TUGAS AKHIR – KS09 1336

ANALISIS RISIKO INSIDER THREAT SECARA DINI DENGAN PENDEKATAN SISTEM DINAMIK (STUDI KASUS PT XYZ)

FAZA FAIKAR CORDOVA
NRP 5210 100 003

Dosen Pembimbing
ERMA SURYANI, S.T., M.T., Ph.D

JURUSAN SISTEM INFORMASI
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2014

FINAL PROJECT – KS09 1336

INSIDER THREAT RISK DETECTION ANALYSIS OF PT XYZ USING SYSTEM DYNAMICS MODELLING APPROACH

FAZA FAIKAR CORDOVA
NRP 5210 100 003

SUPERVISOR
ERMA SURYANI, S.T., M.T., Ph.D

INFORMATION SYSTEM DEPARTMENT
FACULTY OF INFORMATION TECHNOLOGY
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2014

ANALISIS RISIKO INSIDER THREAT SECARA DINI DENGAN PENDEKATAN SISTEM DINAMIK (STUDI KASUS PT XYZ)

Nama Mahasiswa : FAZA FAIKAR CORDOVA
NRP : 5210 100 003
Jurusan : SISTEM INFORMASI FTIF-ITS
Dosen Pembimbing : ERMA SURYANI S.T., M.T., Ph.D

ABSTRAK

Perkembangan teknologi informasi di Indonesia semakin maju dengan pesat. Hal ini terbukti dengan banyaknya berbagai perusahaan dan organisasi di Indonesia yang menggunakan Sistem Informasi dan Teknologi Informasi (SI/TI), salah satunya adalah PT. XYZ, perusahaan surat kabar nasional. Dengan mengimplementasikan SI/TI maka perusahan memiliki aset baru yaitu aset informasi. Dimana informasi merupakan aset bisnis yang memiliki nilai esensial dan harus dilindungi sekuritasnya. Adapun risiko yang dapat terjadi adalah adanya penyerangan dari dalam perusahaan atau dikenal dengan insider attacks. Tetapi hingga saat ini sistem yang digunakan oleh PT XYZ untuk mencegah risiko terhadap aset informasi sampai saat ini belum bisa menanggulangi tingkah laku dari orang dalam, rata-rata sistem yang digunakan hanya dapat mencegah serangan sekuritas informasi dari luar saja. Maka dari itu diperlukan suatu

prosedur keputusan yang dapat menemukan parameter-parameter tertentu untuk membantu manajemen PT. XYZ dalam mendeteksi risiko adanya insider attack. Metode yang dapat digunakan untuk mendeteksi lebih dini insider attack adalah dengan menggunakan sistem dinamik, dimana metode ini mendeskripsikan dan mensimulasikan perilaku sistem yang terkait dengan insider risk dan insider threat. Sehingga dengan adanya Tugas Akhir ini guna memberikan acuan dalam membuat keputusan terkait dengan risiko orang dalam di perusahaan PT. XYZ.

.

Kata kunci*: *Sistem Dinamik, Ancaman orang dalam,Diagram kausatik

INSIDER THREAT RISK DETECTION ANALYSIS OF PT XYZ USING SYSTEM DYNAMICS MODELLING APPROACH

Name : **FAZA FAIKAR CORDOVA**
NRP : **5210 100 003**
Department : **INFORMATION SYSTEM FTIF-ITS**
Supervisor : **ERMA SURYANI S.T., M.T., Ph.D**

ABSTRACT

The Development of information technology in Indonesia is advancing at a rapid pace. One of the evidence of is , now many companies and organization in Indonesia is using Information Technology and Information System (IS/IT) in their business process. One of the company that is using it is PT XYZ, a national newspaper companies. By implementing IS/IT in the company, PT XYZ gains new asset which is information technology assets.Nowdays information is a business asset that has value and has to be protected by the company. One of the risk that can be happen is an attack from within the company,known as insider threat. But until now the security system used by PT XYZ could not cope with the insider threat within the company. The average security system only prevent information technology security from the outside not from the insider (the one who attack from the inside). Therefore there is a need of decision procedure to assist the management of PT. XYZ in detecting the presence of risk of insider threat. A method that can be used for ealy detection of insider attack is system dynamic

which can describe and simulate the behavior of the system associated with the risk onf insider threat. So the goal of this final project is to provide a preference in making decisions related to the risk and threat of an insider in PT XYZ.

***Keywords*: System Dynamic, Insider Threat, Causal Loop Diagram**

ANALISIS RISIKO INSIDER THREAT SECARA DIN DENGAN PENDEKATAN SISTEM DINAMIK (STUDI KASUS PT XYZ)

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

FAZA FAIKAR CORDOVA
5210 100 003

Surabaya, Juli 2014

KETUA
JURUSAN SISTEM INFORMASI

Dr. Eng. Febriliyan Samopa S.Kom, M.Kom
NIP 19730219.199802.1.001

Halaman ini sengaja dikosongkan

ANALISIS RISIKO INSIDER THREAT SECARA DINI DENGAN PENDEKATAN SISTEM DINAMIK (STUDI KASUS PT XYZ)

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

FAZA FAIKAR CORDOVA
5210 100 003

Disetujui Tim Penguji : Tanggal Ujian : Juni 2014
Periode Wisuda : September 2014

Erma Suryani S.T., M.T., Ph.D **(Pembimbing 1)**

Wiwik Anggraeni, S.Si, M.Kom. **(Penguji 1)**

Retno Aulia Vinarti, S.Kom., M.Kom **(Penguji 2)**

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Alhamdulillahirobbil ‘alamiin. Allahumma sholli’alaa Muhammad, wa ‘alaa aali sayyidina Muhammad. Tiada Dzat yang Maha Perkasa yang mampu menolong selain Allah SWT sehingga penulis dapat menyelesaikan buku tugas akhir dengan judul:

ANALISIS RISIKO INSIDER THREAT SECARA DINI DENGAN PENDEKATAN SISTEM DINAMIK (STUDI KASUS PT XYZ)

yang merupakan salah satu syarat kelulusan pada Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya.

Secara khusus penulis akan menyampaikan ucapan terima kasih yang sedalam-dalamnya kepada:

1) Allah SWT yang telah memberikan kesehatan dan kesempatan untuk bisa menyelesaikan tugas akhir ini.
2) Ibu, Ayah, dan Adik yang selalu mengganggu, dan memberi *support* pada saat pengerjaan tugas akhir.
3) Annis Paramita Dilla yang setia banget menemani dan memberikan semangat dengan caranya sendiri. Good luck buat kita berdua semoga mimpi dan harapan mu dan aku menjadi kenyataan. You and me against the world.
4) Ibu Erma Suryani, S.T., M.T, Ph.D selaku dosen pembimbing yang super sekali. Terimakasih sudah menjadi ibu kedua saya di kehidupan kampus.
5) Teman-teman selama masa kuliah Mamed, Vinda, Afrizal, Amel, Dian, Yance, Yoga, Ijal, Tacul, dan Yuda dan lain-lainnya.

6) Keluarga Foxis, yang menemani masa empat tahun perkuliahan.
7) Seluruh dosen pengajar beserta staf dan karyawan di Jurusan Sistem Informasi, FTIF ITS Surabaya yang telah memberikan ilmu dan bantuan kepada penulis selama ini.
8) Terima kasih kepada D1SC 2001, NFORS 2002, SI SHOGUN CO. 2003, NARSIIS 2004, PHOENIC 2005, ANONIMS 2006, GENESIS 2007, 8IOS 2008, AE9IS 2009 dan BASILISK 2011 atas semua bantuan ketika penulis berkuliah di Sistem Informasi.
9) Serta semua pihak yang telah membantu dalam pengerjaan Tugas Akhir ini yang belum mampu penulis sebutkan diatas.

Terima kasih atas segala bantuan, dukungan, serta doanya.Semoga Allah SWT senantiasa melimpahkan rahmat hidayah serta membalas kebaikan-kebaikan yang telah diberikan kepada penulis.

Surabaya, 17 Juni 2014

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PERSAMAAN

BAB 1
PENDAHULUAN

Bagian ini menjelaskan beberapa hal dasar mengenai pengerjaan tugas akhir yang meliputi: latar belakang masalah yang menyebabkan studi kasus ini diangkat, tujuan, manfaat, batasan masalah, keterkaitan dengan penelitian lain, serta sistematika pengerjaan tugas akhir

1.1 Latar Belakang

Perkembangan teknologi informasi di Indonesia semakin maju dengan pesat. Hal ini terbukti dengan banyaknya aplikasi sistem informasi (SI) dan Teknologi Informasi (TI) diberbagai perusahaan dan organisasi di Indonesia. Peran SI/TI di berbagai perusahaan di Indonesia sangatlah besar, salah satunya adalah untuk bertahan dalam menghadapi era globalisasi dimana perusahaan dituntut untuk berkembang dan bersinergi dengan SI dan TI [1]. Aset informasi dalam konteks bisnis merupakan aset bisnis yang memiliki nilai esensial dan harus dilindung sekuritasnya [2].

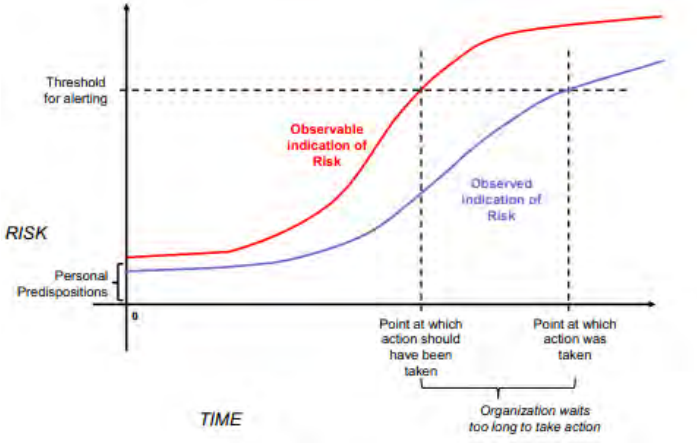
Kenyamanan dalam menggunakan teknologi informasi dan sistem informasi berbanding terbalik dengan keamanan aset informasi di perusahaan. Hal ini memberikan peluang baru terhadap munculnya risiko-risiko terkait aset informasi. Risiko terhadap aset informasi dapat dikategorikan menjadi dua yaitu risiko yang muncul dari dalam (*insider attacks*) dan luar (*outsider attacks*). Pada tahun 2011 survey yang dilakukan oleh CyberSecurity Watch di Amerika menemukan bahwa 27% serangan sekuritas informasi yang dilakukan pada organisasi disebabkan oleh orang dalam [3]. Bahkan pada tahun 2010,

CyberSecurity Watch juga menemukan bahwa menurut 67% responden yang diwawancarai menyatakan bahwa *insider attacks* lebih merugikan biaya yang besar pada perusahaan dan organisasi. *Insider attack* disebabkan oleh seseorang dari organisasi yang baik secara sadar maupun tidak sadar menyebabkan kerugian pada aset organisasi [4].

PT. XYZ adalah perusahaan surat kabar nasional yang mengefektifkan teknologi informasi dalam proses bisnisnya .Untuk memudahkan serta mengefisiensikan proses bisnisnya PT. XYZ mulai mengimplementasikan SI/TI mulai dari tahun 1998 yaitu dengan penggantian mesin ketik dengan komputer. Saat ini PT. XYZ sudah mempunyai bagian teknologi informasi sendiri dan *data center*. SI/TI di PT. XYZ membantu para jurnalisnya dalam berbagai proses salah satunya editing berita, penyimpanan berita, dan pemilihan berita.

Dalam menjaga aset informasinya PT. XYZ sudah mengimplementasikan manajemen resiko untuk meminimalisasi risiko terhadap aset informasi. Sistem yang digunakan untuk mencegah risiko terhadap aset informasi sampai saat ini belum bisa menanggulangi tingkah laku dari orang dalam, rata-rata sistem yang digunakan hanya dapat mencegah serangan sekuritas informasi dari luar saja [5]. Untuk lebih jelasnya tentang bagaimana rata-rata organisasi mendeteksi ancaman risiko terkait *insider risk* dapat dilihat pada gambar 1.Pada Gambar 1 dijelaskan momen dimana organisasi mengobservasi risiko dan harus merespon terhadap risiko tersebut. Garis biru dibawah mengidikasikan risiko yang diobservasi organisasi. Waktu 0 mengindikasikan kapan orang tersebut dipekerjakan, dimana mereka memulai dengan nilai positif pada risikonya. Organisasi nantinya akan mengambil tindakan ketika risiko tersebut meningkat lebih dari batas aman risiko tersebut. Garis merah yang

diatas merepresentasikan indikasi risiko yang dapat muncul dari orang dalam. Semakin dini organisasi mengetahui aksi dari orang dalam, maka akan semakin cepat orang dalam tersebut melewati garis peringatan di organisasi.



Gambar 1.1 Contoh observasi *insider's Threat* pada organisasi [6]

Berdasarkan permasalahan inilah, diperlukan suatu prosedur keputusan yang dapat menemukan parameter-parameter tertentu untuk membantu manajemen PT. XYZ dalam mendeteksi risiko adanya *insider attack*. Salah satu metode yang dapat digunakan untuk mendeteksi lebih dini *insider attack* adalah dengan menggunakan sistem dinamik. Ancaman orang dalam (*Insider threat*) merupakan permasalahan kompleks serta harus dikaji secara holistik dan dinamis. Selain itu sistem dinamik merupakan alat analisis yang efektif untuk menemukan solusi jangka panjang [7]. Deksripsi perilaku sistem terkait dengan *insider risk* dan *insider threat* akan disimulasikan perkembangannya sejalan dengan variabel waktu. Dalam studi ini peneliti akan membuat

model berdasarkan parameter-parameter yang diuji pada studi yang telah dilakukan oleh peneliti sebelumnya.

Dalam membuat model sistem dinamik perangkat lunak yang digunakan adalah VENSIM. VENSIM digunakan karena mempunyai kelebihan dalam hal memudahkan pembuat model dikarenakan perangkat lunak ini menyediakan *icon* dan mempunyai fitur *drag and drop*. Hasil yang dapat dianalisis dari perangkat lunak ini adalah *Graph, Causes Strip*, dan *Time Table* yang dihubungkan dengan *insider risk*.Mengingat sulitnya mengidentifikasi *insider risk* bagi perusahaan dan akibatnya yang begitu besar apabila hal tersebut terjadi, maka melalui studi ini diharapkan dapat membuat model analisis yang dapat memberikan acuan dalam membuat keputusan terkait dengan risiko orang dalam di perusahaan PT. XYZ.

1.2 Rumusan permasalahan

Berdasarkan latar belakang diatas, maka didapatkan perumusan masalah yang akan dibahas pada usulan tugas akhir ini adalah:

1. Bagaimana cara mengidentifkasi risiko-risiko yang mengakibatkan terjadinya *insider threat*?
2. Bagaimana menganalisis fase-fase *insider threat* pada perusahaan PT. XYZ dengan pendekatan sistem dinamik?
3. Bagaimana meminimalkan risiko *insider threat* pada perusahaan PT. XYZ?

1.3 Batasan Permasalahan

Dari perumusan masalah yang telah dipaparkan sebelumnya, maka yang menjadi batasan dalam tugas akhir ini adalah sebagai berikut:

a) Permasalahan sekuritas yang dianalisis hanya berbasiskan *insider threat* yang disengaja oleh karyawan PT. XYZ terkait teknologi informasi dan sistem informasi.
b) Perspektif analisis yang digunakan adalah karyawan (*insider*) yang mempunyai keahlian dalam bidang teknologi informasi/sistem informasi di PT. XYZ.

1.4 Tujuan

Adapun tujuan dari pengerjaan tugas akhir ini antara lain:

1. Mengidentifikasi risiko-risiko yang mengakibatkan terjadinya *insider threat*
2. Menganalisis dan mengembangkan model fase-fase *insider risk* pada perusahaan PT. XYZ dengan pendekatan sistem dinamik.
3. Meminimalkan risiko *insider threat* pada perusahaan PT. XYZ.

1.5 Manfaat

Manfaat yang dapat diperoleh dari pengerjaan tugas akhir ini adalah:

1. Bagi peneliti, model yang dikembangkan dapat menjadi masukan dalam mengembangkan model *insider threat.*
2. Bagi perusahaan PT. XYZ, hasil penelitian ini dapat dijadikan acuan dalam membuat sistem yang dapat mendeteksi adanya *insider threat* serta bagaimana meminimalkan risiko tersebut.

1.6 Keterkaitan dengan Penelitian Lain

Dalam mengerjakan tugas akhir ini terdapat penelitian terkait yang digunakan, berikut informasi singkat mengenai penelitian tersebut:

1. S.-C. Yang and Y.-L. Wang, "Insider Threat Analysis of Case Based System Dynamics," *Advanced Computing: An International Journal*, vol. 2, no. 2, pp. 1-17, 2011, yang membahas tentang analisis *insider threat* dengan menggunakan studi kasus pada sebuah perusahaan di Taiwan berbasis *event based*.
2. P. Moore, A. M. David and M. L. Collins, "A System Dynamics Model for Investigating Early Detection of Insider Threat Risk," in *SystemDynamics.org*, 2013, yang membahas tentang pembuatan model sistem dinamik untuk mendeteksi *insder threat* sejak dini pada suatu perusahaan.
3. C. Melara, J. M. Sarriegui, J. J. Gonzales, A. Sawicka and D. L. Cooke, "A System Dynamics Model of an Insider Attack on an Information System," in *Proceedings of the 21st International Conference of the System Dynamics Society*, 2003., yang membahas tentang model sistem dinamik untuk *insider attack* pada sistem informasi di perusahaan dengan suatu studi kasus.

1.7 Sistematika Penulisan

Dalam tugas akhir ini, sistematika penulisan laporan disesuaikan dengan pelaksanaan penelitian dan disusun secara runtut dengan memperhatikan keterkaitan anatara bab yang satu dengan yang lain. Penulisan ini dibagi menjadi 6 bab dan masing-

masing bab terdiri dari beberapa sub bab untuk memberikan penjelasan yang lebih detail. Tahapan penulisan laporan penelitian tugas akhir ini dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini akan dijelaskan tentang latar belakang, rumusan permasalaham tugas akhir, tujuan tugas akhir, relevansi dan manfaat tugas akhir, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan dijelaskan tentang referensi-referensi yang berkaitan dengan tugas akhir dan beberapa hal yang berkaitan dengan metode sistem dinamik yang mampu membantu pemahaman pengerjaan tugas akhir.

BAB III METODE PENELITIAN

Bab ini berisi penjelasan mengenai masing-masing tahap dalam pembuatan tugas akhir atau urutan langkah yang harus dilakukan oleh penulis dalam mengerjakan tugas akhir agar dapat berjalan sistematis, terstruktur dan terarah.

BAB IV MODEL DAN IMPLEMENTASI

Pada bab ini dijelaskan mengenai implementasi dan pembuatan model simulasi. Pada bagian ini teradapt penjelasan mengenai pembuatan model, keterhubungan antar variabel yang mempengaruhi, persamaan dalam *basemodel*, dan proses verifikasi dan validasi model.

BAB V PEMBUATAN SKENARIO DAN ANALISIS HASIL

Bab ini menjelaskan tentang uji coba model yang telah valid untuk dilakukan beberapa skenariosasi dengan dua tahap yaitu:

skenario terstruktur dan skenario parameter untuk menghasilkan analisis kebijakan bagi perusahaan.

BAB VI PENUTUP

Bab ini berisi kesimpulan dan saran dari seluruh percobaan yang telah dilakukan untuk dibandingkan dengan tujuan dan permasalahan yang sudah dibuat pada bab pendahuluan.

BAB 2
TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai teori-teori terkait yang bersumber dari buku, jurnal, artikel, ataupun tugas akhir terdahulu yang berfungsi sebagai dasar dalam melakukan pengerjaan tugas akhir. Agar dapat memahami konsep atau teori penyelesaian permasalahan yang ada.

2.1. Proteksi Aset Informasi

Dalam beberapa penelitian yang sudah telah dilakukan, banyak peneliti yang setuju bahwa sekuritas dalam bidang informasi hanya berkutat pada kontrol teknis dan pengendaliannya. Padahal banyak aspek lain yang penting yang juga harus dikaji, khususnya terkait dengan proteksi aset informasi. Proteksi aset informasi adalah suatu tindakan yang dilakukan perusahaan untuk melindungi aspek-aspek seperti sumber daya manusia(SDM), faktor organisasi, teknologi, dan lingkungan kerja [8]. Agar proteksi aset informasi dapat berjalan dengan baik, Dhillon dalam Melara *et al.* menawarkan tiga jenis kontrol sekuritas sistem informasi, diantaranya adalah [9]:

1. Kontrol teknis: yaitu suatu mekanisme yang melindungi sistem dari resiko kejadian dan juga serangan, contoh kontrol teknis antara lain: *software* antivirus, hak akses, *backups*, dan *recovery*.
2. Kontrol formal: adalah struktur bisnis dan proses yang memastikan proses bisnis yang benar telah berjalan sehingga dapat mengurangi resiko kejadian dan juga

serangan. Contoh kontrol formal antara lain: memisahkan departemen sekuritas informasi dengan departemen TI lainnya, desain hak akses dan kontrol bagi masing-masing karyawan sesuai dengan perannya dalam perusahaan, dan evaluasi risiko pada perusahaan secara rutin.

3. Kontrol informal: merupakan sebuah kontrol yang berhubungan dengan budaya dan nilai perusahaan. Contoh kontrol informal antara lain adalah meningkatkan kesadaran terhadap isu-isu sekuritas dengan edukasi dan *training*.

Tujuan dalam melakukan keamanan teknologi informasi dan asetnya adalah untuk memastikan bahwa teknologi informasi dapat memberikan kerahasiaan, integritas, dan tersedianya aset informasi dari perusahaan [10].

2.2. Ancamana Keamanan Aset Informasi

Asset Teknologi Informasi (TI) merupakan suatu barang berwujud maupun tidak berwujud yang dinilai dapat memberikan manfaat bagi proses bisnis oleh suatu perusahaan atau organisasi. Dari segi manfaat asset teknologi informasi dibagi menjadi dua yaitu: (1) aset TI *tangible* seperti *hardware,* server*,* dan lain-lain; (2) aset TI *intangible* seperti perangkat lunak, informasi, hak cipta, *knowledge*, dan lain-lain. Asset TI tersebut merupakan aset yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar maupun dalam organisasi [11].

Menurut Krutz dan Vines (2006), ancaman (*threats*) merupakan peristiwa yang apabila terjadi dapat menyebabkan

kerusakan pada sistem dan membuat hilangnya kerahasiaan, ketersediaan, maupun integritas organisasi [12]. Menurut Fiberlink, ancaman yang dapat mengancam kemananan asset informasi suatu organisasi terbagi menjadi dua, yaitu [13]:

1. *Insider Threat*, berasal dari seorang individu dari dalam perusahaan yang memiliki akses mudah ke dalam data perusahaan. Contoh: karyawan perusahaan.
2. *Outsider Threat,* berasal dari seseorang yang tidak memiliki wewenang untuk mengakses data dan tidak memiliki hubungan formal dengan perusahaan. Contoh: *hacker*.

2.3. *Insider Threat*

Insider threat didefinisikan sebagai seorang karyawan atau mantan karyawan, kontraktor, dan partner bisnis yang mempunyai akses pada sistem informasi, jaringan, data di perusahaan yang secara sengaja maupun tidak sengaja dapat merusakan konfidentialitas dan integritas dari aset informasi di perusahaan [14]. Dalam penelitian ini yang akan dibahas adalah *insider threat* yang dilakukan secara sengaja oleh *malicious insider*. Istilah *malicious insider* adalah seseorang yang menyalahgunakan kepercayaan yang diberikan oleh perusahaan dan menyebabkan kerusakan pada aset informasi [15]. Serangan dari dalam yang disengaja dapat berupa: penggelaman, sabotase, dan eksploitasi informasi organisasi [16]. Beberapa macam asset yang ditarget oleh *insiders* adalah informasi pelanggan, *source code*, *business plan*, rahasia perdagangan, informasi internal organisasi, dan aplikasi berbayar milik organisasi. Perusahaan konsultan Delotte

menyebutkan bahwa terdapat 4 area yang rentan terhadap ancaman *insiders* seperti:

1. Kerusakan aset utama dan peralatan penting organisasi
2. Pencurian aset utama dan peralatan penting organisasi
3. Menghapus besar-besaran atau merusak catatan dan *file* organisasi
4. Kebocoran informasi organisasi yang rahasia.

Dalam berbagai penelitian yang dikutip dari jurnal Yang dan Wang tentang penelitian terhadap *insider threat*, ditemukan beberapa *framework* yang mempunyai fokus kepada masing-masing kepada sumber daya manusia, proses dan juga teknologi [5]. Beberapa analisis *insider threat* dan atribut yang telah dilakukan oleh Yang dan Wang [17] dapat dilihat pada tabel 2.1 dibawah ini.

Tabel 2.1 Penelitian tentang *Insider Risk*

Peneliti	Metodologi	Klasifikasi
Anderson(1999)	4 Kategori *insider threat*	Proses
Anderson(2000)	8 pendekatan umum	Teknologi
Symonenko et al.(2004)	6 Indikator *framework*	Teknologi
Keeney et al.(2005)	MERIT	Teknologi
Liu dan Martin (2005)	KNN *outlier detection algorithm*	Teknologi/Proses/SDM
Chichani (2005)	Pemodelan	Teknologi
Stanton et al. (2005)	*End user security behaviors*	Teknologi
Park dan	Kontrol berbasikan	Teknologi

Peneliti	Metodologi	Klasifikasi
Guordano(2006)	peran	
Maybury (2006)	Algoritma pendeteksi kejahatan orang dalam	Teknologi
Cappeli et al. (2006)	MERIT	Teknologi
Band et al. (2006)	Sistem dinamik	Teknologi/Proses/SDM
Ha et al. (2007)	ICMAP	Teknologi/Proses/SDM
Ali et al. (2008)	Crystal Report Generation	Teknologi
Bishop dan Gates (2008)	Definisi *insider*	Proses
Greitzer et al. (2008)	MERIT	Teknologi
McCormick (2008)	EDLP	Teknologi
Moore et al. (2008)	Ssitem dinamik	Teknologi/Proses/SDM
Chagarlamudi et al. (2009)	Pendekatan berbasis implementasi	Teknologi
Jabbour dan Menasce (2009)	*Insider Threat Security Architecture*	Teknologi
Nelikar S (2010)	*Scalable Simulation Framework*	Teknologi
Niekerk dan Solms (2010)	Model konseptual	Proses

Dari tabel 2.1 diatas, diperoleh suatu temuan menarik dimana sebagian besar fokus penelitian lebih menfokuskan

pada teknologi saja. Salah satu elemen terpenting dalam studi tentang *insider threat* adalah sumber daya manusia. Sumber daya manusia serta faktor lain seperti proses dan teknologi memiliki peran penting untuk menganalisis *insider threat*. Salah satu metode yang dapat menjangkau berbagai faktor baik internal dan eksternal secara komprehensif adalah metode sistem dinamik. Oleh karena itulah pada penelitian kali ini peneliti memilih untuk menggunakan sistem dinamik sebagai *tools* untuk menganalis *insider threat*.

2.4. Faktor penyebab *Insider Threat*

Faktor-faktor penyebab utama yang berkontribusi dalam mendukung tingkat laku *insider threat* telah dipelajari dalam riset-riset sebelumnya. Faktor-faktor penyebab terjadinya *insider threat*, nantinya akan dikembangkan menjadi model dan disesuaikan dengan sistem aktual di dunia nyata (PT XYZ) .

a) Akses dan Tingkat Kepercayaan

Dalam beberapa perusahaan saat ini mulai memberikan akses ke *database* kepada karyawannya termasuk juga auditor, kontraktor, dan juga distributor. Semakin berkembangnya dan banyaknya akses yang diberikan maka tingkat kemungkinan terjadinya pencurian dan penyalahgunaan hak akses akan semakin meningkat [18]. Selain itu, Althebyan dan Pand juga menambahkan bahwa keahlian dan juga akses memungkinkan *insider* untuk merencanakan serangan ke dalam organisasi dengan sukses serta membuat serangan tersebut susah untuk dicegah dan ditemukan [19]. Berdasarkan hasil penelitian dari Moore *et al.* ditemukan bahwa sebanyak 67% dari *insider* mempunyai

akses kepada informasi yang mereka curi [20]. Hal ini menunjukkan bahwa faktor akses dan tingkat kepercayaan yang diberikan organisasi bisa menjadi peluang kejahatan apabila tidak dikelola dengan baik.

b) Posisi Teknis dan Keahlian Teknis

Menurut White dan Panda, pegawai yang mempunyai keahlian terutama di bidang TI dapat menggunakan keahliannya untuk merusak sistem organisasi dengan berbagai aktivitas yang ilegal [21]. White dan Panda juga menambahkan bahwa tingkat keahlian TI pegawai tersebut juga menentukan keahlian mereka dalam melakukan serangan dari dalam, tingkat keahlian TI tersebut dibagi menjadi [21]:

- *Novice*: yaitu pengguna akhir dengan tingkat keahlian TI yang rendah.
- *Ordinary*: yaitu pengguna akhir dengan tingkat keahlian TI sedang sehingga ia bisa menggunakan beberapa aplikasi
- *Advanced*: yaitu pengguna akhir dengan tingkat keahlian TI tinggi sehingga ia dapat menggunakan aplikasi serta sistem perusahan.

Dari analisis yang dilakukan Moore *et al.* dan Hanley *et al.* menemukan bahwa kurang lebih dari 50% *insider* yang mereka teliti mempunyai posisi teknis dan selain itu dalam penelitian lain ditemukan juga bahwa *insider* yang tidak mempunyai posisi teknis mempunyai tingkatan jumlah kurang dari 20% [20] [22] [23].

c) Kebijakan keamanan informasi

Beberapa hal yang perlu digaris bawahi dalam kebijakan keamanan informasi adalah faktor manusia. Dimana faktor manusia dapat di kategorikan menjadi tiga komponen utama yaitu: peran sistem, alasan menyalahgunakan dan konsekuensi digunakannya sistem [24]. Secara umum kebijakan keamanan informasi dapat menentukan aksi mana yang diperbolehkan pada pengguna dan tujuan tertentu. Pengguna dapat menggunakan ototritasnya karena memang sistem komputer tidak mengenali orang tersebut hanya akun penggunanya saja [25]. Dalam studi yang dilakukan Kowalski, Cappeli, dan Moore menemukan bahwa dari 62% kasus , *insider* melanggar dan menyalahgunakan kelemahan sistem di segi kebijakan, proses, prosedur atau aplikasi. Kebanyakan kasus ini terjadi dikarenakan kurangnya akses kontrol teknis secara fisik. [26].

2.5. Indikator penyebab terjadinya *Insider Threat*

Selain faktor penyebab terjadinya *insider threat* diperusahaan, terdapat indikator-indikator yang dapat digunakan untuk mengidentifikasi adanya *insider threat*. Dalam penelitian ini digunakan dua indikator utama untuk mendeteksi tingkat *insider threat* di PT XYZ, yaitu dengan indikator tingkah laku dan indikator teknis [27]. Selain kedua indikator tersebut, terdapat satu indikator lagi yang digunakan dalam penelitian ini yaitu indikator kebebasan *insider* [28].

- **Indikator tingkah laku**

  Indikator tingkah laku merupakan kombinasi permasalahan terkait psikologi dan sosial. Menurut penelitian yang dilakukan oleh Greitzer dan Homier

terkait pemodelan tingkah laku manusia untuk mengantisipasi *insider attack*, implementasi dari indikator tingkah laku dapat didapatkan dengan pengamatan data personal ataupun *record* /data historis pengamatan yang dilakukan oleh supervisor karyawan [29]. Dalam penelitiannya Greitzer dan Hohimer juga mengemukakan beberapa contoh tingkat risiko *insider threat* tingkah laku yaitu: ketidakpuasan karyawan, tidak masuk kerja, isu performa, dan tidak mematuhi aturan perusahaan [29].

- **Indikator teknis**

  Indikator teknis merupakan pendekatan yang dalam pengambilan datanya digunakan pendekatan sinyal deteksi berupa batasan dalam *log* / data histori yang dilakukan oleh karyawan. Dalam implementasinya banyak perusahaan yang menggunakan deteksi berupa alarm aplikasi yang dapat mendeteksi adanya tindakan penyalahgunaan aplikasi teknologi informasi dan sistem informasi di perusahaan [30] .

- **Indikator kebebasan *insider***

  Indikator kebabasan *insider*, merupakan salah satu indikator yang banyak digunakan di berbagai penelitian terkait insider threat. Salah satu penelitian yang menggunakan indikator tersebut adalah penelitian Cappelli et. al terkait studi kasus sabotase *insider* [28]. Salah satu cara untuk mendapatkan nilai indikator kebebasan *insider* didapatkan dari observasi dan wawancara secara langsung di perusahaan atau organisasi.

2.6. Teknologi Informasi di PT XYZ

PT. XYZ sebagai perusahaan surat kabar memiliki dua divisi TI di perusahaanya. Divisi pertama adalah Management Information System (MIS) dan yang kedua adalah News Room Information System (NRIS). Kedua Divisi tersebut memiliki peran dan jam berbeda dalam membantu proses bisnis di PT. XYZ. MIS lebih berfokus untuk membantu proses bisnis di divisi periklanan, keuangan, sirkulasi koran, dan personalia. Sedangkan NRIS lebih aktif di waktu malam, dimana divisi ini bertugas untuk mengelola sistem informasi di redaksi koran PT XYZ.

Aplikasi dan sistem informasi di PT XYZ merupakan hasil pengembangan sendiri dari divisi TI. Beberapa contoh aplikasi yang dikembangkan adalah: aplikasi keuangan, piutang, periklanan, dan sirkulasi koran. Aplikasi-aplikasi tersebut didukung dengan infrastuktur TI yang tersimpan di lantai 4 dan 5.

Kesemua aplikasi ini diintegrasikan dan mempunyai keamanan berupa hak akses yang identik pada setiap karyawan. Selain itu dalam sistem yang terintegrasi tersebut terdapat proses cek ulang berupa otorisasi agar tidak terjadi kecurangan. Keamanan dari dalam di PT. XYZ juga dibantu dengan database administrator yang mengecek log karyawan setiap harinya apabila disinyalir terdapat kejanggalan pada penggunaan hak ases pada sistem dan aplikasi.

2.7. Pemodelan dan Simulasi

Proses merancang model matematis atau logik dari sistem selanjutnya melakukan eksperimen dengan model tersebut untuk menggambarkan, menjelaskan dan

memprediksi kelakukan dari sistem. Adapun dasar pertimbangan digunakannya metode simulasi diantaranya adalah [7]:

a. Simulasi merupakan alternatif yang tepat, tidak semua sistem dapat direprenstasikan dengan model matematis.
b. Dapat bereksperimen tanpa adanya resiko pada sistem nyata
c. Mendapatkan studi jangka panjang dengan waktu yang singkat input data yang akan dimasukkan bervariasi
d. Banyaknya ketidakpastian yang terjadi pada suatu masalah sehingga mengharuskan untuk menggunakan simulasi untuk penanganannya
e. Butuh waktu yang cepat untuk menyelesaikan permasalahan

2.8. Simulasi

Simulasi merupakan suatu teknik meniru operasi-operasi atau proses-proses yang terjadi dalam suatu sistem dengan bantuan perangkat computer dan dilandasi oleh beberapa asumsi tertentu sehingga sistem tersebut dapat dipelajari secara ilmiah [31]. Dengan simulasi, sistem yang dibangun dapat digambarkan karakteristiknya sehingga dapat dianalisis untuk menghasilkan sistem yang lebih efektif dan efisien.

Simulasi dapat digunakan untuk memprediksi kinerja sistem yang dibangun ataupun dikembangkan. Dengan melakukan hal tersebut, maka kemungkinan kegagalan ataupun kerugian dalam memenuhi tujuan tertentu dapat

dikurangi. Maria berpendapat bahwa dengan melakukan simulasi, kinerja sistem dapat dioptimalkan tanpa menggunakan biaya yang besar karena dalam melakukan simulasi dapat dilakukan hanya menggunakan komputer

Erma Suryani dalam bukunya menjabarkan langkah-langkah dalam melakukan simulasi sebagai berikut [32]:

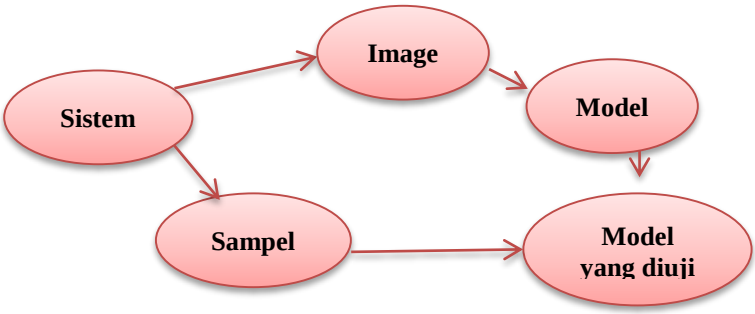
1. Pendefinisian sistem yang meliputi penetuan batasan sistem dan juga indentifikasi variabel yang signifikan.
2. Formulasi model yang meliputi perumusan hubungan antar komponen-komponen model.
3. Pengambilan data yang meliputi identifikasi data yang dperlukan sesuai dengan tujan pembuatan model.
4. Pembuatan model yang meliputi penyusunan model yang telah disesuaikan dengan jenis bahasa simulasi yang akan digunakan.
5. Verifikasi model yang meliputi pengecekan apakah model telah bebas dari error.
6. Validasi model yang meliputi proses pengujian terhadap kesesuaian model dengan sistem nyata.

Skenariosasi meliputi langkah-langkah yang dilakukan untuk memperbaiki kinerja sistem sesuai dengan keinginan dari peneliti.

2.9. *Pemodelan*

Model adalah contoh sederhana dari sistem dan menyerupai sifat – sifat sistem yang di pertimbangkan, tetapi tidak sama dengan sistem. Penyerdahanaan sistem sangat penting agar dapat di pelajari secara seksama. Model di

kembangkan dengan tujuan utama yang menyusun sistem dan interaksinya antara satu dengan yang lain [7]. Jadi pengembangan model adalah suatu pendekatan yang tersedia untuk mendapatkan pengetahuan yang layak akan sistem. Model berperan penting dalam pengembangan teori karena berfungsi sebagai konsep dasar yang menata rangkaian aturan yang digunakan untuk menggambarkan sistem. Penggunaan model sendiri sangat bermanfaat pada kehidupan sebenarnya, dengan adanya model ini sendiri penitili tidak harus menggunakan sistem yang actual secara asli sehingga menghambat proses analisis. Proses dari pembuatan model itu sendiri ditunjukkan pada gambar 2.1.



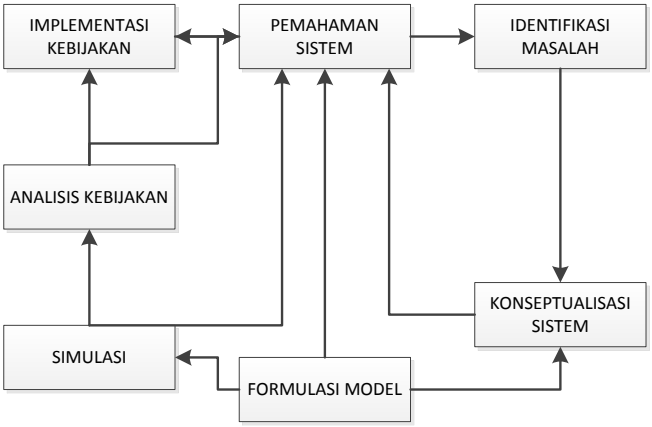
Gambar 2.1 Pembuatan Model [7]

2.10.Model Sistem Dinamik

Sistem Dinamik adalah konsep ilmu yang digagas oleh professor MIT (Masachussets Institute of Technology), Jay Forrester. Pada perkembangannya sistem dinamik yang berasal dari ilmu manajemen dan teori kontrol modern telah digunakan diberbagai disiplin ilmu seperti sosial,ekonomi, fisika, biologi dan lain-lain.Sterman dalam bukunya

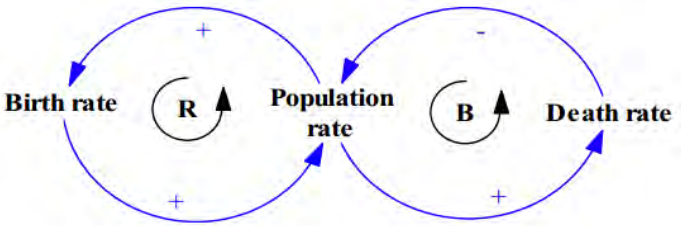
mengatakan bahwa sistem dinamik adalah sebuah perspektif dan seperangkat alat yang membuat kita dapat memahami struktur dan dinamika dari suatu sistem yang kompleks. [7]. Fokus dari sebuah studi mengenai sistem dinamik bukanlah pada sistem, tetapi pada sebuah permasalahan. Kelakuan dari sebuah sistem yang melewati waktu dan keputusan baru yang harus dibuat adalah tipe dari problem manajemen yang penting yang membutuhkan analis untuk menangani pokok persoalan bagaimana sebuah sistem memberi reaksi terhadap dorongan dinamik dan bagaimana reaksi tersebut membentuk kelakuannya dan yang akan mengubah kondisi yang akan datang juga.

Hubungan dan interaksi antar variabel dinyatakan dalam diagram kausatik. Tahapan Pengembangan Model Sistem Dinamik ditunjukkan oleh gambar 2.2:



Gambar 2.2 Pengembangan Model Sistem [32]

Dasar dalam pembuatan simulasi dengan menggunakan model sistem dinamik adalah hubungan sebab akibat yang berbentuk *close loop* yang menentukan sifat dari sistem. *Causal loop* memiliki dua jenis, yaitu positif dan negatif. Suatu *Causal loop* dinyatakan positif bila hubungan antar dua variabel menambah nilai untuk variabel lain. Sedangkan bila hubungan tersebut mengurangi variabel lain, maka *Causal loop* dinyatakan negatif. Untuk lebih jelasnya terlihat pada gambar 2.3 yang merupakan contoh dari *Causal Loop Diagram.*



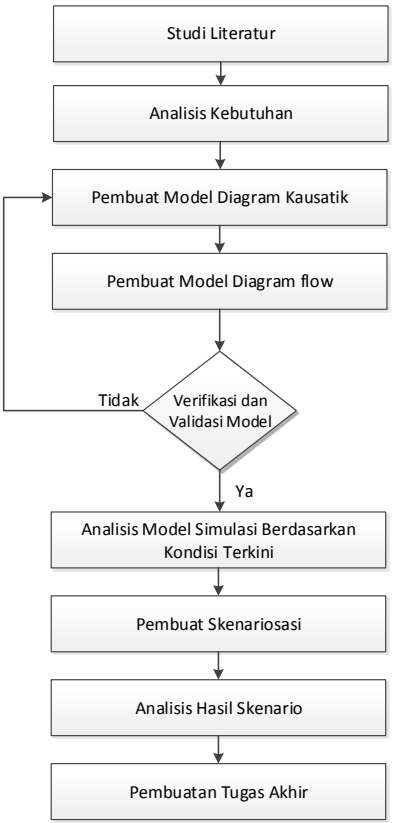
Gambar 2.3 Contoh Diagram causal loop [7]

Untuk mengetahui sifat dari suatu sistem, apakah positif atau negatif, bisa dilihat dari jumlah nilai *causal loop* – nya. Suatu sistem dikatakan bersifat positif apabila jumlah dari negatifnya adalah genap, sedangkan bila sifat negatifnya berjumlah ganjil maka sistem tersebut dikatakan ganjil. Tujuan dari *causal loop* ini adalah untuk menggambarkan pengaruh sebab akibat dari antar variabel sesuai dengan kehidupan yang sebenarnya [32].

Halaman ini sengaja dikosongkan

BAB 3
METODE PENGERJAAN TUGAS AKHIR

Pada bab ini akan diuraikan mengenai metodologi yang akan dilakukan oleh penulis dalam pembuatan tugas akhir. Metodologi juga digunakan sebagai panduan dalam pengerjaan tugas akhir agar terarah dan sistematis.



Gambar 3.1 Metodologi Penelitian

3.1 Studi Lapangan

Tahapan paling awal dalam pengerjaan tugas akhir adalah studi literatur. Dalam aktivitas ini, penulis akan dibantu dengan referensi dan berbagai studi literatur yang terkait dengan judul penulis yaitu **"Analisis Deteksi Risiko Insider Threat Secara Dini dengan Pendekatan Sistem Dinamik (Studi Kasus PT. XYZ)".**

Beberapa literatur yang dijadikan referensi oleh penulis adalah:

1. Suryani, E. (2005). *Pemodelan dan Simulasi.* Yogyakarta: Grha Ilmu.
2. Sterman, J. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World.* Homewood: McGraw-Hill.
3. S.-C. Yang and Y.-L. Wang, "Insider Threat Analysis of Case Based System Dynamics," *Advanced Computing: An International Journal,* vol. 2, no. 2, pp. 1-17, 2011.
4. P. Moore, A. M. David and M. L. Collins, "A System Dynamics Model for Investigating Early Detection of Insider Threat Risk," in *SystemDynamics.org*, 2013.
5. C. Melara, J. M. Sarriegui, J. J. Gonzales, A. Sawicka and D. L. Cooke, "A System Dynamics Model of an Insider Attack on an Information System," in *Proceedings of the 21st International Conference of the System Dynamics Society*, 2003.

3.2 Analisis Kebutuhan

Setelah dilakukannya studi literatur maka dimulailah analisis kebutuhan dimana peneliti akan mencari input berupa

data dan informasi. maka selanjutnya dilakukan analisis kebutuhan dimana pada tahap ini akan dianalisis kebutuhan faktor variabel-variabel yang mempengaruhi pembuatan model dari hasil pengumpulan data informasi. Dalam tahap ini, sistem yang akan dibuat juga didefinisikan dari variabel-variabel yang akan digunakan menjadi kategori *level, auxiliary, rate/flow, source and sink* , dan lain-lain. Tujuan analisis kebutuhan ini adalah untuk mengetahui gambaran yang jelas tentang kondisi kekinian PT. XYZ terkait dengan *insider threat*. Analisis kebutuhan penting untuk dilakukan karena dengan analisis kebutuhan peneliti dapat menentukan batasan dan mengidentifikasi variabel yang signifikan untuk membantu dalam pengambilan data yang dibutuhkan untuk fase selanjutnya yaitu pembuatan model diagram kausatik. Data yang dibutuhkan dari PT. XYZ diantaranya adalah:

a) Proses bisnis di PT XYZ
b) Permasalahan sekuritas TI di PT XYZ yang melibatkan *insider*
c) Faktor-faktor yang mengakibatkan *insider threat* berdasarkan referensi yang digunakan
d) Hasil wawancara dengan perwakilan pihak TI dan bagian personalia di PT XYZ (Lihat Lampiran A).
e) Data terkait kebebasan karyawan/*actual freedom*, tanda tingkah laku buruk karyawan/*behavioral precursors*,tanda penyalahgunaan teknologi informasi/ *technical precursors*, kebijakan sekuritas (*IT security policy*), dan investasi terkait sekuritas TI (*security investments*). Lihat Lampiran B.

3.3 Pembuatan Model diagram Kausatik

Model Kausatik dibuat dengan menggunakan *software Ventana Simulation (VENSIM)* setelah diketahui variabel-varibel mana yang berpengaruh yang nantinya akan membantu dalam proses pembuatan model diagram *flow*. Model diagram kausatik dibuat agar variabel-variabel yang berkaitan dengan sistem tidak terlewatkan dan lebih memudahkan dalam melakukan simulasi. Dalam pembuatan model diagram kausatik dibutuhkan data dan informasi yang telah diambil di tahap analisis kebutuhan.

3.4 Pembuatan Model Diagram *Flow*

Langkah selanjutnya adalah pembuatan model matematis, dengan acuan model diagram *flow* yang pada sebelumnya variabel-variabel sudah diklasifikasikan variabel mana saja yang termasuk ke dalam *level, rate atau flow, auxiliary*, dan klasifikasi yang lain. Setelah ditentukan dan terbentuk, selanjutnya dibuat model matematis yang dapat merumuskan hubungan dari variabel satu ke variabel lainnya menggunakan persamaan. Pada pembuatan model diagram *flow* diaplikasikan teori pendeteksi signal serta informasi-informasi yang didapatkan dari model diagram kausatik.

3.5 Verifikasi dan Validasi Model

Selanjutnya model diverifikasi dengan tujuan apakah model diagram *flow* yang telah dirancang telah sesuai dan tingkat error tidak melebihi batas yang ditentukan yaitu. Selanjutnya dilanjutkan dengan validasi model dengan tujuan agar model dapat berjalan sesuai dengan sistem yang ada, sehingga model

tersebut dapat dikatakan model sistem dinamik. Terdapat dua cara untuk menguji validitas dari model, yaitu:

a) Perbandingan Rata-Rata (*mean comparison)*

$$E1 = \frac{\left[\bar{S} - \bar{A}\right]}{\bar{A}} \quad \ldots (1)$$

$$\bar{S} = nilai\_rata - rata\_hasil\_simulasi$$

$$\bar{A} = nilai\_rata - rata\_data$$

Model dianggap valid bila E1 ≤ 5%

b) Perbandingan Variasi Amplitudo (% *error variance*)

$$E2 = \frac{|Ss - Sa|}{Sa} \quad \ldots (2)$$

Dimana:
S_s= Standar deviasi model
S_a = Standar deviasi data
Model dianggap valid bila E2 ≤ 30%

3.6 Analisis Model Simulasi Berdasarkan Kondisi Terkini

Dari model yang sudah valid kemudian akan dilakukan analisis terhadap *insider risk* berdasarkan kondisi saat ini di PT. XYZ. Nantinya hasil analisis ini akan digunakan sebagai acuan dalam membuat skenariosasi model sistem dinamik.

3.7 Pembuatan Skenariosasi Berdasarkan Model Sistem Dinamik

Selanjutnya pada tahap ini setelah model diagram *flow* diverifikasi dan divalidasi, maka tahapan selanjutnya adalah merancang skenario-skenario untuk memperbaiki kinerja sistem sesuai dengan objektif dan tujuan dari penelitian yaitu untuk meningkatkan sekuritas informasi dari insider threat secara dini pada perusahaan PT XYZ. Skenario yang akan dikembangkan adalah skenario untuk meminimalkan *insider risk*.

3.8 Analisis Hasil Skenario

Setelah pemodelan dan simulasi dilakukan, kemudian dilakukan analisis kepada terhadap skenario-skenario model. Dari hasil analisis yang dilakukan menghasilkan analisis berupa *Causes Strip Graph, Graph,* dan *Time Table* dibuatlah kesimpulan dari skenario yang dapat memberikan solusi terhadap studi kasus **"Analisis Risiko Insider Threat Secara Dini dengan Pendekatan Sistem Dinamik (Studi Kasus PT. XYZ)"** Pada tahapan ini akan didapatkan hasil analisis kebijakan yang diambil oleh PT. XYZ agar dapat meminimalisir *insider risk threat*.

3.9 Pembuatan Laporan Tugas Akhir

Tahapan terakhir yaitu menyusun laporan tugas akhir, yang dibuat dalam bentuk buku tugas akhir. Dalam buku ini diharapkan dapat memberikan manfaat sebagai referensi dan juga acuan penelitian dengan metode yang sejenis.

BAB 4
PENGUMPULAN DAN PENGOLAHAN DATA

Bab ini menjelaskan mengenai pembuatan model yang disesuaikan dengan sistem nyata-nya. Model tersebut nantinya akan digunakan untuk menyelesaikan permasalahn dalam tugas akhir dengan menggunakan bantuan aplikasi Ventana System (VENSIM).

4.1 Informasi masukan

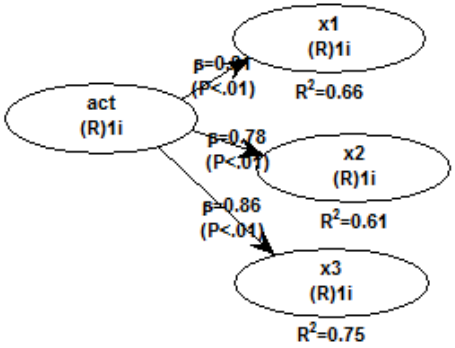
Data atau input yang diproses pada model simulasi ini didapatkan dari hasil wawancara dengan pihak TI dan observasi langsung untuk mengetahui sekuritas teknologi infromasi di PT XYZ. Selain itu wawancara tersebut juga untuk mendapatkan informasi berupa:

- Proses bisnis teknologi informasi di PT XYZ
- Permasalahan sekuritas TI di PT XYZ yang melibatkan *insider*
- Faktor-faktor yang mengakibatkan *insider threat* berdasarkan referensi yang digunakan
- Hasil wawancara dengan perwakilan pihak TI di PT XYZ(Lampiran A).
- Data terkait kebebasan karyawan/*actual freedom*, tanda tingkah laku burk karyawan/*behavioral precursors*,tanda penyalahgunaan teknologi informasi/ *technical precursors*, kebijakan sekuritas/*IT security policy*, dan investasi terkait sekuritas TI/*security investments* (Lampiran B).

4.2 Pengolahan Data Kebebasan Karyawan

Dalam melakukan pengolahan data kebebasan karyawan, digunakan data-data yang diolah dari sumber data dalam satu tahun periode (2012-2013). Data-data tersebut adalah data *firewall* log , *proxy* log, dan *action* log berupa *malicious software caught* atau software berbahaya yang ketahuan pada saat pengecekan rutin tiap bulannya(data terlampir di lampiran B). Dalam mengolah data kebebasan karyawan digunakan metode SEM-PLS yng merupakan sebuah pendekatan pemodelan kausal yang bertujuan untuk memaksimalkan variansi dari variabel laten criterion yang dapat dijelaskan oleh variabel laten predictor. Aplikasi dan metode ini digunakan karena SEM-PLS dapat bekerja secara efisien dengan ukuran sample yang kecil dan model yang kompleks. SEM-PLS dapat mengukur variabel model secara reflektif dan formatif tanpa menimbulkan permasalahan dalam mengidentifikasi data (normaslisasi). Pada gambar 4.1 dibawah ini terdapat hasil pengolahan variabel dengan menggunakan metode SEM-PLS diaplikasi warp PLS 4.0.

Variabel act = *Actual Freedom*
Variabel x1 = *Malicious Software Caught*
Variabel x2 = *Firewall log*
Variabel x3 = *Proxy* log



Gambar 4.1 Hasil pengolahan data kebebasan karyawan

Dari hasil pemodelan SEM-PLS pada gambar diatas, diketahui bahwa ketiga variabel reflektif yaitu x1,x2, dan x3 mempunyai nilai P Values < 0.1 yang berarti bahwa variabel tersebut signifikan terhadap variabel act. Setelah dilakukan pengecekan signifikasi dibuatlah persamaan antara ketiga variabel tersebut agar dapat digunakan dalam pemodelan sistem dinamik, persamaan tersebut dapat dilihat pada tabel persamaan 4.1 dibawah ini:

Act(Actual Freedom) = Firewall log*(0.78/2.4) + Malicious software caught*(0.81/2.4) + Proxy log*(0.86/2.4)

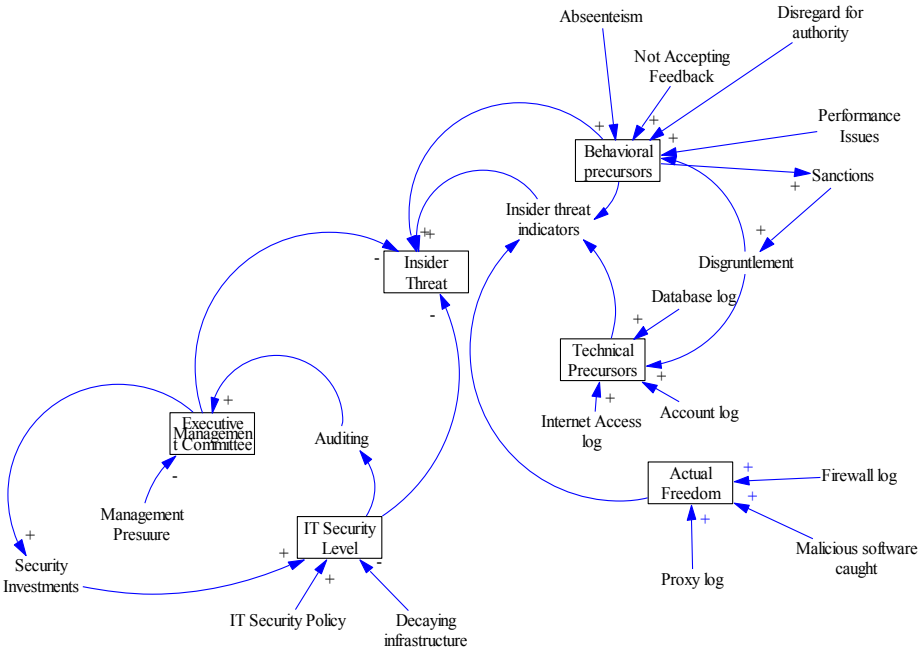
Persamaan 4.1 Kebebasan Karyawan

4.2. Pembuatan Model Konseptual

Pembuatan model konseptual atau model diagram kausatik. Langkah ini diperlukan untuk mengetahui

hubungan sebab akibat antar variabel yang telah didapatkan dari sumber, yaitu wawancara, data dari perusahaan, dan observasi langsung terkait *insider threat*.

Diagram kausatik *insider threat* meliputi identifikasi risiko insider threat , faktor yang menyebabkan insider threat (ditinjau dari literatur), dan variabel-variabel lain yang relevan dengan studi kasus ini. Pada gambar 4.2 dibawah ini dapat dilihat diagram kausatik risiko insider threat pada PT XYZ.



Gambar 4.2 Diagram kausatik insider threat di PT XYZ

Setelah membuat diagram kausatik, data masukan selanjutnya adalah hasil wawancara yang telah dilakukan pada bagian TI dan personalia PT XYZ. Berdasarkan hasil

wawancara terdapat tiga variabel utama yang mempengaruhi *insider threat*, yaitu kebebasan yang diharapkan oleh karyawan(*actual freedom*), faktor perilaku (*behavioral precursors*),dan faktor teknis(*technical precursors*). Selain itu terdapat juga variabel-variabel yang dapat mengurangi tingkat *insider threat* yaitu level sekuritas dari PT XYZ dan komitmen manajemen dalam meningkatkan sekuritas. Kebebasan yang diharapkan oleh karyawan berpengaruh positif terhadap peningkatan persentase insider threat di perusahaan. Variabel kebebasan yang diharapkan oleh karyawan juga dipengaruhi oleh berbagai variabel lain seperti software berbahaya yang terdeteksi di komputer karyawan (*malicious software caught*), *firewall log,* dan *proxy log*. Ketiga variabel tersebut mempunyai relasi positif dengan variabel *actual freedom*.

Faktor perilaku adalah salah satu indikator yang dapat menyebabkan ketidakpuasan dan menyebabkan organiasasi juga memberikan sanksi bagi karyawannya yang menyebabkan risiko ditempat kerja. Sanksi memang efektif untuk membuat jera karyawan akant tetapi juga mempunyai efek yang berbahaya, yaitu dapat meningkatkan ketidakpuasan karyawan. Secara garis besar hubungan antar variabel tersebut dapat dilihat sebagai berikut:

1) Berelasi positif : tingkat ketidak puasan karyawan, performa buruk karyawan, seringnya tidak masuk kerja, tidak mampu menerima masukan, dan ketidakpatuhan terhadap peraturan.
2) Berelasi negatif : waktu saat organisasi mengetahui karyawan tersebut dapat berdampak buruk dilingkungan kerja.

Faktor teknis merupakan indikator terakhir yang dapat menyebabkan naiknya tingkat insider threat di PT XYZ. Faktor teknis juga dipengaruhi oleh variabel-variabel yang dapat meningkatkan persentase dari insider threat. Secara garis besar hubungan antara variabel tersebut dapat dilihat sebagai berikut:

- Berelasi positif : log akun, log database, tingkat ketidakpuasan karyawan, dan log akses internet
- Berelasi negatif : Waktu manajemen menyadari karyawan melakukan hal buruk.

Selanjutnya adalah variabel-variabel utama yang dapat mengurangi tingkat *insider threat*,yaitu komitmen manajemen dan level sekuritas. Salah satu variabel tersebut adalah komitmen dari manajemen untuk meningkatkan sekuritas. Komitmen manajemen dipengaruhi secara positif oleh peningkatan komitmen yang merupakan informasi yang didapatkan dari hasil audit. Dari hasil audit tersebut perhatian manajemen terhadap sekuritas akan meningkat. Selanjutnya komitmen dari manajemen juga dapat berkurang, hal ini dikarenakan sekuritas yang ketat juga dapat membatasi keleluasaan dan juga membutuhkan investasi yang besar, oleh karena itulah terdapat tekanan sendiri dari manajemen untuk mengurangi komitmen yang dipengaruhi oleh waktu.

Level sekuritas di PT XYZ dipengaruhi positif oleh tiga variabel yaitu variabel kebijakan sekuritas, investasi sekuritas, dan peningkatan prosedur. Variabel kebijakan sekuritas dipengaruhi oleh waktu, dimana karyawan dan manajemen mempunyai kecenderungan untuk mengetatkan kebijakan sekuritas pada awal bulan sampai pertengahan bulan dan berkurang pada akhir bulan. Selanjutnya peningkatan

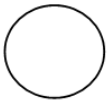
prosedur dipengaruhi secara positif oleh hasil audit dari level sekuritas di PT XYZ. Level sekuritas juga dipengaruhi negative oleh masa infrastruktur dimana infrastruktur tidak selamanya berada dalam kondisi prima.

4.3. Pemodelan Diagram *Flow* dan Asumsi model

Setelah memetakan diagram kausatik dan hubungan antar variabel, langkah selanjutnya yang dilakukan adalah membuat diagram *flow* dari model dasar. Pada tahap pembuatan model dasar ini terdapat 5 jenis variabel yang digunakan, yaitu:

1. **Auxiliary**

   Auxiliary merupakan variabel dinamis yang dapat dihitung dari variabel lain dalam satu periode waktu yang ditentukan.



Gambar 4.3 Model *Auxiliary*

2. **Level**

   Level merupakan variabel yang berisi persamaan akumulasi dari variabel rate.

Gambar 4.4 Model *Level*

3. **Rate**

   Rate merupakan nilai aliran masuk atau aliran keluar dari sebuah level

Gambar 4.5 Model *Rate*

4. Konstanta

Konstanta merupakan nilai tetap dan tidak berubah-ubah. Variabel ini tidak memiliki bentuk apapun, hanya berupa nama variabel itu sendiri.

Management
Pressure

Gambar 4.6 Model Konstanta

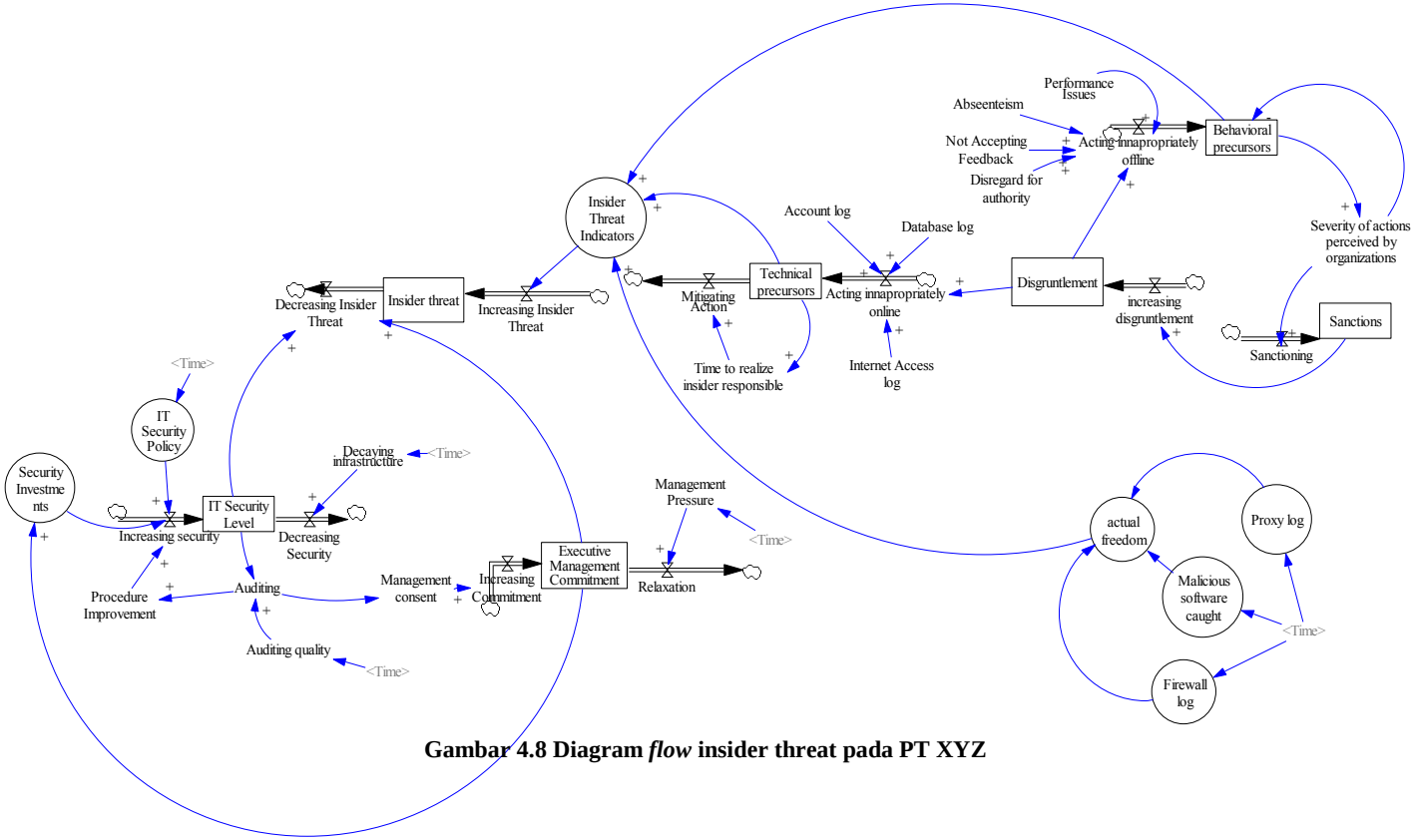
5. Variabel bayangan

Variabel bayangan merupakan suatu variabel yang tidak mempunyai nilai tetapi mempengaruhi nilai dari variabel lainnya.

<Time>

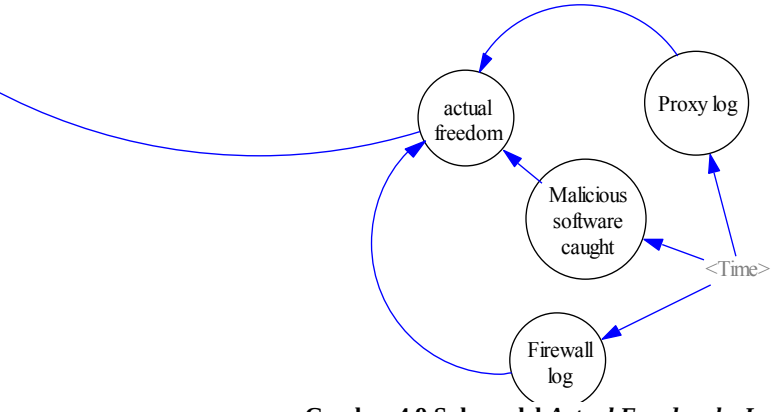
Gambar 4.7 Variabel bayangan

Berikut ini pada gambar 4.8 merupakan diagram *flow* dari base model insider threat di PT XYZ.



Gambar 4.8 Diagram *flow* insider threat pada PT XYZ

4.4.1. Sub Model Actual Freedom



Gambar 4.9 Sub model *Actual Freedom by Insider*

Sub model *Actual Freedom* merupakan sub model yang digunakan untuk mengetahui kebebasan karyawan dalam menggunakan teknologi informasi di PT XYZ .Variabel Actual freedom dibentuk dari tiga variabel yang mempunyai korelasi hubungan positif yaitu variabel *malicious software caught* , *proxy log*, dan , *firewall log*. Sub model ini terdiri dari 5 variabel, yaitu:

1. ***Time***

   Merupakan variabel yang melambangkan waktu simulasi. Variabel *time* bernilai antara 1-12 yang artinya waktu yang digunakan dalam simulasi berjumlah 12 bulan atau 1 tahun.

2. ***Actual Freedom***

   Merupakan variabel yang merepresentasikan kebebasan yang didapatkan oleh karyawan di perusahaan. *Actual*

freedom dipengaruhi oleh variabel *malicious software caught*, *firewall log* , dan *proxy log* . Persamaan variabel *actual freedom* didapatkan dari hasil pengolahan variabel dengan menggunakan PLS-SEM.

Actual Freedom = Firewall log(0.78/2.4) + Malicious software caught*(0.81/2.4) + Proxy log*(0.86/2.4)*

Persamaan 4.2 *Actual Freedom*

3. *Proxy Log*

Merupakan variabel *auxiliary* yang mempengaruhi bertambahnya nilai *Actual Freedom*. Nilai variabel *proxy log* didapatkan dari data yang didapatkan di PT XYZ.

Proxy Log = IF THEN ELSE (Time <=3 ,RANDOM UNIFORM(0.55, 0.6, 1), IF THEN ELSE (Time<=10, RANDOM UNIFORM (0.6, 0.65, 1), RANDOM UNIFORM (0.65, 0.72, 1)))

Persamaan 4.3 *Proxy Log*

4. *Malicious Software Caught*

Merupakan variabel *auxiliary* yang mempengaruhi bertambahnya nilai variabel *actual freedom*. Nilai *malicious software caught* didapatkan dari hasil pengambilan data di PT XYZ.

Malicious Software Caught = IF THEN ELSE (Time <=6, RANDOM UNIFORM (0.55, 0.65, 1), RANDOM UNIFORM (0.7, 0.73, 1))

Persamaan 4.4 ***Malicious Software Caught***

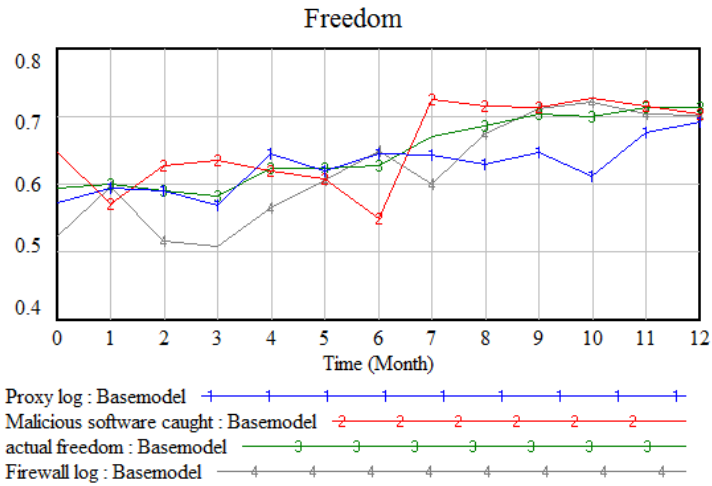
5. ***Firewall Log***

Merupakan variabel *auxiliary* yang mempengaruhi bertambahnya nilai variabel *actual freedom*. Nilai *Firewall log* didapatkan dari hasil pengambilan data di PT XYZ.

Firewall Log = IF THEN ELSE (Time <=4 , RANDOM UNIFORM (0.5, 0.6, 1), IF THEN ELSE (Time<=8, RANDOM UNIFORM (0.6, 0.7, 1), RANDOM UNIFORM (0.7, 0.73, 1)))

Persamaan 4.5 ***Firewall log***

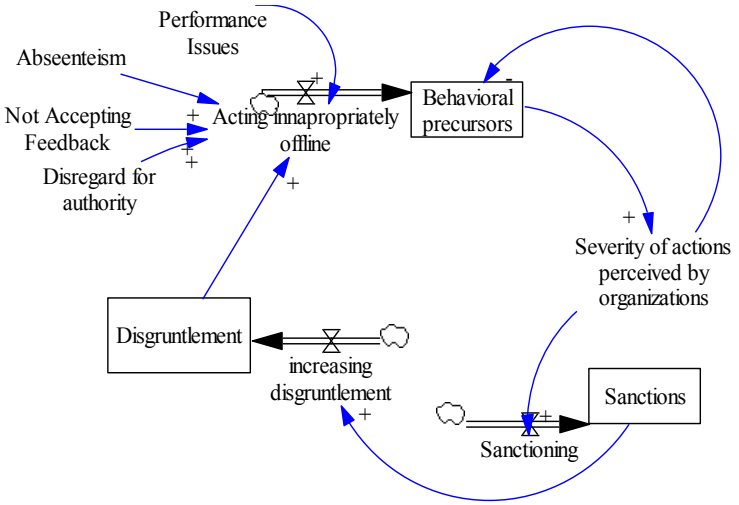
Hasil grafik dari variabel *actual freedom* dapat dilihat pada gambar 4.10 dibawah ini.



Gambar 4.10 Grafik sub model *actual freedom by insider*

Dari grafik tersebut dapat dilihat bahwa nilai awal dari *actual freedom* atau kebebasan yang didapatkan oleh karyawan adalah 60%, nilai ini cenderung stagnan dan hanya naik pada bulan empat, enam, delapan, dan sebelas. Nilai *actual freedom* dipengaruhi oleh tiga variabel yaitu *proxy log* (garis warna biru), *malicious software caught* (warna merah), dan *firewall log* (garis warna abu-abu). Nilai Actual freedom pada tugas akhir ini merepresentasikan bagaimana karyawan menggunakan kebebasannya dalam perusahaan. PT XYZ sendiri mengimplementasikan kebijakan kebebasan yang tidak mengekang karyawan tetapi mempunyai batasan di nilai 75%.

4.4.2. Sub Model Behavioral precursors



Gambar 4.11 Sub model *behavioral precursors*

Sub model *behavioral precursors* merupakan submodel yang digunakan untuk mengetahui tanda-tanda tingkah laku yang tidak baik oleh karyawan yang nantinya bisa menjurus kepada pemberian sanksi hingga ketidakpuasan karyawan. Dalam sub model ini variabel *time* tidak dibahas karena sudah dibahas dalam sub model sebelumya.Sub model *behavioral precursors* terdiri dari 11 variabel, yaitu:

1. ***Disregard for Authority***

   Disregard for authority atau tidak mematuhi aturan perusahaan merupakan konstanta yang nilainya menjadi masukan bagi variabel *rate acting innapropriately offline.* Nilai konstanta ini didapatkan dari hasil

wawancara pada PT XYZ yaitu diantara 1% hingga 5% pada tiap bulannya.

Disregard for authority = RANDOM UNIFORM (0.01, 0.05, 1)

Persamaan 4.6 ***Disregard for authority***

2. *Not Accepting Feedback*

Not accepting feedback atau tidak mau menerima masukan merupakan konstanta yang nilainya menjadi masukan bagi variabel *rate acting innapropriately offline.* Nilai konstanta ini didapatkan dari hasil wawancara pada PT XYZ yaitu diantara 1% hingga 5% pada tiap bulannya.

Not Accepting Feedback = RANDOM UNIFORM (0.01, 0.05, 1)

Persamaan 4.7 ***Not accepting feedback***

3. *Abseenteism*

Abseenteism atau tidak masuk kerja merupakan konstanta yang nilainya menjadi masukan bagi variabel *rate acting innapropriately offline.* Nilai konstanta ini didapatkan dari hasil wawancara pada PT XYZ yaitu diantara 1% hingga 5% pada tiap bulannya.

Abseenteism = RANDOM UNIFORM (0.01, 0.05, 1)

Persamaan 4.8 ***Abseenteism***

4. *Performance Issues*

Performance Issues atau isu performa kerja merupakan konstanta yang nilainya menjadi masukan bagi variabel *rate acting innapropriately offline.* Nilai konstanta ini didapatkan dari hasil wawancara pada PT XYZ yaitu diantara 1% hingga 5% pada tiap bulannya.

Performance Issues = RANDOM UNIFORM (0.01, 0.05, 1)

Persamaan 4.9 *Performance issues*

5. *Acting innapropriately Offline*

Merupakan variabel *rate* yang didapatkan dari penjumlahan antara variabel *performance issues*, *abseenteism*, *not accepting feedback*, *disregard for authority*, dan *disgruntlement*.

Acting Innapropriately Offline = Abseenteism + Disgruntlement + Disregard for authority + Not Accepting Feedback + Performance Issues

Persamaan 4.10 *Acting innapropriately offline*

6. *Behavioral Precursors*

Behavioral precursors adalah variabel *level* yang merupakan tanda-tanda karyawan bertingkah laku buruk. Nilai *behavioral precursors* didapatkan dari total nilai *acting innapropriately offline*. Selain itu nilai *behavioral precursors* juga dipengaruhi oleh bagaimana perusahaan merespon risiko dari dampak risikot tersebut. Apabila

risiko tersebut termasuk risiko yang rendah maka perusahaan tidak memitigasi dampak risiko tersebut, tetapi apabila risiko tersebut termasuk risiko sedang, dan tinggi maka perusahaan akan mencoba untuk mengurangi nilai risiko tersebut.

IF THEN ELSE (Severity of actions perceived by organizations=1, Acting innapropriately offline, IF THEN ELSE (Severity of actions perceived by organizations=2 , Acting innapropriately offline-0.1, Acting innapropriately offline-0.3))

Persamaan 4.11 ***Behavioral precursors***

Initial value= 0.3

7. Severity of Actions Perceived by Organizations

Variabel *auxiliary* ini merupakan variabel yang dapat diartikan sebagai resiko kerugian yang ditimbulkan dari tindakan buruk karyawan bagi organisasi. Nilai variabel *Severity of actions perceived by Organizations* didapatkan dari hasil nilai variabel *behavioral precursors*, apabila nilai tersebut melebihi batas yang ditentukan oleh organisasi maka organisasi telah menganggap tindakan yang dilakukan oleh karyawan sudah merugikan. Nilai variabel ini juga mempengaruhi variabel *behavioral precursors* secara negatif.

Severity of actions perceived by Organizations = IF THEN ELSE (Behavioral precursors >= 0.6, 3, IF THEN ELSE (Behavioral precursors >= 0.4, 2, 1))

Persamaan 4.12 ***Severity of actions perceived by organizations***

8. *Sanctioning*

Sanctioning adalah variabel *rate* yang berarti sanksi atau hukuman. Nilai variabel *Sanctioning* didapatkan dari nilai variabel *severity of actions perceived by organizations*.

Sanctioning = severity of actions perceived by organizations.

Persamaan 4.13 ***Sanctioning***

9. *Sanction*

Sanksi atau *Sanctions* merupakan variabel *level* yang didapatkan dari variabel *sanctioning* Variabel *sanctions* berfungsi untuk memberikan poin pada karyawan dimana poin tersebut merepresentasikan hukuman yang akan diberikan pada karyawan.

Sanction = Sanctioning

Persamaan 4.14 ***Sanction***

Initial value= 0

10. Increasing Disgruntlement

Merupakan variabel *rate* yang nilainya merupakan masukan positif terhadap variabel *level disgruntlement*. Variabel ini dipengaruhi oleh variabel *sanctions*. Nilai dari *Increasing disgruntlement* juga didapatkan dari seberapa berat sanksi yang didapatkan oleh karyawan dimana dibagi menjadi tiga sanksi yaitu sanksi ringan (teguran), sanksi sedang (surat evaluasi), dan sanksi berat (pemotongan gaji).

Increasing Disgruntlement = IF THEN ELSE(Sanctions<=6 , 0 , IF THEN ELSE(Sanctions<=15 ,0.025 , 0.05))

Persamaan 4.15 *Increasing Disgruntlement*

11. Disgruntlement

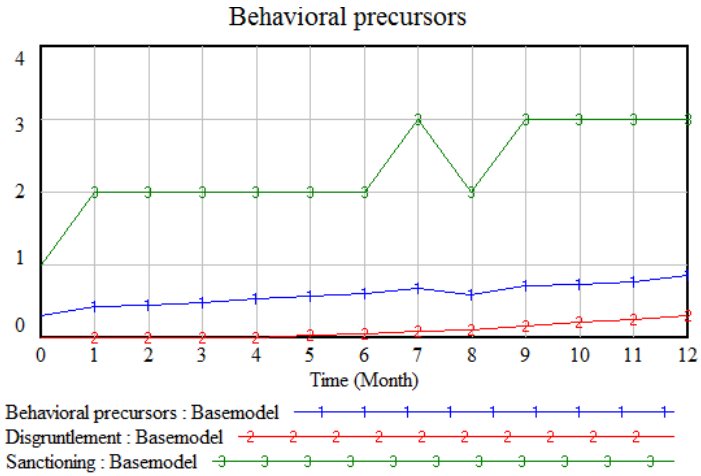
Merupakan variabel *level* yang menandakan ketidakpuasaan karyawan di perusahaan. Nilai dari *disgruntlement* didapatkan dari variabel *rate increasing disgruntlement*. Disgruntlement mempunyai nilai awal/*initial value* sebesar 0 dikarenakan asumsi dari PT XYZ dimana tidak ada karyawan yang tidak puas.

Disgruntlement = increasing disgruntlement

Persamaan 4.16 Disgruntlement

Initial Value = 0

Hasil grafik dari variabel *behavioral precursors* terkait hubungannya dengan variabel yang berelasi dapat dilihat pada gambar 4.12 dibawah ini:

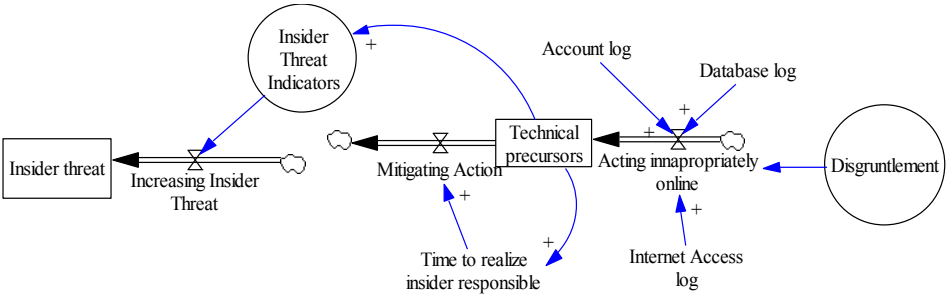


Gambar 4.12 Grafik Behavioral precursors

Dari grafik diatas dapat dilihat bahwa terdapat 3 variabel yaitu *behavioral precursors, disgruntlement,* dan *sanctioning*. Variabel *behavioral precursors* dilukiskan pada garis tersebut dengan warna biru dengan nilai awal 30% sesuai yang digambarkan oleh PT XYZ, dimana sampai saat ini rata-rata tanda-tanda karyawan yang berkelakukan buruk tersebut masih dibawah 50% dan hanya sekitar 30%. Berikutnya gambar tersebut akan naik diiringi dengan naiknya variabel *disgruntlement* yang dilambangkan dengan garis merah. *Disgruntlement* mencapai puncak tertinggi pada bulan 12, hal ini menyebabkan perusahaan menerima risiko dan akibat dari tanda-tanda perlakukan buruk dari karyawan, sehingga karyawan yang melakukan perlakuan buruk dan

mengganggu iklim kerja perlu dikenakan sanksi. Lambang sanctioning ditunjukkan dengan garis warna hijau dimana pada bulan 5 dimulailah perusahaan memberikan sanksi (ditunjukkan dari yang sebelumnya merupakan angka 1 berubah menjadi 2 dan 3) pada karyawannya yang berkelakukan buruk. Sejak dimulainya sanksi itulah variabel *behavioral precursors* mulai berkurang secara perlahan akan tetapi dikarenakan karyawan tersebut tidak puas sehingga nilai *behavioral precursors* tetap tinggi dan naik seiring dengan berjalannya waktu. Perlu diketahui juga bahwa ketidakpuasan karyawan tidak hanya bisa diselesaikan dengan memberi sanksi saja, karena sanksi hanya akan mengurangi tindakan buruk dari karyawan dan tidak mengurangi ketidakpuasaan dari karyawan atau malah dapat menambah nilai *disgruntlement* seperti ditunjukkan pada grafik diatas.

4.4.3. Sub Model Technical Precursors



Gambar 4.13 Sub model *Technical Precursors*

Sub model *technical precursors* merupakan submodel yang digunakan untuk mengetahui tanda-tanda tingkah laku yang tidak baik oleh karyawan yang dilakukan dalam ranah penggunaan teknologi informasi dan sistem informasi yang

nantinya bisa menjurus meningkatknya tingkat risiko insider threat di perusahaan. Dalam sub model ini variabel *disgruntlement* dan variabel *time* tidak dibahas karena sudah dibahas dalam sub model sebelumya.Sub model *behavioral precursors* terdiri dari 8 variabel, yaitu:

1. ***Database Log***

   Database log atau catatan penggunaan database oleh karyawan merupakan konstanta yang nilainya menjadi masukan bagi variabel *rate acting innapropriately omline.* Nilai konstanta ini didapatkan dari hasil wawancara pada PT XYZ yaitu diantara 1% hingga 5% pada tiap bulannya.

   Database log = RANDOM UNIFORM (0.01 , 0.05, 1)

   Persamaan 4.17 ***Database Log***

2. ***Account Log***

   Account log atau catatan penggunaan akun oleh karyawan merupakan konstanta yang nilainya menjadi masukan bagi variabel *rate acting innapropriately omline.* Nilai konstanta ini didapatkan dari hasil wawancara pada PT XYZ yaitu diantara 1% hingga 5% pada tiap bulannya.

   Account log = RANDOM UNIFORM (0.01, 0.05, 1)

   Persamaan 4.18 ***Account Log***

3. ***Internet Access Log***

Internet access log atau catatan penggunaan internet oleh karyawan merupakan konstanta yang nilainya menjadi masukan bagi variabel *rate acting innapropriately omline.* Nilai konstanta ini didapatkan dari hasil wawancara pada PT XYZ yaitu diantara 1% hingga 5% pada tiap bulannya.

Internet access log = RANDOM UNIFORM (0.01, 0.05, 1)

Persamaan 4.19 ***Internet Access Log***

4. ***Time to Realize Insider Responsible***

Time to realize insider responsible atau waktu dimana perusahaan mengetahui kerusakan yang dilakukan oleh karyawan pada aset teknologi informasi dan sistem informasi. Nilai variabel ini didapatkan dari hasil wawancara , dalam skala persentase untuk menunjukkan upaya perusahaan dalam meningkatkan nilai *mitigating action*, atau aksi mitigasi.

Time to realize insider responsible = IF THEN ELSE (Technical precursors>=0.7, RANDOM UNIFORM (0.3, 0.4, 1),IF THEN ELSE (Technical precursors>=0.5, RANDOM UNIFORM (0.2, 0.3, 1), 0))

Persamaan 4.20 ***Time to Realize Insider Responsible***

5. ***Acting Innapropriately Online***

Merupakan variabel *rate* hasil penjumlahan dari tiga variabel konstanta dan satu variabel *auxiliary*, ketiga variabel tersebut adalah *disgruntlement*,*database log*,*account log*, dan *internet access log*. Variabel *acting innapropriately online* digunakan untuk meningkatkan tingkat *technical precursors* dari karyawan.

Acting innapropriately online = Account log + Disgruntlement + Database log + Internet Access log

Persamaan 4.21 ***Acting Innapropriately Online***

6. ***Mitigating Action***

Mitigating Action adalah aksi yang dilakukan perusaaan untuk mengurangi *technical precursors* dari perusahaan. Variabel ini dipengaruhi oleh variabel *time to realize insider responsible* dan variabel *time*. Nilai dari variabel ini dipengaruhi sekali oleh waktu dimana, sebenarnya perusahaan sudah mempunyai standar yang dilakukan setiap bulan untuk mengurangi laju *technical precursors*, akan tetapi aksi itu kurang maksimal apabila benar-benar belum terjadi permasalahan teknologi informasi dan sistem informasi di PT XYZ. Nilai *mitigating action* apabila

Mitigating Action = Time to realize insider responsible

Persamaan 4.22 ***Mitigating Action***

7. ***Technical Precursors***

Technical precursors merupakan variabel *level* yang nilainya merupakan hasil pengurangan dari dua variabel *rate* antara lain *acting innapropriately online* dan *mitigating action*.

Technical Precursors = Acting innapropriately online - Mitigating Action

Persamaan 4.23 ***Technical Precursors***

Initial Value = 0.4

Nilai awal dari variabel didapatkan dari hasil wawancara dimana dalam bulan awal ditemukan terdapat 40% tingkat tanda-tanda pelanggaran dari sisi teknis (teknologi informasi dan sistem informasi).

8. ***Insider Threat Indicators***

Variabel ini merupakan variabel *auxiliary* yang didapatkan dari rata-rata jumlah tiga variabel yaitu *technical precursors*, *behavioral precursors*, dan *actual freedom*.

Insider Threat Indicators = (Behavioral precursors + actual freedom + Technical precursors)/3

Persamaan 4.24 ***Insider Threat Indicators***

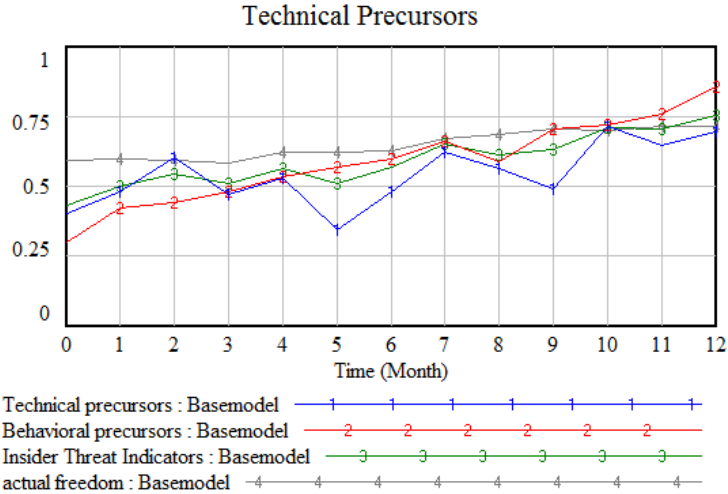
9. ***Increasing Insider Threat***

Increasing insider threat merupakan variabel *rate* yang nilainya didapatkan dari variabel *insider threat indicators*.

Increasing Insider Threat = Insider Threat Indicators

Persamaan 4.25 *Increasing Insider Threat*

Hasil grafik dari variabel *technical precursors* terkait hubungannya dengan variabel yang berelasi dapat dilihat pada gambar 4.14 dibawah ini.

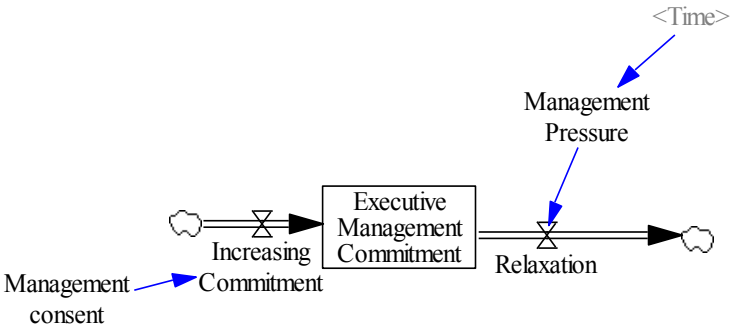


Gambar 4.14 Grafik sub model *technical precursors*

Pada grafik diatas terdapat 3 variabel yaitu *technical precursors* yang digambarkan dengan warna biru, *behavioral precursors* yang digambarkan dengan warna merah, *insider threat indicators* digambarkan dengan warna hijau, dan *actual*

freedom digambarkan dengan warna abu-abu. Variabel *technical precursors* mempunyai nilai awal sebesar 40% atau 0.4 sesuai dengan hasil wawancara yang didapatkan di PT XYZ. Variabel *technical precursors* dan variabel *behavioral precursors* pada grafik diatas sangat mempengaruhi variabel *insider threat indicators* dikarenakan nilai variabel tersebut hampir sama. Variabel *actual freedom*, disini mempunyai nilai awal yang tinggi yaitu sebesar 60%.

4.4.4. Sub Model Executive Management Commitment



Gambar 4.15 Sub Model *Executive Management Commitment*

Sub model *Executive management commitment* merupakan submodel yang digunakan untuk mengurangi tingkat *insider* threat di PT XYZ. Pada sub model *executive management commitment* dijelaskan bagaimana pengaruh komitmen manajemen PT XYZ untuk mengurangi tingkat *insider threat* di perusahaan, terdapat beberapa variabel yang tidak dijelaskan kembali dalam sub model ini yaitu variabel *time*,dikarenakan sudah dijelaskan pada bagian sub model sebelumnya. Sub model *IT security level* terdiri dari 5 variabel, yaitu:

1. ***Management Consent***

   Variabel ini merupakan variabel constant yang masukannya didapatkan dari *variabel auditing*. *Management Consent* merupakan persetujuan dari manajemen untuk bersama-sama meningkatkan komitmen dalam sekuritas berdasarkan hasil auditing yang dilakukan. Perumusan dari Variabel *management consent* dapat dilihat pada persamaan dibawah ini. Nilai dari variabel *management consent* didapatkan dari bobot tengah nilai audit [28].

$$Management\ Consent = Auditing/2$$

Persamaan 4.26 ***Management Consent***

2. ***Increasing Commitment***

   Variabel *increasing commitment* merupakan variabel *rate* yang bertujuan untuk meningkatkan laju variabel *executive management commitment*. Variabel ini dipengaruhi oleh variabel *management consent*.

$$Increasing\ Commitment = Management\ Consent$$

Persamaan 4.27 ***Increasing Commitment***

3. ***Management Pressure***

   Tekanan manajemen atau *management pressure* merupakan variabel konstanta yang dapat mempengaruhi nilai variabel *relaxation*. Variabel ini mengekspresikan tekanan manajemen dalam menjalakan komitmen untuk

meningkatkan level sekuritas. Terdapat banyak faktor yang mempengaruhi hal tersebut seperti faktor finansial dan faktor kebebasan. Nilai *management pressure* dipengaruhi oleh waktu dimana pada waktu-waktu (variabel *time*) tertentu nilainya dapat berubah-ubah, dimana dari hasil wawancara terdapat waktu-waktu dimana perusahaan lebih rileks atau menjalani masa *relaxation*.

Management Pressure = IF THEN ELSE (Time <= 5, RANDOM UNIFORM (0.2, 0.3, 1), IF THEN ELSE (Time <=7, RANDOM UNIFORM (0.2, 0.4, 1), RANDOM UNIFORM (0.2, 0.3, 1)))

Persamaan 4.28 ***Management Pressure***

4. ***Relaxation***

Relaxation merupakan variabel *rate* yang nilainya dipengaruhi oleh variabel *management pressure*. Variabel ini mempengaruhi laju keluar atau mengurangi nilai variabel *executive management commitment*.

Relaxation = Management Pressure

Persamaan 4.29 ***Relaxation***

5. ***Executive Managament Commitment***

Variabel *executive management commitment* merupakan variabel jenis *level* yang nilai masukannya dipengaruhi oleh dua variabel rate yaitu *increasing commitment* dan

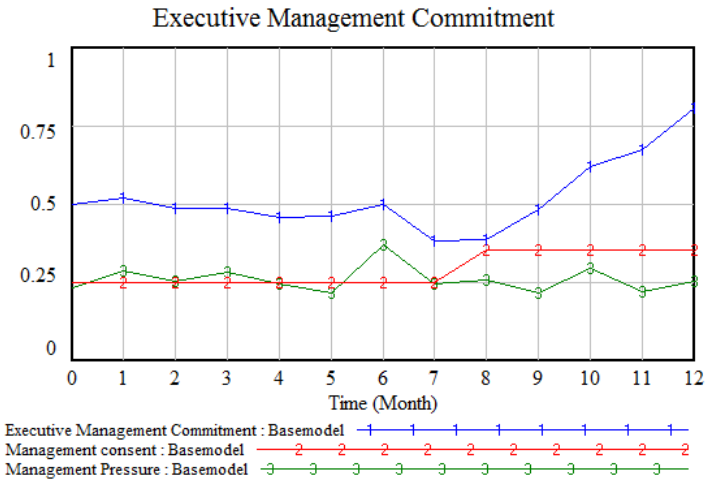
relaxation. Variabel ini juga mempunyai nilai awal atau *initial value*.

Executive Management Commitment = Increasing Commitment-Relaxation

Persamaan 4.30 ***Executive Management Commitment***

Initial Value = 0.5

Hasil grafik dari sub model *executive management commitment* dapat dilihat pada gambar 4.16 dibawah ini.

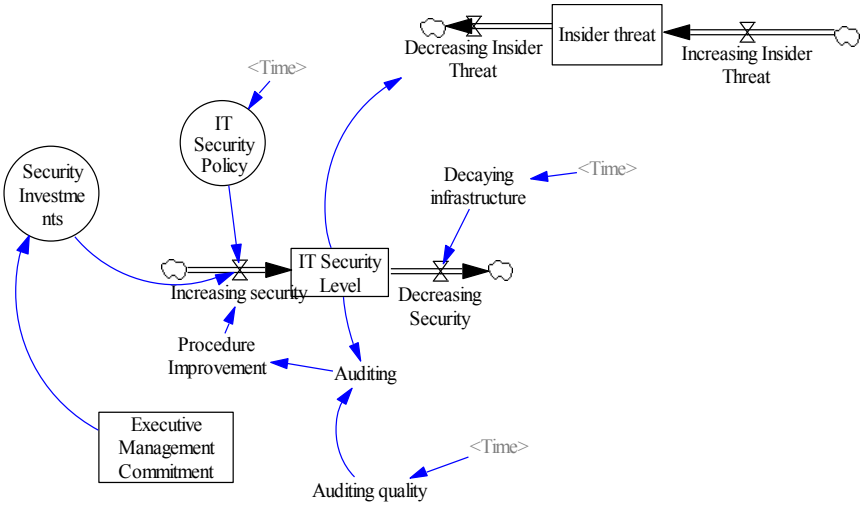


Gambar 4.16 Grafik submodel ***executive management commitment***

Dari grafik diatas dapat dilihat terdapat tiga garis yang mempunyai 3 warna yang berbeda yaitu biru, merah, dan hijau secara berurutan. Ketiga garis tersebut melambangkan

variabel *executive management commitment, management consent*, dan *management pressure*. Variabel *executive management commitment* pada gambar tersebut dipengaruhi oleh dua variabel *management consent* dan *management pressure*. Dapat dilihat pada bulan 8 hingga bulan 12 terjadi kenaikan nilai *management consent* yang menyebabkan nilai *executive management commitment* meningkat. Ditambah lagi dengan *variabel management pressure* yang nilainya berkurang atau turun secara signifikan. Hal inilah yang menyebabkan variabel *executive management commitment* naik pada bulan-bulan terakhir yaitu pada bulan 9 sampai dengan bulan 12.

4.4.5. Sub Model IT Security Level



Gambar 4.17 Submodel *IT Security Level*

Sub model *IT security level* merupakan submodel yang digunakan untuk mengurangi tingkat *insider* threat di PT

XYZ. Pada sub model *IT security level*, terdapat beberapa variabel yang tidak dijelaskan kembali yaitu variabel *time* dan *increasing insider threat,*dikarenakan sudah dijelaskan pada bagian sub model sebelumnya. Sub model *IT security level* terdiri dari 12 variabel, yaitu:

1. ***Security Investments***

   Security Invesments merupakan variabel *auxiliary* yang menjelaskan seberapa besar manajemen menginvestasikan uangnya kepada sekuritas dalam bidang TI. Variabel ini sangat dipengaruhi oleh variabel *level executive management commitment*, dimana semakin besar komitmen manajemen maka investasi sekuritas akan semakin besar pula.

   Security Investments = IF THEN ELSE (Executive Management Commitment > 0.7, RANDOM UNIFORM (7.3e+006 , 8.3e+006, 1) , IF THEN ELSE (Executive Management Commitment > 0.5 , RANDOM UNIFORM (4.8e+006, 5.8e+006 , 1), RANDOM UNIFORM (3.1e+006, 4.1e+006 , 1)))

   Persamaan 4.31 *Security Investments*

2. ***Auditing Quality***

   Auditing quality atau kualidas audit merupakan variabel konstanta yang dipengaruhi oleh waktu/*time,*dimana sesuai dengan hasil wawancara terdapat waktu dimana nilai kualitas audit bernilai sebesar 0.3 atau 0.6 . Variabel ini merupakan variabel yang dapat mempengaruhi nilai *variabel auditing*.

Auditing Quality = IF THEN ELSE (Time<8, 0.3 ,0.6)

Persamaan 4.32 ***Auditing quality***

3. ***Auditing***

Variabel ini merupakan *variabel auxiliary* yang juga masukannya dipengaruhi oleh 2 variabel yaitu variabel *IT security level* dan *auditing quality*. Variabel ini mempengaruhi nilai dari variabel *Procedure Improvement*.

Auditing = IF THEN ELSE (IT Security Level>=0.7, Auditing quality + 0.1, IF THEN ELSE (IT Security Level >= 0.5, Auditing quality + 0.2 , Auditing quality + 0.3))

Persamaan 4.33 Auditing

4. ***Procedure Improvement***

Variabel ini merupakan variabel constant yang masukannya didapatkan dari *variabel auditing*. *Procedure improvement* merupakan hasil dari audit yang dapat diimplementasikan sehingga dapat meningkatkan nilai level sekuritas TI. Perumusan dari Variabel *Procedure improvement* dapat dilihat pada persamaan 4.34 dibawah ini.

Procedure Improvement = Auditing/2

Persamaan 4.34 ***Procedure Improvement***

5. ***IT Security Policy***

IT security policy merupakan variabel *auxiliary* yang berarti kebijakan sekuritas di perusahaan. Kebijakan sekuritas pada PT XYZ memang selalu ditegakkan tetapi tidak sepenuhnya dipatuhi oleh karyawan dan hal tersebut dipengaruhi oleh waktu.

IT Security Policy = IF THEN ELSE (Time <7 , RANDOM UNIFORM (0.3, 0.4, 1), IF THEN ELSE (Time = 11:OR: Time=12, RANDOM UNIFORM (0.2, 0.3, 1), RANDOM UNIFORM (0.4 , 0.5, 1)))

Persamaan 4.35 ***IT Security Policy***

6. ***Increasing Security***

Increasing security merupakan variabel dengan jenis *rate*. Variabel ini dipengaruhi oleh variabel *IT security policy*, *procedure improvement*, dan *security investments*. Nilai persamaan variabel *increasing security* didapatkan dari hasil rata-rata penambahan variabel *IT Security Policy* dan variabel *procedure improvement* dan juga proporsi dari nilai variabel *security investments* yang ditentukan oleh manajemen.

Increasing Security = IF THEN ELSE (Security Investments>7e+006, 0.15 + (Procedure Improvement+IT Security Policy)/2, IF THEN ELSE (Security Investments>5e+006, 0.1 + (Procedure Improvement+IT Security Policy)/2, IF THEN ELSE (Security Investments >3e+006, 0.075 + (Procedure Improvement + IT Security Policy)/2, 0.05 + (Procedure Improvement + IT Security Policy)/2)))

Persamaan 4.36 ***Increasing Security***

7. ***Decaying Infrastructure***

Infrastruktur yang memburuk atau *decaying infrastructure* merupakan variabel konstanta yang dapat mempengaruhi nilai variabel *decreasing security*. Variabel ini mengekspresikan kerusakan atau waktu rusak yang diakibatkan Faktor yang mempengaruhi variabel *decaying infrastructure* adalah variabel *time*. Nilai variabel *decaying infrastructure* dipengaruhi nilainya dapat berubah-rubah sesuai dengan waktu yang sumbernya didapatkan dari hasil wawancara tentang waktu-waktu tertentu dimana infrastruktur TI sering rusak. Nilai dan persamaan dari *decaying infrastructure* dapat dilihat pada persamaan dibawah ini.

Decaying Infrastructure = IF THEN ELSE (Time<8, RANDOM UNIFORM (0.3, 0.4, 1), IF THEN ELSE (Time<4, RANDOM UNIFORM (0.2, 0.3, 1), RANDOM UNIFORM (0.4, 0.5, 1)))

Persamaan 4.37 ***Decaying infrastructure***

8. ***Decreasing Security***

Decreasing security merupakan variabel dengan jenis *rate*. Variabel ini dipengaruhi oleh variabel *Decaying infrastructure*.

Decreasing Security = Decaying infrastructure

Persamaan 4.38 ***Decreasing Security***

9. ***IT Security Level***

Variabel *IT Security level* atau level sekuritas TI merupakan variabel jenis *level* yang nilai masukannya dipengaruhi oleh dua variabel rate yaitu *increasing security* dan *decreasing security*. Variabel ini juga mempunyai nilai awal atau *initial value* .

IT Security Level= Increasing security-Decreasing Security

Persamaan 4.39 ***IT Security Level***

Initial Value= 0.3

10. ***Decreasing Insider Threat***

Decreasing Insider Threat merupakan variabel dengan jenis *rate*. Variabel ini dipengaruhi oleh dua variabel *level* yaitu variabel *executive management commitment* dan *IT security level*.

IT Security Level= Increasing security - Decreasing Security

Persamaan 4.40 ***Decreasing Insider Threat***

11. ***Insider Threat***

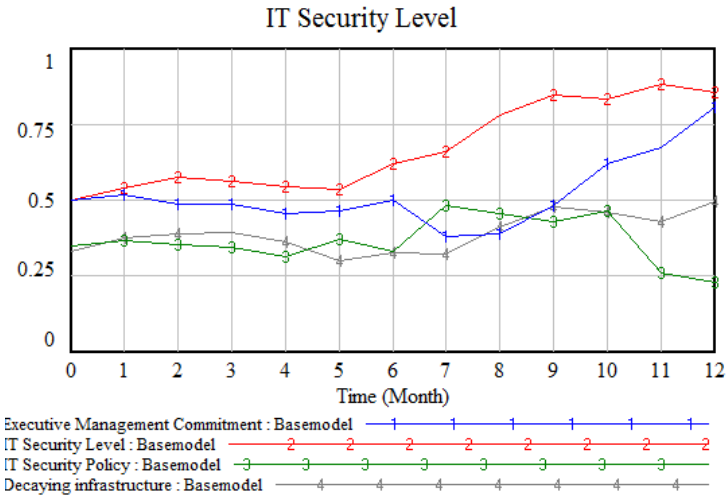
Insider Threat merupakan variabel dengan jenis *level*. Variabel ini adalah variabel utama yang menjadi tujuan dibuatnya pemodelan.Menurut hasil wawancara ,apabila nilai *insider threat* telah melebihi 60% maka PT XYZ perlu waspada terhadap serangan dari *insider*.

Insider Threat= Increasing Insider Threat- Decreasing Insider Threat

Persamaan 4.41 ***Insider Threat***

Initial Value= 0.2

Hasil grafik dari sub model *IT security* level dapat dilihat pada gambar 4.18 dibawah ini.

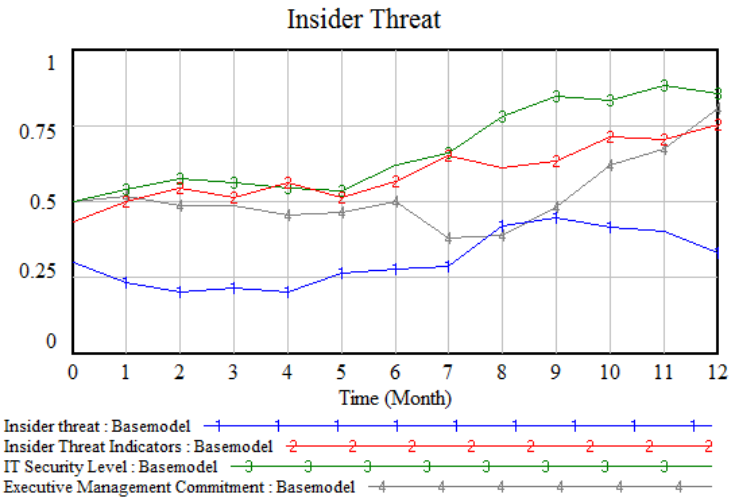


Gambar 4.18 Grafik submodel *IT security level*

Grafik diatas menunjukkan hubungan antara keempat variabel yaitu *executive management commitment*(garis warna biru), *IT security level* (garis warna merah), *IT security policy* (garis warna hijau), dan *decaying infrastructure* (garis warna abu-abu). Pada grafik diatas dapat dilihat bahwa nilai variabel *IT security level* sangat dipengaruhi oleh variabel *executive management commitment* atau komitmen manajemen. Selain variabel *executive management commitment*, *variabel IT security policy* juga berpengaruh terhadap variabel *IT security level*. Variabel *executive management commitment* mulai naik nilanya pada bulan 9 hingga bulan 12,, hal inilah yang menyebabkan variabel *IT Security level* tetap mempunyai nilai yang tinggi di bulan-bulan terakhir.

Selanjutnya terdapat model grafik secara keseluruhan

yaitu grafik model *insider threat*. Grafik tersebut dapat dilihat pada gambar 4.19 dibawah ini.



Gambar 4.19 Grafik model *insider threat*

Terdapat empat variabel pada grafik model *insider threat* diatas. Keempat variabel tersebut adalah *insider threat* , *insider threat indicators*, *IT security level*, dan *executive management commitment*. Dalam grafik tersebut dijelaskan pengaruh variabel *IT security level* terhadap turunnya nilai variabel *IT security level*. *IT Security level* (garis warna hijau), mengalami peningkatan tajam pada bulan 6 hingga bulan 9. Salah satu penyebabnya adalah respon manajemen terhadap nilai variabel *insider threat*(garis warna biru) yang melebih batas normal yaitu 44% atau 0.44. Selanjutnya dapat dilihat juga variabel *insider threat indicators* (garis warna merah) yang juga mengalami penurunan sejak bulan ke 7 hingga bulan ke 12, juga menyebabkan turunnya nilai variabel *insider threat*. Disamping itu variabel *executive management commitment* (garis warna abu-abu) mengalami kenaikan mulai dari bulan 8 hingga bulan 12, dimana hal ini terjadi karena

mendekati akhir tahun, manajemen melakukan audit tutup buku secara keseluruhan yang membuat manajemen menyadari nilai potensial risiko dari ancaman *insider*.

4.4. Validasi Model

Pada tahap validasi model, akan dilakukan pembuktian bahwa model tersebut sudah merepresentasikan dengan sistem nyata. Validasi dilakukan dengan menggunakan perbandingan rata-rata dan perbandiangan variasi amplitude pada data hasil simulasi. Terdapat dua cara dalam melakukan validasi model yaitu dengan menghitung perbandingan rata-rata (*means comparison*) dan dengan menghitung perbandingan variasi amplitude (*amplitude variations comparison*).

a) Perbandingan Rata-Rata (*mean comparison)*

$$E1 = \frac{\left[\overline{S} - \overline{A}\right]}{\overline{A}}$$

$$\overline{S} = nilai\_rata - rata\_hasil\_simulasi$$

$$\overline{A} = nilai\_rata - rata\_data$$

Model dianggap valid bila E1 ≤ 5%

b) Perbandingan Variasi Amplitudo (% *error variance*)

Dimana: $E2 = \frac{|Ss - Sa|}{Sa}$

S_s= Standar deviasi model

S_a = Standar deviasi data

Model dianggap valid bila E2 ≤ 30%

Variabel yang divalidasi pada tugas akhir ini adalah variabel-variabel yang dapat mempengaruhi tujuan dari simulasi yaitu untuk mendeteksi dan mengurangi risiko *insider threat*. Berikut adalah variabel-variabel yang dapat divalidasi sesuai dengan data dan hasil wawancara yang didapatkan.

4.4.1. Validasi sub model Actual Freedom by Insider

Pada sub model ini terdapat satu variabel yang dapat divalidasi yaitu variabel *actual freedom*, variabel ini mempunyai relasi positif terhadap variabel *insider threat indicators*. Untuk memvalidasi *actual freedom*, dibutuhkan masing-masing rata-rata dan standar deviasi dari data actual dan hasil simulasi dari sub model *Actual Freedom by insider*.

Diketahui:

Rata-rata aktual = 67.08%
Standard deviasi aktual = 5.42%
Rata-rata simulasi = 64%
Standard deviasi simulasi = 5.36%

Proses Validasi:

- Error Mean (E1)

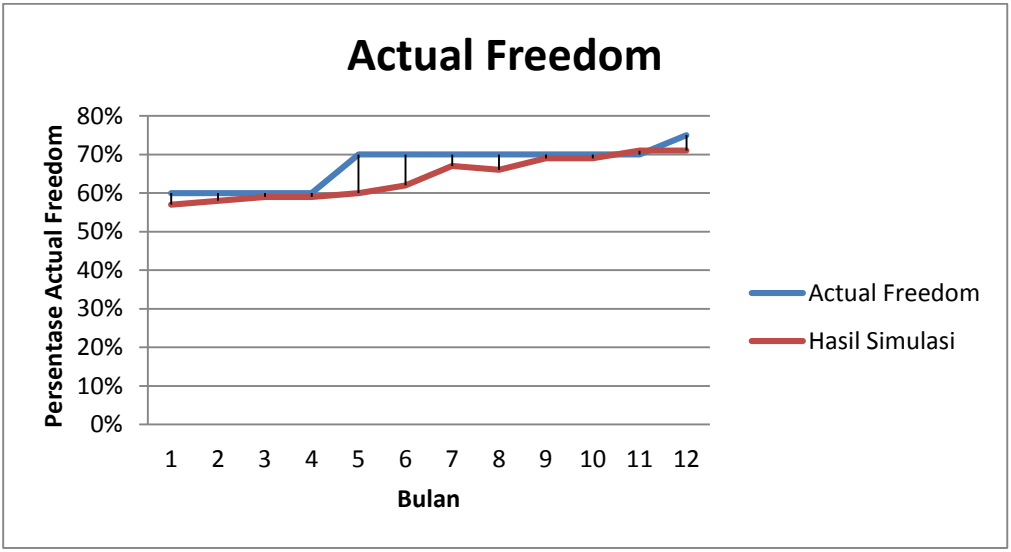
$$\frac{|0.64 - 0.6708|}{0.6708} = 4.59\%$$

- Error Variance (E2)

$$\frac{|0.536 - 0.542|}{0{,}542} = 1.07\ \%$$

Syarat nilai valid dapat dilihat apabila E1 ≤ 5% dan E2 ≤ 30%, maka dapat disimpulkan bahwa nilai *actual freedom* valid.

Pada grafik dibawah ini dapat dilihat hasil perbandingan antara data actual dan data hasil simulasi *actual freedom* (lihat gambar 4.20).



Gambar 4.20 Grafik Perbandingan validasi *actual freedom*

4.4.2. Validasi sub model *Behavioral precursors*

Pada sub model ini terdapat satu variabel yang dapat divalidasi yaitu variabel *behavioral precursors*, variabel ini mempunyai relasi positif terhadap variabel *insider threat indicators* yang merupakan variabel utama yang dapat meningkatkan persentase *insider threat* di perusahaan. Untuk memvalidasi *behavioral precursors*, dibutuhkan masing-

masing rata-rata dan standar deviasi dari data aktual dan hasil simulasi dari sub model *Behavioral precursors*. Data aktual *behavioral precursors*, didapatkan berdasarkan hasil wawancara terhadap kasus pelanggaran terkait tingkah laku yang buruk pada tahun-tahun sebelumnya di PT XYZ.

Diketahui:

Rata-rata aktual = 58.17%
Standard deviasi aktual = 13.76%
Rata-rata simulasi = 60.50%
Standard deviasi simulasi = 13.26%

Proses Validasi:

- Error Mean (E1)

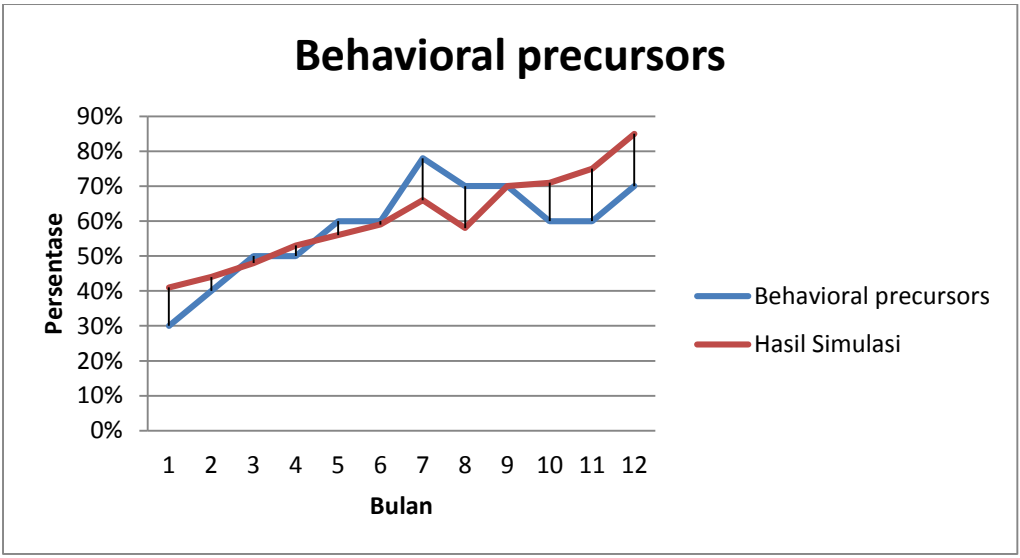
$$\frac{|0.6050 - 0.5817|}{0.5817} = 4.01\%$$

- Error Variance (E2)

$$\frac{|0.1326 - 0.1376|}{0{,}1376} = 3.63\ \%$$

Syarat nilai valid dapat dilihat apabila E1 ≤ 5% dan E2 ≤ 30%, maka dapat disimpulkan bahwa nilai *behavioral precursors* valid.

Pada grafik dibawah (gambar 4.21) ini dapat dilihat hasil perbandingan antara data aktual dan data hasil simulasi *behavioral precursors*



Gambar 4.21 Grafik perbandingan validasi *behavioral precursors*

4.4.3. Validasi sub model Technical precursors

Pada sub model ini terdapat satu variabel yang dapat divalidasi yaitu variabel *technical precursors* variabel ini mempunyai relasi positif terhadap variabel *insider threat indicators* yang merupakan variabel utama yang dapat meningkatkan persentase *insider threat* di perusahaan. Untuk memvalidasi *technical precursors*, dibutuhkan masing-masing rata-rata dan standar deviasi dari data aktual dan hasil simulasi dari sub model *technical precursors*. Data aktual *technical precursors*, didapatkan berdasarkan hasil wawancara terhadap kasus pelanggaran terkait tingkah laku yang buruk pada tahun-tahun sebelumnya di PT XYZ.

Diketahui:

Rata-rata aktual = 52.92%
Standard deviasi aktual = 8.91%
Rata-rata simulasi = 54.75%
Standard deviasi simulasi = 10.87%

Proses Validasi:

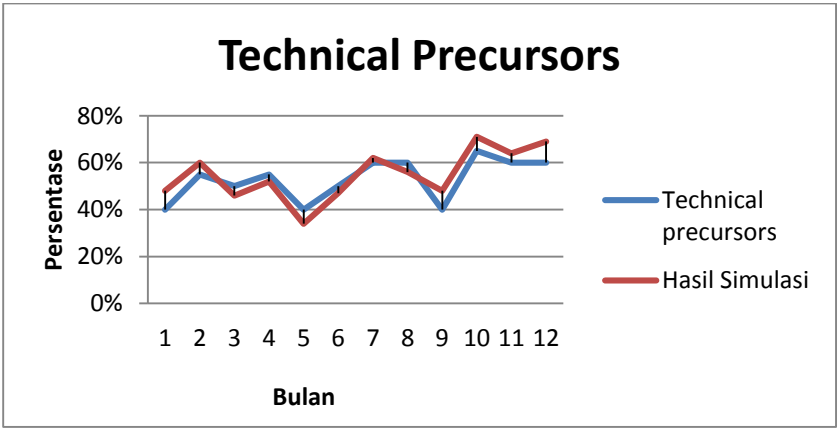
- Error Mean (E1)

$$\frac{|0.5475 - 0.5292|}{0.5292} = 3.46\%$$

- Error Variance (E2)

$$\frac{|0.1087 - 0.891|}{0.891} = 22.04\ \%$$

Syarat nilai valid dapat dilihat apabila E1 ≤ 5% dan E2 ≤ 30%, maka dapat disimpulkan bahwa nilai *behavioral precursors* valid. Pada gambar 4.22 dibawah ini dapat dilihat hasil perbandingan antara data aktual dan data hasil simulasi *technical precursors.*



Gambar 4.22 Grafik perbandingan validasi *technical precursors*

4.4.4. Validasi sub model IT Security Level

Dari data yang didapatkan, terdapat dua variabel yang dapat divalidasi dari sub model *IT Security level* , kedua variabel tersebut adalah *security investments* dan *IT security policy*. Sedangkan untuk sub model *executive management commitment* tidak didapatkan variabel yang dapat divalidasi karena permasalahan data, akan tetapi kedua variabel yang sudah disebutkan sebelumnya sudah cukup mewakili validasi dalam *executive management commitment*, terutama variabel *security investments* karena variabel tersebut merupakan hasil luaran dari sub mode *executive management commitment*.

1. Validasi *security investments*

Diketahui:

Rata-rata aktual = 42.75%
Standard deviasi aktual = 12.8%
Rata-rata simulasi = 42.86%
Standard deviasi simulasi = 13.8%

Proses Validasi:

- Error Mean (E1)

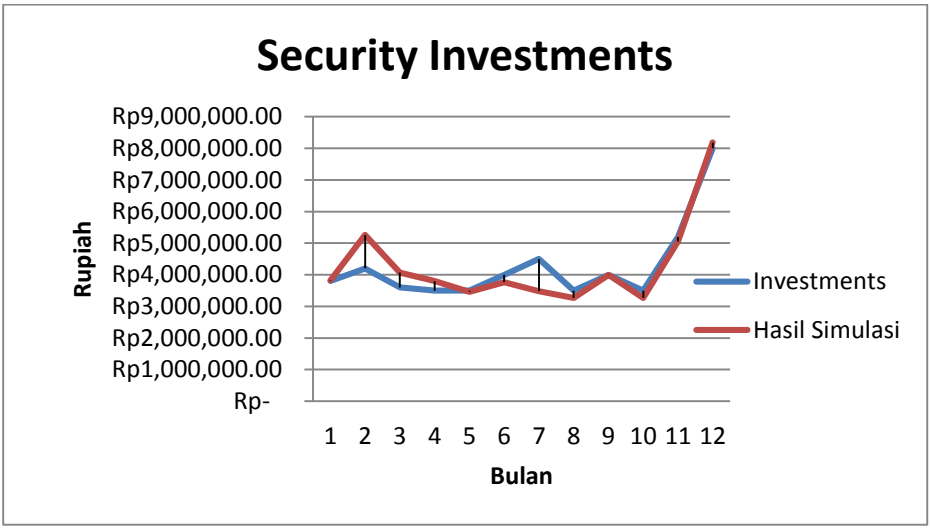
$$\frac{|4{,}286{,}550 - 4{,}275{,}000|}{4{,}275{,}000} = 0.27\%$$

- Error Variance (E2)

$$\frac{|1{,}380{,}842 - 1{,}280{,}003{,}55|}{1{,}280{,}003{,}55} = 8\ \%$$

Syarat nilai valid dapat dilihat apabila E1 ≤ 5% dan E2 ≤ 30%, maka dapat disimpulkan bahwa nilai *security investments* valid.

Pada grafik dibawah ini dapat dilihat hasil perbandingan antara data aktual dan data hasil simulasi *security investments* (lihat gambar 4.23)



Gambar 4.23 Grafik *perbandingan security investments*

2. Validasi *security policy*

Diketahui:

Rata-rata aktual = 34.58%
Standard deviasi aktual = 7.82%
Rata-rata simulasi = 36.17%
Standard deviasi simulasi = 8.08%

Proses Validasi:

- Error Mean (E1)

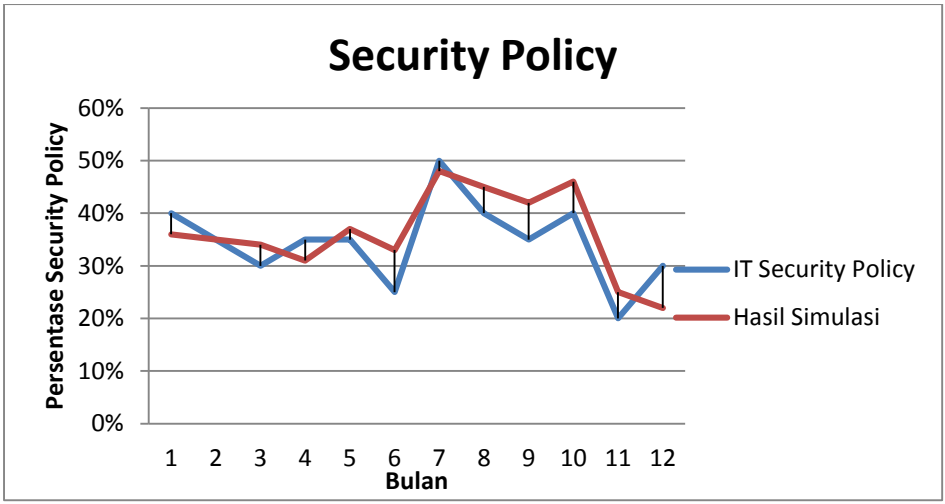
$$\frac{|0.3617 - 0.3458|}{0.3458} = 4.58\%$$

- Error Variance (E2)

$$\frac{|0.808 - 0.782|}{0{,}782} = 3.27\ \%$$

Syarat nilai valid dapat dilihat apabila E1 ≤ 5% dan E2 ≤ 30%, maka dapat disimpulkan bahwa nilai *security policy* valid.

Pada grafik dibawah ini dapat dilihat hasil perbandingan antara data aktual dan data hasil simulasi *security investments* (lihat gambar 4.24)



Gambar 4.24 Grafik perbandingan *IT security policy*

4.4.5. Kesimpulan Hasil Validasi

Dari hasil validasi yang dilakukan pada model *insider threat*, model dapat dikatakan valid karena telah memenuhi syarat nilai error. Syarat nilai error seperti yang sudah dijelaskan di awal bab mempunyai nilai sebesar 5% untuk E1

dan 30% untuk E2.Untuk lebih jelasnya,rangkuman tabel hasil validasi dapat dilihat pada tabel 4.1 dibawah ini.

Tabel 4.1 Rangkuman hasil validitas

Data Sub Model	Nilai deteksi persentase E1	Nilai deteksi persentase E2	Status
Actual freedom	4.59%	1.076%	**Valid**
Behavioral precursors	4.01%	3.63%	**Valid**
Technical precursors	3.46%	22.04%	**Valid**
IT Security Level*	0.27%	8%	**Valid**
IT Security Level**	4.58%	3.27%	**Valid**

*Security Investments **Security Policy

Halaman ini sengaja dikosongkan

BAB 5
ANALISIS DAN PEMBAHASAN

Bab ini membahas proses pembuatan skenariosasi serta analisis terhadap hasil dari masing-masing skenario berdasarkan basemodel yang telah dibuat sebelumnya. Selanjutnya akan dilakukan analisis terhadap hasil yang akan diperoleh dari pembuatan skenario.

5.1 Pengembangan Skenario

Dalam mengembangkan skenario perlu diketahui terlebih dahulu bahwa terdapat dua jenis skenario model , yaitu:

a. Skenario Parameter
Pada skenario ini akan dilakukan perubahan nilai parameter dari variabel penjualan seperti harga jual produk karena merupakan variabel yang memiliki hubungan sebab akibat yang sama pada profit.

b. Skenario Struktur
Pada skenario ini akan dilakukan dengan merubah struktur model saluran distribusi. Pada model ini, skenario yang akan dibuat berupa menambahkan variabel berpengaruh seperti diskon sehingga produk yang terjual lebih banyak dan profit perusahaan meningkat.

Dalam studi kasus ini digunakan dua jenis skenario model sesuai yang sudah disebutkan diatas.Pada skenario pertama yaitu skenario parameter , terdapat variabel yang akan diubah parameternya agar model tersebut nilai *insider threat* semakin menurun. Pada skenario kedua, yaitu skenario

struktur terdapat variabel yang ditambahkan untuk mengurangi nilai *insider threat*. Kunci dalam pengembangan model dan skenariosasi adalah sesuai dengan tujuan pembuatan model dimana model tersebut digunakan untuk mengurangi tingkat *insider threat* di PT XYZ.

5.2 Landasan Dasar Skenario

Dari hasil analisis grafik yang dilakukan pada bab empat, untuk skenario parameter ditemukan bahwa salah satu parameter yang paling berpengaruh adalah variabel *IT security policy* diperusahaan. *IT security policy* merupakan salah satu variabel yang mempunyai fungsi sebagai masukan positif kepada variabel *level IT security level*. Seperti yang diketahui bahwa di PT XYZ, sudah terdapat kebijakan untuk penganganan sekuritas terkait TI. Akan tetapi kebijakan tersebut sangat susah untuk dipatuhi oleh karyawan. Berdasarkan data yang didapatkan , kebijakan sekuritas yang dipatuhi oleh karyawan tidak melebihi dari 50% kebijakan yang disosialisasikan oleh PT XYZ. Dari fakta tersebut, maka perlu sebuah skenariosasi parameter yang dapat mengurangi tingkat nilai *insider threat* di PT XYZ sesuai dengan tujuan pembuatan skenario,sehingga apabila dirangkum keputusan dalam pemilihan skenario ini didasarkan dari:

1. Rendahnya nilai *IT Security Policy* yaitu sebesar 30-50%
2. Kurangnya kontrol informal kebijakan sekuritas yang dilakukan PT XYZ.

Landasan dasar untuk skenario struktur yang pertama dapat diketahui juga dari hasil grafik pada *base model*. Diketahui bahwa salah satu variabel utama yang

menyebabkan tingginya tingkat *insider threat* di PT XYZ adalah *behavioral precursors*, yang disebabkan oleh *disgruntlemet* atau ketidakpuasan karyawan. Salah satu usaha dari PT XYZ dalam menangani tingkat *behavioral precursors* adalah dengan menggunakan sanksi bagi karyawan yang mengganggu iklim kerja secara *offline*. Usaha tersebut memang dapat mengurangi nilai *behavioral precursors* akan tetapi tidak mengurangi nilai ketidakpuasan dari karyawan, oleh karena itulah perlu sebuah intervensi untuk karyawan dari perusahaan dalam hal ini dapat ditangani oleh *supervisor*. Dari penjelasan tersebut, maka skenario struktur pertama adalah *supervisor intervention*.Apabila dirangkum keputusan dalam pemilihan skenario ini didasarkan dari:

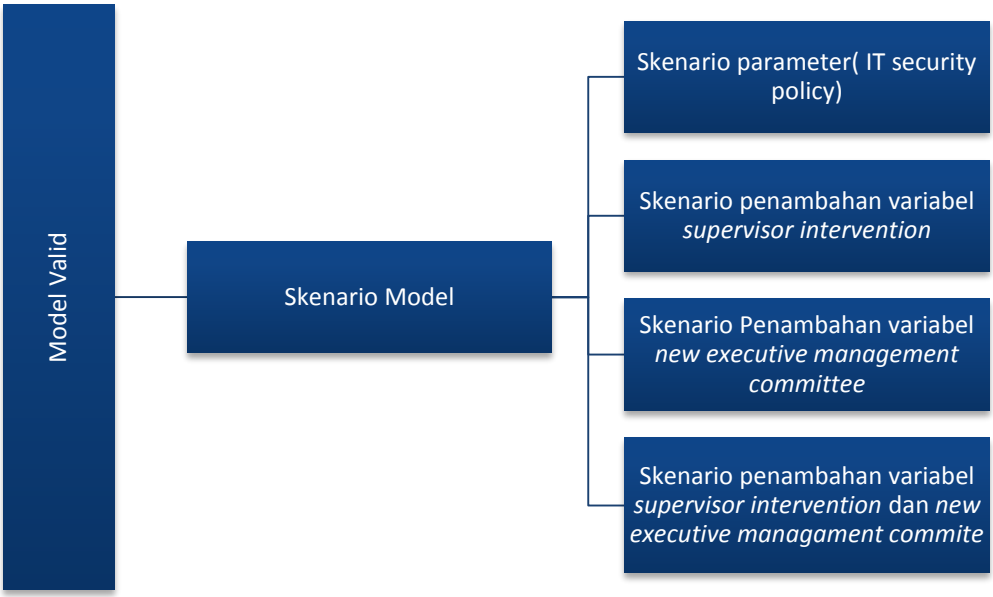
1. Meminimalisir karyawan yang tidak puas, karena karyawan yang tidak puas dapat meningkatkan tingkat nilai *insider threat*.
2. Berdasarkan kondisi eksisting, dimana kurang adanya intervensi yang dilakukan pihak manajemen bagi karyawan yang melakukan tindakan buruk.

Untuk skenario yang kedua, sub model yang akan ditinjau adalah sub model *executive management commitment*. Salah satu sebab utama tingginya komitmen manajemen pada bulan-bulan terakhir adalah merupakan respon dari manajemen terhadap tingginya nilai *insider threat* atau kejadian yang terjadi, sehingga kurang adanya komitmen manajemen terhadap aksi preventif yang dapat dilakukan oleh *insider* atau karyawan. Oleh karena itu diperlukan sebuah pemicu yang dapat meyakinkan dan tetap meningkatkan komitmen manajemen eksektufi terkait sekuritas. Salah satu solusi dari hal tersebut adalah dengan mengangkat karyawan ataupun

manajer yang mempunyai bidang ilmu teknologi informasi dan sistem informasi. Hal ini merupakan solusi yang dapat dilakukan karena sampai saat ini di PT XYZ, latar belakang manajemen eksekutif belum ada yang dari bidang teknologi informasi , dan hanya dari bidang finansial, dan juga wartawan. Dari penjelasan diatas, maka skenario struktur kedua adalah *new executive management committee* atau penambahan anggota manajemen eksekutif. Apabila dirangkum keputusan dalam pemilihan skenario ini didasarkan dari:

1. Kurangnya komitmen eksekutif manajemen dalam menanggulangi *insider threat*.
2. Belum adanya manajemen eksekutif yang mempunyai latar belakang ilmu sistem informasi dan teknologi informasi.

Untuk skenario struktur yang terakhir, nantinya akan digabungkan dua skenario struktur yaitu intervensi supervisor dan manajer eksekutif baru. Untuk lebih jelasnya, berikut adalah gambar 5.1 yang merupakan diagram skenario dari pemodelan simulasi tugas akhir.



Gambar 5.1 Diagram skenario *insider threat*

5.3 Skenario Parameter *IT Security Policy*

Dalam skenario parameter *IT security policy*, akan dilakukan perubahan data kualitatif masukan pada variabel *IT security policy*. Sebelumnya telah diketahui dari wawancara yang dilakukan pada PT XYZ, bahwa nilai *IT security policy* dipengaruhi oleh waktu, oleh karena itu pada skenario parameter *IT security policy*, yang diubah hanyalah data masukan. Sebelumnya persamaan pada base model untuk *IT security policy* dapat dilihat pada persamaan dibawah ini:

IT Security Policy = IF THEN ELSE (Time <7, RANDOM UNIFORM (0.3, 0.4, 1), IF THEN ELSE (Time = 11:OR: Time=12, RANDOM UNIFORM (0.2, 0.3, 1), RANDOM UNIFORM (0.4, 0.5, 1)))

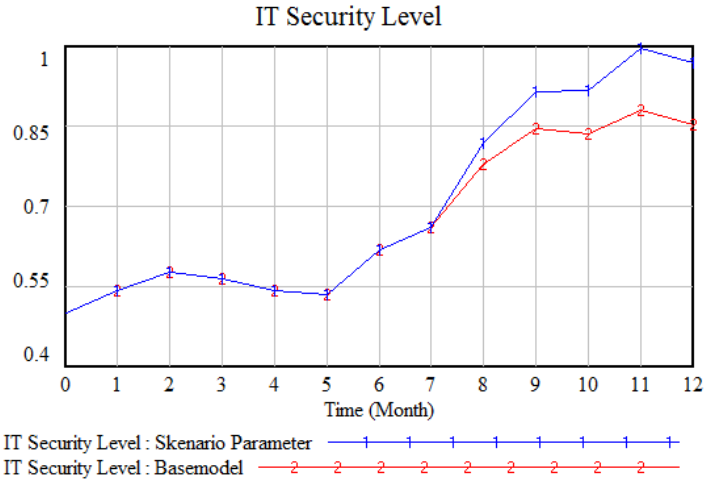
Persamaan 5.1 ***IT security policy base model***

Pada hasil simulasi sebelumnya didapatkan hasil grafik *IT Security policy* yang tidak melebihi nilai 50%, maka pada skenariosasi ini nilai persamaan *IT security policy* akan ditingkatkan menjadi persamaan dibawah ini.

IT Security Policy = IF THEN ELSE(Time <7 , RANDOM UNIFORM(0.3 , 0.4 , 1) ,IF THEN ELSE(Time = 11:OR: Time=12 , RANDOM UNIFORM(0.2 , 0.3 , 1) , RANDOM UNIFORM (0.4 , 0.6, 1)))

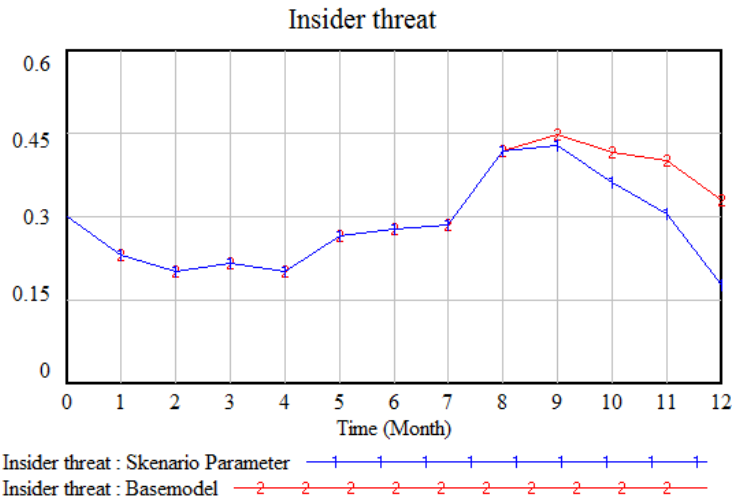
Persamaan 5.2 ***IT security policy skenario parameter***

Dari hasil persamaan tersebut dapat dilihat perbedaan grafik antara *IT security policy* antara *base model* dan skenario pada gambar 5.2 dibawah ini:



Gambar 5.2 Perbandingan grafik *IT security policy*

Gambar 5.2 diatas menunjukkan perbandingan antara hasil simulasi base model dengan hasil simulasi skenario parameter *IT security policy*. Perbedaan yang dapat dilihat adalah lebih besarnya nilai dari hasil simulasi skenario parameter *IT security policy*. Hal ini sesuai dengan peningkatan nilai persamaan variabel *IT security policy*, akan tetapi parameter tersebut juga perlu dilihat akan tujuan dari model yaitu untuk mengurangi nilai insider threat. Berikut adalah grafik perbandingan hasil insider threat setelah dilakukan skenario parameter *IT security policy* yang dapat dilihat pada gambar 5.3.



Gambar 5.3 Perbandingan grafik *insider threat* skenario parameter

5.4 Analisis hasil Skenario Parameter *IT Security Policy*

Dari gambar 5.3, yaitu grafik perbandingan *insider threat* skenario parameter dapat dilihat bahwa terjadi penuruan nilai *insider threat* pada tiap bulannya melebihi dari simulasi *base model* sebelumnya. Hal ini dikarenakan variabel *IT security policy* mempunyai pengaruh yang cukup besar terhadap penurunan nilai *insider threat* di PT XYZ.

Terkait dengan layak tidaknya skenario ini diimplementasikan, terdapat analisis *cost benefit* yang dilakukan pada tabel 5.1 dibawah ini.

Tabel 5.1 Cost Benefit Analysis IT Security Policy

Dampak	Manfaat		Keterangan	Nilai Rupiah
	Tangible	Intangible		
Mengurangi kemungkinan terkena serangan kemanan dari luar dan dalam perusahaan	Meningkatkan produktifias operasional		Meningkatkan produktifitas sampai dengan 10% pada tiap bulan	Rp 180,000,000
		Meningkatkan kualitas keamanan TI	Dengan adanya kebijakan diperkiranan 2% dari keuntungan akan meningkat	Rp 36,000,0000
Total				**Rp 216,000,000**
Pengeluaran				**Nilai Rupiah**
Pembelian software dan infrastruktur keamanan TI				Rp 70,000,000

Pengeluaran	Nilai Rupiah
Biaya auditor dari luar perusahaan (1 tim = 2 orang, per orang = 7jt,1 tahun 2 kali audit)	Rp 28,000,000
Biaya controlling SI/TI	Rp 60,000,000
TOTAL	**Rp 138,000,000**
TOTAL KEUNTUNGAN (*Benefit-Cost*)	**Rp 58,000,000**

Dari hasil analisis *cost benefit*, perusahaan diperkirakan mendapatkan keuntungan sebesar Rp 58,000,000 apabila mengimplementasikan skenario tersebut dengan pertimbangan yang sudah dipaparkan pada tabel. Selain itu perlu dipertimbangkan juga kesulitan-kesulitan yang akan dihadapi apabila mengimplementasikan skenario ini, beberapa permasalahan tersebut yang dapat diidentifikasi yaitu:

1. Penambahan kebijakan memerlukan waktu yang sangat lama untuk diimplementasikan.
2. Perlu dukungan penuh dari *top management* hingga karyawan.
3. Dalam proses perubahan dari kebijakan lama sampai dengan kebijakan baru kemungkinan terjadipermasalahan yang dapat mengurangi laba perusahaan.

Selain itu juga terdapat keuntungan dalam mengimplementasikan skenario ini yaitu:

1. Secara jangka panjang perubahan kebijakan yang lebih baik dapat memberikan keuntungan bagi perusahaan
2. Perusahaan akan lebih terlindungi dari serangan aset informasi baik dari luar maupun dari dalam.

Perbedaan nilai *insider threat* tersebut semakin terlihat lebih jelas. Apabila dirata-rata dalam 12 bulan, jumlah selisih persentase perbedaannya sebesar ± 2%, yang berarti kurang signifikan .Perbandingan nilai deteksi persentase *insider threat* antara base model dengan skenario parameter *IT security policy* dapat dilihat pada tabel 5.2 dibawah ini.

Tabel 5.2 Perbandingan nilai deteksi persentase *insider threat*

Variabel	Rata-rata dalam satu periode	Selisih perbedaan
Insider Threat *base* model	30.36%	2.75%
Insider Threat skenario *IT security policy*	27.61%	

Agar skenario ini dapat diimplementasikan, juga harus dilihat variabel-variabel yang mempengaruhi nilai variabel *IT Security Policy* di PT XYZ. Variabel-variabel tersebut adalah variabel persentase kontrol teknis, persentase kontrol formal. Nilai masukan dari ketiga variabel tersebut dapat dilihat pada lampiran B. Ketiga variabel tersebut akan diuji dengan metode regresi untuk menemukan hubungan dan variabel mana yang harus ditingkatkan oleh PT XYZ.

Hasil persamaan regresi dari ketiga variabel tersebut dengan IT Security policy adalah:
X1= persentase kontrol teknis
X2= persentase kontrol formal
X3= persentase kontrol informal

$$Y = IT\ Security\ policy = --0.01137+1.060518* x1 + 0.892738*x2 +1.15818*x3$$

Persamaan 5.3 Regresi *Security Policy*

Dari persamaan 5.3 diatas dapat diketahui bahwa:

1. Intercept sebesar -0.01137 berarti tanpa adanya variabel persentase kontrol teknis, kontrol formal, dan kontrol

informal maka nilai persentase *IT Security policy* bernilai -0.01137

2. Variabel kontrol teknis mempunyai nilai sebesar 1,060518% berarti hubungan antara variabel kontrol teknis dan variabel *IT security policy* mempunyai nilai positif. Hasil angka tersebut juga berarti bahwa setiap kenaikan variabel persentase kontrol teknis sebesar 1% akan meningkatkan nilai variabel persentase IT Security policy sebesar 1.060518%.
3. Variabel kontrol formal sebesar 0.892738% (positif). Artinya setiap kenaikan persentase nilai persentase kontrol formal sebesar 1% maka persentase IT Security plicy akan naik sebesar 0.892738%.
4. Variabel kontrol informal sebesar 0.892738% (positif). Artinya setiap kenaikan persentase nilai persentase kontrol formal sebesar 1% maka persentase IT Security plicy akan naik sebesar 0.892738%.

Dari hasil analisis regresi didapatkan bahwa variabel kontrol teknis mempunyai nilai paling tinggi yaitu sebesar 1.060518% ,oleh karena itu untuk meningkatkan nilai persentase *IT Security Policy* PT XYZ perlu meningkatkan kontrol teknis sekuritas perusahaan.

5.5 Skenario Struktur

5.6.1. Skenario Struktur Supervisor Intervention

Pada skenario penambahan variabel *supervisor intervention*, manajemen akan menugaskan *supervisor* pada karyawan yang berbuat buruk di tempat kerja untuk mencoba menyelesaikan permasalahan karyawan tersebut secara

personal atau melakukan konseling terhadap karyawan yang melanggar. Skenario ini juga digunakan pada penelitian Dawn M. Cappeli et al di penelitiannya yang berjudul "*Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers Information, Systems, or Networks*" [28]. Dari hasil diskusi,wawancara, dan referensi terkait ,didapatkan skala dampak persentase bagi ketidakpuasaan yang mungkin dapat dimitigasi yaitu sebesar 3% (*expert judgement*).

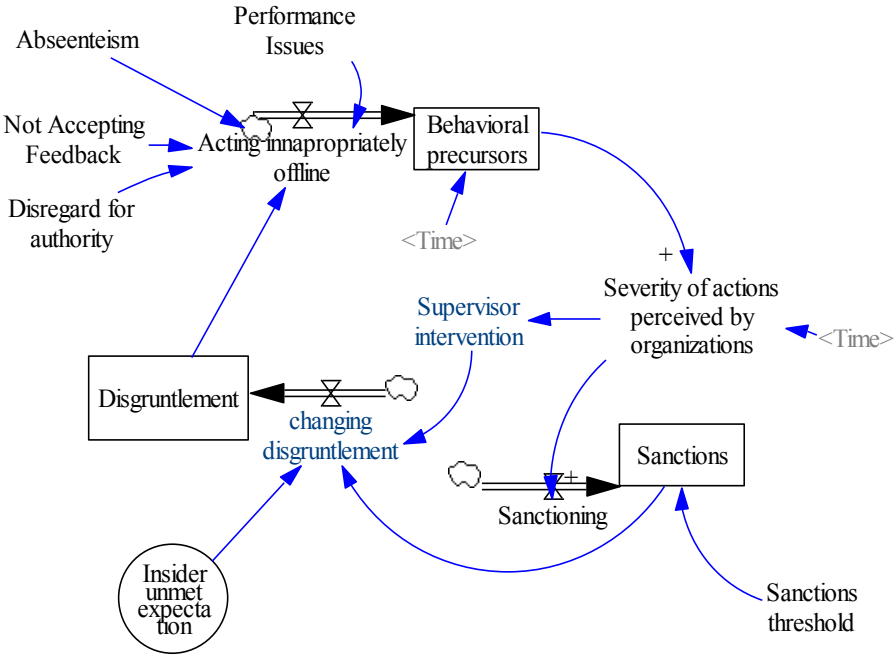
Relasi antar Variabel yang baru setelah adanya skenario *Supervisor Intervention*:

1. Supervisor intervention:merupakan variabel *auxiliary* yang mempunyai relasi positif dengan nilai variabel *severity of actions perceived by organizations* dan mempengaruhi secara negatif nilai varabel *changing disrgruntlement*.
2. *Changing disgruntlement*: merupakan variabel *rate* yang mempunyai relasi positif dengan nilai variabel *sanctions* dan *insider unmet expectation* serta memiliki relasi negatif dengan variabel *supervisor intervention*. Nilai variabel ini secara positif mempengaruhi nilai laju variabel level *disgruntlement*.

Tujuan dari skenario struktur ini adalah untuk mengurangi ketidakpuasaan/*disgruntlement* sehingga nilai *insider threat* yang berhubungan dengan *behavioral precursors* dan *technical precursors* dpat berkurang.

Dalam pembuatan skenario terdapat beberapa variabel-variebel baru yang ditambahkan ke dalam model. Variabel-variabel tersebut antara lain *changing disgruntlement* dan *supervisor intervention*. Diagram *flow* skenario struktur

supervisor intervention, dapat dilihat pada gambar 5.4 dibawah ini.



Gambar 5.4 Diagram *flow* skenario struktur variabel *supervisor intervention*

Penjelasan dari variabel tambahan pada gambar 5.4 diagram *flow* skenario struktur variabel *supervisor intervention* adalah sebagai berikut:

1. ***Supervisor Intervention***

   Supervisor intervention merupakan usaha dari manajemen untuk mengurangi persentase nilai variabel *disgruntlement* pada karyawan yang bertingkah laku buruk. Variabel *supervisor*

intervention ini merupakan variabel *auxiliary* yang berelasi positif pada variabel *changing disgruntlement*.

Supervisor Intervention = IF THEN ELSE (Severity of actions perceived by organizations=3, RANDOM UNIFORM (0.005, 0.02,), 0)

Persamaan 5.4 *Supervisor Intervention*

2. ***Changing Disgruntlement***

Merupakan jenis variabel *rate* yang menjadi masukan pada variabel *disgruntlement*. Variabel ini dipengaruhi secara negatif oleh *supervisor intervention* sehingga mempengaruhi nilai luaran dari *base model*.

Changing Disgruntlement = IF THEN ELSE (Sanctions<=6, 0, IF THEN ELSE (Sanctions<=15, 0.025 - supervisor intervention, 0.05 - supervisor intervention))

Persamaan 5.5 *Changing Disgruntlement*

5.6.2. Skenario Struktur new executive management committee

Skenario struktur kedua adalah menambahkan variabel *new executive management committee*. Dalam skenario ini, PT XYZ akan menambahkan anggota komite eksekutif baru yang mempunyai latar belakang dan keahlian dalam bidang teknologi informasi dan sistem informasi. Komite baru yang ditunjuk akan bertanggung jawab kepada tata kelola teknologi

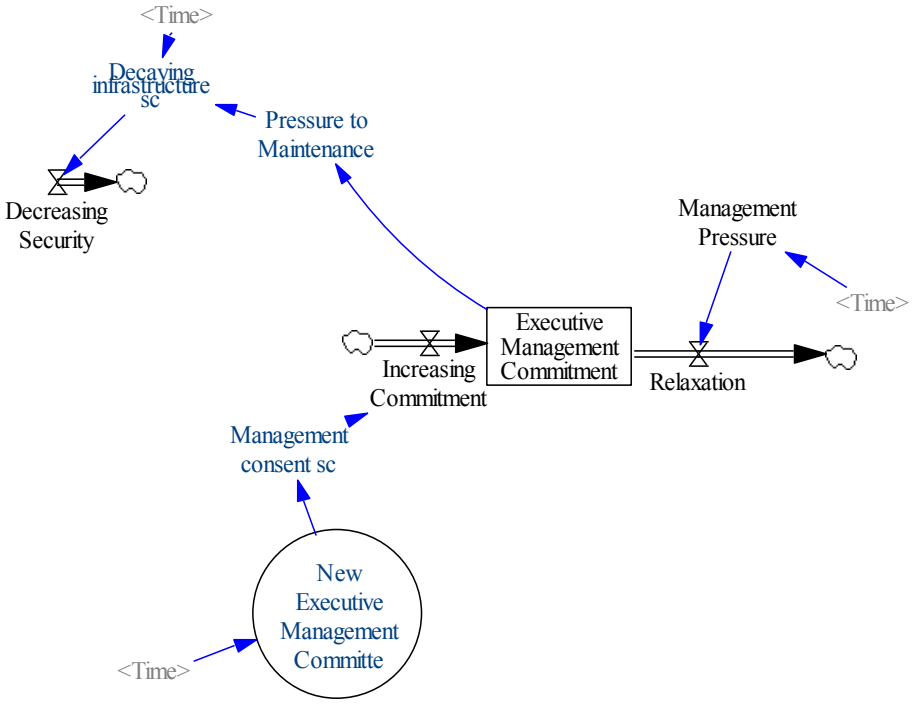
informasi di PT XYZ , dan yang paling penting akan bertanggung jawab juga dengan sekuritas teknologi inforamsi dan sistem informasi. Selain itu komite manajemen eksekutif yang baru diasumsikan dapat membuat kebijakan dan tekanan bagi manajemen untuk lebih merawat infrastruktur yang berhubungan dengan teknologi informasi, karena salah satu penyebab kurangnya *IT security level* di PT XYZ, adalah infrastruktur TI yang kurang terawat hingga menyebabkan infrastruktur TI tersebut tidak dapat beroperasi secara maksimal.

Relasi antar Variabel yang baru setelah adanya skenario *new executive management committee*:

1. New executive management committee: nilai variabel ini dipengaruhi oleh variabel waktu, dimana pada bulan 3, komite manajemen eksekutif baru mulai dilantik, variabel ini mempengaruhi secara positif nilai variabel *management consent sc*.
2. Management sc: nilai variabel ini dipengaruhi secara positif oleh variabel *new executive management committee* dan mempengaruhi nilai variabel *rate increasing commitment* secara positif.
3. *Pressure to maintenance*:nilai variabel ini dipengaruhi secara positif oleh variabel *level executive management commitment* dan mempengaruhi secara negative nilai variabel *decaying infrastructure*.
4. *Decaying infrastructure*: nilai variabel ini dipengaruhi secara negatif oleh variabel *pressure to maintenance* dan mempengaruhi variabel *rate decreasing security* secara positif.

Tujuan dari skenario struktur ini adalah untuk meningkatkan nilai *executive management commitment* sehingga nilai *IT security level* semakin meningkat dan variabel *rate decreasing insider threat* semakin berkurang.

Dalam pembuatan skenario terdapat beberapa variabel-variebel baru yang ditambahkan ke dalam model. Variabel-variabel tersebut antara lain *new executive management committee* dan *pressure to maintenance* Diagram *flow* skenario struktur *new executive management committee*, dapat dilihat pada gambar 5.5 dibawah ini.



Gambar 5.5 Diagram *Flow* skenario struktur variabel *new executive management committee*

Penjelasan dari variabel tambahan pada gambar 5.5 diagram *flow* skenario struktur variabel *new executive management committee* adalah sebagai berikut:

1. ***New executive management committee***

   New executive management committte merupakan pelantikan komite eksekutif baru dari manajemen untuk meningkatkan persentase nilai variabel *management consent* agar dapat meningkatkan komitmen manajemen. Variabel *new executive management committee* ini merupakan variabel *auxiliary* yang berelasi positif pada variabel *management consent*. Dalam skenario ini diasumsikan bahwa anggota baru manajemen eksekutif akan dilantik pada bulan 5 , sehingga dampak dari pekerjaannya baru dapat dirasakan pada bulan-bulan selanjutnya.

   New executive management committee = IF THEN ELSE (Time =5 ,1, 0)

   Persamaan 5.6 ***New Executive Management Committee***

2. ***Pressure to Maintenance***

   Merupakan jenis variabel *auxiliary* yang berelasi negatif pada variabel *decaying infrastructure*. Variabel ini dipengaruhi secara positif oleh variabel *executive management commitment*s sehingga mempengaruhi variabel *IT security level* secara positif. Dalam variabel ini terdapat batasan dimana dengan adanya anggota eksektif manajemen yang

baru, anggota tersebut dapat meyakinkan manajemen untuk berkomitmen lebih dalam mengelola infrastruktur TI/SI.

Pressure to Maintenance = IF THEN ELSE (Executive Management Commitment >0.6, 0.01, 0))

Persamaan 5.7 ***Pressure to Maintenance***

3. ***Management Consent sc***

Variabel *management consent sc* merupakan variabel yang sebenarnya sudah ada di *base model*, akan tetapi dikarenakan terdapat skenario struktur *new executive management committee*, maka variabel ini persamaannya berubah. Dengan adanya manajemen eksekutif baru yang berelasi positif pada variabel *management consent*, nilai variabel *rate increasing commitment* akan semakin tinggi sehingga dapat mengurangi nilai *insider threat* di PT XYZ.

Management Consent sc = IF THEN ELSE(New Executive Management Committee =1 , ((Auditing/2)+0.05) , Auditing/2)

Persamaan 5.8 Management Consent sc

4. ***Decaying Infrastructure sc***

Sama dengan variabel *management consent sc*, variabel *decaying infrastructure sc* adalah variabel yang persamaannya berubah dikarenakan terdapat

variabel baru yang menjadi masukan terhadap variabel tersebut. Nilai variabel *decaying infrastructure sc*.

Decaying infrastructure sc = IF THEN ELSE (Time<8, RANDOM UNIFORM (0.3, 0.4, 1) - Presssure to Maintenance, IF THEN ELSE (Time<4, RANDOM UNIFORM (0.2, 0.3, 1) - Presssure to Maintenance, RANDOM UNIFORM (0.4, 0.5, 1) - Presssure to Maintenance))

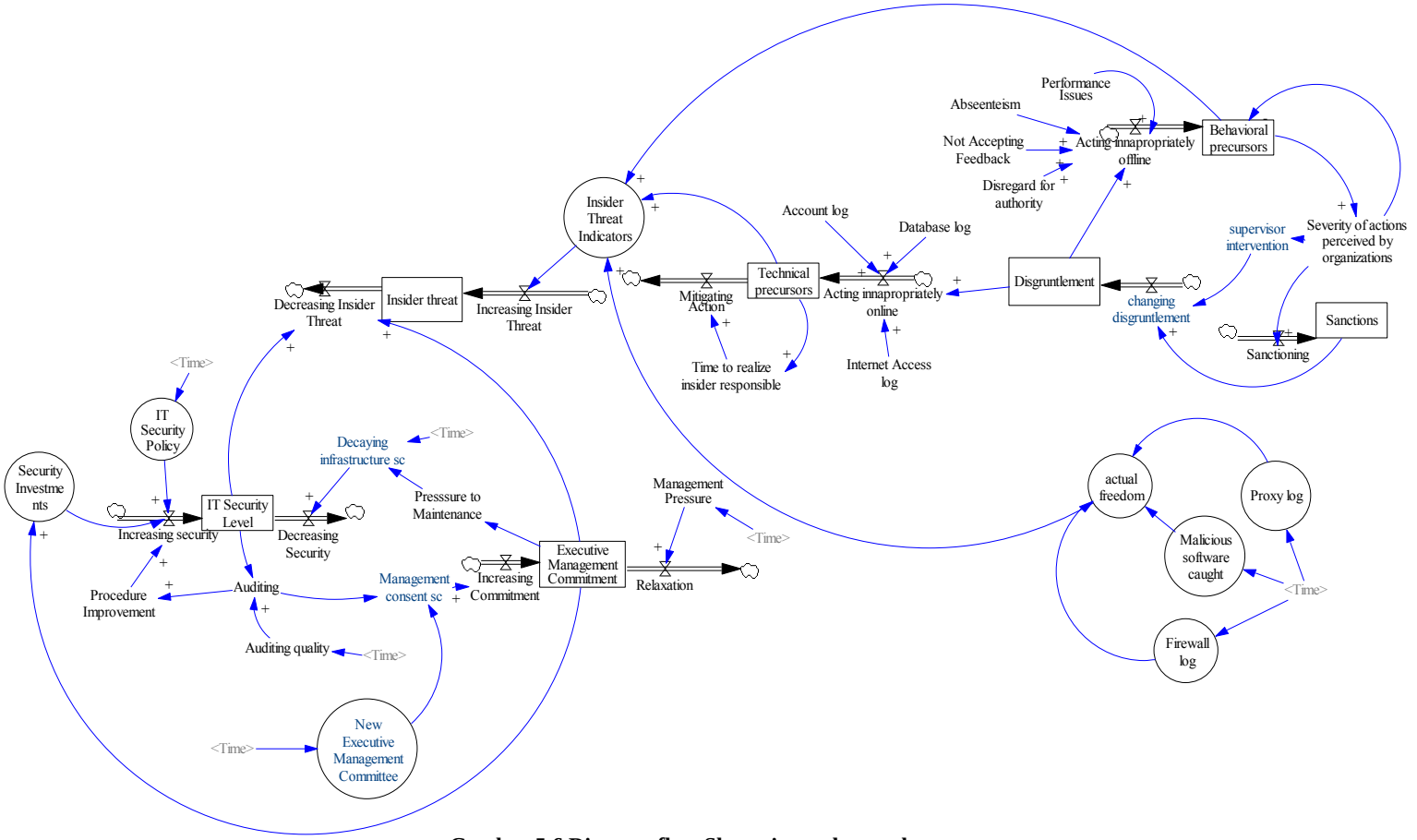
Persamaan 5.9 ***Decaying Inrastructure sc***

5.6.3. Skenario Struktur Supervisor Intervention dan New Executive Management Committee

Skenario struktur *supervisor intervention* dan *new executive management committee* merupakan gabungan antara skenario 1 (*supervisor intervention*) dan skenario 2 (*new executive management committee*). Tujuan dibuatnya skenario ini adalah untuk mengurangi nilai deteksi persentase *insider threat* agar *insider threat* tersebut dapat dideteksi dan dimitigasi oleh PT XYZ sebelum hal tersebut terjadi.

Skenario struktur ini dilakukan dengan menambahkan variabel-variabel baru kedalam model. Variabel baru yang ditambahkan antara lain *supervisor intervention*, *changing disgruntlement*, *new executive management committee*, dan *pressure to maintenance*.

Model diagram *flow* skenario struktur *supervisor intervention* dan *new executive management committee* dapat dilihat pada gambar 5.6 dibawah ini



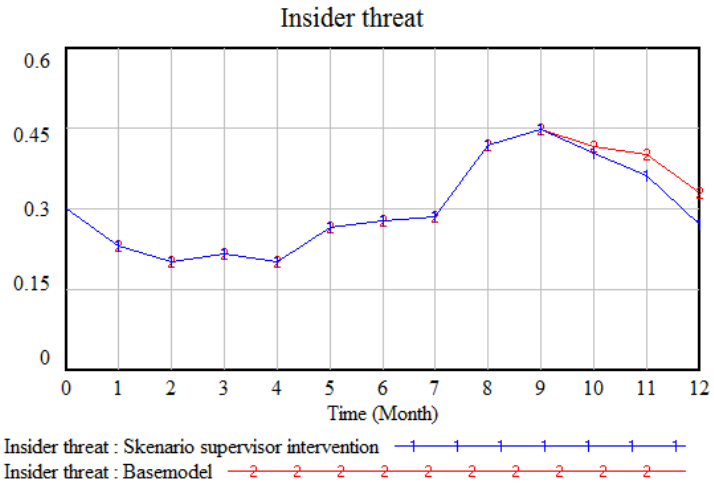
Gambar 5.6 Diagram flow Skenario struktur gabungan

5.6 Analisis Hasil Skenario Struktur

Pada tahap ini dilakukan pengamatan hasil skenario terkait dengan besarnya pengaruh skenario struktur *supervisor intervention* dan *new executive management committee* terhadap tingkat *insider threat* di PT XYZ. Analisi dilakukan dengan mengamati hasil dari masing-masing skenario serta membandingkannya dengan *base model*. Data-data dari hasil masing-masing skenario akan dilampirkan pada halaman lampiran D.

5.6.1 Analisis Skenario Supervisor intervention

Untuk memulai analisis skenario *supervisor intervention* digunakan hasil simulasi dari skenario struktur *supervisor intervention*. Selanjutnya berdasarkan hasil tersebut dilakukan perbandingan hasil simulasi sebelum dan sesudah ditambahkan skenario *supervisor intervention*. Hasil perbandingan nantinya akan dianalisis berdasarkan kesesuainnya dengan tujuan penelitian, yaitu untuk mengurangi tingkat *insider threat* di PT XYZ. Dari hasil perbandingan ini dapat dilihat seberapa besar perbandingan pengurangan tingkat *insider threat* setelah dilakukan intervensi karyawan oleh supervisor atau dengan penambahan struktur variabel baru.



Gambar 5.7 Perbandingan tingkat insider threat skenario *supervisor intervention*

Pada gambar 5.7 diatas dapat dilihat perbandingan nilai deteksi persentase *insider threat* tanpa penambahan variabel (*basemodel*) dan juga dengan penambahan variabel *supervisor intervention*. Darfi grafik diatas , dapat dilihat ada perbedaan tingkat *insider threat* yang kurang signifikan setelah adanya intervensi dari supervisor pada karyawan yang berkelakukan buruk serta mendapat sanksi dari pihak manajemen. Perubahan kecil tersebut dapat dilihat mulai bulan 8 dimana karyawan telah mendapatkan sanksi dan telah dintervensi oleh manajemen.

Terkait dengan layak tidaknya skenario ini diimplementasikan, terdapat analisis *cost benefit* yang dilakukan pada tabel 5.3 dibawah ini:

Tabel 5.3 Cost Benefit Analysis Supervisor Intervention

Dampak	Manfaat		Keterangan	Nilai Rupiah
	Tangible	Intangible		
Mengurangi ketidakpuasan karyawan	Meningkatkan produktifias operasional		Meningkatkan produktifitas sampai dengan 10% pada tiap bulan	Rp 90,000,000
		Tingkat karyawan yang berkelakukan buruk dapat berkurang	Loyalitas pegawai meningkat sehingga karyawan tidak "menyerang perusahaan"	
Total				**Rp 216,000,000**
Pengeluaran				**Nilai Rupiah**
Tugas baru supervisor (Bonus sebesar 15% dari gaji sebelumnya Rp 5,000,000				Rp 69,000,000

Pengeluaran	Nilai Rupiah
Pelatihan pada supervisor(1 kali dalam setahun)	Rp 10,000,000
TOTAL	**Rp 79,000,000**
TOTAL KEUNTUNGAN(*Benefit-Cost*)	**Rp 11,000,000**
Pelatihan pada supervisor(1 kali dalam setahun)	Rp 10,000,000

Dari hasil analisis *cost benefit*, perusahaan diperkirakan mendapatkan keuntungan sebesar Rp 11,000,000 apabila mengimplementasikan skenario tersebut dengan pertimbangan yang sudah dipaparkan pada tabel. Selain itu perlu dipertimbangkan juga kesulitan-kesulitan yang akan dihadapi apabila mengimplementasikan skenario ini, beberapa permasalahan tersebut yang dapat diidentifikasi yaitu:

1. Supervisor yang dipilih harus mampu menyelesaikan permasalahan dengan karyawan secara personal, jika tidak karyawan akan tetap merasa tidak puas.
2. Intervensi harus dilakukan secara berkala agar karyawan yang bermasalah dapat dipantau untuk dilihat perkembangan tingkah lakunya.

Selain itu juga terdapat keuntungan dalam mengimplementasikan skenario ini yaitu:

1. Biaya yang dikeluarkan tidak besar.
2. Tidak memerlukan perubahan kebijakan yang sangat signifikan.

Apabila kedua perbandingan hasil tersebut dirata-rata dalam satu tahun (12 bulan) maka perbandingan nilai tingkat persentase *insider threat* di PT XYZ mempunyai selisih sebesar 2.2%. Hasil lebih jelasnya tentang perbandingan simulasi rata-rata dalam satu tahun dapat dilihat pada tabel 5.4 dibawah ini.

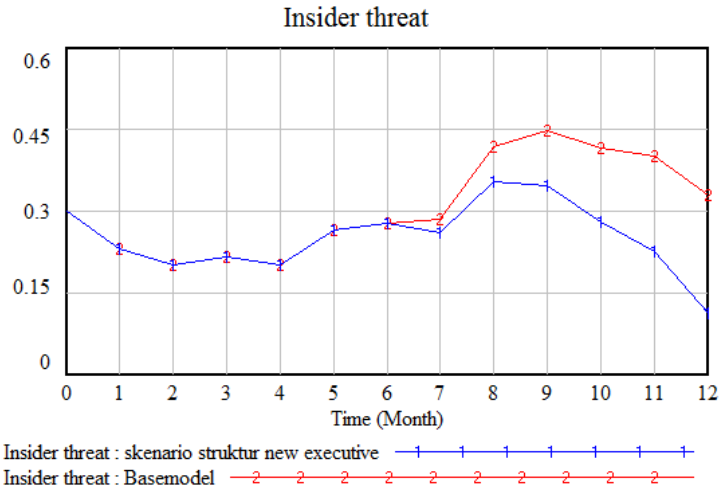
Tabel 5.4 Perbandingan nilai deteksi persentase insider threat skenario struktur *supervisor intervention*

Skenario	Rata-rata dalam satu periode	Selisih perbedaan
Insider Threat *base* model	31.41%	2.20%
Insider Threat skenario *supervisor intervention*	29.21%	

Dari tabel tersebut , diketahui bahwa skenario struktur *intervention* kurang memiliki dampak yang signifikan terhadap turunnya nilai *insider threat*. Akan tetapi solusi skenario ini juga mempunyai sisi positif yaitu solusi ini sangat aplikatif dan mudah untuk dilakukan di PT XYZ, dimana *supervisor* dapat berperan lebih aktif dalam menjaga sekuritas *insider threat* di PT XYZ .

5.6.2 Analisis Skenario New Executive Management Committee

Analisis hasil skenario struktur *new executive management committee* dilakukan dengan langkah yang sama dengan analisis skenario *supervisor intervention*, yaitu dengan membandingkan hasil simulasi sebelum dan sesudah ditambahkannya struktur variabel baru. Selanjutnya struktur variabel baru tersebut akan dievaluasi berdasarkan tujuan dari pembuatan skenario yaitu untuk mengurangi tingkat *insider threat* di PT XYZ. Hasil grafik perbandingan antara *base model* dan skenario struktur *new executive management committee* dapat dilihat pada gambar 5.8 dibawah ini.



Gambar 5.8 Perbandingan tingkat insider threat skenario *New Executive Employee Committee*

Pada gambar 5.8 diatas dapat dilihat perbandingan nilai deteksi persentase *insider threat* antara *base* model dan skenario struktur *new executive employee committee*. Dari grafik diatas , dapat dilihat ada perbedaan tingkat *insider threat* yang kecil setelah adanya manajemen eksekutif baru pada bulan 5 buruk serta mendapat sanksi dari pihak manajemen. Perbedaan antara base model dan model skenario struktur dapat dilihat mulai dari bulan 6, setelah 2 bulan pengangkatan manajemen eksekutif baru dengan latar belakang keahlian TI dan SI. Disamping itu anggota manajemen eksekutif baru juga memberikan tekanan bagi manajemen untuk melakukan perawatan pada infrastruktur TI/SI di PT XYZ.

Halaman ini sengaja dikosongkan

Terkait dengan layak tidaknya skenario ini diimplementasikan, terdapat analisis *cost benefit* yang dilakukan pada tabel 5.5 dibawah ini.

Tabel 5.5 Cost Benefit Analysis New Executive Management

Dampak	Manfaat		Keterangan	Nilai Rupiah
	Tangible	Intangible		
Perubahan kebijakan baru	Efisiensi produktifitas terkait sistem informasi dan teknologi informasi		Peningkatan produktifitas surat kabar diperkirakan mencapai 10% sehingga 10% * laba per bulan * 12 bulan	Rp 180,000,000
		Kebijakan terkait SI/TI yang dapat meningkatkan laba perusahaan	Dengan strategi SI/TI yang baru laba diperkirakan dapat bertambah sebesar 10% dalam 12 bulan	Rp 180,000,000

Total	**Rp 360,000,000**
Pengeluaran	**Nilai Rupiah**
Biaya gaji komite manajemen baru (1orang = 20jt /bulan)	Rp 240,000,000
Biaya pengelolaan infrastruktur TI (5jt/bulan)	Rp 60,000,000
TOTAL	**Rp 300,000,000**
TOTAL KEUNTUNGAN(*Benefit-Cost*)	**Rp 60,000,000**
Biaya pengelolaan infrastruktur TI (5jt/bulan)	Rp 60,000,000

Dari hasil analisis *cost benefit*, perusahaan diperkirakan mendapatkan keuntungan sebesar Rp 60,000,000 apabila mengimplementasikan skenario tersebut dengan pertimbangan yang sudah dipaparkan pada tabel. Selain itu perlu dipertimbangkan juga kesulitan-kesulitan yang akan dihadapi apabila mengimplementasikan skenario ini, beberapa permasalahan tersebut yang dapat diidentifikasi yaitu:

1. Keputusan ini perlu dipertimbangkan secara matang karena mengangkat komite manajemen baru memerlukan waktu dan persetujuan yang sangat lama.
2. Sulitnya mengubah paradigma risiko terkait *insider threat*, yang memang sebenarnya jarang dapat terjadi akan tetapi jika tidak diperhatikan dapat memberikan kerugian yang sangat besar bagi perusahaan.
3. Biaya yang dikeluarkan sangat besar.
4. Perlu dipikirkan secara matang-matang untuk memilih orang yang tepat sebagai manajemen komite baru.

Selain itu juga terdapat keuntungan dalam mengimplementasikan skenario ini yaitu:

1. Dampak jangka panjang skenario ini sangat baik terkait level sekuritas dan pemeliharaan infrastruktur teknologi informasi
2. Dapat Mengurangi tingkat nilai *insider threat* secara signifikan

Apabila kedua perbandingan hasil tersebut dirata-rata dalam satu tahun (12 bulan) maka perbandingan nilai tingkat persentase *insider threat* di PT XYZ mempunyai selisih sebesar 5.97%. Hasil lebih jelasnya tentang perbandingan

simulasi rata-rata dalam satu tahun dapat dilihat pada tabel 5.6 dibawah ini.

Tabel 5.6 Perbandingan nilai deteksi persentase insider threat skenario struktur *new executive employee committee*

Skenario	Rata-rata dalam satu periode	Selisih perbedaan
Insider Threat *base* model	30.75%	5.97%
Insider Threat skenario *new executive employee committee*	24.78%	

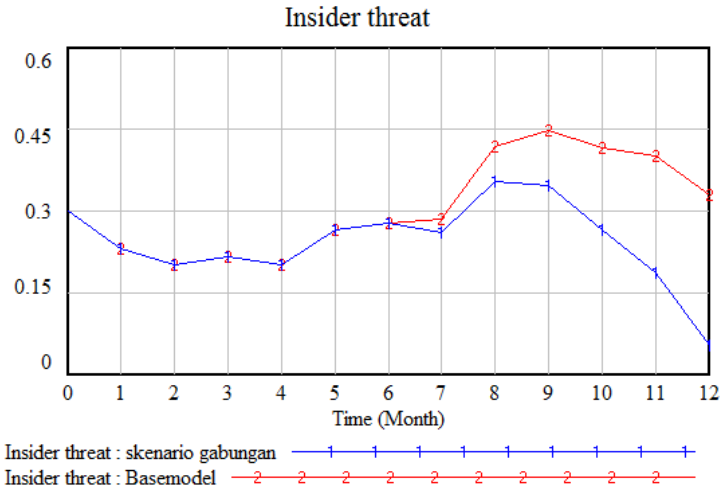
Dari tabel diatas dapat dilihat bahwa hasil perbandingan nilai *insider threat* dari skenario sebelumnya lebih signifikan. Pada skenario struktur kedua ini, dampak variabel yang ditambahkan dapat mengurangi tingkat *insider threat* lebih besar daripada kedua skenario sebelumnya. Solusi ini juga dapat diaplikasikan akan tetapi jika skenario ini diimplementasikan maka hal ini merupakan hal yang pertama di PT XYZ dikarenakan PT XYZ belum pernah memasukkan anggota komite baru yang berlatarbelakang ilmu SI/TI sebelumnya.

5.6.3 Analisis Skenario Supervisor Intervention dan New Executive Management Committee

Skenario struktur ini merupakan skenario gabungan antara skenario struktur pertama yaitu *supervisor intervention* dan *new executive management committee*. Tujuan dari skenario ini adalah untuk mengurangi nilai deteksi persentase

insider threat dari sisi laju penambahnya yaitu indikator *behavioral precursors* dan juga dari sisi laju pengurang yaitu *executive management commitment*.

Pada gambar 5.9 dibawah ini dapat dilihat grafik perbandingan nilai *insider threat* dari *base model* dan skenario gabungan *supervisor intervention* dan *new executive management committee*.



Gambar 5.9 Perbandingan nilai *insider threat* dengan skenario gabungan

Gambar 5.9 diatas menunjukkan perbedaan yang sangat signifikan dari kedua skenario struktur sebelumnya yaitu skenario struktur *supervisor intervention* dan *new executive management committee*. Pada skenario ini total nilai deteksi persentase *insider threat* yang berkurang lebih besar dibandingkan kedua skenario sebelumnya dikarenakan usaha yang dilakukan PT XYZ dalam menangani *insider threat* lebih banyak dan dilakukan dikedua sisi yang berbeda yaitu

sisi pertama dengan mengurangi nilai deteksi persentase ketidakpuasan karyawan dan yang kedua dengan menambah nilai deteksi persentase komitmen manajemen.

Terkait dengan layak tidaknya skenario ini diimplementasikan, terdapat analisis *cost benefit* yang dilakukan pada tabel 5.7 dibawah ini.

Tabel 5.7 Cost Benefit Analysis Supervisor Intervention and New Executive Management

Dampak	Manfaat		Keterangan	Nilai Rupiah
	Tangible	Intangible		
Mengurangi ketidakpuasan karyawan	Meningkatkan produktifias operasional		Meningkatkan produktifitas sampai dengan 10% pada tiap bulan	Rp 90,000,000
		Tingkat karyawan yang berkelakukan buruk dapat berkurang	Loyalitas pegawai meningkat sehingga karyawan tidak "menyerang perusahaan"	
Perubahan Kebijakan Baru	Efisiensi produktifitas terkait sistem informasi dan teknologi informasi		Peningkatan produktifitas surat kabar diperkirakan mencapai 10% sehingga 10% * laba per bulan * 12 bulan	Rp 180,000,000

		Kebijakan terkait SI/TI yang dapat meningkatkan laba perusahaan	Dengan strategi SI/TI yang baru laba diperkirakan dapat bertambah sebesar 10% dalam 12 bulan	Rp 180,000,000
Total				**Rp 450,000,000**
Pengeluaran				**Nilai Rupiah**
Tugas baru supervisor (Bonus sebesar 15% dari gaji sebelumnya Rp 5,000,000				Rp 69,000,000
Pelatihan pada supervisor(1 kali dalam setahun)				Rp 10,000,000
Biaya gaji manajemen komite (1 orang = 20jt/bulan)				Rp 240,000,000
Biaya pengelolaan infrastruktur TI (5jt/bulan)				60,000,000
TOTAL				**Rp 90,000,000**
TOTAL KEUNTUNGAN(*Benefit-Cost*)				**Rp 11,000,000**

Dari hasil analisis *cost benefit*, perusahaan diperkirakan mendapatkan keuntungan sebesar Rp 90,000,000 apabila mengimplementasikan skenario tersebut dengan pertimbangan yang sudah dipaparkan pada tabel. Selain itu perlu dipertimbangkan juga kesulitan-kesulitan yang akan dihadapi apabila mengimplementasikan skenario ini, beberapa permasalahan tersebut yang dapat diidentifikasi yaitu:

1. Sebaiknya mengimplementasikan skenario satu persatu terlebih dahulu terutama skenario *supervisor intervention*, dikarenakan tidak membutuhkan biaya dan *resource* yang besar.
2. Permasalahan yang ada pada skenario ini sama dengan paparan permasalahan dua skenario sebelumnya , dimana permasalahan yang paling besar adalah perlunya pertimbangan yang sangat matang dalam mengangkat manajemen eksekutif baru.

Selain itu juga terdapat keuntungan dalam mengimplementasikan skenario ini yaitu:

1. Apabila diimplementasikan tingkat nilai *insider threat* akan berkurang secara signifikan (gambar 5.9)

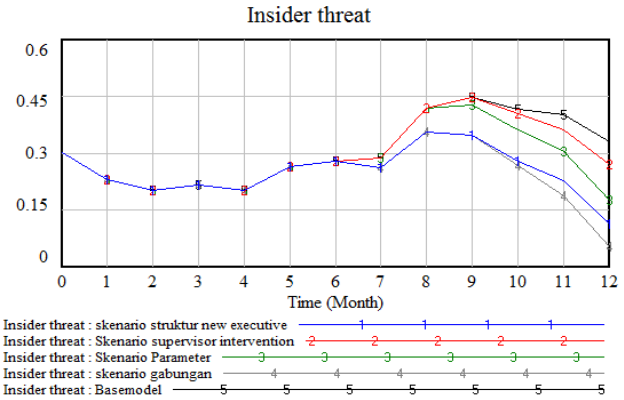
Apabila kedua perbandingan hasil tersebut dirata-rata dalam satu tahun (12 bulan) maka perbandingan nilai tingkat persentase *insider threat* di PT XYZ mempunyai selisih sebesar 6.92%. Hasil lebih jelasnya tentang perbandingan simulasi rata-rata dalam satu tahun dapat dilihat pada tabel 5.8 dibawah ini.

Tabel 5.8 Perbandingan nilai deteksi persentase insider threat skenario struktur *supervisor intervention* dan *new executive employee committee*

Skenario	Rata-rata dalam satu periode	Selisih perbedaan
Insider Threat *base* model	30.77%	6.92%
Insider Threat skenario *gabungan*	23.85%	

5.7 Analisis Seluruh Skenario

Dalam melakukan analisis skenario yang paling baik dan efektif, perlu dilakukan perbandingan antara skenario yang sudah dipaparkan sebelumnya. Setelah skenario tersebut dibandingkan, maka hasil perbandingan tersebut dapat diamati dan dianalisis kesesuaiannya dengan tujuan pembuatan model yaitu untuk mengurangi nilai *insider threat* di PT XYZ.



Gambar 5.10 Perbandingan nilai deteksi persentase *insider threat* keseluruhan skenario

Pada gambar 5.10 diatas terdapat empat skenario yang dibandingan yaitu:

1. Skenario parameter *IT security policy*.
2. Skenario struktur *supervisor intervention*.
3. Skenario struktur *new executive management committee*.
4. Skenario struktur *supervisor intervention* dan *new executive management committee*..

Detail dari rata-rata *insider threat* tiap skenario pertahun (12 bulan) dapat dilihat pada tabel 5.9 dibawah ini.

Tabel 5.9 Rata-rata nilai *insider threat* tiap skenario

Skenario	Rata-rata dalam satu periode
Insider Threat *IT security policy*	27.61%
Insider Threat *Supervisor intervention*	29.21%
Insider Threat New Executive Employee Committee	24.78%
Insider Threat skenario *gabungan*	23.85%

Dari hasil keempat perbandingan tersebut dapat dilihat bahwa nilai *insider threat* yang paling tinggi adalah skenario struktur *supervisor intervention* dengan nilai 29.21%. Hal ini dikarenakan konseling atau intervensi yang dilakukan mempunyai dampak kurang signifikan secara keseluruhan apabila dikaji secara sistem. Salah satu solusi yang dapat dikembangkan dari solusi skenario *supervisor intervention* ini adalah untuk melakukan konseling pada karyawan yang

terindikasi bertingkah laku buruk tanpa menunggu karyawan tersebut diberikan sanksi terlebih dahulu.

Skenario kedua yang paling tinggi adalah skenario parameter *IT security policy* dengan nilai 27.61%. Skenario ini merupakan skenario yang susah dikontrol variabelnya dikarenakan berhubungan dengan ketaatan karyawan dalam menjalankan kebijakan sekuritas perusahaan. Walaupun begitu apabila skenario dapat diimplementasikan, maka nilai persentasi *insider threat* dapat dikurangi dan ditangani lebih baik. Untuk melakukan pengembangan skenario parameter *IT security policy* , PT XYZ dapat menata kebijakan SI/TI di perusahaan atau dapat juga dengan mengimplementasikan sistem *reward and punishment* (sanksi dan hadiah) bagi para karyawan.

Skenario ketiga merupakan skenario yang cukup baik karena nilai *insider threat* secara signifikan sudah berkurang. Skenario ini mempunyai nilai deteksi persentase insider threat sebesar 24.78%. Skenario ini seperti yang sudah dijelaskan sebelumnya merupakan skenario yang agak susah diimplementasikan, akan tetapi apabila PT XYZ dapat mengimplementasikan hal ini maka nilai deteksi persentase *insider threat* di PT XYZ akan berkurang secara drastis.

Skenario terakhir dan yang mempunyai persentase *insider threat* terendah adalah skenario gabungan *supervisor intervention* dan *new executive management committee* dengan nilai sebesar 23.85%. Skenario gabungan ini mempunyai nilai deteksi persentase *insider threat* yang sangat dikarenakan skenario ini dapat mengutilisasi adanya anggota manajemen eksektif baru dan juga adanya intervensi dari supervisor untuk mengurangi persentase *insider threat*

Terkait dengan hasil analisis *cost benefit*, pada tabel 5.10 dibawah ini didapatkan bahwa skenario yang paling mungkin diimplementasikan bagi perusahaan adalah skenario struktur *supervisor intervention* dikarenakan skenario ini tidak membutuhkan biaya yang tinggi dan tingkat kesulitannya paling mudah. Walaupun skenario struktur *supervisor intervention* termasuk skenario yang paling mudah, tidak berarti keuntungan yang didapatkan paling tinggi y aitu hanya Rp 11,000,000.Hal ini dapat dilihat pada skenario struktur gabungan *supervisor intervention* dan *new executive employee committee* yang mempunyai keuntungan paling tinggi yaitu sebesar Rp 71,000,000 yang mempunyai tingkat kesulitan tinggi , sehingga tidak disarankan untuk diimplementasikan pada PT XYZ. Skenario yang dapat diimpelementasikan selanjutnya adalah skenario *new executive employee committee* yang mempunyai keuntungan sebesar Rp 60,000,000 dan mempunyai tingkat kesulitan implementasi dilevel sedang.

Analisis juga dilakukan kepada variabel yang mempunyai hubungan yang signifikan pada model dalam kaitannya dengan *insider threat*. Variabel yang sangat berperan tersebut adalah variabel *actual freedom* yang dipengaruhi oleh nilai variabel *malicious software caught*, variabel *proxy log*, dan variabel *firewall log*. Dari hasil analisis dengan menggunakan SEM-PLS pada sub bab sebelumnya ditemukan bahwa variabel yang sangat mempengaruhi kebebasan adalah variabel *proxy log*. Variabel *proxy log* atau hasil observasi *proxy log* di PT XYZ, yang mencerimankan banyak karyawan yang tidak mematuhi kebijakan terkait kebebasan dalam menggunakan internet (seperti: browsing pada situs-situs *social media*). Beberapa solusi yang dapat dilakukan oleh PT

XYZ adalah: memberikan kebijakan baru seperti hanya memperbolehkan akses pada situs-situs pada jam istirahat, memblokir akses pada situs tersebut pada jam kerja, dan mengurangi *bandwith* internet.

Tabel 5.10 Review Hasil Cost Benefit Analysis Skenario

Skenario	Proyeksi Nilai rupiah	Biaya	Keuntungan	Tingkat kesulitan implementasi
Skenario parameter *IT Security policy*	Rp 216,000,000	Rp 158,000,000	Rp 58,000,000	Tinggi
Skenario struktur *supervisor intervention*	Rp 90,000,000	Rp 79,000,000	Rp 11,000,000	Rendah
Skenario struktur *new executive employee committee*	Rp 360,000,000	Rp 300,000,000	Rp 60,000,000	Sedang
Skenario struktur *supervisor intervention* dan *new executive employee committee*	Rp 450,000,000	Rp 379,000,000	Rp 71,000,000	Tinggi

Halaman ini sengaja dikosongkan

BAB 6
KESIMPULAN DAN SARAN

Bab ini berisi mengenai simpulan yang didapatkan dari hasil penelitian yang telah dilakukan. Simpulan ini diharapkan dapat menjawab tujuan yang telah ditetapkan di awal penelitian. Saran diberikan untuk digunakan dalam penelitian selanjutnya.

6.1 Kesimpulan

Dari pelaksanaan penelitian tugas akhir ini di dapatkan kesimpulan:

1. PT XYZ merupakan perusahaan yang mempunyai potensi terjadi risiko *insider threat*. Hal ini diindikasikan dari tiga indikator utama, yaitu: kebebasan aktual karyawan, tanda-tanda tingkah laku buruk karyawan, dan tanda-tanda pemanfaatan SI/TI yang tidak benar. PT XYZ juga mempunyai langkah-langkah dan usaha untuk mencegah tingginya nilai *insider threat* yaitu dengan adanya komitmen dari manajemen dan keamanan sekuritas teknologi informasi. Dari informasi tersebut, dibuatlah *base model* yang bertujuan untuk meminimalisir nilai *insider threat*.
2. Dari hasil perhitungan validasi seluruh sub model dapat dikatakan valid dengan rincian sebagai berikut:
   a) Sub model *Actual Freedom* memiliki nilai E1 = 4,59%, dan E2 = 1,07%
   b) Sub model *Behavioral precursors* memiliki nilai E1 = 4,01%, dan E2 = 3,63%

c) Sub model *Technical Precursors* memiliki nilai E1 = 3,46%, dan E2 = 22,04%
d) Variabel *Security Investments* memiliki nilai E1 = 0,27%, dan E2 = 8%
e) Variabel *IT Security Policy* memiliki nilai E1 = 4,58%, dan E2 = 3,27%

3. Dari hasil pembuatan base model ditemukan bahwa nilai persentase deteksi *insider threat* paling tinggi mencapai 44.79%. Berdasarkan nilai tersebut yang didapatkan dari hasil simulasi terkait kasus *insider threat*, sebelumnya bahwa kemungkinan PT XYZ terkena risiko *insider threat* termasuk sedang. Beberapa cara untuk mengurangi risiko tersebut adalah dengan membatasi kebebasan karyawan dalam mengakses internet, dan meningkatkan kebijakan sekuritas teknologi informasi terutama dari segi budaya perusahaan.
4. Dari hasil skenario tersebut didapatkan bahwa skenario yang paling baik adalah skenario struktur *supervisor* intervention dan *new executive management committee*. Skenario tersebut mempunyai nilai rata-rata *insider threat* paling rendah sebesar 23.85% serta merupakan skenario paling efektif dalam mengurangi tingkat *insider threat* di PT XYZ .Detail hasil skenariosasi adalah sebagai berikut:
    a) Skenario parameter *IT security policy* dengan nilai *insider threat* rata-rata sebesar 27.61%
    b) Skenario struktur *supervisor intervention* dengan nilai *insider threat* rata-rata sebesar 29.21%
    c) Skenario struktur *new executive management committee* dengan nilai *insider threat* rata-rata sebesar 24.78%

d) Skenario struktur *supervisor* intervention dan *new executive management committee* dengan nilai *insider threat* rata-rata sebesar 23.85%

5. Dari hasil skenariosasi pada tugas akhir ini, skenario yang paling mungkin untuk diimplementasikan adalah skenario struktur *supervisor intervention*. Skenario ini yang paling mungkin dimplementasikan karena skenario ini tidak membutuhkan biaya yang besar dari perusahaan dan tidak perlu mengganti banyak peraturan ataupun kebijakan di PT XYZ. Selanjutnya skenario yang paling efektif untuk diimplementasikan adalah skenario *new executive employee committee* yang dapat memberikan keuntungan sangat besar apabila kesulitan implementasinya dapat diatasi perusahan.Apabila ingin mengimplementasikan gagasan hasil skenario yang lain, perlu dipertimbangkan terlebih dahulu akibatnya sesuai dengan analisis *cost benefit* yang telah dipaparkan.

6.2 Saran

Dari pelaksanaan penelitian tugas akhir ini dapat diberikan saran untuk penelitian selanjutnya antara lain:

1. Terdapat banyak hal yang bisa dikembangkan dari model ini terutama ditinjau dari faktor-faktor lain yang dapat menyebabkan terjadinya *insider threat*. Salah satu faktor yang perlu dipertimbangkan adalah seperti faktor latar belakang dari karyawan penting untuk dimasukkan agar dapat memperkaya penelitian sebelumnya serta kajian yang dilakukan menjadi lebih komprehensif

2. Walaupun topik *insider threat* merupakan topik yang sangat sensitif bagi perusahaan, akan lebih baik dalam mengembangkan model apabila dari perusahaan terutama yang rentan terkena *insider threat* untuk berkolaborasi dalam mengurangi tingkat *insider threat* dan mengembangkan model yang lebih baik.
3. Dalam pengerjaan model ini digunakan waktu dengan satuan bulan/*month*. Akan tetapi dikarenakan *insider threat*, merupakan permasalahan yang kompleks dan dapat terjadi kapan saja, apabila ada data dan informasi yang lebih detail disarankan untuk menggunakan waktu simulasi (*Time Step*) dengan satuan mingguan (*Weekly*).
4. Berdasarkan hasil analisis regresi didapatkan bahwa dua variabel yang dapat mempengaruhi naik turunnya tingkat *insider threat* adalah variabel *IT Security policy* dan *actual freedom*. Untuk mengurangi tingginya nilai *insider threat* PT XYZ dapat meningkatkan nilai variabel kontrol teknis serta mengurangi nilai variabel yang mempengaruhi kebebasan karyawan seperti akses internet , dan installasi software.

DAFTAR PUSTAKA

[1] O. James, Introduction to Information Systems.Eight Edition, New York: Irwin McGraw-Hill, 1997.

[2] J. Bisson and R. Saint-Germain, "The BS 7799/ISO 17799 Standard: For a better approach to information security," 2000.

[3] C. S. Watch, "CyberSecurity Watch Survey: Organization Need More Skilled Cyber Professionals to Stay Secure," CSO Magazine, Deloitte, 2011.

[4] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems: Special Issue: Behavioral and Policy Issues in Information,* vol. 18, no. 2, pp. 101-105, 2009.

[5] S.-C. Yang and Y.-L. Wang, "Insider Threat Analysis of Case Based System Dynamics," *Advanced Computing: An International Journal,* vol. 2, no. 2, pp. 1-17, 2011.

[6] A. P. Moore, A. M. David and M. L. Collins, "A System Dynamics Model for Investigating Early Detection of Insider Threat Risk," in *SystemDynamics.org*, 2013.

[7] J. Sterman, Business Dynamics: Systems Thinking and Modeling for a Complex World, Homewood: McGraw-Hill, 2000.

[8] Carayon, Pascalel and S. Kraemer, "Macroergonomics in WWDU: What about computer and information

system security?," in *International Scientific Conference*, Berlin, 2002.

[9] C. Melara, J. M. Sarriegui, J. J. Gonzales, A. Sawicka and D. L. Cooke, "A System Dynamics Model of an Insider Attack on an Information System," in *Proceedings of the 21st International Conference of the System Dynamics Society*, 2003.

[10] J. Slay and A. Koronios, "Information technology security & risk management," Wiley, 2006, p. 7.

[11] B. Supradono, "Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation)," *Media Elektrika,* vol. 2, no. 1, pp. 4-8, 2009.

[12] R. Krutz and D. Vines, The CISSP Prep Guide - Mastering the Ten Domains of Computer Security, CA: Wiley Computer Pubilishing, 2006.

[13] Fiberlink Communications Corp, "Mobile Security - Outsider Threat vs Insider Threat," 2011. [Online]. Available: http://www.maas360.com/maasters/blog/mobilitymanagement/mobile-security-outsider-threat-vs-insider-threat/. [Accessed 21 March 2014].

[14] J. Predd, S. Pfleeger, K. Hunker and C. Bulford, "Insiders Behaving Badly," *IEEE Security and Privacy,* vol. 6, pp. 66-70, 2008.

[15] D. Cappelli, A. Moore, R. Trzeciak and T. Shimeall, Common Sense Guide to Prevention and Detection of Inisder Threat 3rd Edition, Carnegie Mellon

University: Software Engineering Insitute, 2009.

[16] M. G. Gelles and T. Mahoutchian, "Mitigating the Insider," Deloitte Consulting LLP, 2012.

[17] S.-C. Yang and Y.-L. Wang, "System Dynamics Based Insider Threats Modeling," *International Journal of Network Security & Its Applications (IJNSA),* vol. 3, no. 3, pp. 1-14, 2011.

[18] S. M. Bellovin, "The Insider Attack Problem Nature and Scope," *Insider Attack and Cyber Security,* pp. 1-4, 2008.

[19] Q. Althebyan and B. Panda, "A Knowledge-Based Bayesian Model for Analyxing a System after an Insider Attack," in *Proceedings of the IFIP TC-Information Security Conference*, Boston, 2008.

[20] A. Moore, D. Cappeli, T. Caron, E. Shaw and R. Trzeciak, "Insider Theft of Intellectual Property for Business Advantage:A preliminary Model," *CERT Program,* 2009.

[21] J. White and B. Panda, "Automatic Identification of Critical Data Items in a Database to Mitigate the Effects of Malicious Insiders," *Information Systems Security,* pp. 208-221, 2009.

[22] M. Hanley, T. Dean, W. Schroeder and M. H, "An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases.," Software Engineering Institute, 2011.

[23] D. Cappeli, T. Caron, R. Trzeciak and A. Moore, "Spotlight On: Programming Techniques Used as an Insider Attack Tool," 2008.

[24] G. B. Maglakras and S. M. Furnell, "Insider Threat Prediction Tool:Evaluating the Probability of IT Misuse," *Computers & Security,* vol. 21, no. 1, pp. 62-73, 2001.

[25] M. S. Bishop, S. Engle S Peisert:Whalen and C. Gates, "We have met the enemny and he is us," in *Proceedings of the 2008 worhsop on new security paradigms*, California, 2008.

[26] E. Kowalski, T. Conway, S. Keverline, M. D. Williams, B. Cappeli, Willke and A. Moore, "Insider Threat Study: Illicit Cyber Activity in the Government Sector," *U.S Secret Service and CERT/SEI,* 2008.

[27] J. Hunker and C. W. Probst, "Insiders and Insider Threats - An Overview of Defintions and Mitigagation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA),* vol. 2, no. 1, pp. 4-27, 2011.

[28] D. M. Cappelli, A. G. Desai, A. P. Moore, T. J. Shimeall, E. A. Weaver and B. J. Wilke, Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information Systems, or Networks, Pittsburgh: Cert Program, 2007.

[29] F. L. Greitzer and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," *Journal of Strategic Security,* vol. 4, no. 2, pp. 25-48, 2011.

[30] C. Langin and S. Rahimi, "Soft Computing in Intrusion Detection:the State of the Art," *Journal of AMbient Intelligence and Humanized Computing,* pp. 133-45,

2010.

[31] W. D. Kelton and A. M. Law, Simulation Modelling and Analysis, McGraw-Hill, 1991.

[32] E. Suryani, Konsep Dasar Sistem Simulasi, Surabaya, 2006.

[33] A. Munshi, P. Dell and H. Armstrong, "Insider Threat Behavior Factors: A comparison of theory with reported incidents," in *Hawaii International Conference on System Sciences*, Hawaii, 2012.

[34] CPNI, Personnel Security Risk Assessment, Centre for the Protection of National Infrastructure, 2013.

[35] J. Royds, "Virtual Battlefield," *CIR Magazine,* 2009.

[36] I. Crinson, "Assesing the insider-outsider threat' duality in the context of the development of public-private partnerships delivering choice' in healthcare services," *Information Security Technical Report,* vol. 13, no. 4, pp. 202-206, 2008.

[37] Department of Defense, "DoD Insider Threat Mitigation".

[38] R. J. Simmons, Working with the Risk Assessment Matrix, 2010.

[39] M. Kramarz and W. Kramarz, "Simulation Modelling of Complex Distribution Systems," *Procedia Social and Behavioral Sciences,* pp. 283-291, 2011.

[40] J. Rahmawati, Aplikasi Model Sistem Dinamis dalam Perencanaan Strategis CRM di Perusahaan Telekomunikasi (Studi Kasus: PT Telekomunikasi Indoenesia), Surabaya, 2012.

[41] P. Kotler, Marketing Management Millenium Edition, Prentice-Hall Inc., 2000.

[42] W. D. Perreault and E. J. McCarthy, Basic Marketing - A Managerial Approach, New York: McGraw-Hill, 2002.

[43] P. Kotler, Marketing Management: Analysis, Planning, Implementation and Control, Pearson Custom Publishing, 1993.

[44] A. M. Law and W. D. Kelton, Simulation Modelling and Analysis, McGraw-Hill, 1991.

[45] J. D. Wishart, *Modelling, Simulation, Testing, and Optimization of Advanced Hybrid,* 2008.

[46] I. M. I. Hasan, Pokok-Pokok Materi Teori Pengambilan Keputusan, Jakarta: Ghalia Indonesia, 2002.

[47] G. P. Richardson, "Reflections on The Foundations of System Dynamics," *System Dynamic Reviews,* pp. 219-243, 2011.

[48] G. P. Richardson, "Problems with causal loop diagrams," *System Dynamic Reviews,* pp. 158-170, 1986.

[49] D. Sherwood, Seeing the Forest for the Trees: A Manager's Guide to Applying Systems Thinking, Boston, London: Nicholas Brealey, 2002.

[50] E. G. Anderson and L. J. Black, "Accumulations of Legitimacy: Exploring," in *25th International Conference of the System Dynamics Society*, Boston, Massachusetts, 2007.

[51] E. Suryani, Pemodelan dan Simulasi, Yogyakarta: Graha Ilmu, 2006.

[52] A. Maria, *Introduction to Modeling And Simulation,* Ney York, 1997.

[53] B. L. Alford and A. Biswas, "The Effects of Discount Level, Price Consciousness and Sale Proneness on Consumers' Price Perception and Behavioral Intention," *Journal of Business Research,* pp. 775-783, 2002.

[54] BPS, "Penduduk Menurut Wilayah dan Agama yang Dianut," 2010. [Online]. Available: http://sp2010.bps.go.id/index.php/site/tabel?search-tabel=Penduduk+Menurut+Wilayah+dan+Agama+yang+Dianut&tid=321&search-wilayah=Indonesia&wid=0000000000&lang=id.

[55] BPS, "Penduduk Menurut Wilayah dan Agama yang Dianut - Provinsi Jawa Barat," 2010. [Online]. Available: http://sp2010.bps.go.id/index.php/site/tabel?search-tabel=Penduduk+Menurut+Wilayah+dan+Agama+yang+Dianut&tid=321&search-wilayah=Provinsi+Jawa+Barat&wid=3200000000&lang=id.

[56] D. E. Kieso, J. J. Weygandt and T. D. Warfield, Intermediete Accounting Eleventh Edition, John Wiley & Sons, Inc., 2004.

[57] W. W. Pyle and K. D. Larson, Fundamental Accounting Principles, Homewood, Illinois: Richard D. Irwin, Inc., 1984.

[58] B. Hoke, Profit Is Not A Dirty Word, Philadelpia: Ekoh, Inc., 2007.

[59] B. Bix, "Are discounts a good way to increase sales?," *BB Marketing Plus,* 21 April 2010.

[60] P. J. Eisen, Accounting, New York: Barron's Education Series,Inc., 2007.

[61] M. A. Stiving, Impact Pricing: Your Blueprint for Driving Profits, Madison: Jere Calmes, 2011.

[62] G. Brooks, R. Mortimer and C. Smith, Marketing for Dummies, Britain, 2011.

BIODATA PENULIS

Penulis lahir di Surabaya, 18 Desember 1991, merupakan anak pertama dari dua bersaudara. Penulis telah menempuh pendidikan formal di TK Ya-bunayya Surabaya, SD Muhammadiyah 4 Surabaya, SMP Al-Hikmah Surabaya, dan SMA Negeri 16 Surabaya. Setelah menerima kelulusan SMA, Penulis melanjutkan kejenjang pendidikan selanjutnya pada tahun 2010 di Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya, dan terdaftar sebagai mahasiswa dengan NRP 5210 100 003.

Selama menjadi mahasiswa, penulis telah mengikuti kegiatan kemahasiswaan dan aktif anggota staff Himpunan Mahasiswa Sistem Informasi (HMSI). Penulis juga tercatat sebagai asisten praktikum Pengantar Sistem Informasi (PSI), Pengelolaan Hubungan Pelanggan (PHP), Kewirausahaan Teknologi Informasi (KWUTI) dan Perencanaan Sumber Daya Perusahaan (PSDP).

Pada Jurusan Sistem Informasi, penulis mengambil bidang minat Laboraturium SPK dengan topik simulasi sistem dinamik dalam pengerjaan tugas akhir.

Halaman ini sengaja dikosongkan

LAMPIRAN A
DATA HASIL WAWANCARA

- **Rangkuman Hasil Wawancara**

  Wawancara dilakukan dengan manajer TI pada PT XYZ, supervisor aplikasi bagian TI, dan supervisor aplikasi bagian jaringan. Berikut ini adalah pertanyaan-pertanyaan yang ditanyakan pada PT. XYZ:

  1. Seperti apakah proses bisnis di PT XYZ?
  2. Permasalahan sekuritas apa saja yang pernah ada di PT XYZ terkait *insider threat* terkait dengan faktor penyebab *insider threat* seperti akses dan tingkat kepercayaan,posisi teknis dan keahlian teknis, dan kebijakan keamanan informasi?
  3. Dalam persentase 0-100 seberapa ketatkah peraturan terkait penggunaan teknologi informasi di PT XYZ?
  4. Sanksi apa yang diberikan kepada karyawan yang melanggar prosedur terkait dengan kelakukan yang tidak pantas di tempat kerja?
  5. Dalam persentase 0-100 berapa batas toleran awal dari tingkah laku yang dilakukan karyawan terkait penggunaan teknologi informasi.
  6. Apa saja faktor-faktor yang dapat mempengaruhi karyawan dapat dihukum oleh perusahaan?
  7. Bagaimana cara manajemen dalam mengurangi indikasi tingkah laku buruk dari karyawan?
  8. Apa saja faktor-faktor yang dapat mempengaruhi bagian TI untuk mengidentifikasi serangan dari dalam?

9. Bagaimana usaha dari manajemen untuk mengurangi tingkat serangan dari dalam?
10. Bagaimana peran audit dalam meningkatkan sekuritas TI terkait *insider threat*?
11. Seberapa besar investasi yang dikeluarkan oleh manajemen dalam meningkatkan sekuritas?
12. Apa saja yang mempengaruhi sekuritas di PT XYZ?
13. Apa saja hal yang harus diperhatikan terkait pemberian sanksi di PT XYZ?
14. Apakah ada hububungannya antara sanksi dan peningkatan ketidakpuasan karyawan?
15. Seberapa besar peran sekuritas TI saat ini serta manajemen dalam mengurangi resiko insider threat?
16. Bagaimana cara perusahan dalam memitigasi aksi teknis yang dapat merugikan perusahaan?
17. Menurut bapak, apakah ada cara-cara baru yang dapat menanggulangi tingginya tingkat *insider threat*?

- **Jawaban dari wawancara**

1. Proses bisnis di PT XYZ dibantu dengan dua IT Support yaitu divisi MIS yaitu Management Information System dan News Room IS. MIS mengelola proses bisnis berupa periklananan, keuangan, sirkulasi koran, dan personalia serta bagian umum. Bagian News Room IS mengelola sistem informasi pada bagian redaksi dan bekerja aktif pada saat malam hari.

2. Permasalahan sekuritas biasanya dilakukan oleh pihak luar yang ingin mencoba memaksa masuk ke jaringan ataupun database di PT XYZ. Terkait dengan faktor-faktor yang menyebabkan dapat menyebabkan terjadinya *insider threat* sebenarnya sangat berbeda dengan perusahaan karya yang jarang terjadi akan tetapi dapat terjadi apabila karyawan mengalami rasa tidak puas dan memang ingin memanfaatkan celah dari kebebasan dia dalam menggunakan sistem informasi dan teknologi informasi.
3. Manajer TI:60%
   Bagian Personalia:60%
   Supervisor bagian jaringan TI:70%
   Supervisor bagian aplikasi TI:50%
   Hal ini dikarenakan pada saat awal karyawan masuk , karyawan masih tidak ingin mencoba2 atau mengutak-atik hal-hal yang berkaitan dengan si/ti
4. Terdapat tiga sanksi yaitu sanksi ringan, sanksi sedang, dan sanksi berat . Sanksi yang paling berat adalah pemecatan tetapi hal tersebut perlu dikaji terlebih dahulu oleh bagian manajemen
5. Manajer TI:40%
   Bagian Personalia:50%
   Supervisor bagian jaringan TI:30%
   Supervisor bagian aplikasi TI:40%
   Sekitar 40% karena awal-awal memang kami sudah ketat disitu.
6. Beberapa faktor yang dapat mempengaruhi karyawan dihukum adalah masalah absensi, ketidak patuhan terhadap peraturan, isu performa, dan

kurangnya respon terhadap feedback dari rekan kerja. Faktor-faktor tersebut apabila dipersentasekan mempunyai persentase sekitar 1 sampai dengan 5 persen

7. Faktor-faktor yang mempengaruhi adalah log dari akun , database, dan internet dari karyawan. Faktor-faktor tersebut apabila dipersentasekan mempunyai persentase antara 1 sampai dengan 5%/
8. Dalam melakukan mitigasi aksi tingkah laku buruk bagi karyawan manajemen menentukan tingkat risiko tersebut sebesar 40% dan 60% maka manajemen akan menganggap karyawan telah melebihi nilai indikasi tingkah laku buruk. Pada saat sanksi telah diberikan pada manajemen dengan melakukan sosialisasi kepada karyawan. Selain itu terdapat langkah-langkah seperti memperketat pengawasan pada karyawan oleh supervisor, teguran bagi karyawan, dan briefing tiap pagi hari untuk meningkatkan motivasi karyawan. Apabila dipersentasekan , langkah-langkah tersebut dapat mengurangi indikasi tingkah laku karyawan yang buruk sebesar 10% untuk tingkah laku buruk yang sedang hingga sampai dengan 30% untuk tingkah laku buruk yang dikategorikan merugikan sekali bagi perusahaan.
9. Manajemen melakukan audit dan berinvestasi pada sekuritas teknologi informasi di PT XYZ. Hasil audit mempengaruhi banyaknya investasi yang dilakukan oleh manajemen. Selain itu infrastruktur sekuritas juga dapat obsolete atau rusak. Hal ini sering terjadi pada akhir bulan. Biasanya pada bulan

biasa hanya berkurang sekitar 20%- 30% tetapi pada saat akhir bulan level sekuritas bisa berkurang sampai 30%- 50%.

10. Audit mempunyai peran esensial dikarenakan sebagian hasil dari audit mempengaruhi keputusan manajemen dan juga peningkatan prosedur operasional dalam peningkatan sekuritas.
11. Tergantung dari komitmen manajemen, dalam dua tahun terakhir kira-kira hampir sekitar 2 milyar untuk investasi teknologi informasi dan sistem informasi, akan tetapi untuk sekuritas mungkin dapat diambilsekitar 50 juta .Apabila dirasa perlu oleh manajemen untuk meningkatkan besar investasinya maka investasi akan lebih tinggi. Sempat pada waktu itu investasi sekuritas lebih dari 100jt dikarenakan memang tingkat keamanan teknologi informasi perlu dibenahi karena hasil audit teknologi informasi menunjukkan perlunya peningkatan sekuritas.
12. Beberapa hal yang mempengaruhi tingkat sekuritas di PT XYZ adalah kebijakan sekuritas yang kami rasa hanya dipatuhi sekitar 50% saja karena masih banyak penyimpangan terkait si/ti yang dilakukan oleh karyawan, target sekuritas , investasi, komitmen manajemen, dan juga audit yang dilakukan oleh PT XYZ bersama pihak luar (pihak ketiga). Selain itu juga terdapat faktor lain berupa perawatan infrastruktur TI , dimana infrastruktur TI kami dapat juga usang atau *obsolete*, sehingga dapat mengurangi performa dalam menanggulangi serangan-serangan sekuritas. Apabila infrastruktur

TI kami usang, maka sekuritas akan lebih rentan terkena serangan. Infrastruktur TI apabila usang dapat mengurangi nilai sekuritas apabila dipersentasekan sekitar 30% hingga 50%.

13. Sanksi diberikan apabila menurut manajemen tingkah laku yang disebabkan oleh karyawan telah melebihi batasan yang diberikan oleh manajemen dalam bentuk poin. Apabila karyawan telah melalui poin 6-15 maka karyawan tersebut akan terkena sanksi sedang seperti surat peringatan. Apabila sudah melebihi poin 15 maka sanksi yang dikenakan dapat berupa pengurangan gaji. Sanksi sendiri memiliki poin 0 pada awalnya.
14. Ada hubungannya . Bagi kami rata-rata karyawan yang mendapatkan sanksi selalu berhubungan dengan kebebasan dan jenis sanksi yang diberikan. Apabila sanksi yang diberikan ringan maka karyawan tetap biasa saja. Tetapi apabila sanksi yang diberikan bersifat sedang dan berat, maka karyawan tersebut dapat saja mengalami rasa ketidakpuasan. Kira-kira jika dipersentasekan rasa tidak puas tersebut dapat bertambah sebesar 2.5% sampai 5%.
15. Keduanya mempunyai peran penting dalam mengurangi risiko *insider threat*. Akan tetapi saat ini permasalahan *insider threat* bukan menjadi masalah utama sehingga level sekuritas dan komitmen manajemen masih kurang dalam menangani permasalahan *insider threat*.
16. Usaha yang kami lakukan dalam memitigasi tindakan buruk teknis karyawan adalah melakukan

pengecekan tindakan tidak normal *malicious*, mematikan jaringan internet, mengunci semua komputer secara terpusat, serta membatasi akses akun karyawan. Setelah dilakukan mitigasi, biasanya kejadian terkait indikasi penyerangan dari dalam langsung berkurang sebesar 20 sampai dengan 40%.

17. Ada beberapa cara, saya setuju dengan referensi yang mengimplementasikan intervensi supervisor, dikarenakan sampai saat ini masih belum ada kebijakan tersebut dan dapat diimplementasikan dengan mudah. Kami yakin dengan mengimplementasikan hal tersebut nilai persentase ketidakpuasan dapat berkurang sebesar 5% sampai dengan 10%. Selain cara ini juga terdapat cara lain yaitu dengan melobi manajemen eksektif agar lebih *concern* kepada permasalahan sekurits dan teknologi informasi, dikarenakan belum adanya *background* ilmu teknologi informasi di bagian manajemen eksekutif.

Halaman ini sengaja dikosongkan

LAMPIRAN B
DATA MASUKAN

Pada lampiran B ini ditampilkan data-data masukan yang digunakan dalam pengerjaan tugas akhir ini. Berikut adalah tabel dari data-data tersebut.

1. Data Persentase Kebebasan Karyawan Tahun 2013-2014

Tabel B.1 Persentase Kebebasan Karyawan 2013-2014

No	Bulan	*Actual Freedom*
1	Jan'13	60%
2	Feb'13	60%
3	Mar'13	60%
4	Apr'13	60%
5	Mei'13	70%
6	Jun'13	70%
7	Jul'13	70%
8	Ags'13	70%
9	Sep'13	70%
10	Okt'13	70%
11	Nov'13	70%
12	Des'13	75%

2. Data Persentase tanda tingkah laku buruk karyawan Tahun 2013-2014

Tabel B.2 Persentase Tanda Tingkah Laku Buruk Karyawan 2013-2014

No	Bulan	*Behavioral Precursors*
1	Jan'13	30%
2	Feb'13	40%
3	Mar'13	50%
4	Apr'13	50%
5	Mei'13	60%
6	Jun'13	60%
7	Jul'13	78%
8	Ags'13	70%
9	Sep'13	70%
10	Okt'13	60%
11	Nov'13	60%
12	Des'13	70%

3. Data Persentase Tanda Penyalahgunaan SI/TI Karyawan Tahun 2013-2014

Tabel B.3 Persentase Tanda Penyalahgunaan SI/TI Karyawan Tahun 2013-2014

No	Bulan	*Technical Precursors*
1	Jan'13	40%
2	Feb'13	55%
3	Mar'13	50%
4	Apr'13	55%
5	Mei'13	40%

No	Bulan	*Technical Precursors*
6	Jun'13	50%
7	Jul'13	60%
8	Ags'13	60%
9	Sep'13	40%
10	Okt'13	65%
11	Nov'13	60%
12	Des'13	60%

4. Data Persentase Kebijakan Sekuritas TI Tahun 2013-2014

Tabel B.4 Persentase Kebijakan Sekuritas TI 2013-2014

No	Bulan	*IT Security Policy*
1	Jan'13	40%
2	Feb'13	35%
3	Mar'13	30%
4	Apr'13	35%
5	Mei'13	35%
6	Jun'13	25%
7	Jul'13	50%
8	Ags'13	40%
9	Sep'13	35%
10	Okt'13	40%
11	Nov'13	20%
12	Des'13	30%

5. Data Keuangan Investasi Sekuritas TI Tahun 2013-2014

Tabel B.5 Keuangan Investasi Sekuritas TI 2013-2014

No	Bulan	*Security Investments*
1	Jan'13	Rp3,800,000.00
2	Feb'13	Rp4,200,000.00
3	Mar'13	Rp3,600,000.00
4	Apr'13	Rp3,500,000.00
5	Mei'13	Rp3,500,000.00
6	Jun'13	Rp4,000,000.00
7	Jul'13	Rp4,500,000.00
8	Ags'13	Rp3,500,000.00
9	Sep'13	Rp4,000,000.00
10	Okt'13	Rp3,500,000.00
11	Nov'13	Rp5,200,000.00
12	Des'13	Rp8,000,000.00

6. Data Persentase kebebasan karyawan (yang melanggar) TI Tahun 2013-2014

Tabel B.6 Data Presentase Kebebasan Karyawan

Bulan	Firewall Log	Proxy Log	Malicious Software Caught
Jan'13	58.74%	56.40%	56.67%
Feb'13	53.63%	58.96%	66.67%
Mar'13	51.69%	59.32%	53.33%
Apr'13	58.41%	63.18%	60.00%
Mei'13	62.63%	66.01%	66.67%

Bulan	Firewall Log	Proxy Log	Malicious Software Caught
Jun'13	56.74%	67.36%	63.33%
Jul'13	60.46%	64.10%	70.00%
Ags'13	67.49%	64.85%	73.33%
Sep'13	68.76%	71.07%	70.00%
Okt'13	71.80%	68.10%	73.33%
Nov'13	71.38%	71.13%	70.00%
Des'13	73.31%	72.39%	73.33%

7. Data Persentase detail kebijakan TI (IT Security Policy) Tahun 2013-2014

Tabel B.7 Detail Kebijakan TI

Bulan	Persentase kontrol teknis	Persentase kontrol formal	Persentase kontrol informal
Jan'13	25%	10%	5%
Feb'13	20%	10%	5%
Mar'13	15%	10%	5%
Apr'13	15%	20%	5%
Mei'13	10%	15%	10%
Jun'13	15%	5%	5%
Jul'13	20%	25%	5%
Ags'13	15%	5%	10%
Sep'13	10%	10%	5%
Okt'13	25%	10%	5%
Nov'13	10%	5%	5%
Des'13	15%	15%	10%

Halaman ini sengaja dikosongkan

LAMPIRAN C
DATA HASIL SIMULASI *BASEMODEL*

Pada lampiran C ini ditampilkan data-data hasil simulasi yang dijalankan dengan menggunakan software Vensim. Data simulasi ini menjadi acuan untuk validasi model sistem dengan membandingkan dengan data aktualnya

8. Data Simulasi Persentase Kebebasan Karyawan Tahun 2013-2014

Tabel C.1 Simulasi Persentase Kebebasan Karyawan 2013-2014

No	Bulan	*Actual Freedom*
1	Jan'13	57%
2	Feb'13	58%
3	Mar'13	59%
4	Apr'13	59%
5	Mei'13	60%
6	Jun'13	62%
7	Jul'13	67%
8	Ags'13	66%
9	Sep'13	69%
10	Okt'13	69%
11	Nov'13	71%
12	Des'13	71%

9. Data Persentase Simulasi tanda tingkah laku buruk karyawan Tahun 2013-2014

Tabel C.2 Persentase Simulasi tanda tingkah laku buruk karyawan 2013-2014

No	Bulan	*Behavioral Precursors*
1	Jan'13	41%
2	Feb'13	44%
3	Mar'13	48%
4	Apr'13	53%
5	Mei'13	56%
6	Jun'13	59%
7	Jul'13	66%
8	Ags'13	58%
9	Sep'13	70%
10	Okt'13	71%
11	Nov'13	75%
12	Des'13	85%

10. Data Simulasi Persentase Tanda Penyalahgunaan SI/TI Karyawan Tahun 2013-2014

Tabel C.3 Simulasi Persentase Tanda Penyalahgunaan SI/TI Karyawan 2013-2014

No	Bulan	*Technical Precursors*
1	Jan'13	43%
2	Feb'13	46%
3	Mar'13	50%
4	Apr'13	55%

No	Bulan	*Technical Precursors*
5	Mei'13	48%
6	Jun'13	60%
7	Jul'13	46%
8	Ags'13	52%
9	Sep'13	34%
10	Okt'13	47%
11	Nov'13	62%
12	Des'13	56%

11. Data Simulasi Persentase Kebijakan Sekuritas TI Tahun 2013-2014

Tabel C.4 Simulasi Persentase Kebijakan Sekuritas TI 2013-2014

No	Bulan	*IT Security Policy*
1	Jan'13	36%
2	Feb'13	35%
3	Mar'13	34%
4	Apr'13	31%
5	Mei'13	37%
6	Jun'13	33%
7	Jul'13	48%
8	Ags'13	45%
9	Sep'13	42%
10	Okt'13	46%
11	Nov'13	25%
12	Des'13	22%

12. Data Keuangan Investasi Sekuritas TI Tahun 2013-2014

Tabel C.5 Keuangan Investasi Sekuritas TI 2013-2014

No	Bulan	*Security Investments*
1	Jan'13	Rp3,822,440.00
2	Feb'13	Rp5,259,160.00
3	Mar'13	Rp4,068,100.00
4	Apr'13	Rp3,801,890.00
5	Mei'13	Rp3,461,540.00
6	Jun'13	Rp3,766,050.00
7	Jul'13	Rp3,480,950.00
8	Ags'13	Rp3,271,150.00
9	Sep'13	Rp3,995,340.00
10	Okt'13	Rp3,270,050.00
11	Nov'13	Rp5,058,710.00
12	Des'13	Rp8,183,230.00

LAMPIRAN D
HASIL SKENARIOSASI

Pada lampiran D ini ditampilkan data-data hasil simulasi seluruh skenario dan base model, yaitu skenario parameter *IT security policy*, skenario struktur *supervisor intervention*, skenario struktur *new executive employee committee*,dan skenario struktur *IT security policy* dan *new executive employee committee* yang terkait dengan *insider threat*.

13. Hasil Simulasi persentase *insider threat* base model

Tabel D.1 Hasil Simulasi persentase insider threat base model

No	Bulan	*Insider Threat*	*Rata-Rata persentase dalam 12 bulan*
1	Jan'13	23.33%	31.41%
2	Feb'13	23.17%	
3	Mar'13	21.50%	
4	Apr'13	20.17%	
5	Mei'13	26.48%	
6	Jun'13	27.67%	
7	Jul'13	28.57%	
8	Ags'13	41.79%	
9	Sep'13	44.79%	
10	Okt'13	44.79%	
11	Nov'13	41.68%	
12	Des'13	33.00%	

14. Hasil Simulasi persentase *insider threat* skenario *supervisor intervention*

Tabel D.2 Hasil Simulasi persentase insider threat skenario supervisor intervention

No	Bulan	*Insider Threat*	*Rata-Rata persentase dalam 12 bulan*
1	Jan'13	23.33%	29.21%
2	Feb'13	20.06%	
3	Mar'13	21.50%	
4	Apr'13	20.17%	
5	Mei'13	26.48%	
6	Jun'13	27.67%	
7	Jul'13	28.57%	
8	Ags'13	41.79%	
9	Sep'13	44.79%	
10	Okt'13	39.68%	
11	Nov'13	34.15%	
12	Des'13	22.35%	

15. Hasil Simulasi persentase *insider threat* skenario *new executive employee committee*

Tabel D.3 Hasil Simulasi persentase insider threat skenario new executive employee committee

No	Bulan	*Insider Threat*	*Rata-Rata persentase dalam 12 bulan*
1	Jan'13	23.11%	24.78%
2	Feb'13	20.06%	
3	Mar'13	21.50%	
4	Apr'13	20.17%	
5	Mei'13	26.48%	
6	Jun'13	27.76%	
7	Jul'13	26.07%	
8	Ags'13	35.54%	
9	Sep'13	34.79%	
10	Okt'13	27.93%	
11	Nov'13	22.65%	
12	Des'13	11.26%	

16. Hasil Simulasi persentase *insider threat* skenario *IT security policy* dan *new executive employee committee*

Tabel D.4 Hasil Simulasi persentase insider threat skenario IT security policy dan new executive employee committee

No	Bulan	*Insider Threat*	*Rata-Rata persentase dalam 12 bulan*
1	Jan'13	23.33%	23.85%
2	Feb'13	20.06%	
3	Mar'13	21.50%	
4	Apr'13	20.17%	
5	Mei'13	26.48%	
6	Jun'13	27.77%	
7	Jul'13	26.07%	
8	Ags'13	35.54%	
9	Sep'13	34.79%	
10	Okt'13	26.60%	
11	Nov'13	18.65%	
12	Des'13	5.26%	