, hal itu juga perlu.</p>	<p>P : Apakah pernah mendapatkan sosialisasi melalui konten di desktop komputer/laptop tentang anti fraud?</p> <p>N : Ya.. Selain BPD DIY memang rutin 3 bulan sekali ada sosialisasi, hal itu juga perlu.</p>	<p>P : Bagaimana koordinasi antara Manajemen Risiko dan SKAI?</p> <p>N : Untuk penilaian risiko dilakukan oleh Manajemen Risiko, tapi untuk menentukan risiko yang perlu di audit lebih lanjut itu nanti tergantung kebijakan SKAI. SKAI nanti akan membuat rencana audit dari hasil penilaian risiko MR. Jika memang nanti perlu dilakukan tindaklanjut atas indikasi fraud maka akan ditindaklanjuti Unit Anti Fraud kalau sekarang ya namanya.</p> <p>P : Dalam penilaian risiko apakah MR menyediakan draft tersendiri untuk SKAI ataupun divisi lain?</p> <p>N : Betul sekali, itu ada. Jadi hal itu merupakan salah satu strategi kita untuk melihat apakah penilaian MR dan permasalahan setiap divisi sudah sesuai atau belum.</p> <p>P : Jadi nanti Manajemen Risiko itu menganalisis, lalu laporan tahun lalu yang menurut Manajemen Risiko perlu ditindaklanjuti SKAI nanti akan diberikan ke SKAI itu bisa?</p> <p>N : Benar sekali. Itu tadi, kalau SKAI merasa perlu dipelajari lebih lanjut tentang indikasi fraud maka akan dilakukan oleh Unit Anti Fraud.</p>

	I : Employee Awareness melalui sosialisasi	J : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud	K : Identifikasi Kerawanan	L : Koordinasi Manajemen Risiko dalam menilai risiko dengan Unit Anti Fraud
6 : Bapak Suwasono Adi Kurniawan	<p>Dari teman-teman cabang sendiri juga kita bekali terutama supervisor atau pemimpin cabang yaitu indikasi fraud begitu.</p> <p>P : Kalau untuk red flags sendiri bagaimana pak? N : Kami bekali juga untuk hal-hal seperti itu, walaupun tidak khusus memantau karena jobnya banyak. Indikasi fraud apa saja, mereka membantu memantau staff-staffnya yang agak aneh seperti pergantian pola hidup seperti itu. Kalau tidak report kesini bisa ke KIC. Semua memang dari kantor-kantor cabang, termasuk semua itu membuat pemetaan titik-titik kerawanan. Misalnya proses pembukaan tabungan, itu titik rawannya dimana. Kalau di risk based audit itu nanti kan kita harus memperhatikan mana yang menimbulkan risiko tertinggi.</p>	<p>Nanti kalau pencegahan kita melalui sosialisasi, kalau untuk pegawai nanti di desktop semua komputer akan berganti background dengan konten-konten berhubungan dengan anti fraud, dan akan ada kampanye juga tentang anti fraud ke kantor-kantor cabang.</p> <p>P : Kalau untuk kampanye sosialisasi budaya anti fraud itu bagaimana pak? N : Jadi itu kita keliling ke kantor-kantor cabang untuk sosialisasi anti fraud. Kemarin sudah keliling ke cabang sleman, dari kantor cabang pembantu sampai ke kantor kas, itu kita kumpulkan sehari-hari, kita sosialisasikan, yang rawan dimana, indikasi-indikasinya, penyebab fraud secara teori seperti ini dan kalau hasil survey seperti ini.</p>	<p>Semua memang dari kantor-kantor cabang, termasuk semua itu membuat pemetaan titik-titik kerawanan. Misalnya proses pembukaan tabungan, itu titik rawannya dimana. Kalau di risk based audit itu nanti kan kita harus memperhatikan mana yang menimbulkan risiko tertinggi.</p> <p>P : Apakah kecurangan dari eksternal seperti phishing, skimming, money laundering, penggunaan kartu palsu, pencurian informasi bank pernah terjadi? N : Ini semuanya bisa terjadi di kita, kalau sering relatif tidak. Khusus yang eksternal seperti money laundering ini kan kita tidak bisa mengontrol asalnya darimana. Biasanya kita hanya tahu ada tim PPATK, mereka akan minta keterangan apakah nasabah ini mempunyai rekening disini atau tidak. Biasanya nama-nama pejabat yang ditanyakan. KPK juga biasanya begitu.</p> <p>Jadi pernah kita alami dulu ada anak SMA buka deposito sebesar 100 juta, itu kan besar sekali dan tidak sesuai profil, nah itu harus kita pantau. Jadi MR itu rutin melaporkan transaksi-transaksi yang mencurigakan setiap bulan wajib ke PPATK. Kalau kita cukup mendalami dilihat dari form yang diisi, ini uang darimana. Nah itu ternyata bapaknya jual tanah dan membukakan deposito atas nama anaknya untuk tabungan masa depan. Jadi sudah clear.</p>	<p>P : Apakah ada kerjasama dengan manajemen risiko? manajemen risiko itu lebih ke pra kejadian jadi untuk pencegahan. Nah SKAI itu setelah kejadian. Jadi di kita itu dikenal dengan three line of defense. Jadi menghadapi risiko yang pertama itu yang di front office, yang di cabang berhadapan dengan nasabah. Yang kedua yang mengawasi mereka itu manajemen risiko. Nah yang ketiga itu setelah kejadian untuk SKAI sendiri, itu kita mengaudit apa yang telah terjadi</p> <p>P : Seperti apa identifikasi kerawanan dalam proses penilaian risiko? N : Contohnya ini, risiko operasional, internal fraud : Penerbitan kartu debit palsu oleh karyawan Menerbitkan kartu ATM tanpa persetujuan pejabat yang berwenang Pencurian informasi kartu ATM oleh karyawan Penarikan dana oleh karyawan dengan kartu ATM palsu Mitigasi nya : Sosialisasi budaya risiko pada karyawan Sosialisasi nilai perusahaan Jadi memang di setiap produk kita itu sudah ada identifikasi kerawanan / mitigasi nya. Eksternal fraud : Pemalsuan kartu / hacking Penarikan dana ATM Skimming Mitigasi nya : Edukasi terhadap nasabah Memberikan pengetahuan yang cukup kepada nasabah saat membuka rekening Pengamanan mesin ATM Asuransi terhadap mesin ATM Pengamanan sistem</p>

--	--	--	--

I : Employee Awareness melalui sosialisasi	J : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud	K : Identifikasi Kerawanan
--	--	----------------------------

<p>8 : Ibu Nur Aeni</p>	<p>P : Kalau sosialisasi itu seminar atau bagaimana? N : Bukan, jadi dikumpulkan kayak pendidikan. Jadi dijelaskan WBS itu bagaimana, jika ada teman yang melakukan pelanggaran dan merasa tidak enak ya lewat WBS. Kan WBS lebih tidak diketahui yang melapor. P : Jadi WBS di sosialisasikan ke semua jajaran organisasi atau ke pimpinan saja? N : Tidak tidak, ke semua jajaran organisasi. Sosialisasi ini paling tiga bulan sekali. SKAI melihat ada indikasi fraud selain dari laporan audit juga dari laporan - laporan lain.</p>	<p>kalau bicara anti fraud itu pencegahannya itu satu, dia akan melakukan sosialisasi. P : Kalau sosialisasi itu nanti lewat apa bu dalam internal? N : Seperti mas adi (Unit Anti Fraud), dia melakukan sosialisasi ke cabang - cabang. Jadi menilai risiko di kantor pusat dan cabang, audit pun di kantor pusat dan cabang.</p>	<p>Kita akan mendapatkan penilaian manajemen risiko masing - masing cabang itu kita lihat, misalnya ada disini 7 cabang, dari 7 cabang itu ternyata hanya 5 ini yang memiliki risiko operasional tertinggi, makannya di 5 cabang ini SKAI akan melakukan audit operasional yang lebih dalam. Mungkin yang 2 enggak, disini bukan risiko operasional tapi risiko hukum, bisa jadi kan. Memang SKAI dan manajemen risiko itu terkait. P : Kalau semisal nasabah berupa perusahaan gitu apakah pernah bu mereka terlibat seperti money laundering? Ada nasabah menyetorkan uang tunai 1 Milyar. Nah sulitnya mengidentifikasi nilai uang yang mencurigakan, karena walaupun hanya 100 ribu juga bisa dianggap mencurigakan. Jadi di kita di sistem, misalnya ni saya, misal gaji saya sebulan 10 juta, apabila di rekening saya terjadi transaksi melebihi 5 kali gaji saya, itu akan ada warning di sistem kita, dianggap transaksi mencurigakan. Akan dilihat darimana asal uang. Misal ternyata saya mendapatkan transferan itu dari hasil penjualan tanah, yasudah tidak ditindaklanjuti.</p>
-------------------------	--	--	--

<p>M : Mengetahui latar belakang pegawai dimulai dari pola rekrutmen</p>	
<p>6 : Bapak Suwasono Adi Kurniawan</p>	<p>P : Bagaimana proses know your employee dilakukan sejak perekrutan pegawai? Di Anti Fraud kita sudah melaksanakan tapi tidak sebesar di SDM. Semua dilaksanakan mulai dari proses perekrutan sampai sudah jadi pegawai. Kalau saat perekrutan kita mengawasi, kan wewenangnya SDM. Harus diumumkan di koran, kalau tidak kan nanti bisa jadi hanya orang - orang tertentu saja yang akses. Seperti yang ada disini (BPP Anti Fraud) yang melakukan know your employee itu dilaksanakan oleh divisi SDM. Hasil pelaksanaannya dilaporkan ke Direktur Utama lalu ditembuskan ke kita (Anti Fraud) dan Manajemen Risiko. Proses rekrutmen misalnya menilai setiap calon pegawai dengan standar minimal mencakup kompetensi, psikologis, dan sebagainya. Kebijakan penilaian calon pegawai juga melalui penilaian karakter pegawai, jadi melalui asesment. Seperti pendidikannya apa, pelatihan yang pernah diikuti, pengalaman bekerja atau lamanya bekerja di kita atau di sebelumnya, kepribadian pegawai, penghargaan yang pernah diterima, sanksi yang pernah diterima, informasi terkait anggota keluarga, mengenai rekening pegawai nah kalau ini cuma yang sebatas di rekening kita, hubungan kekerabatan pegawai dengan pegawai lainnya seperti anak, bapak, ibu, suami dan istri, jika selain itu maka akan menjadi perhatian khusus. Perhatian khusus itu seperti proses masuknya sesuai prosedur atau tidak, melalui pendaftaran, jika saat sudah diterima benar atau tidak dalam pekerjaannya. Hasil asesment ini berguna sebagai masukan initial profil pegawai.</p>
<p>8 : Ibu Nur Aeni</p>	<p>P : Kalau perekrutan SDM itu bagian yang merekrut ada kualifikasi bahwa SDM nya kompeten? N : Kita ada, standar itu ada. Kita bisa buka informasi debitur, dari OJK namanya indeb (identitas debitur). Kalau kita mau merekrut itu nanti kita ambilkan indeb. Misal ternyata dia ini punya kredit macet di bank lain, kenapa bisa macet? Apa karena ngemplang atau tidak punya i'tikad yang baik, kemudian kita minta SKCK, tidak menggunakan narkoba. Kalau masalah kompeten pendidikan kita kan kerjasama sama UGM untuk rekrutmen.</p>

	<p>N : Mekanisme Pengaduan pada WBS</p>
--	---

<p>6 : Bapak Suwasono Adi Kurniawan</p>	<p>P : Melindungi pelapor itu bagaimana pak? N : Dalam bentuk kerahasiaan ya, kalau perilaku seperti undang - undang kan kita susah. Harus dijaga rumahnya, kan kita gak punya wewenang kesitu</p> <p>P : Whistleblowing system ini melalui internet atau sms pak? N : Melalui intranet. Jadi di kantor kita ini semua terhubung satu jaringan untuk internal saja. Sementara kita untuk internal dulu</p> <p>P : Bagaimana mekanisme penerapan deteksi fraud melalui whistleblowing system? N : Ini kita masih pakai yang lama karena kan sudah berlaku sejak 2012. Surat edaran petunjuk pelaksanaan penyampaian pelaporan pengakuan indikasi tindak pelanggaran beserta pelanggarnya (menunjuk buku mekanisme penerapan whistleblowing system) jadi lewat sini semua, langkah - langkahnya ada. Asas WBS : Kerahasiaan, tidak diskriminatif, perlindungan Yang bisa dilaporkan itu yang memenuhi beberapa atau satu kriteria : Termasuk kategori pelanggaran Laporan terjadi paling lama 2 tahun sejak tanggal pelaporan Ini websitenya, wbs.intranet.co.id, ini yang bisa buka hanya 1 orang 2 orang. Ini yang lama, untuk aturan baru hanya kita ulangi. Yang bertanggung jawab atas WBS itu direktur utama. Yang bisa diberi kewenangan untuk membuka ada laporan atau tidak itu SKAI. Nah untuk unit anti fraud belum tahu, kita bisa membuka atau hanya sekedar diberi laporan, ini ada kejadian disana silahkan ditindaklanjuti tanpa tahu siapa yang melaporkan.</p> <p>P : Siapa yang bertanggung jawab dalam mengelola pengaduan melalui whistleblowing system? N : Nah untuk whistleblowing system yang bertanggung jawab untuk saat ini Direktur Utama, nah yang ditunjuk oleh Direktur Utama untuk membuka laporan itu karena tidak semua diperbolehkan itu pemimpin SKAI dan pemimpin Manajemen Risiko. Jadi password nya cuma di 2 orang itu.</p>
<p>8 : Ibu Nur Aeni</p>	<p>P : Jadi kalau aduan seperti itu melalui website atau sms? N : Hanya kalau di kita internal. Kalau bicara eksternal biasanya lewat surat kaleng. Kalau bicara di sistem itu website. Jadi khusus untuk internal melalui website. WBS yang mengelola ya tim anti fraud.</p> <p>P : Jadi kalau menemukan aduan yang signifikan untuk diperdalam akan lapor ke SKAI dulu? N : Iya. Nanti otomatis SKAI akan meminta dibuatkan surat tugas dari direktur utama.</p> <p>P : WBS kalau untuk eksternal bagaimana? N : Kalau untuk yang sistem WBS hanya internal, kita belum berani ke eksternal. Kalau eksternal kan kadang ada laporan yang hanya buat - buat saja. Jadi lebih ke surat kaleng begitu.</p>

	O : Sosialisasi WBS		O : Sosialisasi WBS		O : Sosialisasi WBS
1 : Bapak Andrianto Dwi P.	<p>P : Seperti apa sosialisasi mengenai WBS yang didapatkan?</p> <p>N : Kami mendapatkannya lewat itu tadi konten di desktop atau pengumpulan karyawan setelah jam kantor selesai untuk diberikan materi - materi mengenai fraud dan strategi anti fraud itu sendiri.</p>	2 : Bapak Daryoko	<p>P : Seperti apa sosialisasi mengenai WBS yang didapatkan?</p> <p>N : Mencakup jenis - jenis tindakan fraud atau bentuk perilaku dan aktivitas mencurigakan yang mengindikasikan fraud, dampak jika kita enggan melaporkan sehingga untuk para pegawai pasti akan berpikir 2 kali jika akan melakukan kecurangan.</p>	3 : Bapak Ivan Nugroho	<p>P : Seperti apa sosialisasi mengenai WBS yang didapatkan?</p> <p>N : Menyadarkan pentingnya melaporkan tindakan kecurangan yang ada di dalam organisasi. Dan dijelaskan juga dampak kerugian yang kita (pegawai) dapatkan atas kerugian perusahaan. Sama cara mengakses nya sih lewat intranet.</p>
5 : Bapak Pandu Kuncoro	<p>P : Seperti apa sosialisasi mengenai WBS yang didapatkan?</p> <p>N : Mulai dari intranet yang diakses, apa saja aduan yang bisa dilaporkan, dampak jika kita tidak melaporkan tindakan kecurangan di dalam organisasi.</p>	6 : Bapak Suwasono Adi Kurniawan	<p>P : Bagaimana cara menumbuhkan budaya untuk melaporkan tindakan fraud?</p> <p>Yang bisa membuka whistleblowing itu sementara ini tim SKAI. Kita sedang dalam proses mau merombak juga tampilannya agar terlihat lebih familiar karena kan sudah ada unit anti fraud.</p>	8 : Ibu Nur Aeni	<p>P : Kalau sosialisasi itu seminar atau bagaimana?</p> <p>N : Bukan, jadi dikumpulkan kayak pendidikan. Jadi dijelaskan WBS itu bagaimana, jika ada teman yang melakukan pelanggaran dan merasa tidak enak ya lewat WBS. Kan WBS lebih tidak diketahui yang melapor.</p> <p>P : Jadi WBS di sosialisasikan ke semua jajaran organisasi atau ke pimpinan saja?</p> <p>N : Tidak tidak, ke semua jajaran organisasi. Sosialisasi ini paling tiga bulan sekali.</p>

	P : Surprise Audit	Q : Surveillance System
6 : Bapak Suwasono Adi Kurniawan	<p>P : Bagaimana mekanisme penerapan strategi anti fraud pada kantor cabang?</p> <p>N : Kita setelah ada unit, kita kan selain SKAI yang di kantor pusat, juga ada namanya Kontrol Intern Cabang, ada 1 orang KIC dengan 1 staff, untuk kantor cabang besar seperti sleman, kita ada 2 orang staff, itu adalah tim SKAI kita yang ada di cabang. Di cabang dia bertanggung jawab langsung terhadap pemimpin SKAI.</p> <p>P : KIC melakukan tugasnya setiap kapan saja?</p> <p>Mulai dari verifikasi, kadang juga surprise audit untuk teller, diminta untuk langsung cek jumlah uang, karena dia auditor juga jadi bisa melakukan itu.</p> <p>Nah dari kantor cabang ada report berkala langsung ke sini (kantor pusat), kalau ada audit dari kantor pusat juga nanti dia (KIC) juga akan ikut tim kita.</p> <p>P : Apakah surprise audit dilakukan di semua kantor cabang?</p> <p>N : Ya, surprise audit dilakukan di semuanya tanpa pandang bulu, cuman kan tidak setiap saat dapat dilakukan,</p> <p>Nanti KIC bisa, unit anti fraud juga bisa. Tapi tidak semua melulu tentang uang. Bisa inventaris dicek kertas HVS atau alat tulis yang tersedia tinggal berapa, buku tabungan, surat berharga, materai.</p> <p>P : Seperti apa hambatan dalam melakukan surprise audit?</p> <p>N : Kalau kita hambatannya mungkin tidak dapat berlangsung secara maksimal, karena kan pasti orang - orang di kantor pusat yang dulu pernah jabat di kantor cabang itu kan masih berhubungan sama orang yang di kantor cabang, nah saat orang yang di kantor pusat itu tau kita mau audit mendadak begitu sudah dikabarin dulu ke temennya di cabang. Jadi ya terpaksa kadang kita bohong.</p>	<p>P : Siapakah pihak independen yang bertanggungjawab dalam surveillance system?</p> <p>N : Kalau di kita surveillance system itu tindakan melakukan audit secara diam - diam tanpa diketahui orangnya.</p> <p>jika ada laporan misal di kantor cabang sana jadi kita secara diam - diam ke kantor, dokumen - dokumennya kita minta melalui KIC, dan melalui mobile banking itu juga kita cek.</p> <p>surveillance system yang dilakukan untuk memantau kinerja nya SKAI itu sendiri. Pihak SKAI dinilai efektivitasnya. Yang memeriksa nanti pihak luar, bisa KAP bisa BPKP. Disamping itu 3 tahun sekali SKAI itu wajib di review oleh pihak ketiga. Kita terakhir itu tahun 2017 kemarin oleh BPKP, jadi kode etik kita ada yang dilanggar tidak, cara kerja kita sudah sesuai PBI nggak itu nanti di review. Mereka juga akan survei ke lapangan - lapangan mengenai kinerja auditor - auditor terkait. Misal bisa jadi ada laporan oh auditor yang itu tidak menguasai, kemarin mengaudit tanpa mengirim konfirmasi tiba - tiba dijadikan temuan padahal kejadiannya tidak seperti itu. Lapornya itu nanti langsung disampaikan ke OJK. Kita biasanya selama ini pakai BPKP, karena selain milik negara juga gratis.</p>

	R : Customer Awareness untuk mencegah eksternal fraud
6 : Bapak Suwasono Adi Kurniawan	<p>P : Bagaimana pelaksanaan customer awareness?</p> <p>N : Ini kita melakukannya hanya semacam sosialisasi dengan bantuan kantor cabang untuk sosialisasi ke instansi mana, nah itu kita selipkan materi tentang strategi anti fraud. Kita juga sudah mempersiapkan brosur, selain kita membuat brosur tentang produk kita, kita juga akan membuat brosur tentang pelaksanaan strategi anti fraud. Tapi ini masih dalam proses karena kan unit anti fraud masih baru. Dan nantinya kan tayangan tv yang ada di bawah yang langsung terlihat oleh customer biasanya hanya informasi tentang rate, nilai kurs dan produk kita, nantinya akan kita munculkan materi tentang strategi anti fraud.</p>
8 : Ibu Nur Aeni	<p>P : Kalau seperti itu kan merugikan nasabah dan menurunkan citra bank, itu nasabahnya diberikan sosialisasi tidak?</p> <p>N : Jadi sosialisasi itu tugasnya semua bank. Itu kalau di kita yang membuat divisi perencanaan sebelum tim fraud ada. Nanti akan mengundang nasabah - nasabah kita, nanti kita bentuk seperti gathering. Kita beri sosialisasi bahwa saat akan memakai ATM diperiksa dahulu ada skimmer tidak, dan pin itu hanya punya kita pribadi jangan dikasih orang lain. Itu ada PBI nya juga. Namanya orang juga kan gak semua bisa karena udah tua, cuman minta tolong orang waktu di ATM dan kebetulan dapat orang yang tidak baik. Jika ada laporan juga kita buka ni kapan transaksinya, jam berapa, di terminal mana, kan ada CCTV nya disetiap ATM kita buka. Nanti kita tunjukan ke nasabah, kenal tidak, ada itu kejadian ternyata anaknya sendiri. Ibu nya pernah tidak memberikan pin ke anaknya? Biasanya pernah karena minta diambilkan, mungkin karena usianya sudah lanjut dan tidak memungkinkan, atau diminta tolong ambilkan pensiunan. Kadang kan tergantung, kalo anaknya tidak baik atau diri kita yang lupa. Karena ada itu ternyata kesalahan nasabah sendiri.</p>

Sumber : Data Diolah dari NVivo11

LAMPIRAN 17

Framework Matrix Pengembangan SDM Unit Anti Fraud

	S : Jejak Rekam Pegawai Saat Pola Rekrutmen	T : Sertifikasi dan Pelatihan untuk Pegawai
<p>3 : laporan_tahunan_bpddiy_2016</p>	<p>Rekrutmen dan Seleksi Pegawai yang Efektif Bank BPD DIY melalui pengelola khusus SDM melakukan menjaringan SDM dengan selektif agar menciptakan sistem kerja yang kompetitif antara pegawai. Proses seleksi telah mempertimbangkan kebutuhan pegawai yang memiliki kualifikasi sesuai dengan core bisnis Perusahaan. Tahapan seleksi pegawai Bank BPD DIY menerapkan sistem gugur dengan rangkaian tes berikut: 1. Seleksi Administrasi 2. Wawancara 3. Kemampuan Tertulis 4. Tes Potensi Akademik 5. Psikotes 6. Tes Kesehatan</p> <p>Rencana Pengembangan SDM Tahun 2017 Pada tahun 2017 telah mempersiapkan beberapa strategi yang bertujuan untuk meningkatkan kapabilitas dan meningkatkan daya saing pegawai. Strategi tersebut adalah: 1. Meningkatkan kualitas sistem rekrutmen pegawai sehingga menghasilkan SDM yang unggul dan siap menghadapi dunia perbankan.</p>	<p>Pengembangan SDM Bank BPD DIY menyadari bahwa keberhasilan Bank BPD DIY untuk menghadapi seluruh tantangan usaha bergantung pada kualitas dan kapasitas SDM yang dimiliki. Upaya untuk memiliki SDM yang berkualitas dan profesional dilakukan oleh Manajemen Bank BPD DIY melalui berbagai program pendidikan dan pelatihan yang diselenggarakan secara in house maupun bekerjasama dengan lembaga lain. Sehingga diharapkan Bank BPD DIY mampu memiliki keunggulan bersaing. Bentuk pendidikan dan pelatihan yang telah dilaksanakan antara lain meliputi program pendidikan karir, pendidikan profesi, ketrampilan, serta berbagai kursus, latihan, penataran, seminar, lokakarya dan pelatihan manajemen dan teknis yang disesuaikan dengan kebutuhan. pengembangan program pelatihan dan pendidikan, serta pengembangan dan pemantauan nilai-nilai budaya kerja Bank berdasarkan ketentuan-ketentuan dan praktikpraktik pengelolaan SDM yang terbaik.</p> <p>Program Pengembangan Kompetensi Pegawai Program pengembangan kompetensi bagi pegawai difasilitasi oleh Bank BPD DIY yaitu melalui program pendidikan dan pelatihan yang diselenggarakan melalui in house training maupun bekerja sama dengan pihak ketiga. Bentuk pendidikan yang telah diikuti oleh pegawai Bank BPD DIY antara lain dalam bentuk workshop, sosialisasi, lokakarya dan seminar. Menyelenggarakan pendidikan dan pelatihan terutama pelatihan produk-produk valas, layanan internet banking dan aktivitas bisnis lainnya yang dapat dilakukan oleh Bank kategori Buku 2. Meningkatkan pengetahuan dan wawasan pegawai</p> <p>Sebagai upaya peningkatan kompetensi para auditor, melalui koordinasi dengan Divisi SDM dan Umum, dalam tahun 2016 seluruh auditor telah diikutsertakan dalam berbagai kegiatan dan pelatihan serta beberapa seminar. Adapun auditor SKAI yang telah melakukan sertifikasi auditor internal sebanyak 13 orang.</p>

	S : Jejak Rekam Pegawai Saat Pola Rekrutmen		S : Jejak Rekam Pegawai Saat Pola Rekrutmen
6 : Bapak Suwasono Adi Kurniawan	<p>P : Bagaimana proses know your employee dilakukan sejak perekrutan pegawai?</p> <p>N : Sudah berlangsung tapi di kita adalah hal baru, karena kita unit baru. PBI nomer berapa saya lupa tapi kita sudah melaksanakannya, di SDM. Di Anti Fraud kita sudah melaksanakan tapi tidak sebesar di SDM. Semua dilaksanakan mulai dari proses perekrutan sampai sudah jadi pegawai. Kalau saat perekrutan kita mengawasi, kan wewenangnya SDM. Harus diumumkan di koran, kalau tidak kan nanti bisa jadi hanya orang - orang tertentu saja yang akses. Kalau seperti itu nanti ya kita sempit.</p>	8 : Ibu Nur Aeni	<p>P : Kalau perekrutan SDM itu bagian yang merekrut ada kualifikasi bahwa SDM nya kompeten?</p> <p>N : Kita ada, standar itu ada. Kita bisa buka informasi debitur, dari OJK namanya indeb (identitas debitur). Kalau kita mau merekrut itu nanti kita ambilkan indeb. Misal ternyata dia ini punya kredit macet di bank lain, kenapa bisa macet? Apa karena ngemplang atau tidak punya i'tikad yang baik, kemudian kita minta SKCK, tidak menggunakan narkoba. Kalau masalah kompeten pendidikan kita kan kerjasama sama UGM untuk rekrutmen.</p> <p>P : Kalau rekrut pegawai ada syarat harus sertifikasi tidak bu?</p> <p>N : Ooh tidak ada.. Tapi kalau dia udah punya sendiri tidak masalah.</p>

	T : Kebijakan Cuti Pegawai		T : Kebijakan Cuti Pegawai		T : Kebijakan Cuti Pegawai
2 : Bapak Daryoko	<p>P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?</p> <p>N : Tidak bisa kalau itu.</p>	3 : Bapak Ivan Nugroho	<p>P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari?</p> <p>N : Tidak pasti kalau itu, tapi untuk saat ini ada yang ambil satu dua hari, ada juga yang kolektif.</p> <p>P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?</p> <p>N : Tidak bisa.</p>	8 : Ibu Nur Aeni	<p>Lalu untuk mitigasi karyawan tidak berbuat fraud itu dibuat namanya cuti. Cuti itu harus di ambil. Pada saat dia cuti kan digantikan sama teman lain yang satu unit. Bisa jadi kan dia (temennya) menemukan.</p> <p>P : Untuk jatah cuti itu bagaimana sistemnya bu?</p> <p>N : Satu tahun 12 hari, boleh diambil kapan saja dan wajib diambil. Biasanya pegawai hanya ambil satu dua hari, kalau seperti itu susah digantikan pegawai lain, karena kan jika digantikan teman dan waktunya cukup lama, kemungkinan ditemukan hal yang tidak wajar jad lebih besar.</p> <p>P : Kalau jatah cuti tidak diambil boleh diganti gaji?</p> <p>N : Nggak boleh.</p>
4 : Bapak Muhammad Agus Salam S.	<p>P : Apakah bapak biasanya mengambil semua jatah cuti?</p> <p>N : Tidak semua kadang, biasanya satu atau dua hari. Kalau berhari - hari ya nunggu momen liburan.</p> <p>P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?</p> <p>N : Selama ini sih tidak bisa.</p>	5 : Bapak Pandu Kuncoro	<p>P : Bisakah jatah cuti yang tidak diambil digantikan dengan gaji?</p> <p>N : Tidak bisa mba. Jadi memang harus kita ambil semua.</p> <p>P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari?</p> <p>N : Itu tergantung keadaan kita, kalau mau diambil kolektif saat momen - momen libur panjang diluar cuti bersama biasanya jatah cuti diambil.</p>		

	U : Pengelolaan Teknologi Informasi untuk Mengendalikan Fraud	U : Pengelolaan Teknologi Informasi untuk Mengendalikan Fraud
<p>6 : Bapak Suwasono Adi Kurniawan</p>	<p>Pengamanannya ada tim IT kita yang ruangnya ada di lantai 4 situ, kita juga ada server di lantai 5 ini, cadangan server kita juga ada di Cabang Wates. Jadi kalau semisal ada bencana disini ambruk kita masih tetap bisa berjalan karena ada cadangan di tempat lain.</p> <p>Penyempurnaan Mobile Banking semua tadi membuka kemungkinan kita bekerjasama dengan pihak ketiga, tapi dipertimbangkan lagi biaya yang dikeluarkan dengan biaya yang diselamatkan itu sebanding tidak.</p> <p>P : Bagaimana pengamanan teknologi yang ada di BPD DIY? N : Pengamanan teknologi kita dikembangkan oleh tim IT kita, seperti flashdisk saja tidak bisa diakses jika masuk ke laptop atau komputer. Wifi umum tidak bisa walaupun internet juga kita disediakan layanan proxy dan itu pun terbatas. Kalau dikantor hotspot disediakan di setiap ruangan.</p>	<p>P : Kalau seperti phising, skimming atau pengambilan data nasabah oleh orang luar itu ada tidak? N : Ada, baru saja terjadi, semua bank kena. Itu skimmer nya dipasang di ATM. Nah pengendalian internal yang kita lakukan pada ATM kita itu pada saat kita rutin melihat di mulut ATM. Jadi kalau kamu punya kartu ATM, sebelumnya kalau di mulut ATM ada yang mencurigakan itu jangan kamu masukkan. Jadi ATM kan bisa dilakukan lintas bank, seperti ATM Bersama, nah makannya kena di ATM lain karena terpasang skimmer. Karena itu pengendalian internal itu di kita, setiap hari mulut ATM kita periksa.</p> <p>P : Jadi di BPD ini setiap hari dicek oleh siapa bu? N : Iya, itu dilakukan di bagian pelayanan. Kan ATM kita kebanyakan di kantor kita. Jadi bukan di mall, ya pokoknya yang jauh dari kantor bank. Yang sering terpasang justru ATM - ATM yang jauh, atau tertutup. Kan kalau di mall terbuka, terkadang kalau mau pasang bisa terlihat. Biasanya ATM - ATM yang dikotak - kotaki cuma ada satu.</p> <p>Kita beri sosialisasi bahwa saat akan memakai ATM diperiksa dahulu ada skimmer tidak, dan pin itu hanya punya kita pribadi jangan dikasih orang lain. Itu ada PBI nya juga. Namanya orang juga kan gak semua bisa karena udah tua, cuman minta tolong orang waktu di ATM dan kebetulan dapat orang yang tidak baik. Jika ada laporan juga kita buka ni kapan transaksinya, jam berapa, di terminal mana, kan ada CCTV nya disetiap ATM kita buka. Nanti kita tunjukkan ke nasabah, kenal tidak, ada itu kejadian ternyata anaknya sendiri.</p>

	V : Pengembangan WBS		V : Pengembangan WBS
2 : Bapak Daryoko	<p>P : Apakah ada keluhan dan saran tentang pelaksanaan strategi anti fraud sebelum Unit Anti fraud dibentuk?</p> <p>N : Sejauh ini menurut saya cukup baik ya, karena sebelumnya kan SKAI, mereka sudah cukup kompeten dalam melaksanakan whistleblowing system nya. Tapi mungkin perlu dilakukan namanya reward untuk pegawai yang aktif melaporkan ke WBS, jadi semua lebih aktif.</p>	6 : Bapak Suwasono Adi Kurniawan	<p>Yang bisa membuka whistleblowing itu sementara ini tim SKAI. Kita sedang dalam proses mau merombak juga tampilannya agar terlihat lebih familiar karena kan sudah ada unit anti fraud.</p> <p>Jadi dikita whistleblowing system itu ada, sedang dalam proses penyempurnaan oleh kita. Jadi namanya tadi itukan WBS atau whistleblowing system, besok rencananya kita buat "Surat kepada Direktur Utama" , jadi kita buat tidak menakutkan. Sekarang hanya bisa diakses dengan komputer melalui intranet, besok kita coba dapat diakses melalui gadget. Karena kalau yang di mobile itu kan kita punya BPD DIY Mobile untuk transaksi, yang khusus karyawan kita itu ada BPD DIY Smart itu isinya katalog produk kita. Jadi untuk yang kita tidak tahu langkah - langkahnya dengan produk begitu bisa buka lewat situ, jadi seperti smart kit nya BPD DIY.</p> <p>Tapi kan kalau di bank tidak sama dengan perusahaan lainnya yang produksi bisa langsung di launch, kalau kita harus izin dulu dan sebagainya untuk bisa launch, tapi memang untuk izin sudah bisa semua tinggal launch. Jadi mungkin kedepan BPD DIY Smart itu bisa juga untuk layanan pengaduan. Fungsinya ya semisal ada orang melihat pegawai BPD misalnya masuk ke tempat yang tidak senonoh, nah itu nanti bisa langsung dilaporkan. Misal itu hari sabtu gitu jadi tidak usah menunggu senin keburu lupa, atau malah senin ketemu orang nya terus ditraktir gitu jadi nggak jadi ngelaporkan, jangan sampe, jadi bisa langsung saat itu juga melaporkannya.</p> <p>Jadi terasa terhadap pelaporan whistleblowing system nya, walaupun saya baru melihat setelah saya disini dan juga saya tidak punya akses, tapi saya diberi laporannya, itu partisipasi pelaporannya masih rendah. Apakah benar rendah itu karena tidak ada yang dilaporkan atau karena tidak berani bahkan tidak enak saja. Kita sedang susur penyebabnya. Dan pak Direktur Utama sudah minta dibahas oleh kita. Kita sudah menyampaikan ke Direktur Utama untuk judul whistleblowing system itu kita ganti menjadi Surat Kepada Direktur Utama, lalu jaringan intranetnya diubah tadinya "wbs" menjadi "skdu". Dan untuk pelaporan melalui sms maupun Whatsapp masih perlu dikaji lagi, untuk penanggung jawabnya siapa.</p>
3 : Bapak Ivan Nugroho	<p>Dan WBS mungkin bisa dibuat lebih menarik untuk menarik para pegawai lebih aktif dalam melaporkan setiap tindakan yang mengindikasikan fraud.</p>		
5 : Bapak Pandu Kuncoro	<p>P : Apakah ada keluhan tentang pelaksanaan strategi anti fraud sebelum Unit Anti fraud dibentuk?</p> <p>N : Keluhan sebenarnya tidak ada, karena kita juga zero fraud selama beberapa tahun ini. Mungkin Whistleblowing system nya bisa dilakukan perubahan sehingga pegawai akan lebih berpartisipasi.</p>		

W : Sertifikasi dan Pelatihan untuk Pegawai	
6 : Bapak Suwasono Adi Kurniawan	<p>P : Bagaimana program pendidikan karir, profesi, ketrampilan, pelatihan dan seminar yang diadakan manajemen dalam pengembangan SDM Unit Anti Fraud?</p> <p>N : Walaupun ini unit baru, kita ikut pelatihan ada 2 yang jadi rujukan kita, Lembaga Pengembangan Anti Fraud (LPAF). Itu lembaga yang ditunjuk untuk mengadakan pelatihan, dan pelatihan itu terintegrasi dengan ACFE. Jadi lembaga itu yang membantu nanti untuk ujian. Itu untuk internasional. Kalau yang nasional itu ada CRFA, Certified Forensic Audit. Itu nanti semua wajib ikut yang baru maupun pegawai baru, karena ada dalam Peraturan BI bahwa 5% dari biaya tenaga kerja itu adalah wajib untuk pendidikan. Jadi di kita itu pegawai minimal 2 kali mengikuti pendidikan. Itu semua dibiayai bank. Pendaftaran, transportasi, uang saku dan hotel dibiayai kita. Jadi untuk Anti Fraud itu terprogram, karena kan arahnya sertifikasi. Ini ada contohnya (memegang brosur) lembaga LPAF, ini lembaga bimbingan persiapan ujian CFE, biaya bimbingan per bulan 10 juta, untuk sertifikasi nya USD1150. Selain itu kita juga sertifikasi internal audit bank. Tanggal 15 besok kita juga akan ada refreshment karena sertifikat akan hangus bulan maret ini, hnya berlaku 3 tahun. Dan kalau untuk sertifikasi Anti Fraud kita berdua sendiri memang belum tapi memang menuju ke arah sana. Karena kan kemarin SKAI yang sertifikasi internal audit yang sudah. Sebenarnya sama saja, tetapi kalau sudah sertifikasi Anti Fraud itu bedanya kita sudah bisa menjadi saksi ahli di pengadilan nanti dan ini diakui di luar negri. Kalau sertifikasi yang ini modelnya seperti pemeliharaan, jadi harus mengikuti workshop nya. Kemarin konfrensi internasional nya ada di jogja.</p> <p>P : Saya lihat dilaporan tahunan ada pendidikan yang rutin diikuti pegawai itu bagaimana mekanisme nya?</p> <p>N : Nah contohnya ini (menunjukkan surat usulan mengikuti pendidikan), kita mengajukan 10 orang untuk gelombang 1. Ini tentang fraud kebetulan tema nya: Definisi dan disiplin fraud Pengumpulan bukti dan pelaksanaan audit investigasi Pengumpulan dan evaluasi bukti keuangan Audit investigasi dan kasus produk dana Audit investigasi dan kasus produk kredit Psikologi dan kesiapan mental audit Teknik interview Pelaporan Dirinci biaya nya sekian, peserta mengikuti selama 2 hari di Bandung. Ada 2 gelombang, yang gelombang 1 itu KIC agar mereka juga paham semua tentang fraud, gelombang 2 termasuk saya, sebenarnya saya sudah beberapa kali ikut, tapi karena ini tujuannya untuk refreshment jadi mau gak mau harus ikut. Di awal tahun juga setiap divisi wajib membuat training list analyst. Jadi setahun kedepan itu mau pelatihan di bidang apa saja dan diberikan ke SDM. SDM akan mengolah, nah saat ada penawaran ke SDM dan sesuai dengan apa yang diminta divisi kemarin maka mulai dari kontak dinas, tiket pesawat akan dilakukan oleh bagian SDM. Ini juga merupakan salah satu tindakan pencegahan fraud, dan boarding pass nya juga harus kembali jadi tidak bisa di refund. Hotel juga biaya berapa pun jika memang pendidikan diadakan di hotel itu maka diusahakan menginap juga disitu.</p>

Sumber : Data Diolah dari NVivo11

LAMPIRAN 18

Framework Matrix Kendala yang Dihadapi oleh Unit Anti Fraud

4 : Penerapan MR dalam penggunaan TI	<p style="text-align: center;">U : TI WBS Belum Independen</p> <ol style="list-style-type: none"> 1. Penggunaan Teknologi Informasi diperlukan Bank dalam rangka meningkatkan efektivitas dan efisiensi dalam kegiatan operasional Bank. Selain itu perkembangan Teknologi Informasi memungkinkan Bank untuk meningkatkan pelayanan kepada nasabah melalui produk-produk Electronic Banking. 2. Dalam hal Bank tidak dapat menyelenggarakan sendiri Teknologi Informasi tersebut, Bank dimungkinkan untuk menggunakan pihak penyedia jasa Teknologi Informasi.
--------------------------------------	--

	X : Jumlah SDM Unit Anti Fraud yang Kurang Mencukupi dan Belum Kompeten		X : Jumlah SDM Unit Anti Fraud yang Kurang Mencukupi dan Belum Kompeten		Y : Sedikitnya Pelaporan ke WBS		Y : Sedikitnya Pelaporan ke WBS
1 : Bapak Andrianto Dwi P.	<p>P : Adakah saran yang perlu dilakukan Unit Anti Fraud kedepannya dalam melaksanakan strategi anti fraud?</p> <p>N : Mungkin agar masing - masing strategi anti fraud dalam terlaksana secara maksimal, diperlukan SDM yang lebih banyak dari yang ada sekarang, sehingga setiap orang memiliki tanggungjawab di masing - masing strategi.</p>	4 : Bapak Muhammad Agus Salam S.	<p>P : Adakah saran yang perlu dilakukan Unit Anti Fraud kedepannya dalam melaksanakan strategi anti fraud?</p> <p>N : Kalau setahu saya di Unit Anti Fraud hanya terdiri dari 2 orang ya, mungkin bisa ditambah personilnya. Bisa dicari yang memiliki dasar - dasar kualifikasi yang kompeten saat rekrutmen jadi segera bisa membantu kedua personil yang sekarang.</p>	3 : Bapak Ivan Nugroho	<p>P : Apakah sudah pernah melaporkan indikasi fraud ke WBS? Mudah atau ribet dalam mengaksesnya?</p> <p>N : Sejauh ini belum. Mudah kok mbak, hanya saja kami melaporkan hanya untuk indikasi fraud yang benar - benar signifikan saja</p>	7 : Bapak Zukhroni Ariffin	<p>P : Bagaimana hambatan yang dirasakan dalam pelaksanaan strategi anti fraud?</p> <p>N : Jadi kalau kita menemukan fraud di salah satu cabang, itu akan berpengaruh di penilaian cabang. Sehingga itu yang menyebabkan terkadang cabang itu menyelesaikan masalah itu lama memberi laporan ke kita (Unit Anti Fraud), kan disana kita juga ada KIC, jadi sudah ditangani mereka. Jadi terkadang kalau kita meminta laporan ya agak lama, karena itu tadi, berpengaruh ke score masing - masing cabang itu.</p>
6 : Bapak Suwasono Adi Kurniawan	<p>Jadi baru tahun kemarin ada unit khusus, unit anti fraud namanya. Secara organisasi berada dibawah Satuan Kerja Audit Internal. Dengan personilnya ada 2, saya dan mas Zukhron tadi, dan saya yang jadi pemimpin unit anti fraud nya, dan mas Zukhron sebagai staff.</p>	8 : Ibu Nur Aeni	<p>P : Apakah untuk Unit Anti Fraud sudah semua bersertifikasi?</p> <p>N : Setahu saya karena mereka baru dan hanya terdiri dari dua orang, mereka untuk sertifikasi khusus belum ada, hanya baru sertifikasi untuk internal audit.</p> <p>P : Kalau rekrut pegawai ada syarat harus sertifikasi tidak bu?</p> <p>N : Ooh tidak ada.. Tapi kalau dia udah punya sendiri tidak masalah.</p>				

	Z : Surprise Audit yang Kurang Efisien		Z : Surprise Audit yang Kurang Efisien		AA : Susahnya Ditemukan Indikasi Fraud saat Pegawai Cuti		AA : Susahnya Ditemukan Indikasi Fraud saat Pegawai Cuti		AA : Susahnya Ditemukan Indikasi Fraud saat Pegawai Cuti
7 : Bapak Zuhroni Ariffin	<p>P : Bagaimana hambatan yang dirasakan dalam pelaksanaan surprise audit?</p> <p>N : Kebetulan di kantor cabang itu ada kepanjangan tangan kami namanya KIC. Nah jika kita akan ke kantor cabang, otomatis kita itu akan meminjam kendaraan yang otomatis dari divisi lain, sehingga kami harus konfirmasi ke Divisi Umum mau pinjam kendaraan misal ke Wates. Tapi kalau kami ditanyai buat apa kesana ya kami tidak bisa menutupi itu. Jadi kalau dari Divisi Umum kebetulan dekat dengan orang di cabang lain pasti nanti akan telfon dan memberitahukan kalau kita akan kesana, ya gak jadi surprise audit. Tapi untuk mengatasi itu semua ya mau tidak mau kami berbohong. Dan jika memang harus sesuai prosedur ya pasti akan bocor.</p>	8 : Ibu Nur Aeni	<p>P : Apakah pernah dilakukan surprise audit oleh Unit Anti Fraud?</p> <p>N : Pernah mbak. Tapi karena dulu strategi anti fraud masih SKAI yang menjalankan jadi dilakukan sekalian dengan audit umum. Tapi kalau sekarang mereka biasanya jika akan surprise audit ke cabang gitu ya susahny saat informasi bocor, jadi pihak cabang kayak misal Wates, itu sudah siap - siap dahulu.</p>	2 : Bapak Daryoko	<p>P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari?</p> <p>N : Sesuai individunya mbak. Tapi akan lebih baik secara kolektif, karena disaat pegawai itu cuti dan digantikan pegawai lain, maka kemungkinan kecurangan yang dilakukan pegawai yang cuti tersebut bisa lebih besar.</p>	6 : Bapak Suwasono Adi Kurniawan	<p>Nah tapi setelah ada unit baru ini, itu nggak masuk potongan, dan sudah berlaku sejak tahun kemarin bahwa cuti tetap utuh tanpa dipotong cuti bersama dan kita mewajibkan setelah ada unit itu cuti itu wajib diambil yang secara berurutan ada minimal 3 hari.</p>	8 : Ibu Nur Aeni	<p>Biasanya pegawai hanya ambil satu dua hari, kalau seperti itu susah digantikan pegawai lain, karena kan jika digantikan teman dan waktunya cukup lama, kemungkinan ditemukan hal yang tidak wajar jad lebih besar.</p>

	AB : TI WBS Belum Independen		AB : TI WBS Belum Independen		AC : Belum adanya Rekrutmen dan Sertifikasi untuk Unit Anti Fraud
6 : Bapak Suwasono Adi Kurniawan	<p>Karena beberapa perusahaan itu WBS dikelola oleh pihak ketiga. Tahu kan misalnya E&Y, Deloitte itu mereka menyediakan jasa itu, jadi laporan yang masuk ke web mereka. Mereka sudah membuat web misalnya uii.whistleblowingsystem, nanti laporan yang masuk ke mereka dibaca ini layak atau tidak, memenuhi syarat atau tidak, di verifikasi OK, lalu UII cuma dapetnya ini ada pelanggaran di fakultas mana silahkan tindak lanjuti, tidak tahu pelapornya siapa, jadi kerahasiaan lebih terjamin. Sehingga karyawan itu percaya laporan yang masuk. PERTAMINA itu pakai ini. Jadi KAP itu bukan sekedar memberikan opini wajar tidak wajar saja, ada whistleblowing, investigasi jadi kayak detektif swasta gitu. Nanti sekiranya ada kecurangan di bagian pengadaan gitu ya diturunkan tim forensik, alatnya lengkap karena kan standarnya amerika jadi bisa diungkap.</p> <p>P : Bagaimana pengamanan yang tersedia pada portal pengaduan whistleblowing system untuk melindungi whistleblower?</p> <p>N : Di kita whistleblowing system membangun sendiri ya, jadi tidak ambil dari luar. Kalo di bank lain kan dari vendor. Jadi di BPD DIY ini kita punya tim sendiri yang membangun, jadi memang kelemahannya mungkin tim - tim IT bisa membuka.</p>	8 : Ibu Nur Aeni	<p>P : Siapa yang membuat WBS?</p> <p>N : WBS itu dibuat oleh TI kita, tapi untuk pengelolaannya dilakukan SKAI yang sekarang ada Unit Anti Fraud.</p>	4 : Bapak Muhammad Agus Salam S.	<p>P : Adakah saran yang perlu dilakukan Unit Anti Fraud kedepannya dalam melaksanakan strategi anti fraud?</p> <p>N : Kalau setahu saya di Unit Anti Fraud hanya terdiri dari 2 orang ya, mungkin bisa ditambah personilnya. Bisa dicari yang memiliki dasar - dasar kualifikasi yang kompeten saat rekrutmen jadi segera bisa membantu kedua personil yang sekarang.</p>

	AC : Belum adanya Rekrutmen dan Sertifikasi untuk Unit Anti Fraud		AC : Belum adanya Rekrutmen dan Sertifikasi untuk Unit Anti Fraud		AD : Bocornya Rahasia karena Antar Cabang Saling Kenal
5 : Bapak Pandu Kuncoro	<p>P : Adakah saran yang perlu dilakukan Unit Anti Fraud kedepannya dalam melaksanakan strategi anti fraud?</p> <p>N : Selain WBS juga bisa menambah tingkat kualitas Unit Anti Fraud melalui sertifikasi atau pelatihan - pelatihan.</p>	6 : Bapak Suwasono Adi Kurniawan	<p>P : Apakah Unit Anti Fraud akan ditambah lagi personilnya?</p> <p>N : Rencana untuk kesitu belum ada, tapi mungkin akan segera kami lakukan. Karena kan ini unit nya baru terbentuk juga.</p> <p>Dan kalau untuk sertifikasi Anti Fraud kita berdua sendiri memang belum tapi memang menuju ke arah sana. Karena kan kemarin SKAI yang sertifikasi internal audit yang sudah. Sebenarnya sama saja, tetapi kalau sudah sertifikasi Anti Fraud itu bedanya kita sudah bisa menjadi saksi ahli di pengadilan nanti dan ini diakui di luar negri.</p>	6 : Bapak Suwasono Adi Kurniawan	<p>P : Seperti apa hambatan dalam melakukan surprise audit?</p> <p>N : Kalau kita hambatannya mungkin tidak dapat berlangsung secara maksimal, karena kan pasti orang - orang di kantor pusat yang dulu pernah jabat di kantor cabang itu kan masih berhubungan sama orang yang di kantor cabang, nah saat orang yang di kantor pusat itu tau kita mau audit mendadak begitu sudah dikabarin dulu ke temennya di cabang. Jadi ya terpaksa kadang kita bohong.</p> <p>P : Bagaimana hambatan yang dihadapi Tim Anti Fraud?</p> <p>N : Perusahaan BPD DIY itu kan tidak besar, jadi kita itu kan saling kenal. Beda sama perusahaan nasional, tim audit datang takut semua tidak ada yang kenal. Karena ini perusahaannya lokal jadi harus mengesampingkan rasa tidak enak, bisa jadi karena tetangga atau teman dari kecil. Kalau perusahaan di Jakarta itu kan rekrutmen ya langsung di posisikan di audit, kalau contohnya seperti saya begitu kan sempat di cabang dulu. Otomatis banyak kenal dan kedekatan dengan pegawai lain itu ada, apalagi ini semua wilayah di Jogja. Dan seperti itu sebenarnya kendala</p>
7 : Bapak Zukhroni Ariffin	<p>P : Untuk Unit Anti Fraud sendiri sudah merencanakan apa pak untuk dilakukan rencana pelatihan atau sertifikasi?</p> <p>N : Kalau untuk auditor sendiri ada syarat mengikuti sertifikasi auditor level 1 dan 2 untuk syarat supervisor. Kalau yang level 1 sebagian sudah dan sebagian belum. Kami juga sedang usulkan ke pimpinan untuk bisa mendapatkan sertifikasi yang oleh ACFE.</p>	8 : Ibu Nur Aeni	<p>P : Apakah untuk Unit Anti Fraud sudah semua bersertifikasi?</p> <p>N : Setahu saya karena mereka baru dan hanya terdiri dari dua orang, mereka untuk sertifikasi khusus belum ada, hanya baru sertifikasi untuk internal audit.</p>	7 : Bapak Zukhroni Ariffin	<p>P : Bagaimana hambatan yang dirasakan dalam pelaksanaan surprise audit?</p> <p>N : Kebetulan di kantor cabang itu ada kepanjangan tangan kami namanya KIC. Nah jika kita akan ke kantor cabang, otomatis kita itu akan meminjam kendaraan yang otomatis dari divisi lain, sehingga kami harus konfirmasi ke Divisi Umum mau pinjam kendaraan misal ke Wates. Tapi kalau kami ditanyai buat apa kesana ya kami tidak bisa menutupi itu. Jadi kalau dari Divisi Umum kebetulan dekat dengan orang di cabang lain pasti nanti akan telfon dan memberitahukan kalau kita akan kesana, ya gak jadi surprise audit. Tapi untuk mengatasi itu semua ya mau tidak mau kami berbohong. Dan jika memang harus sesuai prosedur ya pasti akan bocor.</p>

	AE : Jatah Cuti Pegawai yang Tidak Diambil Secara Kolektif		AE : Jatah Cuti Pegawai yang Tidak Diambil Secara Kolektif		AE : Jatah Cuti Pegawai yang Tidak Diambil Secara Kolektif		AF : Kurangnya Kesadaran Melapor Semua Indikasi Kecurangan
1 : Bapak Andrianto Dwi P.	P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari? N : Lebih sering mengambil harian mbak. Kalau untuk kolektif juga bisa dan diambil di momen - momen libur panjang.	3 : Bapak Ivan Nugroho	P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari? N : Tidak pasti kalau itu, tapi untuk saat ini ada yang ambil satu dua hari, ada juga yang kolektif.	6 : Bapak Suwasono Adi Kurniawan	Ini yang belum terlaksana, jadi jujur saja ya, karena ini di kita itu sangat sibuk, cuti itu tidak semua diambil jadi sisa. Kita ini jatahnya 12 hari, tapi dulu itu dipotong cuti bersama 4 hari seperti natal, tahun baru, lebaran jadi sisa 8 hari. Nah tapi setelah ada unit baru ini, itu nggak masuk potongan, dan sudah berlaku sejak tahun kemarin bahwa cuti tetap utuh tanpa dipotong cuti bersama	1 : Bapak Andrianto Dwi P.	P : Apakah sudah pernah melaporkan indikasi fraud ke WBS? Mudah atau ribet dalam mengaksesnya? N : Belum. Sebenarnya mudah, tetapi selama ini saya nggak menemukan hal - hal yang mengarah ke kecurangan dan merugikan ke organisasi secara signifikan. P: Apa saja hambatan yang dirasakan dalam melaporkan indikasi kecurangan? N : Kadang kalau kita merasa beberapa indikasi fraud itu tidak merugikan maka kita memilih tidak melaporkannya ke WBS.
4 : Bapak Muhammad Agus Salam S.	P : Apakah bapak biasanya mengambil semua jatah cuti? N : Tidak semua kadang, biasanya satu atau dua hari. Kalau berhari - hari ya nunggu momen liburan.	5 : Bapak Pandu Kuncoro	P : Dalam pemakaian jatah cuti apakah hanya satu hari atau kolektif beberapa hari? N : Itu tergantung keadaan kita, kalau mau diambil kolektif saat momen - momen libur panjang diluar cuti bersama biasanya jatah cuti diambil.				

	AF : Kurangnya Kesadaran Melapor Semua Indikasi Kecurangan		AF : Kurangnya Kesadaran Melapor Semua Indikasi Kecurangan		AG : Penyedia WBS dibuat oleh Divisi TI Perusahaan Sendiri
3 : Bapak Ivan Nugroho	<p>P : Apakah sudah pernah melaporkan indikasi fraud ke WBS? Mudah atau ribet dalam mengaksesnya?</p> <p>N : Sejauh ini belum. Mudah kok mbak, hanya saja kami melaporkan hanya untuk indikasi fraud yang benar - benar signifikan saja.</p>	7 : Bapak Zukhroni Ariffin	<p>P : Bagaimana hambatan yang dirasakan dalam pelaksanaan strategi anti fraud?</p> <p>N : Jadi kalau kita menemukan fraud di salah satu cabang, itu akan berpengaruh di penilaian cabang. Sehingga itu yang menyebabkan terkadang cabang itu menyelesaikan masalah itu lama memberi laporan ke kita (Unit Anti Fraud), kan disana kita juga ada KIC, jadi sudah ditangani mereka. Jadi terkadang kalau kita meminta laporan ya agak lama, karena itu tadi, berpengaruh ke score masing - masing cabang itu. Jadi ya prinsipnya waktunya saja yang lama untuk melaporkan ke kita.</p>	6 : Bapak Suwasono Adi Kurniawan	<p>P : Bagaimana pengamanan yang tersedia pada portal pengaduan whistleblowing system untuk melindungi whistleblower?</p> <p>N : Di kita whistleblowing system membangun sendiri ya, jadi tidak ambil dari luar. Kalo di bank lain kan dari vendor. Jadi di BPD DIY ini kita punya tim sendiri yang membangun, jadi memang kelemahannya mungkin tim - tim IT bisa membuka.</p>
5 : Bapak Pandu Kuncoro	<p>P : Apakah ada keluhan tentang pelaksanaan strategi anti fraud sebelum Unit Anti fraud dibentuk?</p> <p>N : Keluhan sebenarnya tidak ada, karena kita juga zero fraud selama beberapa tahun ini. Mungkin Whistleblowing system nya bisa dilakukan perubahan sehingga pegawai akan lebih berpartisipasi.</p> <p>P : Biasanya kecurangan apa saja yang perlu dilaporkan melalui WBS?</p> <p>N : Sebenarnya itu sudah terjawab dari sosialisasi yang diadakan pak suwasono ya.. Ya kesadaran kita melaporkan hal - hal yang memang mengarah penting untuk ditindaklanjuti, tidak hanya berupa keluhan.</p>			8 : Ibu Nur Aeni	<p>P : Siapa yang membuat WBS?</p> <p>N : WBS itu dibuat oleh TI kita, tapi untuk pengelolaannya dilakukan SKAI yang sekarang ada Unit Anti Fraud.</p>

Sumber : Data Diolah dari NVivo11

LAMPIRAN 19

Framework Matrix Peningkatan yang Dilakukan Unit Anti Fraud

	AV : Audit Teknologi Informasi dan Peningkatan Keamanan		AV : Audit Teknologi Informasi dan Peningkatan Keamanan
2 : D. Mangala, P. Kumari	<p>Firewall and Password Protection</p> <p>Firewall acts as an intermediate between organisational internal network and less secured external network. Firewall is an effective mechanism to protect our system from network interference. It controls traffic between two or more network for security purpose. It keeps corporate system safe from hackers. Bierstaker et al. (2006) found firewall and password protection as mostly used and most effective method to prevent fraud. On the same track, Rahman & Anwar (2014) claimed protection software as most effective category including password and firewall as most efficient techniques.</p>	6 : S. Siregar, B. Tenoyo	<p>This finding indicates that although many companies have implement IT audit, only few have realize the contribution of IT audit for preventing and detecting fraud. We believe this finding suggest that companies have not used IT audit extensively and optimally to discover fraud.</p> <p>Companies in financial industry may need to have better fraud risk management processes than other industry. Companies need to choose and implement one or several tools to detect or prevent fraud, including perform IT audit.</p>

	AW : Diadakan Gathering yang mengurangi Jatah Cuti Bersama dan Melakukan Rotasi Mingguan antar Karyawan		AW : Diadakan Gathering yang mengurangi Jatah Cuti Bersama dan Melakukan Rotasi Mingguan antar Karyawan		AW : Diadakan Gathering yang mengurangi Jatah Cuti Bersama dan Melakukan Rotasi Mingguan antar Karyawan
6 : S. Siregar, B. Tenoyo	Each employees has to attend a presentation of business ethics and anti-corruption every year and sign a statement of acceptance of the understanding of those presentation and if in the future there is a violation of that acceptance, company has the right to terminate the employee without any further notice. Rotation of key account employees.	7 : S. Suhartono	i. Peningkatan manajemen SDM yang berkualitas.	9 : Y. Ermawati	Dari sudut sistem know your employee, Bank X sudah memiliki sistem dan prosedur yang baik untuk perekrutan pegawai dan monitoring. Bank X juga menanamkan Core Competency untuk menguatkan keprofesionalan dan tanggungjawab pegawainya, namun untuk lebih mengenal jauh bagaimana pegawainya Bank X belum memiliki program khusus. Dari sudut ini Bank X dapat menggunakan alternatif program seperti family gathering yang dikemas khusus dengan sarana outbond untuk melihat bagaimana karakter pegawai dan keluarganya. Atau dengan strategi Manajemen Konflik untuk melihat bagaimana cara kerja pegawai Bank X dalam menyelesaikan suatu permasalahan dan kesempatan.

AX : Dilakukan Training yang Diadakan oleh Badan Sertifikasi dan Merekrut Pegawai yang Bersertifikasi Akuntan Forensik	
2 : D. Mangala, P. Kumari	Forensic Accounting Nowadays continuously increasing fraud and inability of auditors to detect fraud has resulted in increasing demand of forensic accountants (Razaee & Burton, 1997). Forensic accountant improves auditor’s ability to detect fraud and acts as a bridge to audit expectation gap (Okoye & Okaro, 2011). Emeh & Obi (2013) found that only presence of professionalised accountant will not reduce fraud but forensic accountant can reduce. Forensic accountants should be given participative role in preparation of audit plan rather than consultative role. They have ability to use the unique procedure in audit test. Emeh & Obi (2013) found that presence of forensic accountant and number of accountant possessing forensic accounting skill are in negative correlation with the extent of financial fraud. Forensic accountant is in a better position to detect fraud (Okoye & Okaro, 2011) but is not the only available tool for fraud detection (Modugu & Anyaduba, 2013). Chi-Chi & Ebimobowei (2012) argued that if perpetrator fears of being caught by forensic accountant then they would never think of committing crime. Forensic accountants work not only in fraudulent situation but they devote their most of time to non-fraud activities like contract agreement, finance advisory and mediation. They play an effective role against weak internal control and in improvement of financial reporting (Modugu & Anyaduba, 2013). Roles performed by forensic accountants differ according to size of firm. Large size firms employ them for fraud investigation while small firms appoint them mainly for the purpose of expert witness and valuation services (Akkeren et al., 2013).

	AX : Dilakukan Training yang Diadakan oleh Badan Sertifikasi dan Merekrut Pegawai yang Bersertifikasi Akuntan Forensik		AY : Melatih KIC untuk Mempelajari Red Flags Karyawan Maupun Transaksi dan Memastikan SOP Dilakukan		AY : Melatih KIC untuk Mempelajari Red Flags Karyawan Maupun Transaksi dan Memastikan SOP Dilakukan
6 : S. Siregar, B. Tenoyo	<ul style="list-style-type: none"> Need fraud examiners training and should have Certified Internal Auditor certification. 	2 : D. Mangala, P. Kumari	Razaee & Riley (2010) presented 3C’s model to categorise red flags for financial statement fraud as condition (representing benefit from fraudulent act should outweigh its cost), corporate culture (corporate governance mechanism) and choices (depends upon management strategic intention). In nutshell, red flags have been categorised in numerous ways. In the present study, financial statement fraud indicators have been discussed as per categorisation of fraud risk assessment hierarchy and red flags related to assets misappropriation in two categories, namely, susceptibility of assets to misappropriate and inadequacy of control.	6 : S. Siregar, B. Tenoyo	Conduct surprise visits. Should be a group of independent and competent staffs Implementation of good corporate governance, for example, good corporate governance committee and also Enterprise Risk Management function in every part of the organisation.

--	--	--	--	--	--

	AY : Melatih KIC untuk Mempelajari Red Flags Karyawan Maupun Transaksi dan Memastikan SOP Dilakukan	AY : Melatih KIC untuk Mempelajari Red Flags Karyawan Maupun Transaksi dan Memastikan SOP Dilakukan	AZ : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS		
7 : S. Suhartono	<p>Kebanyakan pelaku fraud (fraudster) menunjukkan ciri-ciri perilaku yang dapat digunakan sebagai sinyal fraud. Namun internal control yang tradisional tidak dapat mendeteksi fraud melalui sinyal ini - misal gaya hidup lebih besar pasak daripada tiang atau terlalu melebih-lebihkan masalah control. Maka manajer, karyawan dan auditor harus di edukasi mengenai pola perilaku seperti itu. Mereka harus didorong untuk memperhatikan kejanggalan-kejanggalan dan melaporkannya.</p> <p>Mendeteksi tindak Fraud yang belum tercegah</p> <p>Penyelidikan secara professional terhadap Fraud yang terdeteksi</p> <p>Meningkatkan tingkat kesadaran kepada pihak eksternal perusahaan seperti pelanggan, supplier dan mitra perusahaan</p>	9 : Y. Ermawati	<p>Untuk sistem audit pusat dan cabang memiliki karakter khusus tersendiri. Metode yang biasanya dipakai adalah red flag dengan asumsi bahwa setiap aktivitas dianggap rawan terhadap kemungkinan terjadinya fraud.</p>	1 : BPPK	<p>The result of the questionnaires about the reward were</p> <ol style="list-style-type: none"> 1. Most of the perceptions' respondents (67 %) choose award to whistleblower is mutation or rotation; 2. The second thing of the participant choosing is promotion or special promotion (53 %); 3. The third one of the perceptions' participant choosing about the award to whistleblower is training or short course (43 %); 4. The prize money to award the whistleblower is the last option of the respondents with 31 % agree with this and only 45 % from them has perception that the amount of prize money promised benefits for specific performance TKPKN maximum of ten times the amount of the reporting or other similar benefits will be sufficient.

AZ : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS

2 : D.
Mangala,
P.
Kumari

Red flags are specific indicators representing potential theft occurrences and psychology of committing fraud. Red flags are events and conditions indicating motivation and opportunity for potential or actual fraud occurrences (SA 240). It is important mechanism for early fraud detection but found to be infrequently used by auditors

Cataloging of red flags is must as a specific class of fraud factors alerts auditors about fraud possibilities (KrambiaKapolis, 2002). There are different ways to classify red flags. Cressey presented the most famous approach of red flags classification known as fraud triangle in 1953 (Omar & Din, 2010; Singleton & Singleton, 2010). Cressey interviewed two hundred prisoners who were involved in embezzlement to understand factors responsible for white-collar crimes and presented them in form of fraud triangle. Fraud triangle represents three red flag categories that induce a person to commit fraud, namely, 'pressure', 'rationalisation' and 'opportunity'. Pressure refers to a situation or happening that builds up stress and raises the need to commit fraud. Rationalisation is developing the mindset to justify fraud under present circumstances. Opportunity is the situation responsible for fraud occurrence (Mohamed & Jomitin, 2014).

Fraud may be detected and prevented in an organisation through effective corporate mechanism, internal audit, external audit, whistle-blowing, forensic accounting, fraud risk assessment procedure, anti-fraud policies, firewall, and password protection.

For successful functioning of whistle blowing program proper channel of communication, protection to whistle blower, staff awareness and staff trust is very important (PwC, 2008). Miceli & Near (1984) found that one would not report a fraud through an unknown channel. Therefore, such policies should be clearly defined (Waldron, 2012). Telephone, mail and e-mail are common channels to blow whistle. Near & Miceli (1985) presented a model for whistle-blowing process. Firstly, a person observes wrongdoing and its consequences. Then, with effect of personal and emotional characteristics, that person reports wrongdoing. Finally, organisation decides whether to act over report or not. Okoye & Okaro (2011) found significant agreement about inculcation of whistle blowing in organisation culture. Corrective actions taken on whistle blowing encourage whistle blowing and result in efficient organisational operation (Miceli & Near, 1984). Whistle blower may be external or internal but external whistleblowers are less fearful about its consequences. Sims & Keenan (1998) found supervisor's support as influencing factor for blowing whistle but such employee would prefer to blow externally. There are self-help groups and voluntary organisations to promote whistle blowers (Waldron, 2012). In addition, various regulatory bodies are considering importance of whistle blowing. Security and Exchange Commission, an independent U.S. agency to protect security market and investors, started whistle blowing program in the year 2012. Andrew Ceresney, Director of the SEC's Division of Enforcement, said that SEC gave awards of thirty million dollar for blowing whistle against the fraud that was hard to detect otherwise⁶. Indian government passed Whistle Blowers Protection Act, 2011. Now, companies in India with public deposits or bank loan of more than fifty crore rupees need to establish vigilance committee. The main aim of this committee will be to promote whistle blowers for reporting against any wrongdoing.

AZ : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS

AZ : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS

7 : S. Suhartono	Memberikan proteksi penyampaian pelaporan adanya indikasi Fraud yang dilakukan di dalam perusahaan	9 : Y. Ermawati	Tanpa aturan dan standar operasional prosedur (SOP) yang tepat dan sistematis maka FEWS yang diterapkan juga tidak akan pernah efektif.
---------------------	--	--------------------	---

	<p>AH : Audit Teknologi Informasi dan Peningkatan Keamanan</p>		<p>AI : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS</p>		<p>AI : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS</p>		<p>AI : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS</p>
<p>8 : Ibu Nur Aeni</p>	<p>P : Jadi di BPD ini setiap hari dicek oleh siapa bu? N : Iya, itu dilakukan di bagian pelayanan. Kan ATM kita kebanyakan di kantor kita. Jadi bukan di mall, ya pokoknya yang jauh dari kantor bank. Yang sering terpasang justru ATM - ATM yang jauh, atau tertutup. Kan kalau di mall terbuka, terkadang kalau mau pasang bisa terlihat. Biasanya ATM - ATM yang dikotak - kotaki cuma ada satu.</p>	<p>2 : Bapak Daryoko</p>	<p>P : Apakah ada keluhan dan saran tentang pelaksanaan strategi anti fraud sebelum Unit Anti fraud dibentuk? N : Sejauh ini menurut saya cukup baik ya, karena sebelumnya kan SKAI, mereka sudah cukup kompeten dalam melaksanakan whistleblowing system nya. Tapi mungkin perlu dilakukan namanya reward untuk pegawai yang aktif melaporkan ke WBS, jadi semua lebih aktif.</p>	<p>3 : Bapak Ivan Nugroho</p>	<p>Dan WBS mungkin bisa dibuat lebih menarik untuk menarik para pegawai lebih aktif dalam melaporkan setiap tindakan yang mengindikasikan fraud.</p>	<p>6 : Bapak Suwasono Adi Kurniawan</p>	<p>whistleblowing system, besok rencananya kita buat “Surat kepada Direktur Utama”, jadi kita buat tidak menakutkan. Sekarang hanya bisa diakses dengan komputer melalui intranet, besok kita coba dapat diakses melalui gadget.</p> <p>BPD DIY Mobile untuk transaksi, yang khusus karyawan kita itu ada BPD DIY Smart itu isinya katalog produk kita.</p> <p>Jadi mungkin kedepan BPD DIY Smart itu bisa juga untuk layanan pengaduan. Fungsinya ya semisal ada orang melihat pegawai BPD misalnya masuk ke tempat yang tidak senonoh, nah itu nanti bisa langsung dilaporkan.</p>

Sumber : Data Diolah dari NVivo 11

LAMPIRAN 20

Matrix Coding Analisis Mekanisme Penerapan Strategi Anti Fraud PT Bank BPD DIY

	A : Investigasi, Pelaporan & Sanksi	B : Ditetapkannya Anti Fraud Statement dan tumbuhkan kesadaran tentang anti fraud oleh manajemen	C : Kebijakan Rotasi dan Cuti Pegawai	D : Pengendalian Internal	E : Penggunaan TI untuk mengendalikan fraud	F : Pembentukan Unit Anti Fraud	G : Pemantauan, Evaluasi & Tindak Lanjut	H : Customer Awareness melalui media sosial
1 : Bapak Andrianto Dwi P.	0	0	1	0	0	0	0	0
2 : Bapak Daryoko	0	0	1	0	0	0	0	0
3 : Bapak Ivan Nugroho	0	0	1	0	0	0	0	0
4 : Bapak Muhammad Agus Salam S.	0	0	1	0	0	0	0	0
5 : Bapak Pandu Kuncoro	0	0	1	0	0	0	0	0
6 : Bapak Suwasono Adi Kurniawan	1	1	1	1	1	1	1	1
7 : Bapak Zukhroni Ariffin	1	0	0	0	0	0	1	0
8 : Ibu Nur Aeni	0	0	1	1	1	1	0	1

	I : Employee Awareness melalui sosialisasi	J : Sosialisasi Anti Fraud Statement dan ciptakan budaya zero tolerance pada fraud	K : Identifikasi Kerawanan	L : Koordinasi Manajemen Risiko dalam menilai risiko dengan Unit Anti Fraud	M : Mengetahui latar belakang pegawai dimulai dari pola rekrutmen	N : Mekanisme Pengaduan pada WBS	O : Sosialisasi WBS	P : Surprise Audit	Q : Surveillance System
9 : <i>Anti Fraud Statement</i> untuk Pegawai	1	1	0	0	0	0	0	0	0
10 : <i>Know Your Employee -</i> 1	0	0	0	0	1	0	0	0	0
11 : <i>Know Your Employee -</i> 2	0	0	0	0	1	0	0	0	0
12 : <i>Know Your Employee -</i> 3	0	0	0	0	1	0	0	0	0
13 : <i>Employee, Customer</i> <i>Awareness, Identifikasi</i> <i>Kerawanan</i>	1	0	0	1	0	0	0	0	0
14 : <i>Surprise Audit,</i> <i>Surveillance System</i>	0	0	0	0	0	0	0	1	1
15 : <i>Whistleblowing System</i> 1	0	0	0	0	0	1	0	0	0
16 : <i>Whistleblowing System</i> 2	0	0	0	0	0	1	0	0	0

Sumber : Data Diolah dari NVivo 11

LAMPIRAN 21

Matrix Coding Analisis Pengembangan SDM Unit Anti Fraud PT Bank BPD DIY

	A : Customer Awareness untuk mencegah eksternal fraud	B : Jejak Rekam Pegawai Saat Pola Rekrutmen	C : Kebijakan Cuti Pegawai	D : Pengelolaan Teknologi Informasi untuk Mengendalikan Fraud	E : Pengembangan WBS	F : Sertifikasi dan Pelatihan untuk Pegawai
1 : Bapak Andrianto Dwi P.	0	0	0	0	0	0
2 : Bapak Daryoko	0	0	1	0	1	0
3 : Bapak Ivan Nugroho	1	0	1	0	1	0
4 : Bapak Muhammad Agus Salam S.	1	0	1	0	0	0
5 : Bapak Pandu Kuncoro	0	0	1	0	1	0
6 : Bapak Suwasono Adi Kurniawan	1	1	0	1	1	1
7 : Bapak Zukhroni Ariffin	0	0	0	0	0	1
8 : Ibu Nur Aeni	1	1	1	1	0	1

Sumber : Data Diolah dari NVivo 11

LAMPIRAN 22

Matrix Coding Analisis Kendala yang Dihadapi oleh Unit Anti Fraud PT Bank BPD DIY

	A : Belum adanya Rekrutmen dan Sertifikasi untuk Unit Anti Fraud	B : Bocornya Rahasia karena Antar Cabang Saling Kenal	C : Jatah Cuti Pegawai yang Tidak Diambil Secara Kolektif	D : Kurangnya Kesadaran Melapor Semua Indikasi Kecurangan	E : Penyedia WBS dibuat oleh Divisi TI Perusahaan Sendiri
1 : Bapak Andrianto Dwi P.	0	0	1	1	0
2 : Bapak Daryoko	0	0	0	0	0
3 : Bapak Ivan Nugroho	0	0	1	1	0
4 : Bapak Muhammad Agus Salam S.	1	0	1	0	0
5 : Bapak Pandu Kuncoro	1	0	1	1	0
6 : Bapak Suwasono Adi Kurniawan	1	1	1	0	1
7 : Bapak Zukhroni Ariffin	1	1	0	1	0
8 : Ibu Nur Aeni	1	1	0	0	1

Sumber : Data Diolah dari NVivo 11

LAMPIRAN 23

Matrix Coding Analisis Peningkatan yang Dilakukan Unit Anti Fraud dalam Meminimalkan Fraud PT Bank BPD DIY

	A : Audit Teknologi Informasi dan Peningkatan Keamanan	B : Diadakan Gathering yang mengurangi Jatah Cuti Bersama dan Melakukan Rotasi Mingguan antar Karyawan	C : Dilakukan Training yang Diadakan oleh Badan Sertifikasi dan Merekrut Pegawai yang Bersertifikasi Akuntan Forensik	D : Melatih KIC untuk Mempelajari Red Flags Karyawan Maupun Transaksi dan Memastikan SOP Dilakukan	E : Sistem Reward Berupa Promosi, Refresh Anti Fraud Awareness atas Pemahaman Red Flags dan Pembaruan Berupa Aplikasi untuk WBS
1 : BPPK	0	0	0	0	1
2 : D. Mangala, P. Kumari	1	0	1	1	0
3 : S. Siregar, B. Tenoyo	1	1	0	1	0
4 : S. Suhartono	0	0	0	1	0
5 : Y. Ermawati	0	1	0	1	1
6 : Bapak Adrianto Dwi P.	0	0	0	0	0
7 : Bapak Daryoko	0	0	0	0	1
8 : Bapak Ivan Nugroho	0	0	0	0	1
9 : Bapak Muhammad Agus Salam S.	0	0	0	0	0
10 : Bapak Pandu Kuncoro	0	0	0	0	0
11 : Bapak Suwasono Adi Kurniawan	0	0	0	0	1
12 : Bapak Zukhroni Ariffin	0	0	0	0	0
13 : Ibu Nur Aeni	1	0	0	0	0

Sumber : Data Diolah dari NVivo 11