PENGEMBANGAN METODE INTEGRASI ISO/ IEC 17799:2005 DAN ISO/ IEC 27001:2005 KE DALAM *BALANCED SCORECARD* DEPARTEMEN TEKNOLOGI INFORMASI BANK D UNTUK MENJADI *BALANCED SCORECARD* GENERASI KE-4

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana teknik

DISTYA TARWORO ENDRI
0404070247

UNIVERSITAS INDONESIA
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK INDUSTRI
DEPOK
JULI 2008

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama : Distya Tarworo Endri

NPM : 0404070247

Tanda Tangan :

Tanggal : 10 Juli 2008

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh	:
Nama	: Distya Tarworo Endri
NPM	: 0404070247
Program Studi	: Teknik Industri
Judul Skripsi	: Pengembangan Metode Integrasi ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005 Ke Dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D Untuk Menjadi *Balanced Scorecard* Generasi Ke-4

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Teknik Industri Fakultas Teknik Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Ir. Akhmad Hidayatno, MBT	( )
Penguji	: Ir. Isti Surjandari, Ph.D	( )
Penguji	: Ir. Amar Rachman, MEIM	( )
Penguji	: Ir. Yadrifil, MSc	( )

Ditetapkan di : Depok

Tanggal : 10 Juli 2008

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS
(Hasil Karya Perorangan)

Sebagai civitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Distya Tarworo Endri
NPM/NIP : 0404070247
Program Studi : Teknik Industri
Fakultas : Teknik
Jenis karya : Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

PENGEMBANGAN METODE INTEGRASI ISO/ IEC 17799:2005 DAN ISO/ IEC 27001:2005 KE DALAM *BALANCED SCORECARD* DEPARTEMEN TEKNOLOGI INFORMASI BANK D UNTUK MENJADI *BALANCED SCORECARD* GENERASI KE-4

beserta perangkat yang ada (bila diperlukan). Dengan Hak Bebas Royalti Non-Ekslusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/ mempublikasikannya di internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/ pencipta dan sebagai pemilik Hak Cipta. Segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah ini menjadi tanggungjawab saya pribadi.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 1 Juli 2008
Yang menyatakan

(Distya Tarworo Endri)

UCAPAN TERIMAKASIH

Puji syukur pada ALLAH SWT karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan penelitian ini. Selain itu, penulis mengucapkan terima kasih dari lubuk hati yang terdalam kepada :

1. Ibu, Bapak, Mbak Ammy, Mas Banto, Mbak Cipuk, yang telah memberi cinta kasih tak terhingga, didikan, doa, inspirasi, semangat, teladan, nasehat, dan semua pengalaman teridah dan paling berharga dalam hidupku
2. Bapak Akhmad Hidayatno, selaku pembimbing akademis dan pembimbing skripsi yang telah memberi kepercayaan, masukan, dukungan, pelajaran tentang hidup, dan bantuan yang luar biasa
3. Seluruh dosen Departemen Teknik Industri atas dukungan dan masukan yang diberikan dari awal perkuliahan hingga tahap penyelesaian skripsi
4. Bapak Dwi Kurniawan selaku pembimbing skripsi dari perusahaan yang telah membantu dalam usaha memperoleh data, serta memberi saran dan dukungan
5. Bapak Noviadi S. Miraza, Bapak Djarot Sumantri, dan Bapak Hadi Cahyono yang telah bersedia membantu dalam penyelesaian skripsi ini
6. Asep Haekal yang telah memberi doa, dukungan, saran yang membangun, keceriaan, dan kasih sayang setiap saat
7. Dee, Fahmi, Gode, Cici, Glory, Dika, Mirza, Nadya, Nuri, Ipeh, Ade, Dhanu, Zia, Adi, saudara asuhku Dipi dan Anwar, seluruh rekan-rekan Teknik Industri 2004, serta semua temanku dimanapun kalian berada atas doa, dukungan, dan persahabatan yang indah selamanya
8. Agus, Nana, Kiki, Anggi, Kak Mia, Toni, Bagas, Ari S, Noni, Dita, Pak Andi, dan Pak Ade selaku Tim Proyek LUSI ISO/IEC 27001 atas doa dan dukungan.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 1 Juli 2008

Penulis

RIWAYAT HIDUP PENULIS

Nama : Distya Tarworo Endri

Tempat, Tanggal Lahir : Jakarta, 18 Juli 1986

Alamat : Jl. H. Saiyan No. 57 Rt: 004 Rw: 006, Tanjung Barat, Jagakarsa, Jakarta Selatan

Pendidikan:

1.	SD	SDN Pejaten Timur 17 Pagi	1992-1998
2.	SLTP	SLTPN 41 Jakarta	1998-2001
3.	SMA	SMAN 8 Jakarta	2001-2004
4.	S-1	Departemen Teknik Industri, Fakultas Teknik Universitas Indonesia	2004-2008

ABSTRAK

Nama : Distya Tarworo Endri
Program studi : Teknik Industri
Judul : Pengembangan Metode Integrasi ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005 Ke Dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D Untuk Menjadi *Balanced Scorecard* Generasi Ke-4

Seiring dengan kemajuan teknologi, peningkatan interkonektivitas bisnis Bank D yang berarti peningkatan jumlah dan variasi ancaman serta kerawanan keamanan informasi tak terelakkan. Oleh karena itu, peningkatan daya dukung dan sumber daya teknologi informasi pada Bank D sangat penting.

Salah satu cara untuk menjawab tantangan diatas adalah melalui penerapan *Balanced Scorecard* Departemen Teknologi Informasi di Bank D berdasarkan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005, yang merupakan aplikasi pertama *Balanced Scorecard* generasi ke-4 di Indonesia.

Yang dimaksud dengan metode pengembangan *Balanced Scorecard* generasi ke-4 adalah: a) penggunaan penilaian ahli Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D dan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 pada tiap proses pengembangan *Balanced Scorecard* generasi ke-4, b) penentuan kriteria pemilihan risiko serta Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) dengan skala *Likert*, c) pembobotan kriteria pemilihan indikator (IRU dan IPU) berdasarkan tingkat kepentingan dengan perbandingan berpasangan pada metode *Analytical Hierarchy Process* (AHP), d) penentuan IRU dan IPU dari tiap risiko dengan matriks prioritas, e) pembuatan matriks kontrol risiko, dan f) penentuan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D menggunakan matriks prioritas.

Kata kunci:
Manajemen risiko, ISO/ IEC 17799:2005, ISO/ IEC 27001:2005, *balanced scorecard* generasi ke-4, skala *likert*, *analytical hierarchy process*, matriks prioritas.

ABSTRACT

Name : Distya Tarworo Endri
Study program : Industrial Engineering
Title : Integration Method Development of ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005 Into Information Technology of Bank D Balanced Scorecard To Become 4th Generation of Balanced Scorecard

In accordance with the advancement of technology, so does the incremental business interconnectivity of Bank D. This will bring along a larger amount and variation of threats and vulnerabilities towards IT security.

Therefore, support system and IT resources enhancement becomes critical. One of the ways according with that concern is 4th generation Balanced Scorecard development at the Information Technology Department of Bank D based on ISO/ IEC 17799:2005 and ISO/ IEC 27001:2005 that is – by far – the first concept application to be implemented in Indonesia. This research is dedicated to find methods of putting 4th generation of Balanced Scorecard into practice at Bank D.

Fourth generation Balanced Scorecard development consists of following method: a) involvement of experts judgment that are excel in Key Performance Indicator of Information Technology Department, ISO/ IEC 17799:2005 and ISO/ IEC 27001:2005, b) sort listing of risk and indicator selection criteria using Likert scale, c) weighting of indicator criteria selected using pairwise comparison from Analytical Hierarchy Process, d) setting of Key Risk Indicator (KRI) and Key Control Indicator (KCI) using priority matrix, e) making of risk control matrix, f) setting the relation between KRI, KCI, and KPI of IT Department of Bank D using priority matrix.

Key words:
Risk management, ISO/ IEC 17799:2005, ISO/ IEC 27001:2005, 4th generation of balanced scorecard, Likert scale, analytical hierarchy process, *priority matrix.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

1. PENDAHULUAN

1.1. Latar Belakang

Dalam pencapaian visi dan misi perusahaan, Bank D memiliki tugas utama berkenaan dengan proses bisnisnya. Agar Bank D dapat melaksanakan tugasnya, diperlukan dukungan teknologi informasi pada keseluruhan sistem informasi. Oleh karena itu dibuatlah visi dan misi pada satuan kerja Departemen Teknologi Informasi Bank D. Visinya yaitu menjadi satuan kerja pengelola teknologi informasi Bank D yang sangat kompeten dan dapat diandalkan, sedangkan misinya adalah menyediakan dukungan dan sumber daya teknologi informasi yang berkualitas tinggi secara efektif dan efisien untuk meningkatkan kinerja pelaksanaan tugas Bank D.

Dalam memenuhi visi dan misi tersebut, Departemen Teknologi Informasi Bank D memanfaatkan konsep *Balanced Scorecard* generasi ke-3 sebagai sistem pengelolaan dan pengukuran teknologi informasi. Sehubungan dengan hal ini, berdasarkan penelitian Marc J. Epstein dan Adriana Rejc (2005, hal. 36), *Balanced Scorecard* dapat membantu organisasi untuk menentukan kunci kesuksesan teknologi informasi, menentukan hubungan antar kunci kesuksesan tersebut, dan mengembangkan pengukuran yang sesuai untuk melihat pencapaian kinerja teknologi informasi. Mendukung penyataan Marc J. Epstein dan Adriana Rejc, hasil survei *American Management Association* dan William Scheimann dan rekan (PAMK Bank D, 2006, hal. 11) menunjukkkan bahwa dari 203 perusahaan dengan aset antara $27 juta hingga $50 milyar mengindikasikan bahwa organisasi yang mengelola pengukurannya merupakan *leader* pada 3 tahun terakhir, peringkat tiga besar dari sisi finansial, dan mengalami perubahan signifikan ke arah yang lebih baik dari sisi budaya dan operasional.

Departemen Teknologi Informasi Bank D juga berupaya meningkatkan keamanan informasi dengan menerapkan *Information Security Management System* (ISMS) melalui sertifikasi ISO/ IEC 27001:2005. Sertifikasi ISO/ IEC 27001:2005 dapat memberikan kontrol berkenaan dengan teknologi informasi berdasarkan pedoman

yang ada di ISO/ IEC 17799:2005 yang juga dapat membantu memenuhi persyaratan dari berbagai standar peraturan tergantung dari pemilihan dan cara implementasi kontrol tersebut (Joel Brenner, 2007, hal. 26). ISO/ IEC 27001:2005 menjelaskan persyaratan untuk membuat, mengimplementasikan, mengerjakan, memonitor, mengevaluasi, mempertahankan dan memperbaiki ISMS yang didokumentasikan dalam konteks risiko bisnis sebuah organisasi dan didesain untuk memastikan pemilihan dari kontrol keamanan yang cukup dan proporsional yang mampu melindungi aset dan memberi kepercayaan terhadap pihak yang berkepentingan (ISO/IEC/TMB SAG-Security Secretariat, 2005, hal. 1).

Seiring dengan kemajuan teknologi, peningkatan interkonektivitas bisnis tak dapat terelakkan. Begitu pula pengingkatan interkonektivitas Bank D yang berarti peningkatan jumlah dan variasi baik ancaman maupun kerawanan terhadap keamanan informasi, maka pencapaian misi Departemen Teknologi Informasi yang sekaligus meningkatkan daya dukung dan sumber daya teknologi informasi terhadap misi Bank D sangat penting. Dengan demikian, pengukuran kinerja Departemen Teknologi Informasi yang berkaitan dengan peningkatan kesadaran terhadap manajemen risiko sangat dibutuhkan. Menurut Tomonori Tomura (2006, hal. 1), *Balanced Scorecard* generasi ke-4 "*Beyond Sarbanes Oxley Tool*" *(balancing the profit earning strategy and the internal control strategy: Balanced Scorecard for SOX)* dapat menjawab kebutuhan tersebut.

Perkembangan *Balanced Scorecard* dari yang terdahulu hingga saat ini, antara lain:

a. Generasi pertama "*Multimodal Assessment Tool"* yaitu penambahan perspektif nonfinansial terhadap pengukuran kinerja – *learning and growth, internal business process,* dan *customers* – untuk merepresentasikan *stakeholder* mayor dalam bisnis.
b. Generasi ke-dua "*Top Down Management Tool*" yang merupakan permulaan dari konsep tujuan strategis dimana terdapat penambahan esensi dari strategi organisasi ke dalam tiap perspektif dari BSC pada generasi pertama.

c. Generasi ke-tiga yaitu "*Knowledge-creating and Strategic Communication Tool*" *(based on strategy map)* dimana dibuat *strategy map* yang dapat memberi gambaran tujuan kritikal organisasi dan hubungan antar *Key Performance Indicator* dari tiap perspektif (Steven John Simon, 2005, hal. 11).
d. Generasi ke-4 "*Beyond Sarbanes Oxley Tool*" *(balancing the profit earning strategy and the internal control strategy: Balanced Scorecard for SOX)* menambahkan pentingnya kontrol internal dalam sebuah organisasi berdasar Sarbanes-Oxley Act.

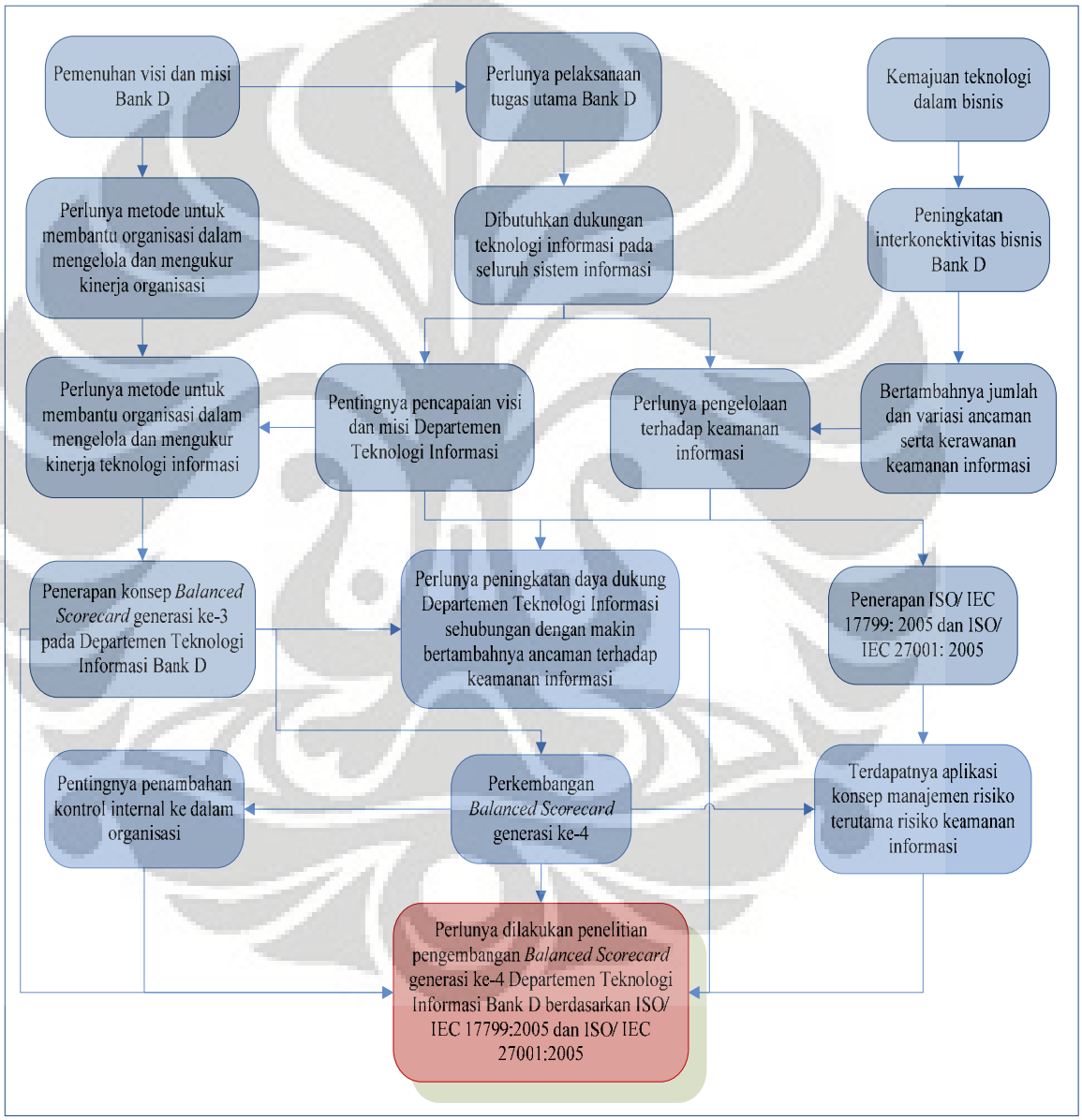
Kelebihan *Balanced Scorecard* generasi ke-4 antara lain meningkatkan kontrol internal, pemahaman lebih lanjut terhadap entitas dari proses, dapat mendeteksi risiko pada proses internal lebih dini, sebagai alat bantu dalam membuat program audit internal yang efektif, meningkatkan transparansi dan akuntabilitas, memperlihatkan *gap* antara target dan kondisi saat ini pada proses internal, meningkatkan nilai organisasi, dan memastikan kontrol proses internal yang mudah dilacak serta dapat diperbaiki secara terus-menerus pada periode selanjutnya atau yang disebut *Kaizen* (Tomonori Tomura, 2006, hal. 5). Namun hingga saat ini, belum ada aplikasi nyata dari pengembangan dan penggunaan *Balanced Scorecard* generasi ke-4 di Indonesia.

Dengan mengkombinasikan antara pentingnya pencapaian visi dan misi Departemen Teknologi Informasi Bank D, metode pengelolaan manajemen dan pengukuran *Balanced Scorecard,* konsep manajemen risiko terhadap keamanan informasi yang terdapat pada ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005, dan penambahan kontrol internal melalui manajemen risiko pada *Balanced scorecard* generasi ke-4; penelitian mengenai pengembangan metode integrasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* generasi ke-4 diharapkan dapat meningkatkan manfaat implementasi dari *Balanced Scorecard* Departemen Teknologi Informasi Bank D pada khususnya dan *Balanced Scorecard* Bank D pada umumnya serta menambah manfaat dari implementasi ISMS berdasarkan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005,

selain dari peningkatan kesadaran keamanan informasi, terhadap daya dukung dan sumber daya teknologi informasi Departemen Teknologi Informasi Bank D.

1.2. Diagram Keterkaitan Masalah

Untuk identifikasi awal dan merumuskan keterkaitan masalah, dibuatlah diagram keterkaitan masalah yang terdapat pada gambar 1.1 di bawah ini.



Gambar 1.1. Diagram Keterkaitan Masalah

1.3. Perumusan Permasalahan

Berdasarkan latar belakang di atas, maka pokok permasalahan yang akan dibahas adalah meneliti pengembangan metode integrasi ISO/ IEC 17799: 2005 dan ISO/ IEC 27001: 2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* Generasi ke-4.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah mendapatkan metode integrasi ISO/ IEC 17799: 2005 dan ISO/ IEC 27001: 2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* Generasi ke-4.

1.5. Batasan Masalah

Dalam penelitian ini dilakukan pembatasan masalah agar pelaksanaan serta hasil yang akan diperoleh sesuai dengan tujuan pelaksanaannya. Adapun batasan masalah penelitian ini melingkupi:

1. Pelaksanaan penelitian dilakukan di Departemen Teknologi Informasi Bank D. Oleh karena itu, entitas yang akan dipertimbangkan dalam pengembangan *Balanced Scorecard* generasi ke-4 merupakan entitas dalam sistem Departemen Teknologi Informasi Bank D
2. Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D yang dikembangkan adalah dari perspektif proses bisnis internal sehubungan dengan ketersediaan data yang ada.

1.6. Metodologi Penelitian

Metodologi penelitian yang digunakan dalam skripsi ini secara sistematis adalah sebagai berikut :

a. Persiapan tahap awal

   Dalam langkah ini ditentukan topik yang akan diteliti, perumusan masalah, tujuan dari penelitian, dan batasan masalah.

b. Penentuan landasan teori

   Tahap selanjutnya adalah menentukan landasan teori yang berhubungan dengan topik sebagai dasar dalam pelaksanaan penelitian. Landasan teori ini

kemudian akan dijadikan acuan dalam pelaksanaan tugas akhir. Adapun landasan teori yang terkait antara lain Manajemen Risiko, *Information Security Management System* pada ISO/ IEC 17799: 2005 dan ISO/ IEC 27001: 2005, *Balanced Scorecard*, pembuatan indikator, metode *rating*, dan matriks prioritas.

c. Pengumpulan data sekunder

Data sekunder yang diperlukan antara lain *risk profile* Bagian Kebijakan, Bagian Administrasi, dan Bagian Operasional sebagai input alternatif kriteria pemilihan risiko; kriteria pemilihan indikator pada Bank D sebagai input untuk alternatif kriteria pemilihan indikator (IRU dan IPU); hasil *risk assessment* pada Bagian Kebijakan, Bagian Administrasi, Bagian Operasional serta pengukuran pada ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 sebagai input alternatif IRU dan IPU; sasaran strategis dan Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D sebagai input dalam penentuan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D.

d. Pengumpulan data primer

Langkah yang dilakukan untuk mengumpulkan data primer yaitu memilih responden yang ahli (*experts*) dalam implementasi *Balanced Scorecard* dan ISMS di Departemen Teknologi Informasi Bank D, membuat alternatif kriteria pemilihan risiko serta Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) pada penyusunan kuesioner tahap I; menentukan skala penilaian; menyebarkan kuesioner tahap I kepada responden untuk mendapatkan penentuan kriteria pemilihan risiko serta IRU dan IPU; jika terdapat kriteria risiko maupun indikator (IRU dan IPU) tambahan dari salah satu responden, maka kriteria tersebut akan dikonfirmasikan ke responden yang bersangkutan dan dinilai oleh responden lain; membuat daftar kriteria pemilihan risiko dan indikator (IRU dan IPU) pada penyusunan kuesioner tahap II; menentukan skala penilaian; menyebarkan kuesioner tahap II untuk mendapatkan bobot kriteria pemilihan indikator, penentuan IRU dan IPU untuk setiap risiko yang telah diseleksi, dan penentuan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D; jika terdapat IRU dan

IPU tambahan maka IRU dan IPU tersebut akan dikonfirmasikan ke responden yang bersangkutan dan dinilai oleh responden lain yang meliputi penilaian untuk mendapatkan IRU dan IPU dari setiap risiko yang telah diseleksi dan penentuan hubungan antara IRU dan IPU tambahan dengan IKU Departemen Teknologi Informasi Bank D.

e. Pengolahan data

Langkah-langkah yang dilakukan dalam pengolahan data adalah mendapatkan kriteria pemilihan risiko dan indikator (IRU dan IPU) berdasarkan skala *likert*, mendapatkan risiko dari hasil *risk profile* yang diseleksi sesuai kriteria pemilihan risiko, mendapatkan pembobotan kriteria pemilihan indikator (IRU dan IPU) secara perbandingan berpasangan menggunakan metode *Analytical Hierarchy Process* (AHP) yang menunjukkan tingkat kepentingan dari tiap kriteria pemilihan indikator (IRU dan IPU), mendapatkan IRU dan IPU terpilih untuk tiap risiko menggunakan matriks prioritas, mendapatkan matriks kontrol risiko Departemen Teknologi Informasi Bank D, mendapatkan hubungan antara IRU dan IPU terpilih untuk tiap risiko dengan IKU Departemen Teknologi Informasi Bank D, dan mendapatkan metode pengembangan *Balanced Scorecard* generasi ke-4 Departemen Teknologi Informasi.

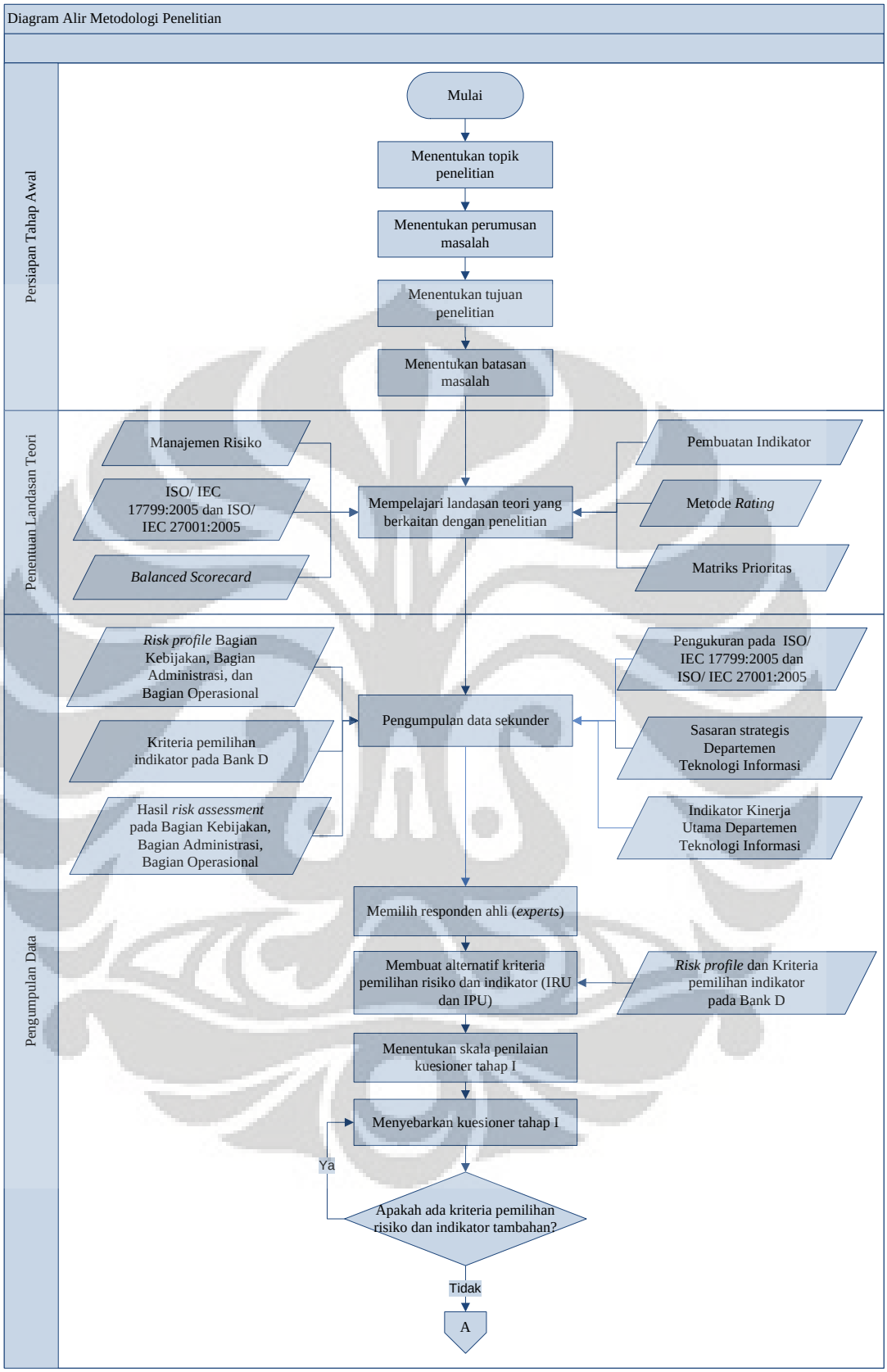
5. Analisis data

Dalam tahap ini dilakukan analisis terhadap seluruh proses dan hasil pengolahan data untuk memperoleh tujuan penelitian yaitu mendapatkan metode pengembangan *Balanced Scoreard* generasi ke-4 Departemen Teknologi Informasi Bank D berdasarkan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005.

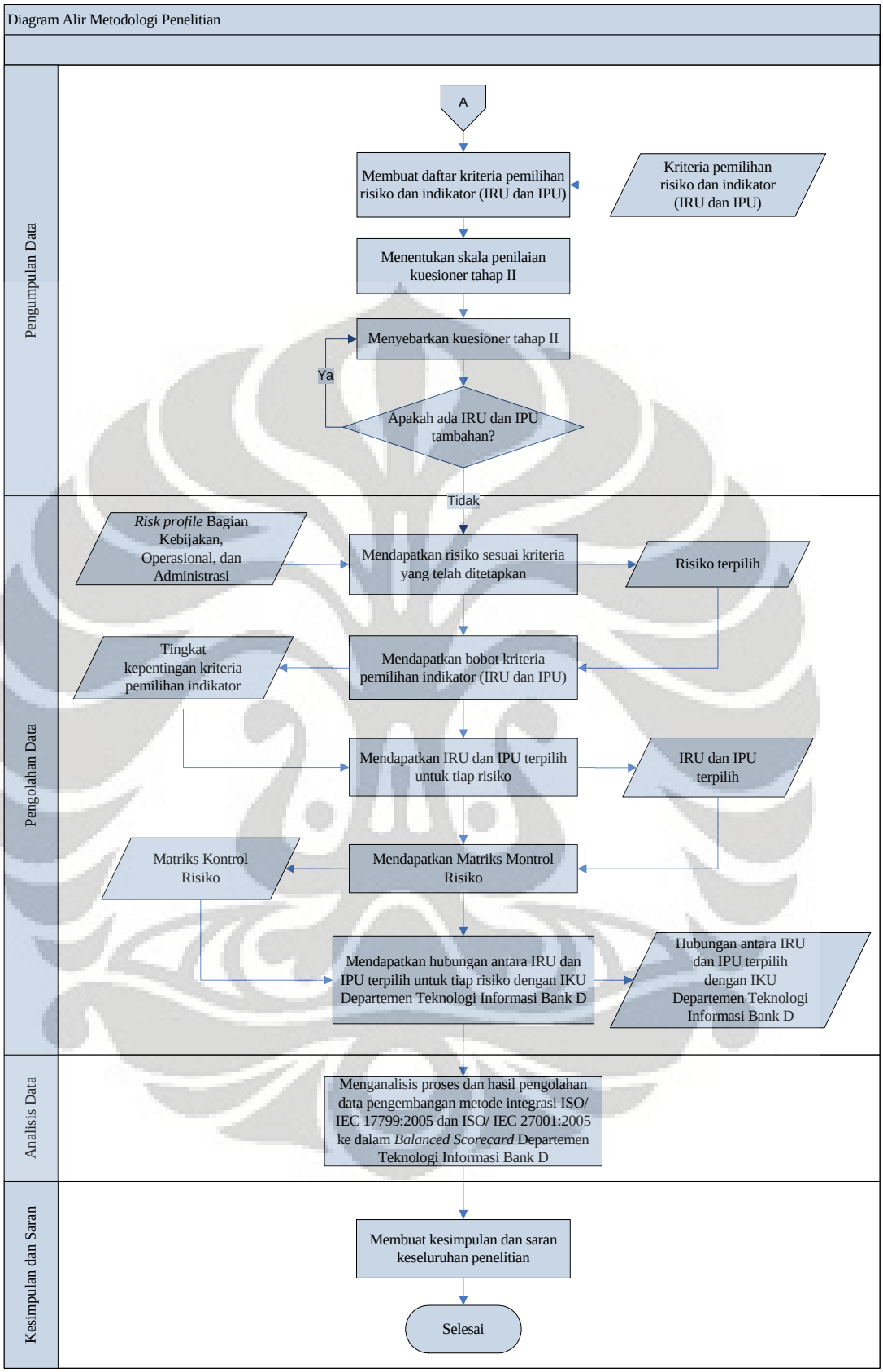
6. Kesimpulan dan saran

Dalam tahapan ini akan didapatkan kesimpulan mengenai keseluruhan penelitian tugas akhir baik proses maupun hasil yang sesuai dengan tujuan penelitian, serta saran yang berguna untuk Departemen Teknologi Informasi Bank D di masa mendatang.

Diagram alir metodologi penelitian yang dilakukan pada penelitian terdapat pada Gambar 1.2 berikut.



Gambar 1.2. Diagram Alir Metodologi Penelitian



Gambar 1.2. Diagram Alir Metodologi Penelitian (Sambungan)

1.7. SISTEMATIKA PENULISAN

Secara umum, pembahasan penelitian ini terdiri dari beberapa bab. Bab pendahuluan menjelaskan mengenai latar belakang dilakukannya penelitian ini, diagram keterkaitan masalah, perumusan permasalahan, tujuan penelitian, batasan masalah, metodologi penelitian, dan sistematika penulisan.

Setelah itu, dipaparkan landasan teori yang berhubungan dengan penelitian ini. Landasan teori yang dibahas meliputi Manajemen Risiko, *Information Security Management System* pada ISO/ IEC 17799: 2005 dan ISO/ IEC 27001: 2005, *Balanced Scorecard*,pembuatan indikator, metode *rating*, dan matriks prioritas.

Profil Departemen Teknologi Informasi Bank D serta pelaksanaan pengumpulan data dijelaskan pada bab selanjutnya. Data yang dikumpulkan antara lain data primer berupa kuesioner yaitu kriteria pemilihan risiko dan indikator (IRU dan IPU), pembobotan kriteria pemilihan indikator, penilaian Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) yang tepat untuk tiap risiko, serta hubungan antara IRU dan IPU dengan Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D. Data sekunder yang diperlukan antara lain *risk profile* Bagian Kebijakan, Bagian Administrasi, dan Bagian Operasional sebagai input alternatif kriteria pemilihan risiko; kriteria pemilihan indikator pada Bank D sebagai input untuk alternatif kriteria pemilihan indikator (IRU dan IPU); hasil *risk assessment* pada Bagian Kebijakan, Bagian Administrasi, Bagian Operasional serta pengukuran pada ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 sebagai input alternatif IRU dan IPU; sasaran strategis dan Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D sehingga dapat dijadikan dasar dalam penentuan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D.

Bab berikutnya berisi pengolahan data dan analisis. Pengolahan data dilakukan dengan skala *Likert* untuk menentukan kriteria pemilihan risiko dan indikator (IRU dan IPU), perbandingan berpasangan dari metode *Analytical Hierarchy Process* (AHP) dan matriks prioritas untuk menentukan risiko, IRU, dan IPU

sesuai kriteria yang telah ditetapkan sebagai input untuk membuat matriks kontrol risiko, serta menentukan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D. Analisis dilakukan terhadap hasil pengolahan data untuk memperoleh tujuan penulisan skripsi.

Bab penutup dari keseluruhan penelitian ini berisi kesimpulan yang diambil akan meliputi pengembangan metode integrasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* generasi ke-4, IRU dan IPU terpilih, dan hasil dari pengembangan metode tersebut serta saran yang diajukan untuk penelitian-penelitian selanjutnya.

2. LANDASAN TEORI

2.1. Manajemen Risiko

2.1.1. Risiko

Risiko didefinisikan dalam berbagai arti seperti kesempatan terjadinya kehilangan, kemungkinan kerugian, ketidakpastian, penyimpangan antara kenyataan dan hasil yang diharapkan, kemungkinan hasil yang berbeda dengan yang diharapkan. Emmet J. Vaughan (1997, hal 8) sendiri berpendapat bahwa risiko adalah kondisi dari keadaan dimana terdapat kemungkinan perbedaan antara hasil yang diinginkan dan yang diharapkan.

Risiko terhadap sistem informasi berdasarkan *International Standard Organization* merupakan potensi bahwa sebuah ancaman akan menyebabkan kerawanan pada 1 aset atau lebih sehingga aset tersebut hilang atau rusak. Dampak atau kerugian relatif dari risiko proporsional terhadap kehilangan atau kerusakan terhadap nilai bisnis dan estimasi frekuensi dari ancaman.

Aset pada sistem informasi sendiri merupakan segala sesuatu yang berusaha dilindungi. Aset dapat meliputi *database*, informasi, personil, fasilitas, aplikasi, perangkat keras, perangkat lunak, dan jaringan telekomunikasi baik perangkat keras maupun lunak (D.P. Dube, 2005, hal. 82).

Menurut Emmet J. Vaughan (1997, hal. 13), risiko dapat diklasifikasikan menjadi:

a. Finansial dan nonfinansial

   Perbedaan antara risiko finansial dan nonfinansial adalah konsekuensi dari suatu kehilangan yang berdampak pada keadaan finansial atau tidak. Risiko finansial merupakan hubungan antara individu atau organisasi dan aset atau pemasukan yang diharapkan yang mungkin hilang. Risiko finansial memiliki 3 elemen yaitu individu atau organisasi yang memiliki kemungkinan kehilangan, asset atau pemasukan yang dapat menyebabkan kerugian finansial, dan sumber risiko.

b. Statis dan dinamis

Risiko dinamis dihasilkan dari perubahan ekonomi. Dua faktor yang mempengaruhi terjadinya risiko ini antara lain faktor internal – keputusan manajemen terhadap produksi dan pemasaran produk – dan eksternal – ekonomi, industri, pesaing, dan konsumen. Risiko statis merupakan kehilangan yang terjadi bahkan tanpa adanya perubahan di bidang ekonomi. Apabila kita dapat mempertahankan selera pasar, pengeluaran dan pemasukan, level stabilitas dari teknologi, beberapa orang akan tetap merasakan kerugian finansial. Kerugian ini terjadi bukan disebabkan oleh perubahan ekonomi, tetapi oleh kejadian lain seperti ketidakjujuran dari individu. Risiko statis umumnya lebih mudah diprediksi karena tingkat kejadiannya yang sering.

c. Murni dan Spekulatif

Risiko spekulatif mendeskripsikan situasi dimana terjadi kemungkinan rugi atau untung, contohnya pada judi. Pada perjudian, risiko dengan sengaja dibuat dengan harapan mendapatkan keuntungan. Risiko murni dibuat untuk situasi dimana hanya terjadi kemungkinan rugi atau tidak rugi. Salah satu contoh risiko murni adalah kemungkinan kehilangan kepemilikan properti.

d. Fundamental dan khusus

Perbedaan antara risiko fundamental dan khusus adalah berdasarkan perbedaan sebab dan konsekuensi dari kehilangan. Risiko fundamental merupakan kerugian yang sebab dan dampaknya melibatkan banyak individu. Risiko fundamental merupakan kelompok-kelompok risiko yang disebabkan oleh fenomena ekonomi, sosial, politik, dan juga dapat disebabkan kejadian fisik yang berpengaruh terhadap pada segmen yang luas atau bahkan kepada seluruh populasi seperti pengangguran, perang, inflasi, gempa bumi, dan banjir. Risiko khusus merupakan kerugian yang terjadi pada individu dan hanya dirasakan oleh individu tersebut. Kerugian tersebut dapat bersifat statis atau dinamis seperti kebakaran rumah dan pencurian.

Definisi risiko operasional adalah risiko kerugian yang berasal dari ketidakcukupan atau kegagalan proses internal, orang, dan sistem, atau dari

peristiwa-peristiwa eksternal (*Bassel Committe on Banking Supervision*, 2001). Risiko operasional adalah risiko yang berhubungan dengan kegiatan-kegiatan untuk menjalankan suatu bisnis.

Menurut Crouhy, Galai, dan Mark (hal. 480), area bisnis yang menjadi bagian dalam risiko operasional sangatlah besar, untuk lebih memudahkan pemahamannya maka risiko operasional dibagi kedalam dua komponen seperti pada gambar 2.1. Komponen-komponen tersebut adalah risiko kegagalan operasional dan risiko strategi operasional. Risiko kegagalan operasional berasal dari potensi terjadinya kegagalan di dalam menjalankan bisnis. Manusia, proses, dan teknologi adalah beberapa alat perusahaan untuk mencapai tujuannya. Oleh karena itu, risiko kegagalan operasional dapat didefinisikan sebagai risiko yang muncul karena terdapat kegagalan manusia, kegagalan proses atau kegagalan teknologi dalam suatu unit bisnis. Risiko kegagalan operasional sulit untuk diantisipasi karena ketidakpastiannya. Risiko strategi operasional muncul dari faktor lingkungan seperti masuknya pesaing baru yang mengubah paradigma bisnis, perubahan kebijakan, tsunami, dan faktor lainnya yang sejenis yang berada di luar kontrol perusahaan. Segala macam bisnis mengandalkan orang, proses, dan teknologi diluar unit bisnis tersebut, dan potensi kegagalan juga terdapat dalan faktor-faktor tersebut. Jenis risiko yang berada di luar kontrol perusahaan juga disebut dengan risiko ketergantungan operasional.

Risiko operasional dapat diklasifikasikan menjadi lima jenis menurut D. Hoffman (2002, hal. 36), yaitu:

a. Risiko Orang

   Risiko kerugian yang diakibatkan, dengan sengaja atau tidak sengaja, oleh seorang atau melibatkan beberapa karyawan. Contohnya adalah kesalahan tindakan karyawan, dan ketidakpatuhan karyawan.

b. Risiko Hubungan

   Kerugian hak cipta atau produksi perusahaan dan ditimbulkan melalui hubungan atau kontrak yang dimiliki perusahaan dengan kliennya, pemegang

saham, pihak ke-tiga, atau pengambil kebijakan permerintah. Contoh risiko hubungan adalah penggantian kerugian kepada klien atau pembayaran penalti.

c. Risiko Teknologi dan Proses

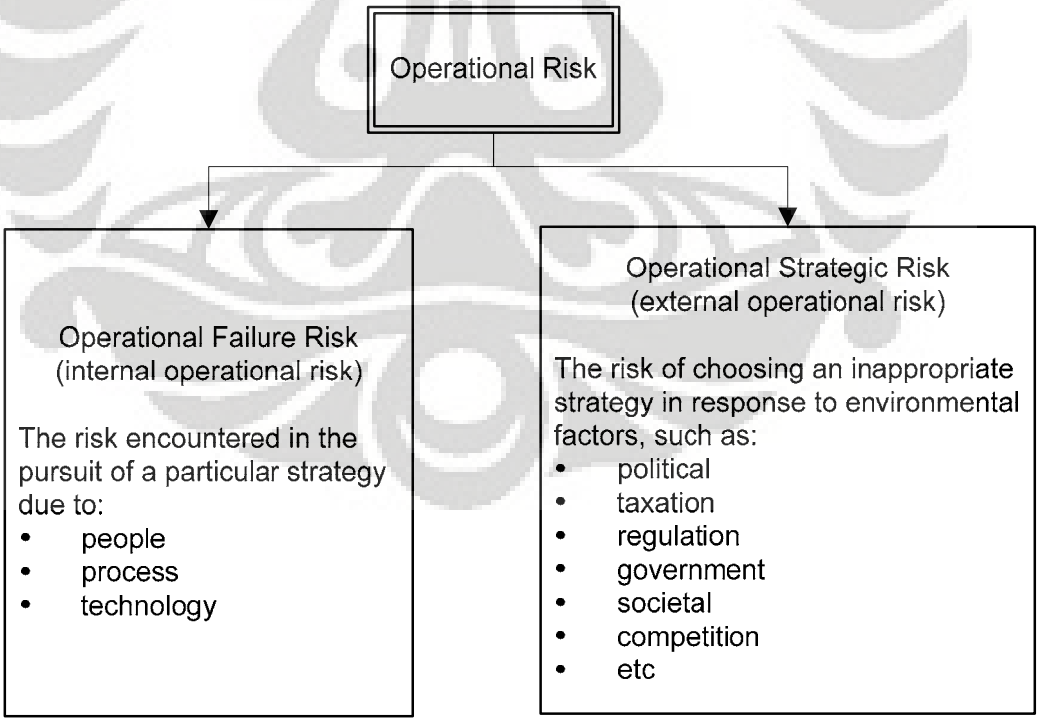
Risiko kerugian oleh kegagalan, kerusakan, atau gangguan lainnya pada teknologi dan/ atau proses. Kerugian akibat pembajakan atau pencurian data atau informasi, dan kerugian akibat kegagalan teknologi dalam memenuhi kebutuhan bisnis yang diinginkan.

d. Risiko Fisik

Risiko kerugian yang dialami melalui kerusakan properti perusahaan atau kerugian pada properti fisik atau aset yang menjadi tanggung jawab perusahaan.

e. Risiko Eksternal lainnya

Risiko kerugian yang diakibatkan oleh tindakan pihak eksternal, seperti tanggung jawab atas tindakan kecurangan di perusahaan, atau perubahan kebijakan pemerintah yang akan mempengaruhi kemampuan perusahaan untuk beroperasi di pasar-pasar tertentu.



Gambar 2.1. Kategori Umum Risiko Operasional

(Sumber: Crouhy, Galai, dan Mark, hal. 480)

2.1.2. Sumber Risiko

Menurut Emmet J. Vaughan (1997, hal. 12), elemen lain dari risiko adalah sumber risiko tersebut yang disebut *hazard. Hazard* bisa kita atasi dengan, pertama kali, mengetahui adanya *hazard* dan kemudian melakukan tindakan untuk mengatasi *hazard* tersebut. Jenis-jenis *hazard* antara lain:

a. *Physical hazard* adalah segala benda fisik yang dapat meningkatkan kemungkinan kerugian. Contohnya tipe konstruksi, lokasi, dan tingkat pemakaian bangunan.
b. *Moral hazard* adalah sumber risiko yang berasal dari kemungkinan niat jahat seseorang. Contohnya, ketidakjujuran seseorang sehingga menimbulkan penipuan terhadap perusahaan asuransi.
c. *Morale hazard* adalah tingkat kecerobohan yang dapat menyebabkan kerugian. Contohnya, tingkat perawatan terhadap benda yang kurang karena merasa perusahaan asuransi akan menggantinya.
d. *Legal hazard* adalah peningkatan frekuensi dan dampak kerugian karena doktrin hukum dari pengadilan. Contohnya peraturan untuk menghapuskan kerugian kerusakan gedung meningkatkan kemungkinan kehilangan.

Menurut D.P. Dube (2005, hal. 85) terminologi lain untuk sumber risiko adalah ancaman (*threat*) yaitu potensi terjadinya kerawanan yang berasal dari sumber ancaman (*threat source*). Sumber ancaman sendiri yaitu segala kondisi atau kejadian yang berpotensi menyebabkan kerugian pada sistem teknologi informasi.

Contoh *threat source* dalam audit sistem informasi antara lain (D.P. Dube, 2005, hal. 87):

1. *Hacker, cracker* yang dapat melakukan *hacking, social engineering,* intrusi terhadap sistem, akses sistem tanpa otorisasi
2. Pelaku kejahatan komputer yang dapat melakukan pencurian informasi, *spoofing,* intrusi terhadap sistem
3. Teroris yang dapat melakukan pemboman, penyerangan terhadap sistem, penetrasi sistem

4. Mata-mata industri yang dapat melakukan pencurian informasi, *social engineering*, akses sistem tanpa otorisasi
5. Pegawai yang dapat melakukan pengancaman, korupsi, pencurian, memasukkan *malicious code* ke dalam sistem, dan sebagainya.

2.1.3. Kerawananan

Kerawanan (*vulnerability*) adalah kekurangan atau kelemahan di dalam sistem keamanan dalam hal prosedur, desain, implementasi, atau kontrol internal yang dapat memicu, baik secara sengaja maupun tidak sengaja menyebabkan gangguan kemananan terhadap kebijakan sistem keamanan (D.P. Dube, 2005, hal. 89).

2.1.4. Kecenderungan

Menurut D.P. Dube (2005 hal. 93), kecenderungan adalah probabilitas dimana terdapat potensi kerawanan yang dapat terjadi karena ancaman dalam suatu lingkungan; yang mempertimbangkan kekuatan dari ancaman, sifat kerawanan, dan keberadaan serta efektivitas kontrol yang telah ada. Seperti telah disebutkan sebelumnya, kerawanan adalah kelemahan yang dapat menjadi risiko secara sengaja atau tidak sengaja, sedangkan ancaman adalah sumber risiko potensial yang menyerang kerawanan. Menurut D.P. Dube (2005), kecenderungan memiliki tingkatan dengan pengertian seperti terdapat pad tabel 2.1 berikut.

Tabel 2.1. Level Kecenderungan

No.	Level	Pengertian
1.	Tinggi	Sumber ancaman sangat tinggi, dan kontrol yang ada untuk mencegah kerawanan terjadi tidak efektif
2.	Sedang	Sumber ancaman cukup tinggi, tetapi kontrol yang telah ada dapat mencegah kerawanan yang mungkin terjadi
3.	Rendah	Sumber ancaman lemah, atau kontrol yang telah ada dapat mencegah atau secara signifikan mengurangi kerawanan

(Sumber: D.P Dube, 2005)

2.1.5. Dampak

Menurut D.P. Dube (2005, hal. 94), dampak adalah akibat dari kerawanan. Dampak dapat dideskripsikan menjadi salah satu atau kombinasi ketiga tujuan pengamanan teknologi informasi yaitu *integrity*, *availability*, dan *confidentiality*. Berikut merupakan penjelasan dari tiap tujuan pengamanan teknolgoi informasi tersebut dan dampak yang dapat ditimbulkannya:

a. Hilangnya integritas (*integrity*)

   Integritas sistem dan data merujuk pada persyaratan dimana informasi harus dilindungi dari modifikasi yang tidak sesuai. Integritas dapat hilang bila terjadi perubahan tanpa otorisasi yang jelas pada sistem dan data teknologi informasi secara sengaja maupun tidak sengaja. Hal in idapat berdampak pada tidak akurat dan tidak validnya keputusan, serta dapat menyebabkan penipuan. Seluruhnya membuat kehilangan integritas mengurangi nilai kepercayaan terhadap sistem teknologi informasi.

b. Hilangnya ketersediaan (*availability*)

   Apabila sistem teknologi informasi kritikal terhadap misi perusahaan tidak dapat digunakan oleh *end-user,* maka dapat berpengaruh terhadap pencapaian misi perusahaan. Contohnya antara lain gangguan pada fungsi sebuah sistem and efektivitas operasional, dapat menyebabkan kerugian pada waktu produktif, sehingga mempengaruhi kinerja dan pencapaian misi.

c. Hilangnya kerahasiaan (*confidentiality*)

   Kerahasiaan sistem dan data merujuk pada perlindungan terhadap informasi dari kebocoran. Dampak dari hilangnya kerahasiaan beragam, dari membocorkan hak pribadi hingga mengganggu keamanan nasional, yang memiliki implikasi hukum.

2.1.6. Tujuan dan Manfaat Manajemen Risiko

Manajemen risiko berdasarkan *International Standard Organization* (ISO/ IEC Guide 73:2002) merupakan aktivitas terkoordinasi untuk mengkontrol organisasi dalam hubungannya dengan risiko.

Tujuan dari manajemen risiko TI adalah melindungi aset TI seperti data, *hardware*, *software*, personil, dan fasilitas dari semua ancaman eksternal (seperti bencana alam) dan internal (seperti kegagalan teknis, sabotase, akses yang tidak terotorisasi) sehingga biaya kerugian yang diakibatkan oleh ancaman-ancaman tersebut bisa dikurangi (Kakoli Bandyopadhyay, 1999, hal. 1). Kegunaan dari manajemen risiko TI adalah untuk mencegah atau mengurangi kerugian dengan memilih dan mengimplementasikan kombinasi pengukuran keamanan yang paling baik.

2.2. ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005

2.2.1. Definisi ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005

Berdasarkan ISO/IEC 2005 (hal. vii), ISO (*the International Organization for Standardization*) atau organisasi standardisasi internasional dan IEC (*the International Elechtrotechnical Commission*) atau komisi elektronika internasional membentuk sistem terspesialisasi untuk standardisasi internasional. Badan-badan nasional yang menjadi anggota ISO atau IEC berpartisipasi dalam pengembangan standar internasional melalui komite teknis yang dibentuk organisasi yang ditunjuk untuk berurusan dengan aktivitas teknis. Pada bidang teknologi informasi, ISO dan IEC membangun komite teknis bersama, ISO/ IEC JTC 1.

ISO/ IEC 17799:2005 merupakan standar internasional yang dibuat sebagai petunjuk dan dasar untuk mempersiapkan, mengimplementasi, memelihara, dan memperbaiki manajemen keamanan informasi pada organisasi.

ISO/ IEC 27001:2005 merupakan standar internasional yang telah dipersiapkan untuk menyediakan model untuk mempersiapkan, mengimplementasi, mengoperasikan, memonitor, mengevaluasi, memelihara, dan memperbaiki *Information Security Management System* (ISMS).

Menurut Joel Brenner (2007, hal. 26), perbedaan antara ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 adalah ISO/ IEC 17799:2005 merupakan *code of practice*

yang berisi petunjuk bagaimana perusahaan dapat mengimplementasikan ISMS dan tidak memiliki sertifikasi karena merupakan bantuan untuk keberhasilan implementasi ISO/ IEC 27001:2005. ISO/ IEC 27001:2005 berisi persyaratan untuk mengembangkan ISMS yang harus dipenuhi perusahaan untuk mendapatkan sertifikasinya.

2.2.2. Keamanan Informasi

Menurut ISO/IEC 2005 (hal. viii), informasi merupakan aset yang penting bagi keberlangsungan bisnis perusahaan dan oleh karenanya harus dilindungi. Hal ini sangat penting mengingat adanya peningkatan interkoneksi lingkungan bisnis. Sebagai hasil dari peningkatan intekonektivitas, informasi menghadapi peningkatan jumlah dan variasi ancaman dan kerawanan terhadap keamanan informasi. Informasi dapat ditemukan dalam berbagai bentuk – cetak, tertulis, tersimpan secara elektronik, ditransmisikan melalui pos atau sarana elektronik, pada film, atau trucap pada kata-kata. Apapun bentuknya, informasi tersebut harus selalu dilindungi.

2.2.3. Tujuan dan Manfaat ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005

Berdasarkan ISO/IEC/TMB SAG-Security Secretariat, (2005, hal. 4) tujuan manajemen risiko terhadap sistem informasi ialah memastikan pemilihan kontrol keamanan yang cukup dan sesuai dalam melindungi aset informasi sehingga memberikan kepercayaan terhadap pihak yang terkait.

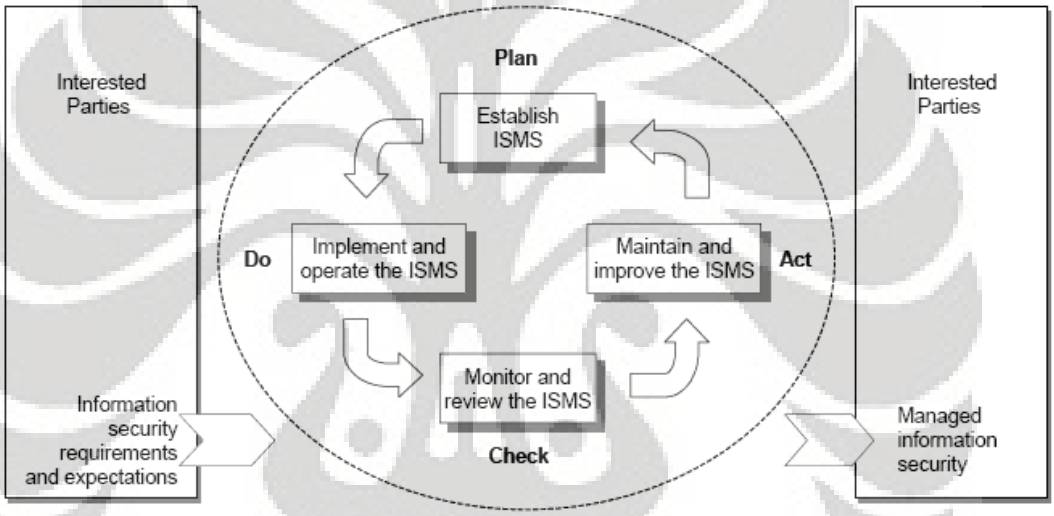
Mengingat bahwa informasi dan pendukung proses, sistem, dan jaringan merupakan aset bisnis yang penting, maka aktivitas mendefinisikan, mencapai, memelihara, dan memperbaiki keamanan informasi sangat penting untuk mempertahankan kemampuan kompetitif, kas, profitabilitas, kesesuaian hukum, dan *image* komersial.

Organisasi dan sistem informasinya serta jaringannya dihadapkan pada ancaman keamanan dari berbagai sumber termasuk penipuan, mata-mata, sabotase, vandalisme, kebakaran, atau banjir. Penyebab kerusakan seperti *malicious code,*

hacking komputer, dan penyerangan pelayanan telah menjadi semakin sering dan agresif. Keamanan informasi menadi penting baik bagi bisnis pemerintah maupun swasta dan untuk melindungi infrastruktur kritikal sehubungan dengan inerkoneksi antara kedua sektor bisnis.

2.2.4. Langkah Implementasi ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005

Implementasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 pada audit sistem informasi mengikuti konsep PDCA – Plan, Do, Check, Action – seperti pada gambar 2.2 berikut.



Gambar 2.2. Siklus PDCA ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005
(Sumber: ISO/IEC/TMB SAG-Security Secretariat, 2005)

Langkah-langkah implementasinya antara lain (ISO/IEC/TMB SAG-*Security Secretariat*, 2005, hal. 4):

a. Merencanakan *Information Security Management System* (ISMS)

   Mendefinisikan ruang lingkup dan batasan ISMS meliputi karakteristik bisnis, organisasi, lokasi, asset, teknologi, serta detil dan alasan segala sesuat yang tidak dimasukkan ke dalam ruang lingkup tersebut; mendefinisikan kebijakan ISMS dalam hal karakteristik bisnis, organisasi, lokasi, aset, dan teknologi yang terdiri dari *framework* penentuan tujuan dan segala hal yang berkaitan dengan pengamanan informasi, ketentuan dokumen legal, sejalan dengan

strategi manajemen risiko perusahaan, dapat menghasilkan kriteria untuk mengevaluasi risiko, dan yang disetujui oleh manajemen; mendefinisikan pendekatan *risk assessment* yang terdiri dari metodologi dan kriteria untuk menerima risiko serta level penerimaannya; mengidentifikasi risiko antara lain dengan cara mengidentifikasi aset, ancaman (*threat*), kerawanan (*vulnerability*), dan dampak; menganalisis dan mengevaluasi risiko dengan menilai dampak risiko terhadap kerugian atau kehilangan dari aspek kerahasiaan, integritas, dan ketersediaan asset, menilai kecenderungan kejadian risiko, mengestimasi level risiko, dan menentukan krieria penerimaan risiko; mengidentifikasi dan mengevaluasi pilihan perlakuan (*treatment*) terhadap risiko antara lain mengaplikasikan kontrol yang sesuai, menerima risiko secara objektif karena telah sesuai dengan tujuan organisasi dan kriteria penerimaan risiko, menghindari risiko, dan mentransfer risiko ke pihak lain; memilih tujuan kontrol dan kontrol yang akan dijalankan terhadap risiko. Tujuan kontrol dan kontrol tersebut dapat dilihat pada Annex A yang merupakan panduan dalam mengkontrol risiko; mendapatkan persetujuan manajemen dari nilai risiko akhir risiko setelah adanya kontrol, mendapatkan otorisasi manajemen untuk mengimplementasikan dan menjalankan ISMS, menyiapkan *Statement of Applicability* yang meliputi tujuan dan alasan pemilihan kontrol, kontrol dan tujuannya yang telah diimplementasikan, daftar kontrol pada Annex A yang tidak diikutsertakan dalam proses kontrol risiko dan alasannya

b. Mengimplementasi dan menjalankan ISMS

Memformulasikan perencanaan perlakuan terhadap risiko (*risk treatment plan*) yang mengidentifikasi langkah manajemen, sumber daya, tanggung jawab, dan prioritas untuk mengelola risiko keamanan informasi; mengimplementasi rencana tersebut untuk mendapatkan kontrol yang seusai tujuan; mengimplementasikan kontrol terpilih untuk memenuhi tujuan kontrol; mendefinisikan bagaimana mengukur efektivitas kontrol; mengimplementasikan latihan dan kesadaran dari program; mengelola operasi ISMS; mengelola sumber daya ISMS; mengimplementasi prosedur dan kontrol

c. Memonitor dan mengevaluasi ISMS

Melakukan monitoring dan evaluasi prosedur dan kontrol untuk mendeteksi error dan insiden lebih awal, memungkinkan manajemen untuk menentukan apakah aktivitas yang didelegasikan atau diimplementasikan dengan teknologi informasi memiliki kinerja seperti yang diharapkan, membantu mendeteksi kejadian berisiko, dan menentukan apakah langkah yang dilakukan untuk menjaga keamanan teknologi informasi efektif; melakukan evaluasi secara berkala untuk melihat efektivitas ISMS; mengukur efektivitas kontrol; mengevaluasi *risk assessment*, nilai risiko akhir, dan level penerimaan risiko dengan mempertimbangkan perubahan pada organisasi, teknologi, tujuan bisnis dan proses, *threat* yang teridentifikasi, efektivitas implementasi kontrol, kejadian eksternal; melakukan audit internal ISMS; melakukan evaluasi manajemen evaluasi ISMS; melakukan *update* rencana keamanan untuk melakukan monitor dan evaluasi; mencatat langkah dan kejadian yang dapat mempengaruhi efektivitas dan kinerja ISMS

d. Memelihara dan memperbaiki ISMS

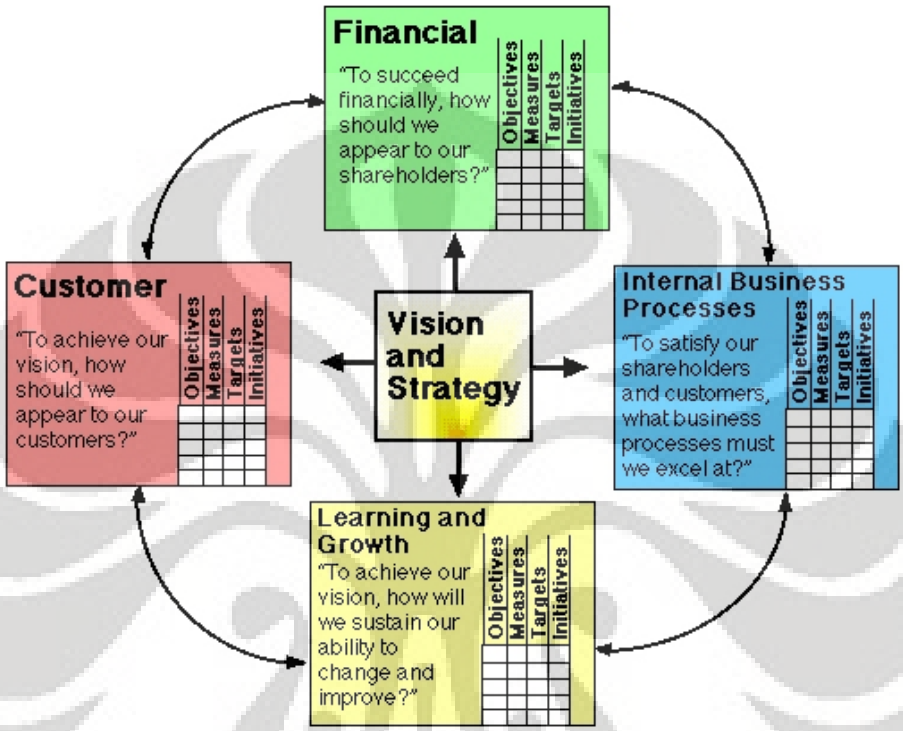
Secara berkala, organisasi harus melakukan implementasi rencana perbaikan ISMS, langkah korektif dan perbaikan untuk seluruh pihak, komunikasi langkah-langkah dan perbaikan untuk seluruh pihak, memastikan bahwa perbaikan menjawab tujuan yang ingin dicapai.

2.3. *Balanced Scorecard*

2.3.1. Konsep *Balanced Scorecard*

Robert S. Kaplan dan David P. Norton memperkenalkan sebuah instrumen yang mampu mengarahkan perusahaan untuk mencapai persaingan di masa depan. Metode tersebut saat ini lebih dikenal dengan nama *Balanced Scorecard.* Menurut Norton dan Kaplan, *balanced scorecard* adalah sebuah metode yang ampuh untuk menerjemahkan misi dan strategi perusahaan ke dalam seperangkat ukuran yang menyeluruh dan memberi kerangka kerja bagi pengukuran dan sistem manajemen strategis. Untuk itu, sistem pengukuran harus fokus kepada strategi perusahaan (Kaplan dan Norton, 2003, hal. 5).

Balanced scorecard lebih dari sekedar sistem pengukuran taktis dan operasional. Keempat perspektif *balanced scorecard* memberikan kerangka kerja untuk menerjemahkan strategi ke dalam kerangka operasional. Hal ini seperti terlihat pada gambar 2.3.



Gambar 2.3. Kerangka Kerja Keempat Perspektif *Balanced Scorecard*
(Sumber : Anonim, http://www.balancedscorecard.org/basics/bsc1.html)

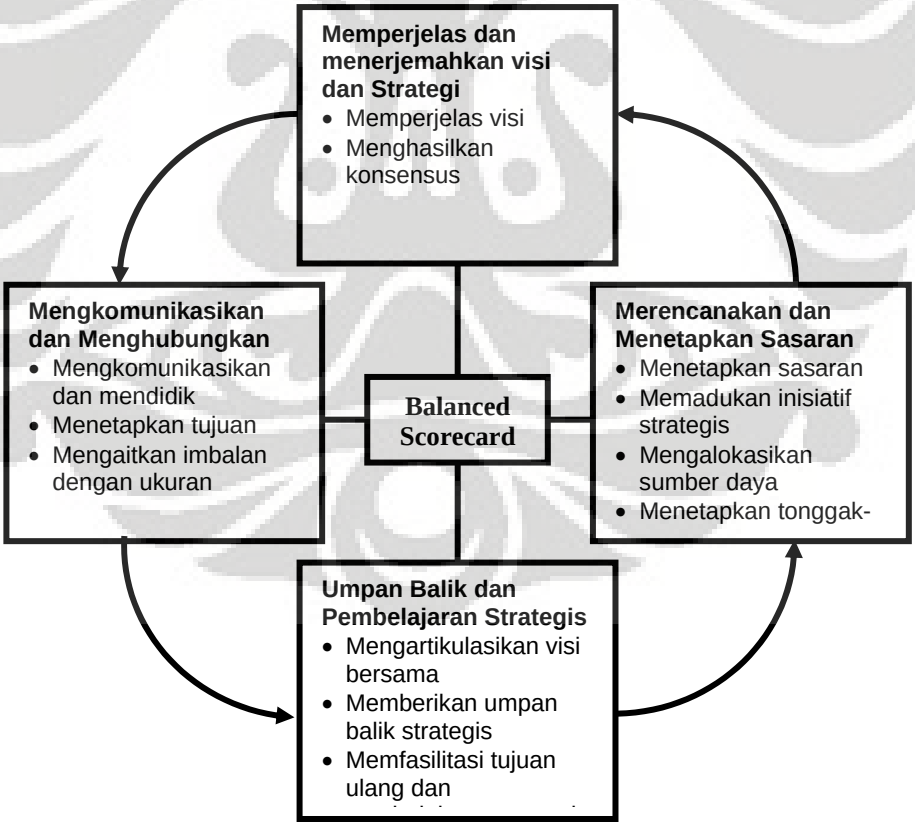
2.3.2. Langkah-Langkah *Balanced Scorecard*

Norton dan Kaplan menjelaskan empat tahap yang harus dilakukan oleh perusahaan untuk menggunakan *balanced scorecard*. Keempat tahap tersebut disebut sebagai kerangka kerja manajemen strategis (Kaplan dan Norton, 1996, hal. 10).

a. Memperjelas dan menerjemahkan visi dan strategi
b. Mengkomunikasikan dan mengaitkan tujuan dan ukuran strategis
c. Merencanakan, menetapkan sasaran, menyelaraskan berbagai inisiatif strategis
d. Meningkatkan umpan balik dan pembelajaran strategis.

Proses yang paling penting dari seluruh proses manajemen *scorecard* adalah menyertakan *balanced scorecard* dalam suatu kerangka pembelajaran strategis yang berarti menjadikannya sebagai suatu prosedur untuk menerima umpan balik strategi dan menguji hipotesis yang menjadi dasar strategi. Dengan demikian *balanced scorecard* memungkinkan manajer untuk memantau dan menyesuaikan pelaksanaan strategi, dan, jika perlu, membuat perubahan-perubahan mendasar terhadap strategi tersebut.

Dalam gambar 2.4 dijelaskan bagaimana keterkaitan antara masing-masing proses manajemen di atas. Proses pembelajaran strategis dimulai dari klarifikasi visi bersama yang hendak dicapai oleh seluruh organisasi. Proses selanjutnya adalah memberikan umpan balik strategis. Hingga proses akhirnya, memfasilitasi tinjauan ulang dan pembelajaran strategi. Keempat proses tersebut merupakan rangakaian proses yang membentuk rantai dan saling berkaitan.



Gambar 2.4. *Balanced Scorecard* Sebagai Kerangka Kerja Tindakan Strategis

(Sumber : Kaplan dan Norton, 1996, hal. 11.)

2.3.3. *Balanced Scorecard* Dan Sistem Pengukuran Kinerja

Sebelum berkembang seperti saat ini pada awalnya *balanced scorecard* hanya dikembangkan sebagai metode penilaian kinerja. Karena itu erat kaitannya antara *balanced scorecard* dengan penilaian kinerja. Menurut Anderson dan Clancy (1991, hal. 1008) pengukuran kinerja adalah*"feedback from the accountant and management that provide informaion about how well the actions represent the plan; it also identifies where managers may need to make corrections or adjustment in futute planning and controling activities"* (Yuwono, Sukarno, dan Ichsan, 2003, hal. 21).

Sementara itu, Anthony, Banker, Kaplan dan Young mendefinisikan pengukuran kinerja sebagai "*the activity of measuring the performance of activity or the entire value chain*" (Yuwono, Sukarno, dan Ichsan, 2003, hal. 23).

Sehingga dapat ditarik kesimpulan bahwa pengukuran kinerja merupakan sebuah aktivitas yang dilakukan terhadap seluruh kegiatan yang ada dalam perusahaan. Hasil pengukuran tersebut nantinya digunakan sebagai *feedback* atau umpan balik yang memberikan informasi tentang keberhasilan peruahaan. Sehingga berdasarkan informasi-informasi tersebut perusahaan dapat menentukan tindakan-tindakan pengendalian.

Balanced scorecard merupakan media pengukuran bagi kinerja strategi dan operasionalisasi strategi melalui *lagging indicator* dan *leading indicator* yang terintegrasi dalam empat perspektifnya. *Lagging indicator* atau ukuran hasil mencerminkan tujuan umum dari berbagai strategi perusahaan. Sedangkan *Leading indicator* adalah ukuran pemacu kinerja yang mencerminkan keunikan strategi unit bisnis. Identifikasi ukuran pemacu kinerja (*performance drivers*) dapat membantu perusahaan dalam mengatasi kelemahan ukuran hasil (*outcomes measure).*

2.3.4. Keempat Perspektif *Balanced Scorecard*

2.3.4.1. Perspektif Finansial

Menurut Norton dan Kaplan tujuan finansial dalam *balanced scorecard* menjadi fokus tujuan dan ukuran di semua perspektif scorecard lainnya. Setiap indikator dan ukuran dari perspektif lain harus mempunyai hubungan sebab akibat dengan tujuan keuangan perusahaan. *Scorecard* harus bisa menjelaskan strategi perusahaan, dimulai dengan strategi finansial jangka panjang, dan kemudian mengaitkannya dengan berbagai urutan tindakan yang harus diambil berkenaan dengan proses finansial, pelanggan, proses internal, dan para pekerja serta sistem untuk menghasilkan kinerja ekonomis jangka panjang yang diinginkan perusahaan.

Penentuan ukuran finansial *scorecard* harus sesuai dengan strategi yang dikembangkannya. Dengan demikian, bisa jadi ukuran-ukuran *scorecard* tersebut berbeda untuk tiap-tiap unit bisnis. Karena itu pihak eksekutif perusahaan tidak bisa memberikan ukuran yang sama pada tiap-tiap unit bisnis yang mereka bawahi, karena unit bisnis yang berbeda mungkin memerlukan strategi yang berbeda pula.

Untuk setiap siklus bisnis, tujuan dan ukuran finansialnya tentu saja berbeda. Menurut Ernest H. Drew (1993, hal. 48), siklus bisnis dibedakan menjadi tiga yaitu:

a. Pertumbuhan (*growth*)

   Pada tahap ini perusahaan masih harus terus membangun kemampuan sistem dan struktur, meningkatkan dan mengembangkan produk dan jasa yang baru sehingga masih memerlukan investasi yang cukup besar. Perusahaan dalam masa bertumbuh mungkin beroperasi dengan arus kas yang negatif, atau pengembalian modal yang rendah. Tujuan finansial perusahaan yang berada dalam tahap bertumbuh adalah presentasi tingkat pertumbuhan pendapatan, tingkat pertumbuhan penjualan diberbagai pasar sarasan, kelompok pelanggan dan wilayah.

b. Bertahan (*sustain*)

Bertahan adalah suatu tahap dimana sebuah perusahaan masih memiliki daya tarik penenaman investasi, tetapi diharapkan mampu menghasilkan pengembalian modal yang tinggi.Target dari unit bisnis seperti ini adalah mempertahankan pangsa pasar yang dimiliki secara bertahap dan bertumbuh dari tahun ke tahun. Kebanyakan unit bisnis yang berada pada tahap bertahan akan menetapkan tujuan finansial yang berkaitan dengan profitabilitas. Ukuran yang bisa dipakai dalam hal ini misalnya adalah laba operasi atau margin kotor (*gross margin*).

c. Menuai (*Harvest*)

Tahap menuai adalah tahap kedewasaan perusahaan. Pada tahap ini perusahaan akan menuai hasil investasi yang dikeluarkan sebelumnya. Bisnis tidak lagi memerlukan investasi yang besar. Investasi yang dikeluarkan cukup untuk pemeliharaan fasilitas dan kapabilitas. Tujuan finansial perusahaan yang ada pada tahap menuai darahkan pada maksimalisasi arus kas dan penghematan modal kerja.

Perspektif finansial mencakup tiga tema utama yaitu : pertumbuhan pendapatan (*revenue growth*), pengurangan biaya (*cost reduction*) dan utilisasi aset (*aset utilization*). Tabel 2.2 memberikan contoh gambaran tema sasaran strategis dan beberapa ukurannya dalam perspektif keuangan.

Tabel 2.2. Sasaran dan Ukuran Perspektif Keuangan

Sasaran	Ukuran
Pertumbuhan Pendapatan	
Meningkatkan jumlah produk baru	Persentase pendapatan dari pproduk baru
Menambah aplikasi baru	Persentase pendapatan dari aplikasi baru
Membangun konsumen dan pasar baru	Persentase pendapatan dari sumber daya
Adopsi strategi penetapan harga baru	Profitabilitas produk dan konsumen

Tabel 2.2 Sasaran dan Ukuran Perspektif Keuangan (Sambungan)

Sasaran	Ukuran
Pengurangan Biaya	
Reduksi biaya unit produk	Biaya produk perunit
Reduksi biaya unit konsumen	Biaya konsumen
Reduksi biaya distribusi	Biaya per saluran distribusi
Utilisasi Aset	
Meningkatkan utilisasi aset	*ROI* *Economic Value Aded*

(Sumber : Hansen, Don R., Mowen, dan Maryanne, 2000, hal. 401)

2.3.4.2. Perspektif Pelanggan

Filosofi manajemen modern menunjukkan betapa pentingnya fokus kepada konsumen dan kepuasan pelanggan dalam bisnis. Beberapa indikator yang selalu digunakan adalah: bila pelanggan tidak merasa puas mereka akan mencari produsen atau *supplier* baru yang bisa memenuhi kebutuhan mereka. Kinerja yang kurang baik dari perspektif ini akan mendorong terjadinya penurunan kinerja perusahaan di masa yang akan datang. Meskipun secara finansial kondisi perusahaan tergambarkan bagus, tetapi bila kinerja perspektif konsumen ini buruk maka di masa datang kondisi tersebut tidak akan bertahan.

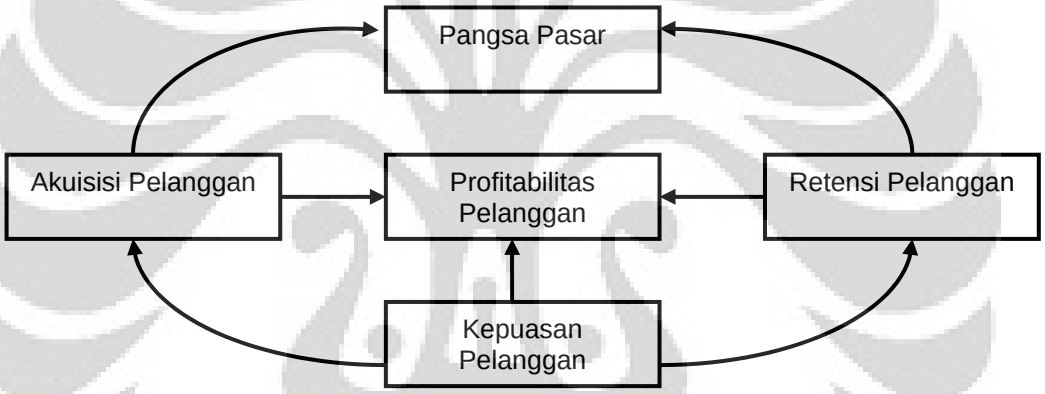
Perspektif pelanggan memungkinkan perusahaan melakukan identifikasi dan pengukuran, secara eksplisit, proposisi nilai yang akan perusahaan berikan kepada pelanggan dan pasar sasaran. Proposisi nilai merupakan faktor pendorong, *leading indicator*, untuk ukuran pelanggan utama.

Menurut Hansen dan Mowen (2000, hal. 401), sekurang-kurangnya ada lima sasaran kunci pada perspektif ini. Sasaran-sasaran tersebut meliputi: meningkatkan pangsa pasar, meningkatkan retensi pelanggan, meningkatkan akuisisi pelanggan, meningkatkan kepuasan pelanggan, dan meningkatkan profitabilitas pelanggan.

Selain sasaran kunci tersebut, Hansen dan Mowen menyebutkan beberapa sasaran lagi yang menyangkut *customer value*. Saaran-sasaran tersebut diantaranya:

a. Menurunkan harga
b. Menurunkan biaya pasca pembelian
c. Meningkatkan fungsionalitas produk
d. Meningkatkan kualitas produk
e. Meningkatkan keandalan pengiriman, dan
f. Meningkatkan citra dan reputasi produk.

Semua ukuran tersebut diatas dapat dikelompokkan dalam suatu rantai hubungan sebab akibat seperti ditunjukkan pada gambar 2.5.



Gambar 2.5. Ukuran Utama Dalam Perspektif Pelanggan
(Sumber: Kaplan dan Norton, 1996)

2.3.4.3. Perspektif Proses Bisnis Internal

Ukuran-ukuran yang dibuat pada perspektif ini memungkinkan manajer untuk mengetahui seberapa baguskah bisnis mereka dijalankan dan apakah produk atau jasa yang dihasilkan sudah memenuhi permintaaan konsumen. Ukuran-ukuran dalam perspektif ini harus didesain oleh orang-orang yang benar-benar paham akan proses yang bersangkutan.

Pada perspektif proses bisnis internal, perusahaan harus mampu mengidentifikasikan berbagai proses yang sangat penting untuk mencapai tujuan

pelanggan dan pemegang saham. Tujuan dan ukuran-ukuran dalam perspektif ini biasanya dirumuskan setelah perusahaan mengidentifikasi tujuan dan ukuran untuk perspektif keuangan dan pelanggan. Urutan ini memungkinkan perusahaan untuk memfokuskan pengukuran proses bisnis internal kepada proses yang akan mendorong tercapainya tujuan yang ditetapkan untuk pelanggan dan pemegang saham.

Menurut Kaplan dan Norton (1996, hal. 96) setiap bisnis mempunyai rangkaian proses tertentu untuk menciptakan nilai bagi pelanggan dan memberikan hasil keuangan yang baik. Kaplan dan Norton melihat bahwa model rantai generik membantu suatu *template* yang yang dapat disesuaikan oleh setiap perusahaan dalam mempersiapkan perspektif setiap bisnis internal. Model ini terdiri atas tiga proses bisnis utama, yaitu:

a. Inovasi

   Dalam proses inovasi, unit bisnis harus meneliti kebutuhan pelanggan yang sedang berkembang atau yang amsih tersembunyi, dan kemudian menciptakan produk atau jasa yang akan memenuhi kebutuhan tersebut. Hal ini memungkinkan perusahaan untuk memberikan perhatian yang cukup besar kepada riset, perancangan, dan proses pengembangan yang menghasilkan produk, jasa dan pasar baru

b. Operasi

   Proses operasi adalah tempat di mana produk dan jasa diproduksi dan disampaikan kepada pelanggan. Proses ini secara historis telah menjadi fokus sebagian besar sistem pengukuran kinerja perusahaan. Proses operasi yang baik dan penghematan biaya dalam berbagai proses manufaktur dan layanan jasa tetap merupakan tujuan penting, tetapi mungkin bukanlah komponen yang paling menentukan dari upaya perusahaan mencapai tujuan keuangan dan pelanggan.

c. Layanan Purna Jual

   Langkah utama ketiga dalam rantai nilai internal adalah layanan kepada pelanggan setelah penjualan atau penyampaian produk dan jasa. Sebagian perusahaan mempunyai strategi yang eksplisit untuk menyediakan layanan

purna jual yang istimewa. Proses layanan purna jual memungkinkan perusahaan untuk menentukan berbagai aspek penting layanan yang diberikan perusahaan setelah produk atau jasa yang dibeli sampai ke tangan pelanggan.

2.3.4.4. Perspektif Pembelajaran dan Pertumbuhan

Perspektif keempat dalam *balanced scorecard* mengembangkan tujuan dan ukuran yang mendorong pembelajaran dan pertumbuhan perusahaan. Tujuan yang ditetapkan dalam perspektif pembelajaran dan pertumbuhan adalah menyediakan infrastruktur yang memungkinkan tujuan dalam ketiga perspektif sebelumnya dapat dicapai. Tujuan dalam perspektif pembelajaran dan pertumbuhan merupakan faktor pendorong dihasilkannya kinerja yang istimewa dalam ketiga perspektif *scorecard* yang pertama. Hansen dan Mowen (2000, hal. 401) menyebutkan, perspektif ini mempunyai tiga sasaran utama yaitu:

a. *Employee Capability* (Kapabilitas karyawan)
b. *Motivation, Empowerment and Alignment* (Motivasi, pemberdayaan dan keselarasan)
c. *Information System Capability* (Kapabilitas sistem informasi).

Menurut Kaplan dan Norton perusahaan menetapkan tujuan pekerja yang ditarik dari tiga pengukuran utama yang berlaku umum. Ketiga ukuran ini kemudian ditambah juga dengan faktor pendorong yang dapat disesuaikan dengan situasi tertentu. Tiga pengukuran tersebut adalah:

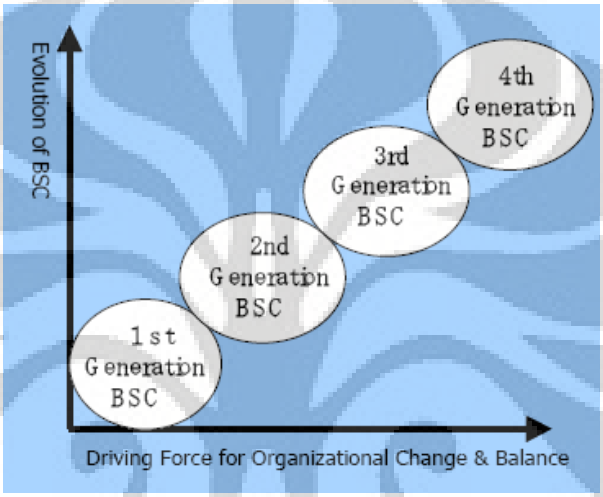
a. Kepuasan karyawan
b. Retensi karyawan
c. Produktivitas karyawan

Dalam kelompok pengukuran ini, tujuan kepuasan karyawan umumnya dipandang sebagai pendorong kedua pengukuran lainnya, retensi karyawan dan produktivitas karyawan.

2.3.5. *Balanced Scorecard* Generasi Ke-4

2.3.5.1. Perkembangan *Balanced Scorecard*

Norton dan Kaplan telah berkontribusi dengan memperkenalkan *balanced scorecard.* Tomori Tomura (2006) memperkenalkan *balanced scorecard for Sarbannes Oxley Act* (*balanced scorecard* generasi ke-4) sebagai perkembangan dari *balanced scorecard* generasi ke-3 yang telah digunakan oleh banyak perusahaan. Transisi *balanced scorecard* dapat dilihat pada gambar 2.6 berikut.



Gambar 2.6. Transisi *Balanced Scorecard*
(Sumber: Tomonori Tomura, 2006)

Perkembangan *balanced scorecard* adalah sebagai berikut:

a. Generasi pertama "*Multimodal Assessment Tool"* yaitu penambahan perspektif nonfinansial terhadap pengukuran kinerja – *learning and growth, internal business process,* dan *customers* – untuk merepresentasikan *stakeholder* mayor dalam bisnis (Steven John Simon, 2005, hal. 11).
b. Generasi ke-dua "*Top Down Management Tool*" yang merupakan permulaan dari konsep tujuan strategis dimana terdapat penambahan esensi dari strategi organisasi ke dalam tiap perspektif dari BSC pada generasi pertama (Steven John Simon, 2005, hal. 11).
c. Generasi ke-tiga yaitu "*Knowledge-creating and Strategic Communication Tool*" *(based on strategy map)* dimana dibuat *strategy map* yang dapat

memberi gambaran tujuan kritikal organisasi dan hubungan antar *Key Performance Indicator* dari tiap perspektif (Steven John Simon, 2005, hal. 11).

d. Generasi ke-4 "*Beyond Sarbanes Oxley Tool*" *(balancing the profit earning strategy and the internal control strategy: Balanced Scorecard for SOX)* menambahkan pentingnya kontrol internal dalam sebuah organisasi berdasar *Sarbanes-Oxley Act.*

Sarbanes-Oxley Act sendiri merupakan undang-undang pemerintah Amerika Serikat untuk meningkatkan tanggung jawab perusahaan. Undang-undang tersebut dibuat untuk mempertahankan kepercayaan investor di pasar publik Amerika Serikat, yang mengalami krisis sebelumnya. Undang-undang tersebut menekankan pada kontrol internal perusahaan (IT *Governance Institute*, 2004, hal. 12).

2.3.5.2. Siklus PDCA Untuk Kontrol Internal

Di Jepang, Agensi Pelayanan Finansial mengembangkan model kubus COSO sendiri yang disebut Japanese style COSO model (J-COSO). Konsep dasar J-COSO hampir sama dengan model COSO original. Perbedaan antara model COSO dan model J-COSO adalah "respon terhadap teknologi informasi" dan "perlindungan terhadap aset" (Tomonori Tomura, 2006, hal. 2).

COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) merupakan dasar untuk membangun kontrol internal yang mendukung efisiensi, meminimalisasi risiko, membantu memastikan reliabilitas pernyataan finansial, dan sesuai dengan hukum dan peraturan yang berlaku. Kontrol internal pada COSO:

a. *control environment*

merepresentasikan langkah awal organisasi untuk mengurangi risiko. Riset menunjukkan bahwa perusahaan akan menghasilkan kinerja lebih baik bila top manajemen membuat komitmen terhadap kontrol internal yang kuat dan membuktikannya dengan tindakan nyata. COSO meyakini bahwa perusahaan

dapat mengurangi risiko adanya tim dan komite audit dari luar organisasi serta juga dengan kesadaran control dari budaya organisasi,

b. *risk assessment*

prinsip utama terkait dengan pencapaian tujuan kontrol antara lain pentingnya tujuan laporan finansial, identifikasi dan analisis risiko, penilaian terhadap risiko. Walaupun tidak semua perusahaan memiliki proses *risk assessment* yang terstruktur, tetapi konsep dasar dari komponen kontrol internal harus terdapat di setiap organisasi.

c. *control activities*

kontrol ini terjadi pada seluruh organisasi, di seluruh level dan fungsi yang menggambarkan karakteristik organisasi termasuk auhorisasi pembuatan keputusan, jangkauan kontrol yang lebih luas, dan rantai komunikasi yang lebih singkat.

d. *information and communication*

seluruh bisnis harus mengidentifikasi, memperoleh, dan mengkomunikasikan informasi yang relevan dalam bentuk dan batas waktu yang memungkinkan orang untuk menjalankan tanggung jawabnya. Penggunaan teknologi informasi dapat membantu perusahaan untuk menstandardisasi kontrol.

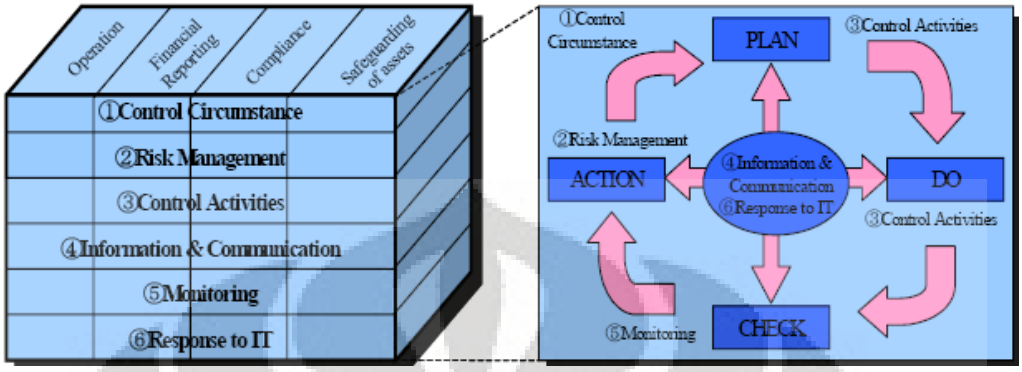
e. *monitoring*

monitoring yang efektif meliputi *ongoing monitoring,* evaluasi terpisah, dan laporan kerusakan. Monitoring memastikan bahwa kelima komponen sesuai dengan kebutuhan, sesuai dengan kondisi organisasi, dan berfungsi secara efektif.

Konsep ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 memiliki persamaan dengan J-COSO model dari kontrol internal berbentuk siklus PDCA yang dapat dilihat pada gambar 2.2 di atas dan 2.7.

Seperti telah diindikasikan oleh banyak artikel, *balanced scorecard* dapat memperbaiki kualitas implementasi strategi, operasi bisnis, komunikasi strategis, dan seterusnya untuk meraih profit dengan konsep siklus PDCA. Pada era SOX,

perusahaan perlu menyeimbangkan *balanced scorecard* untuk memperbaiki control internal sehingga dapat memperbaiki nilai perusahaan.



Gambar 2.7. Model J-COSO dan Kontrol Internal Konsep Siklus PDCA
(Sumber: Tomonori Tomura, 2006)

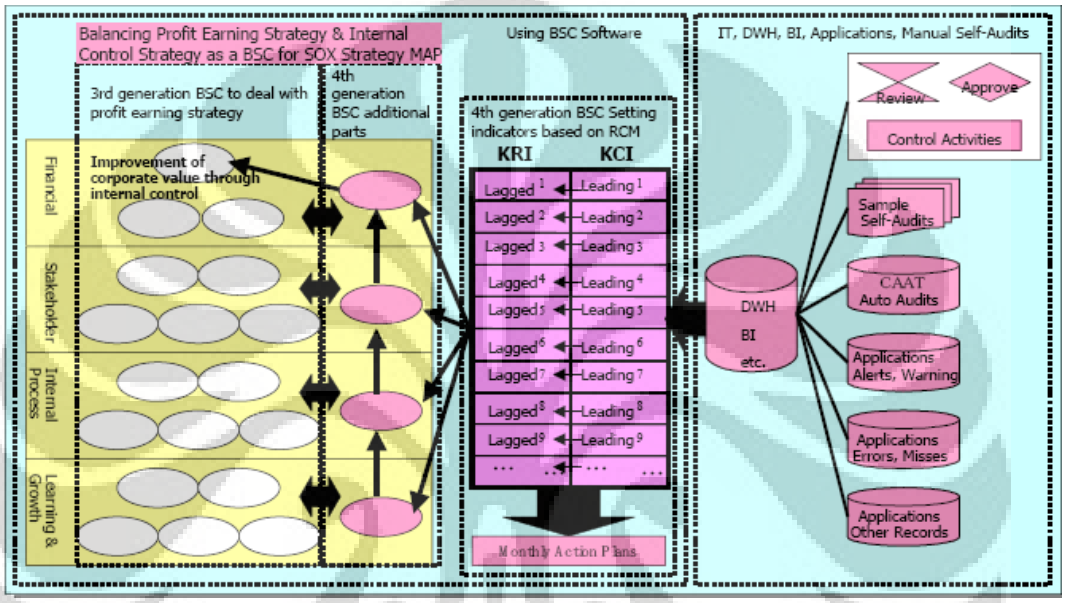
2.3.5.3. Konsep *Balanced Scorecard for SOX*

Informasi dan aktivitas bisnis harus dimonitor oleh orang dan waktu yang tepat. Karena risiko terkait dengan operasi harian berubah tiap harinya, perusahaan harus mengkomunikasikan informasi penting dan memonitor setiap tanda risiko untuk mencegah kegagalan dari audit eksternal. *Balanced scorecard for SOX* dapat membantu perusahaan, top manajemen, direktur, dan *stakeholder* lainnya (Tomonori Tomura, 2006).

Dengan menggunakan teknologi informasi seperti perangkat lunak *balanced scorecard*, Data Warehouse (DWH), Business Intelligence (BI), dan sebagainya, *balanced scorecard* generasi ke-4 dapat menjadi alat yang baik untuk strategi pencapaian profit dan kontrol internal. *Chief Excecutive Offiver* (CEO) dapat memonitor proses implementasi dari kedua strategi dan kemajuan tugas secara langsung. Seluruh anggota dapat berbagi informasi penting yang sama dan seluruh kemajuan pada strategi pencapaian profit dan status kontrol internal dengan perangkat lunak *balanced scorecard* (Tomonori Tomura, 2006).

Balanced scorecard generasi ke-4 menggunakan *balanced scorecard* generasi ke-3 sebagai basis. Strategi pencapaian profit direfleksikan oleh *balanced scorecard*

generasi ke-3, kemudian kontrol internal ditambahkan pada siklus PDCA. Kedua siklus PDCA dari generasi ke-3 dan ke-4 berhubungan pada *balanced scorecard* generasi ke-4. Berdasarkan matriks kontrol risiko (*risk control matrix*), indikator risiko utama (*key risk indicator*) dari tiap risiko sebagai *lagged indicator*, indikator pengendalian utama (*key control indicator*) dari kontrol sebagai *leading indicator*. Gambar 2.8 menggambarkan konsep *balanced scorecard* generasi ke-4.



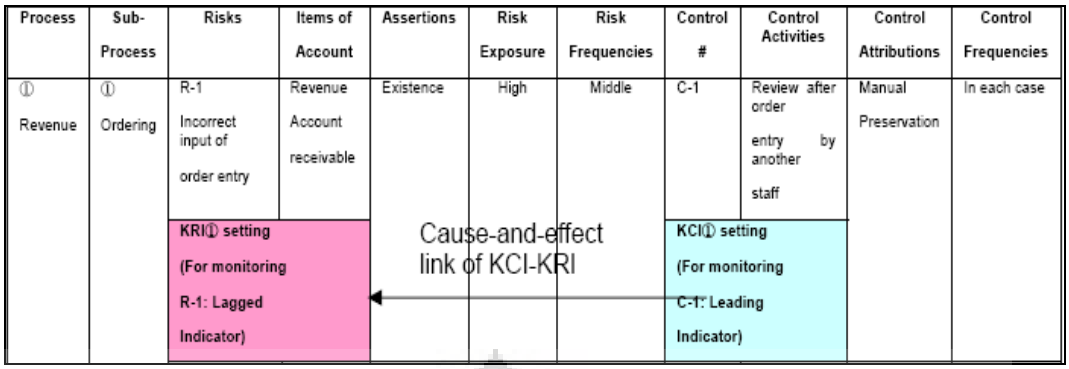
Gambar 2.8. Konsep *Balanced Scorecard* Generasi Ke-4

(Sumber: Tomonori Tomura , 2006)

2.3.5.4. Pembuatan Indikator Pada Matriks Kontrol Risiko

Untuk membuat *balanced scorecard* generasi ke-4 membutuhkan matriks kontrol risiko dimana terdapat identifikasi dan penilaian terhadap risiko, kemudian ditambahkan indikator risiko utama dan indikator pengendalian utama. Gambar 2.9 merupakan contoh matriks kontrol risiko (MKR).

Sesuai dengan risiko dan aktivitas kontrol yang terdapat pada MKR, risiko dan aktivitas kontrol dikuantifikasi dengan Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU). IRU menggambarkan bagaimana risiko dikontrol dan IPU menunjukkan bagaimana aktivitas kontrol diimplementasikan untuk mengurangi risiko.



Gambar 2.9. Contoh Matriks Kontrol Risiko

(Sumber: Tomonori Tomura, 2006)

Jika IPU menunjukkan hasil yang lebih buruk dari periode sebelumnya, perusahaan akan menghadapi permasalahan mengenai manajemen risiko yang dibutuhkan oleh SOX di masa mendatang (dimana memungkinkan hasil IRU yang buruk di masa mendatang). Dengan *balanced scorecard for SOX*, perusahaan dapat memperoleh dan memonitor tanda untuk manajemen risiko lebih awal dari pada auditor. Hal ini dikarenakan baik strategi pencapaian profit maupun strategi kontrol internal membutuhkan pendekatan manajerial (Tomonori Tomura, 2006).

2.3.5.5. Manfaat *Balanced Scorecard* Generasi Ke-4

Menurut Tomonori Tomura (2006), kelebihan *Balanced Scorecard* generasi ke-4 antara lain:

a. memungkinkan kepemilikan proses dengan adanya pembuatan indikator yang meningkatkan kontrol internal
b. dengan pembuatan IRU dan IPU dan perencanaan tindakan, pemilik proses dapat memahami tugas yang dibutuhkan lebih lanjut, waktu pelaksanaan aktivitas kontrol, efek yang dibutuhkan, dsb.
c. dapat mendeteksi risiko potensial pada proses internal lebih dini, sehingga dapat mendeteksi peristiwa yang tidak diinginkan dan mengambil tindakan yang tepat untuk merespon terhadap kejadian yang buruk. Hal ini disebut *Alternate Function of Internal Audit* (AFIA) dimana dilakukan audit internal secara periodik

d. sebagai alat bantu dalam membuat program audit internal yang efektif karena auditor internal dapat mengetahui permasalahan auditor berikutnya dengan mengamati perubahan nilai dari indikator
e. meningkatkan transparansi dan akuntabilitas karena direktur dapat menjelaskan situasi kontrol internal kepada *stakeholder*
f. memperlihatkan *gap* antara target dan kondisi saat ini pada proses internal, sehingga dapat memberi input untuk mengatasi *gap* tersebut
g. meningkatkan nilai organisasi karena kemudahan direktur untuk mengkomunikasikan pesan perubahan organisasi
h. memastikan kontrol proses internal yang mudah dilacak serta dapat diperbaiki secara terus-menerus pada periode selanjutnya.

2.4. Pembuatan Indikator

2.4.1. Kriteria Indikator

Menurut Davies dan Haubenstock (2002, hal. 42) pertimbangan dalam pemilihan indikator risiko adalah:

a. sesuai dengan risiko
   berdasarkan risiko yang ada, pilih metrik yang efektif untuk mengukur risiko yang bersangkutan, desain metrik yang memiliki ketersediaan data, kemudian membuat perencanaan implementasi
b. mengembangkan metrik yang mewakili semua *stakeholder*
   stakeholder di sini meliputi pemegang saham, pelanggan, karyawan, pemasok, pembuat peraturan, dan komunitas
c. memilih metrik yang representatif
   terlalu banyak metrik dapat mengurangi nilai dari pengukuran itu sendiri. Metrik *ex ante* memiliki nilai lebih untuk melihat permasalahan di masa mendatang
d. mendapatkan dukungan dari *senior management*
   pembuatan indikator sebaiknya dikomunikasikan dengan manajemen karena ada kecenderungan bahwa karyawan tidak duka diukur

e. memahami indikator risiko versus kinerja
   indikator cenderung bersifat operasional, sedangkan pengukuran kinerja lebih jangka panjang. Hubungkan antara indikator dengan pengukuran kinerja dari *balanced scorecard*
f. metrik sederhana dan mudah dimengerti
   adanya nilai kesederhanaan dan semua pihak harus mengerti alasan dan pertimbangan rasional metrik dan laporannya
g. metrik memiliki metode pembuatan yang konsisten
   metode yang konsisten ini akan memberikan kredibilitas dan bantuan dalam pelaporan risiko
h. metrik dapat dikuantifikasi
   hal ini dikarenakan ada beberapa hal yang kita ingin ukur tetapi tidak dapat diukur
i. melakukan investasi pada teknologi
   banyak program yang dapat digunakan untuk metrik sehingga dapat dilakukan tepat waktu dan hemat biaya
j. menggunakan kriteria eskalasi
   salah satu kelebihan dari metrik yang dapat dikuantifikasi yaitu target metrik dapat dievaluasi kembali oleh manajemen berdasar kriteria eskalasi
k. indikator sebagai *work in progress*
   pengalaman akan membantu memperbaiki metrik yang lebih sesuai lagi dengan risiko.

Kriteria metrik menurut Patrick PC Ow (n.d.) antara lain:

a. metrik harus dapat dilakukan dan targetnya dapat dicapai
b. metrik dipahami melalui adanya komunikasi dua arah sehingga pengukuran dan target lebih relevan dan valid
c. metrik diprioritaskan dan sejalan dengan tujuan baik secara vertikal maupun horizontal
d. karyawan harus memiliki tingkatan kontrol, authoritas, dan pengaruh yang signifikan dalam pencapaian kinerja metrik
e. kinerja yang baik diberi apresiasi berupa uang atau penghargaan
f. metrik berkaitan dengan pekerjaan dan dapat dikuantifikasi

g. metrik logis dan menggambarkan hubungan yang jelas dengan tujuan
h. metrik spesifik terhadap individu yang bertanggungjawab terhadap kinerja metrik
i. metrik memiliki batas waktu
j. metrik sesuai dengan beban kerja

Menurut James Lam dan rekan (2006), karakteristik dari indikator risiko utama yang efektif antara lain:

a. berdasarkan metodologi dan standar yang konsisten
b. berkaitan dengan faktor risiko: sumber, kecenderungan, akibat, dan korelasi
c. dapat dikuantifikasi
d. dapat ditelusuri dari aspek waktu berdasarkan standar dan keterbatasan
e. mendukung tujuan, pemilik risiko, dan kategori standar risiko
f. seimbang antara *leading* dan *lagging indicators*
g. bermanfaat terhadap keputusan dan tindakan manajemen
h. dapat dibandingkan secara internal dan eksternal
i. hemat waktu dan biaya
j. risiko dapat disederhanakan tanpa kehilangan makna sebenarnya

2.4.2. Metodologi Pembuatan Indikator

Menurut Immaneni, Mastro, dan Haubenstock (2004, hal. 43) tahapan untuk membuat indikator antara lain:

a. identifikasi indikator pada organisasi

   pengembangan indikator risiko dimulai dengan *risk assessment.* Risiko bisnis diidentifikasi, dinilai, dan dibuat katalognya bersama dengan kontrol yang berhubungan dan analisis dari penyebab risiko tersebut. Setelah *risk assessment,* maka dilakukan identifikasi metrik yang telah ada, dan diskusi dengan para ahli (*subject matter experts*) untuk pembuatan indikator baru

b. penilaian *gap*

   setelah diidentifikasi, dilakukan penilaian kesesuaian dan efektivitas metrik terhadap risiko. Penilaian dapat menggunakan matriks dan dinilai dengan skala tertentu. Penilaian ini berguna untuk tahap berikutnya yaitu perbaikan indikator yang telah ada dan potensial (baru dibuat)

c. perbaikan indikator

dalam pemilihan indikator, terlebih dahulu diilihat indikator yang memiliki nilai tinggi. Bila terdapat nilai rendah, dimana faktor tersebut dapat diperbaiki, maka perbaikan terhadap indikator dapat dilakukan agar dapat lebih efektif dalam mengukur risiko

d. validasi dan penentuan level pencapaian

pada tahap ini, dilakukan penilaian korelasi antara indikator dan risiko, terutama indikator yang baru dibuat. Secara ideal, seharusnya validasi dilakukan dengan metode statistik. Namun, pada sebagian besar kasus, data historis tidak tersedia terutama pada kejadian risiko. Karena biasanya bisnis memiliki pemahaman yang baik dari level target dan batasan kontrol dari risiko, korelasi antara pemicu risiko dan indikator risiko memungkinkan kita untuk menetapkan level target dan batasan kontrol dari metrik. Validasi tidak diperlukan untuk setiap indikator risiko dan risiko. Idealnya, setiap risiko akan memiliki satu atau lebih metrik utama yang perlu divalidasi.

e. desain *dashboard*

dashboard didesain sedemikian rupa untuk melaporkan metrik kritikal bagi manajer, pemilik proses, dan *senior management. Dashboard* biasanya menggunakan gambar dan tabel untuk memperlihatkan risiko secara jelas dan menyeluruh

f. membuat perencanaan kontrol dan kriteria eskalasi

tujuan dari perencanaan kontrol adalah memastikan kriteria eskalasi dan peran intervensi telah dibuat. Dokumentasi ini memungkinkan pemilik proses untuk mengikuti protokol yang telah disetujui dan konsisten setiap kali indikator dibuat. Dengan demikian, pemilik proses yang baru dapat dengan mudah memahami prosedur dan level risiko yang akan diterima (*accept*) oleh perusahaan. Perencanaan kontrol dapat berupa 1 halaman dari penjelasan detil terhadap semua tindakan dan akuntabilitas indikator atau penjelasan terpisah untuk tiap indikator. Perencanaan kontrol meliputi metrik dari indikator, frekuensi pengukuran, tujuan, level pemicu, kriteria eskalasi, dan pemilik proses.

2.5. Metode *Rating*

Menurut Concise Oxford Dictionary, *rating* didefinisikan sebagai klasifikasi atau urutan berdasarkan kualitas, standar, atau kinerja. *Rating* juga didefinisikan sebagai nilai dari suatu *property* atau kondisi yang dianggap standar, optimal atau membatasi untuk material, alat, dan lain-lain. Untuk mendapatkan *rating* dilakukan dengan penskalaan. Menurut Trochim (2000) penskalaan adalah memberikan suatu angka pada suatu objek berdasarkan suatu aturan. Skala dapat dibedakan menjadi beberapa jenis sebagai berikut (Saaty, 2003):

a. Skala nominal

   Skala nominal tidak tampak seperti skala. Ketika angka digunakan untuk tujuan identifikasi atau penamaan, angka tersebut adalah skala nominal. Contoh skala nominal adalah nomor telepon

b. Skala ordinal

   Skala ordinal menunjukkan urutan. Contoh skala ordinal adalah peringkat

c. Skala interval

   Skala interval menunjukkan interval atau jarak antara 2 titik pada skala. Contoh skala interval adalah skala termometer

d. Skala Rasio

   Skala rasio dapat juga menunjukkan urutan seperti skala ordinal tetapi rasio tertentu pada bagian yang berbeda pada skala mempunyai arti.

2.5.1. *Analytical Hierarchy Process*

Analytical Hierarchy Process (AHP) merupakan salah satu metode pengambilan keputusan yang dikembangkan oleh Thomas L. Saaty. AHP memecah situasi kompleks dan tidak terstruktur menjadi bagian-bagian komponen; mengatur bagian-bagian atau variabel-variabel ini menjadi hierarki; memberikan penilaian subjektif terhadap kepentingan relatif dari setiap variabel; dan mensintesis penilaian tersebut untuk menentukan variabel mana yang mempunyai prioritas tertinggi dan harus dilakukan untuk mempengaruhi hasil dari situasi tersebut (T.L. Saaty, 1999, hal. 5).

2.5.1.1. Prinsip Dasar AHP

Analytical Hierarchy Process dilandasi oleh prinsip dasar manusia dalam berpikir analitis, yaitu (T.L. Saaty, 1999, hal. 7):

a. pembentukan hierarki

   Untuk pengetahuan yang detail, dibuat struktur dari realitas yang kompleks menjadi bagian-bagian secara hierarki sehingga informasi yang besar dapat diintegrasikan menjadi struktur masalah dan membentuk gambaran yang jelas terhadap keseluruhan sistem.

b. penentuan prioritas

   Untuk mempersepsikan hubungan antara sesuatu yang diamati, membandingkan pasangan sesuatu yang sama terhadap kriteria tertentu, dan membedakan antara pasangan tersebut dengan menilai intensitas satu dengan lainnya. Intensitas tersebut disebut prioritas.

c. konsistensi logis

   Untuk menghubungkan objek atau ide dengan cara tertentu agar tetap koheren, yaitu berhubungan satu sama lain dan hubungan tersebut menunjukkan konsistensi.

Dalam menggunakan prinsip-prinsip dasar tersebut, *Analytical Hierarchy Process* memanfaatkan baik aspek kualitatif maupun kuantitatif dari pikiran manusia, yaitu aspek kualitatif untuk mendefinisikan masalah dan aspek kuantitatif untuk mengekspresikan penilaian (*judgments*) dan pilihan (*preferences*).

2.5.1.2. Pembentukan Hierarki

Sistem kompleks dapat dengan mudah dimengerti dengan memecahnya menjadi elemen-elemen, menyusun elemen-elemen tersebut secara hierarki, dan mengkomposisi atau sintesis penilaian tingkat kepentingan relatif elemen-elemen tersebut pada setiap level pada hierarki ke dalam suatu set prioritas keseluruhan (T.L. Saaty, 1999, hal. 30). Hierarki adalah abstraksi dari struktur suatu sistem untuk mempelajari interaksi fungsi dari komponen-komponennya dan pengaruhnya terhadap keseluruhan system (T.L. Saaty, 1999, hal. 3).

Menurut T.L. Saaty, hierarki dapat diklasifikasikan menjadi 2 jenis yaitu:

a. struktural

   Sistem kompleks disusun menjadi bagian-bagian dalam urutan dari atas ke bawah menurut *structural properties* seperti ukuran, bentuk, warna, atau usia. Hierarki struktur berhubungan erat dengan cara menganalisa kompleksitas dengan memecah objek yang dipersepsikan oleh panca indra menjadi kelompok-kelompok, sub kelompok, dan kelompok yang lebih kecil.

b. fungsional

   Sistem kompleks disusun menjadi bagian-bagian menurut hubungannya yang penting. Setiap set elemen dalam hierarki fungsional menempati suatu level hierarki. Level paling atas yang disebut fokus terdiri dari hanya satu elemen yaitu tujuan keseluruhan yang luas. Level selanjutnya dapat terdiri dari beberapa elemen walaupun jumlahnya biasanya sedikit antara 5 sampai 9. Karena elemen dalam satu level akan dibandingkan satu sama lain terhadap kriteria pada level di atasnya, elemen dalam setiap level harus mempunyai *magnitude* yang sama.

Langkah-langkah dalam menyusun suatu hierarki adalah sebagai berikut (T.L. Saaty, 1999, hal. 35):

a. mengidentifikasi tujuan keseluruhan.
b. mengidentifikasi sub tujuan dari tujuan keseluruhan.
c. mengidentifikasi kriteria yang harus dipenuhi untuk mencapai sub tujuan dari tujuan keseluruhan.
d. mengidentifikasi subkriteria untuk setiap kriteria
e. mengidentifikasi *actors* yang terlibat.
f. mengidentifikasi tujuan *actors*.
g. mengidentifikasi kebijakan dari *actors*.
h. mengidentifikasi pilihan atau hasil.
i. keputusan yang diambil adalah yang memberikan hasil yang terbaik dan bandingan keuntungan dan biaya dari membuat keputusan tersebut dengan tidak membuat keputusan tersebut.
j. melakukan analisis keuntungan/ biaya.

2.5.1.3. Penentuan Prioritas

Prioritas adalah urutan numerik yang diukur dalam suatu skala rasio. Prioritas dapat digunakan untuk memilih alternatif yaitu alternatif dengan skala rasio terbesar. Prioritas dapat juga digunakan untuk mengalokasikan sumber daya secara proporsional kepada alternative (T.L. Saaty, hal. 36).

Menurut Saaty (1999), prioritas dapat dibedakan menjadi 3 level:

1. Prioritas lokal yang diperoleh dari penilaian terhadap suatu kriteria.
2. Prioritas global yang diperoleh dari perkalian dengan prioritas suatu kriteria.
3. Prioritas keseluruhan yang diperoleh dengan menjumlahkan prioritas global.

Untuk memilih alternatif diperlukan prioritas lokal dari alternatif. Untuk mensintesis prioritas lokal dari alternatif menggunakan prioritas global dari kriteria di atasnya, ada 2 *mode*, yaitu

a. *Ideal mode*

   Ideal mode digunakan untuk mendapatkan satu alternatif terbaik tidak tergantung alternatif lainnya. Hal ini dilakukan untuk setiap kriteria dimana untuk setiap kriteria satu alternatif menjadi ideal dengan nilai satu. Pada *ideal mode* tingkat kepentingan bobot dari kriteria menunjukkan tingkat kepentingan yang diberikan pembuat keputusan kepada kinerja relatif dari suatu alternatif terhadap beberapa alternatif *benchmark*.

b. *Distributive mode*

   Dalam *distributive mode*, bobot semua alternatif jika dijumlahkan menjadi bernilai satu. *Distributive mode* digunakan ketika ada ketergantungan antara alternatif-alternatif dan unit prioritas yang didistribusikan ke alternatif-alternatif tersebut. Pada *distributive mode* bobot dari kriteria menunjukkan tingkat kepentingan yang diberikan pembuat keputusan kepada dominasi setiap alternatif relatif terhadap semua alternatif lainnya di dalam kriteria tersebut.

Langkah pertama untuk menentukan prioritas elemen-elemen dalam suatu masalah keputusan adalah dengan membuat perbandingan berpasangan yaitu

dengan membandingkan elemen-elemen berpasangan terhadap suatu kriteria. Untuk perbandingan berpasangan, bentuk yang lebih disukai adalah matriks (T.L. Saaty, 1999, jal. 72). Suatu contoh matriks perbandingan berpasangan dapat dilihat pada tabel 2.3.

Tabel 2.3. Contoh Matriks Perbandingan Berpasangan

C	A_1	A_2	…	A_7
A_1	1	5		
A_2	1/5	1		
⋮	⋮			
A_7				1

(Sumber: Saaty, 1999, hal.72)

Untuk mengisi matriks perbandingan berpasangan digunakan angka untuk mewakili tingkat kepentingan relatif dari suatu elemen terhadap lainnya. Tabel 2.4 menunjukkan skala dasar *Analytical Hierarchy Process* untuk perbandingan berpasangan.

Tabel 2.4. Skala Dasar Perbandingan Berpasangan

Intensitas Kepentingan	**Definisi**	**Penjelasan**
1	Kepentingan sama	Dua aktivitas mempunyai kontribusi yang sama terhadap tujuan
3	Kepentingan *moderate*	Pengalaman dan penilian sedikit lebih memilih satu aktivitas daripada yang lain
5	Kepentingan kuat	Pengalaman dan penilian secara kuat lebih memilih satu aktivitas daripada yang lain
7	Kepentingan sangat kuat	Suatu aktivitas lebih dipilih sangat kuat daripada yang lain

Tabel 2.4. Skala Dasar Perbandingan Berpasangan (Sambungan)

Intensitas Kepentingan	Definisi	Penjelasan
9	Kepentingan ekstrim	Bukti lebih memilih suatu aktivitas daripada yang lain pada tingkatan afirmasi yang tertinggi
2,4,6,8	Untuk nilai tengah dari nilai-nilai diatas	Kadang-kaang seseorang perlu menginterpolasi penilaian di tengah-tengah secara numerik karena tidak ada kata yang tepat untuk menggambarkannya
Kebalikan dari di atas	Jika aktivitas I mempunyai salah satu nilai bukan nol diatas ketika dibandingkan dengan aktivitas j, maka j mempunyai nilai kebalikan ketika dibandingkan dengan i	Suatu perbandingan dilakukan dengan memilih elemen yang lebih kecil sebagai unit untuk mengestimasi elemen yang lebih besar sebagai perkalian dari unit tersebut
1.1-1.9	Untuk aktivitas yang seri	Ketika elemen-elemen berdekatan dan hampir tidak dapat dibedakan, nilai *moderate* adalah 1.3 dan ekstrim adalah 1.9

(Sumber: Saaty, 1999, hal.73)

Ada beberapa alasan mengapa skala perbandingan berpasangan mempunyai batas atas 9 (Saaty, 1999, hal. 55):

a. Pembedaan secara kualitatif sangat penting dan mempunyai elemen presisi ketika sesuatu yang dibandingkan berdekatan dalam kriteria yang digunakan dalam perbandingan.
b. Kemampuan manusia untuk membuat pembedaan secara kualitatif mempunyai 5 atribut yaitu sama, lemah, kuat, sangat kuat, dan absolut. Dalam kelima atribut tersebut ada nilai tengah ketika nilai presisi diperlukan sehingga ada total 9 nilai.
c. Metode pengklasifikasian stimuli menjadi 3 yaitu penolakan, tidak ada pembedaaan, dan penerimaan. Untuk pengklasifikasian selanjutnya ketiganya dibagi menjadi 3 yaitu rendah, sedang, dan tinggi sehingga terdapat 9 pembedaan.
d. Batas psikologis 7 ± 2 dalam perbandingan menyarankan jika sesuatu yang dibandingkan hanya berbeda sedikit satu sama lain diperlukan 9 pembedaan.

Penentuan prioritas atau bobot mempunyai 2 fungsi utama (Cheng, Eddy W.L. dan Heng Li, 2001, hal. 30.):

a. Memeringkatkan elemen sehingga elemen kunci dapat diketahui. Dalam bisnis elemen kunci tersebut diperlukan untuk ukuran kunci kinerja bisnis.
b. Memberi bobot pada elemen kunci sehingga membantu dalam membuat keputusan yang lebih akurat.

2.5.1.4. Konsistensi Logis

Konsistensi dapat berarti ide atau objek yang sama dikelompokkan berdasarkan homogenitas dan relevansi. Contohnya, anggur dan kelereng dapat dikelompokkan menjadi satu apabila bundar adalah kriteria yang relevan dan bukan rasa sebagai kriteria. Arti lain dari konsistensi adalah bahwa intensitas hubungan antara ide atau objek berdasarkan kriteria tertentu menjustifikasi satu sama lain dalam cara yang logis. Sebagai contoh, apabila manis sebagai kriteria, madu dinilai 5 kali lebih manis daripada gula, dan gula dinilai 2 kali lebih manis daripada permen, maka madu harus dinilai 10 kali lebih manis daripada permen. Jika tidak, maka penilaian tersebut tidak konsisten.

Analytical Hierarchy Process mengukur konsistensi keseluruhan dari penilaian dengan menggunakan rasio inkonsistensi. Nilai rasio inkonsistensi harus bernilai lebih kecil atau sama dengan 5% untuk matriks 3x3, 9% untuk matriks 4x4, dan 10% untuk matriks yang lebih besar (T.L. Saaty, 1999, hal. 81).

2.5.1.5. Tujuh Pilar AHP

Menurut T.L. Saaty (1999, hal 1), tujuh Pilar dari *Analytical Hierarchy Process* adalah sebagai berikut:

a. skala rasio

   rasio adalah nilai relatif atau hasil bagi a/b dari dua jumlah a dan b yang sama. Jika dua rasio a/b dan c/d sama disebut proporsional. Skala rasio adalah suatu set angka yang selalu sama di bawah suatu transformasi yang sama (perkalian dengan suatu konstanta positif). Bobot dari suatu set objek dapat distandardisasi dengan melakukan normalisasi sehingga tidak perlu dispesifikasi satuan dari bobot tersebut. Bentuk standar tersebut adalah ukuran yang tidak mempunyai satuan dan merupakan angka absolut.

b. perbandingan berpasangan dan skala dasar

   untuk membandingkan dua hal digunakan suatu nilai dasar dari skala absolut 1-9 untuk mewakili rasio perbandingannya. Skala absolut tersebut adalah pendekatan bilangan bulat (*integer*) dari rasio tersebut. Hal ini merupakan fakta dasar pendekatan pengukuran relatif (*relative measurement*) dalam AHP dan perlunya skala dasar. Skala 1-9 digunakan karena secara kualitatif orang mempunyai kemampuan untuk membedakan respons mereka terhadap stimuli menjadi 3 kategori yaitu tinggi, sedang, dan rendah. Selain itu masing-masing kategori dibedakan intensitasnya menjadi tinggi, rendah, dan sedang sehingga membuat 9 pembagian.

c. sensitivitas vektor eigen

   sensitivitas vektor eigen membatasi jumlah elemen dalam setiap set perbandingan dan membutuhkan homogenitas. Oleh karena itu untuk mengetahui seberapa kurang pentingnya a daripada b digunakan kebalikan dari seberapa lebih pentingnya b daripada a.

d. homogenitas dan klusterisasi

homogenitas dan klusterisasi digunakan untuk memperluas skala dasar dari suatu kelompok ke kelompok berikutnya yang akan memperluas skala 1-9 menjadi 1-tak terhingga.

e. sintesis

sintesis digunakan untuk membuat suatu skala unidimensional dari skala multidimensional dengan menggunakan normalisasi skala rasio.

f. mempertahankan dan mengubah urutan (*rank preservation and reversal*)

Pada pembobotan dapat terjadi perubahan urutan bobot apabila dimasukkan kriteria atau alternatif baru terutama pada pengukuran absolut (*absolute measurement*). Untuk mempertahankan urutan digunakan *ideal mode* sedangkan *distributive mode* memperbolehkan perubahan urutan.

g. penilaian kelompok

Penilaian kelompok diperoleh dengan menggabungkan penilaian-penilaian individu terhadap suatu set alternatif keputusan.

2.5.1.6. Pengukuran Relatif Dan Absolut Dalam AHP

Dalam AHP kedua jenis perbandingan tersebut dapat digunakan untuk mengurutkan alternatif yang terdiri dari 3 jenis *mode* (T.L. Saaty, 1999, hal. 2), yaitu:

a. Relatif

Mode ini mengurutkan alternatif dengan membandingkan secara berpasangan alternatif-alternatif tersebut.

b. Absolut

Mode ini mengurutkan alternatif yang jumlahnya tidak terbatas satu per satu dengan suatu skala intensitas untuk setiap kriteria.

c. Benchmarking

Mode ini mengurutkan alternatif dengan menggunakan suatu alternatif yang sudah diketahui dan membandingkan alternatif lainnya dengan alternatif tersebut.

Mode relatif dikenal dengan pengukuran relatif (*relative measurement*). Pada pengukuran relatif, pembuat keputusan melakukan perbandingan berpasangan pada alternatif terhadap setiap kriteria dengan menyatakan preferensi pada setiap pasang alternatif dengan skala dasar 1-9 dalam perbandingan berpasangan. Skala rasio dari nilai relatif akan diperoleh dari matriks perbandingan berpasangan sehingga terbentuk urutan alternatif (T.L. saaty, 1999, hal 295). Hierarki untuk pengukuran relatif terdiri dari kriteria, sub kriteria, dan alternatif yang bobotnya didapat dari perbandingan berpasangan.

Mode absolut dikenal dengan pengukuran absolut. Pengukuran absolut (*absolute measurement*) yang sering disebut *rating* digunakan untuk memeringkatkan alternatif independen sekaligus berdasarkan *rating intensities* untuk tiap-tiap kriteria. Dalam pengukuran absolut, hierarki dibentuk ke dalam kriteria dan sub-kriteria yang selanjutnya dibagi ke dalam level intensitas. Level intensitas adalah *range* variasi dari kriteria yang membedakan kualitas suatu alternatif berdasarkan suatu kriteria. Bobot setiap level intensitas juga didapat dari perbandingan berpasangan. Untuk mendapatkan rating keseluruhan alternatif, bobot alternatif berdasarkan level intensitas dari semua kriteria dijumlahkan untuk setiap alternatif. Pengukuran absolut sebaiknya digunakan jika alternatif lebih banyak daripada 9 karena perbandingan berpasangan alternatif pada pengukuran relatif akan sangat rumit untuk alternatif lebih banyak daripada 9.

2.5.1.7. Langkah-Langkah AHP

Menurut Saaty (1999, hal. 34), langkah-langkah AHP adalah sebagai berikut:

1. Mendefinisikan masalah dan spesifikasi penyelesaian yang diinginkan.
2. Membentuk hierarki dari sudut pandang manajerial keseluruhan.
3. Membentuk matriks perbandingan berpasangan dari kontribusi relevan suatu level elemen hierarki terhadap level elemen hierarki di atasnya.
4. Mendapatkan penilaian yang diperlukan untuk melengkapi matriks di langkah 3.

5. Dengan mengumpulkan data perbandingan berpasangan, didapat prioritas dan konsistensi diuji.
6. Lakukan langkah 3, 4, dan 5 untuk setiap level dan pengelompokkan dalam hierarki.
7. Menggunakan komposisi hierarki (sintesis) untuk membobotkan vektor prioritas keseluruhan untuk elemen terbawah pada hierarki.
8. Mengevaluasi konsistensi untuk keseluruhan hierarki.

2.5.1.8. Keunggulan AHP

Keunggulan *Analytical Hierarchy Process* adalah sebagai berikut (Saaty, 1999, hal.25):

1. kesatuan (*unity*)
   AHP memberikan model yang tunggal, mudah dimengerti, fleksibel untuk masalah yang luas dan tidak terstruktur.
2. kompleksitas (*complexity*)
   AHP mengintegrasikan pendekatan deduktif dan sistem dalam memecahkan masalah kompleks.
3. ketergantungan (*interdependence*)
   AHP berhubungan dengan interdepedence dari elemen-elemen sistem dan tidak berdasarkan berpikir linear.
4. penyusunan hierarki (*hierarchic structuring*)
   AHP merefleksikan kecenderungan natural pikiran untuk menyusun elemen-elemen sistem ke dalam level yang berbeda dan mengelompokkan elemen-elemen yang sama pada setiap level.
5. pengukuran (*measurement*)
   AHP memberikan skala untuk mengukur satuan yang tidak dapat diukur (*intangibles*) dan metode untuk menentukan prioritas.
6. konsistensi (*consistency*)
   Analytical Hierarchy Process menghitung konsistensi logis dari penilaian yang digunakan dalam menentukan prioritas.

7. sintesis (*synthesis*)

   AHP memberikan estimasi keseluruhan dari lebih dipilihnya setiap alternatif.

8. *Tradeoffs*

   AHP ikut mempertimbangkan prioritas relatif dalam suatu sistem dan membuat orang mampu memilih alternatif terbaik berdasarkan tujuan mereka.

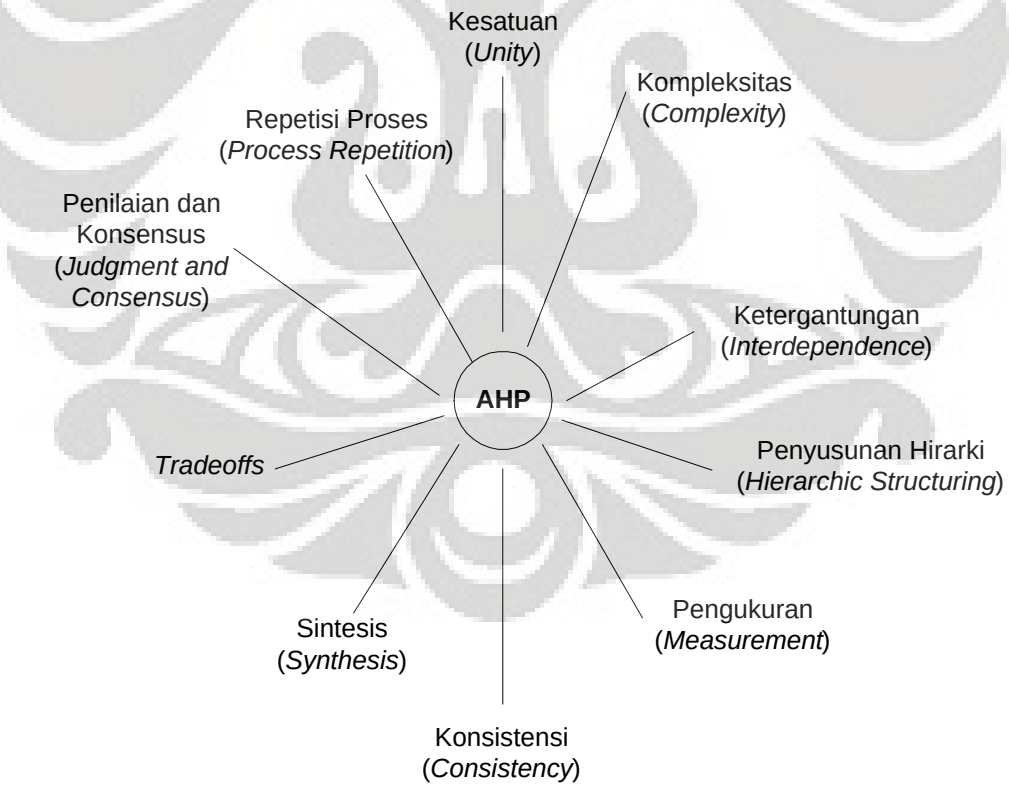
9. penilaian dan konsensus (*judgment and consensus*)

   AHP tidak berdasarkan konsensus tetapi mensintesis representasi hasil dari penilaian yang bermacam-macam.

10. repetisi proses (*process repetition*)

    AHP membuat orang mampu untuk menyempurnakan definisi mereka terhadap masalah dan meningkatkan penilaian dan pemahaman mereka melalui repetisi.

Gambar 2.10 berikut memperlihatkan ilustrasi keunggulan AHP.



Gambar 2.10. Keunggulan *Analytical Hierarchy Process* (AHP)

(Sumber: Saaty, 1999, hal.25)

2.5.2. Metode Alokasi Langsung

Dalam Metode Alokasi Langsung (*Direct Weighting*), pembuat keputusan memberikan angka untuk menggambarkan bobot atribut. Pembuat keputusan diminta untuk membagi 100 nilai untuk di antara atribut-atribut atau memberikan angka yang menunjukkan bobot (Pöyhönen dan Hämäläinen, 1997, hal.2).

2.5.3. SMART

Langkah-langkah menentukan bobot dalam *Simple Multiatribute Rating Technique* (SMART) adalah sebagai berikut (Pöyhönen dan Hämäläinen, 1997, hal.2).

a. Mengurutkan tingkat kepentingan perubahan atribut dari level atribut terendah sampai level terbaik.
b. Membuat estimasi rasio tingkat kepentingan relatif untuk setiap atribut relatif terhadap atribut yang mempunyai tingkat kepentingan yang terendah. Biasanya dilakukan dengan memberikan 10 poin untuk atribut yang mempunyai tingkat kepentingan terkecil. Tingkat kepentingan relatif atribut lainnya dievaluasi dengan memberikan poin 10 ke atas.

2.5.4. SWING

Dengan metode pembobotan SWING, pembuat keputusan diminta untuk mempertimbangkan suatu situasi dimana terdapat alternatif hipotesis yang mempunyai semua atribut pada level terendah. Pertama-tama pembuat keputusan diminta untuk memindahkan satu atribut yang pertama kali ingin diubah ke level terbaiknya dan memberikan 100 poin untuk atribut terpenting ini. Lalu pembuat keputusan diminta untuk memilih suatu perubahan atribut dari level terendah ke level terbaik yang dianggapnya peningkatan kedua yang paling diinginkan dan memberikan poin kurang dari 100 poin untuk perubahan atribut tersebut. Prosedur ini dilakukan untuk semua atribut lainnya (Pöyhönen dan Hämäläinen, 1997, hal.2-3).

2.5.5. Skala *Likert*

Menurut Trochim (2000) Skala *Likert* atau skala *Summative* adalah salah satu metode *unidimensional scaling* (A. Iwan Setiawan, 2004, hal. 19). Langkah-langkah menggunakan skala Likert adalah sebagai berikut:

a. Mendefinisikan fokus permasalahan

   Karena skala adalah metode *unidimensional scaling*, diasumsikan sesuatu yang ingin diukur adalah berdimensi satu.

b. Memilih *items* yang ingin di-*rating*

   Selanjutnya dipilih suatu set *items* yang berpotensi untuk di-*rating*. *Items* tersebut harus dapat di-*rating* pada skala respons Setuju-Tidak setuju 1-5 atau 1-7. Kadang-kadang pemilihan *items* ini dapat dilakukan sendiri berdasarkan pemahaman terhadap subjek yang dibahas tetapi akan lebih membantu jika dilakukan brainstorming untuk memilih *items* tersebut.

c. Me-*rating items* tersebut

   Langkah selanjutnya adalah me-*rating items* yang dilakukan oleh juri. Biasanya digunakan skala *rating* 1-5 seperti pada tabel 2.5.

Tabel 2.5. Skala Likert Untuk Pemilihan *Items* Untuk *Rating* Final

Skala	Keterangan
1	Sangat tidak sesuai dengan konsep
2	Tidak sesuai dengan konsep
3	Netral
4	Sesuai dengan konsep
5	Sangat setuju dengan konsep

(Sumber: William M.K. Trochim, 2000)

d. Memilih *items* yang akan di-*rating* final

   Langkah selanjutnya adalah menghitung korelasi antara semua pasang *items* berdasarkan *rating* juri. Dalam melakukan penilaian *items* yang akan di-*rating* final, beberapa analisa yang dapat dilakukan adalah tidak memilih *items* yang mempunyai korelasi rendah dengan total skor semua *items*. Selanjutnya, untuk semua *items* hitung *rating* rata-rata untuk *quarter* atas dan *quarter* bawah juri.

Lakukan *t-test* perbedaan antara nilai rata-rata untuk item dari *quarter* atas dan *quarter* bawah juri. Semakin tinggi *t-values* berarti ada perbedaan besar antara juri atas dan bawah sehingga *items* dengan *t-values* tinggi adalah pembeda yang baik sehingga harus dipertahankan untuk *rating* final.

e. Mengimplementasikan skala Likert

Setiap responden akan diminta me-*rating* setiap *item* pada skala respons seperti pada tabel 2.5. Terdapat variasi skala respons yang mungkin seperti 1-7, 1-9, 0-4. Semua skala ganjil ini mempunyai nilai tengah yang diberi label Netral. Akan tetapi mungkin digunakan skala respon genap dimana tidak ada nilai tengah yang memaksa responden menentukan apakah mereka lebih setuju atau tidak setuju. Skor final untuk setiap responden adalah jumlah *rating* responden tersebut untuk semua items.

2.5.6. Skala Thurstone

Berdasarkan penelitian W.M.K. Trochim (2000), Thurstone adalah salah satu ahli teori skala yang pertama dan paling produktif. Thurstone menciptakan 3 metode yang berbeda untuk membuat suatu skala *unidimensional* yaitu metode *equal-appering intervals*, *successive intervals*, metode perbandingan berpasangan. Ketiga metode berbeda dalam bagaimana nilai skala dibuat tetapi hasil skala di-*rating* dengan cara yang sama oleh responden. Langkah-langkah menggunakan skala Thurstone metode *equal-appering intervals* adalah sebagai berikut.

a. Mendefinisikan fokus permasalahan.

Karena skala Likert adalah metode *unidimensional scaling*, diasumsikan sesuatu yang ingin diukur adalah berdimensi satu.

b. Memilih *items* yang ingin di-*rating*.

Items yang akan di-*rating* dibuat dalam bentuk pernyataan atau pertanyaan sekitar 80-100 pernyataan yang akan dipilih untuk *rating* final.

c. Me-*rating items* tersebut.

Langkah selanjutnya adalah meminta juri untuk me-*rating* setiap pernyataan dengan skala 1-11 dalam hal seberapa besar setiap pernyataan menunjukkan *favorableness* terhadap fokus permasalahan.

d. Menghitung nilai skor skala untuk setiap *item*.

   Langkah selanjutnya adalah untuk menganalisa data *rating*. Untuk setiap pernyataan perlu menghitung median dan jangkauan interkuartil. Untuk menfasilitasi pemilihan *items* untuk *rating* final, urutkan tabel median dan jangkauan interkuartil dari median yang paling kecil ke yang paling besar. Untuk median yang sama diurutkan dari jangkauan interkuartil yang paling besar ke yang paling kecil.

e. Memilih *items* untuk *rating* final.

   Pernyataan yang dipilih untuk *rating* final adalah pernyataan dalam interval yang sama sepanjang *range* median. Sebagai contoh dipilih satu pernyataan setiap 1 nilai median. Untuk setiap median yang sama dipilih pernyataan dengan jangkauan interkuartil yang terkecil karena pernyataan tersebut mempunyai variabilitas terkecil antar juri. Analisis statistik bukan satu-satunya faktor untuk menentukan *items* untuk *rating* final. Pernyataan yang dipilih adalah pernyataan yang paling masuk akal. Apabila pernyataan yang terbaik secara statistik membingungkan pilihlah pernyataan terbaik selanjutnya yang paling masuk akal.

f. Mengimplementasikan skala Thurstone.

   Setiap responden akan diminta me-*rating* pernyataan yang telah dipilih untuk *rating* final dengan skala Setuju atau Tidak Setuju. Untuk mendapatkan skor skala total untuk setiap responden, skor skala dari semua *items* yang disetujui orang tersebut dirata-rata.

2.5.7. Skala Guttman

Skala Guttman disebut juga skala kumulatif. Tujuan skala Guttman adalah membuat urutan kontinu untuk suatu konsep yang ingin diukur. Dengan skala Guttman, suatu set *items* atau pernyataan dimana responden yang menyetujui suatu pertanyaan spesifik dalam daftar akan juga akan menyetujui semua pertanyaan sebelumnya. Kita dapat memprediksi respons *item* secara tepat hanya dengan mnegetahui skor total untuk responden tersebut. Sebagai contoh bayangkan skala kumulatif 10 *item*. Jika responden mempunyai skor 4 berarti responden tersebut setuju dengan 4 pernyataan pertama. Jika responden

mempunyai skor 8 berarti responden tersebut setuju dengan 8 pernyataan pertama. Tujuannya adalah untuk memperoleh suatu set *items* yang sesuai dengan pola tersebut. Dalam praktek sulit untuk memperoleh pola kumulatif secara sempurna sehingga kita menggunakan *scalogram analysis* untuk memeriksa seberapa dekat suatu set *items* berhubungan dengan ide kumulatif tersebut (Trochim, 2000).

Langkah-langkah menggunakan skala Guttman adalah sebagai berikut (Trochim, 2000):

a. Mendefinisikan fokus permasalahan.
   Pada tahap ini kita mendefinisikan fokus *rating*.
b. Menentukan *items* yang ingin di-*rating*.
   Langkah selanjutnya adalah menentukan *items* yang menggambarkan konsep yang akan di-*rating* sekitar 80-100 pernyataan.
c. Me-*rating items* tersebut.
   Langkah selanjutnya adalah meminta juri untuk me-*rating* pernyataan atau *items* tersebut apakah *favorable* dengan konsep yang ingin di-*rating*. Juri akan menjawab Ya jika suatu pernyataan *favorable* dan menjawab Tidak jika tidak *favorable*.
d. Membuat skala kumulatif
   Kunci skala Guttman adalah analisis. Kita membuat suatu matriks atau tabel yang menunjukkan respons dari semua responden pada semua *items*. Lalu matriks tersebut diurutkan dari responden yang setuju dengan paling banyak pernyataan ke responden yang setuju dengan paling sedikit pernyataan. Untuk responden dengan jumlah setuju sama pernyataan diurutkan dari kiri ke kanan dari yang paling banyak disetujui ke pernyataan yang paling sedikit disetujui.
e. Mengimplementasikan skala Guttman.
   Mengimplementasikan skala Guttman sangat sederhana yaitu dengan meminta responden untuk memilih pernyataan yang disetujui dimana pernyataan yang sudah diurutkan secara kumulatif diacak terlebih dahulu. Setiap *item* mempunyai nilai skala yang didapat dari *scalogram analysis*. Untuk menghitung skor skala responden nilai skala dari setiap *item* yang disetujui dijumlahkan.

2.5.8. Perbandingan Antar Metode *Rating*

Berdasarkan penelitian yang dilakukan Gunawan Halim (2001), kriteria-kriteria berikut digunakan untuk membandingkan metode-metode *rating*.

a. tipe aplikasi dan objek yang dimungkinkan (*applicability*)
   kriteria ini menunjukkan cakupan area aplikasi dan objek yang dimungkinkan sistem *rating*.
b. validitas dan reliabilitas (*validity and reliability*)
   kriteria ini menunjukkan apakah sistem *rating* tersebut layak dari sudut pandang riset ilmiah dan statistik.
c. daya kuantifikasi (*quantifying ability*)
   kriteria ini menunjukkan apakah sistem *rating* tersebut mempunyai kemampuan mengkuantifikasikan data sekalipun data tersebut kualitatif.
d. objektivitas pembobotan (*weighting objectivity*)
   kriteria ini menunjukkan apakah metode pembobotan dalam sistem *rating* mendukung pendetilan pada sub alternatif.
e. struktur *rating* (*rating structure*)
   kriteria ini menunjukkan apakah sistem *rating* mendukung pendetilan pada sub-sub alternatif.
f. fleksibilitas terhadap penambahan (*flexibility in adding alternative*)
   kriteria ini menunjukkan apakah sistem *rating* tersebut penambahan variabel alternatif dengan efisiensi yang stabil.
g. kemudahan dibuat (*ease to construct*)
   kriteria ini menunjukkan apakah sistem *rating* tersebut mudah dibuat atau dikonstruksi dalam kondisi apapun.
h. kemudahan digunakan (*ease to use*)
   kriteria ini menunjukkan apakah sistem *rating* tersebut mudah digunakan dalam kondisi apapun.

Berikut ini adalah tabel perbandingan metode-metode *rating* dibandingkan dengan metode alokasi langsung (*direct*) yang merupakan metode *rating* paling sederhana sebagai standar dimana (-) menunjukkan lebih jelek dari standar, (0) menunjukkan sama baik dengan standar, dan (+) menunjukkan lebih baik dari standar.

Tabel 2.6. Perbandingan Metode *Rating*

No	Kriteria	AHP	Alokasi Langsung	SMART	SWING	*Likert*	*Thurstone*	*Guttman*
1	Tipe aplikasi dan objek	+	0	0	0	0	-	-
2	Validitas dan Reabilitas	+	0	+	+	0	0	0
3	Daya kuantifikasi	0	0	0	0	0	-	-
4	Objektivitas pembobotan	+	0	+	+	+	0	0
5	Struktur *rating*	0	0	0	0	0	-	0
6	Fleksibilitas terhadap penambahan	+	0	0	0	+	+	+
7	Kemudahan dibuat	0	0	-	-	0	-	-
8	Kemudahan digunakan	0	0	0	0	-	-	-

(Sumber: Halim, 2001, hal.42)

2.6. Matriks Prioritas

Matriks prioritas merupakan matriks yang dirancang dalam rangka pemilihan alternatif. Matriks Prioritas yang dirancang didesain sedemikian rupa sehingga perusahaan hanya memerlukan 1 matriks saja yang sederhana untuk memilih alternatif. Contoh matriks prioritas dalam pemilihan indikator untuk *Balanced Scorecard* dapat dilihat pada gambar 2.11.

Matriks Prioritas seperti terlihat pada gambar diatas terdiri atas beberapa bagian dimana bagian yang satu mempunyai fungsi tertentu yang membedakannya dari bagian yang lain. Dengan menggunakan sistem penamaan yang sederhana, berikut ini dijelaskan secara rinci bagian-bagian dari Matriks Prioritas:

a. Sayap atas, berisi kriteria-kriteria tujuan strategis yang baik

   Perusahaan dapat menentukan kriteria tujuan strategis ini sesuai dengan kriteria yang ditentukan sendiri masing-masing perusahaan.

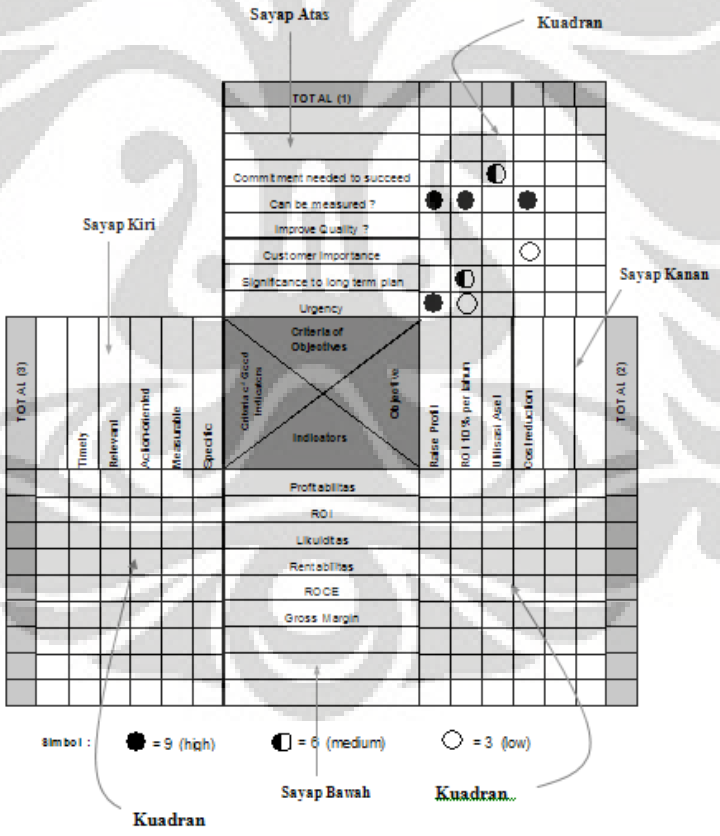
b. Sayap kanan, diisi dengan keseluruhan alternatif tujuan strategis yang ingin dicapai perusahaan

   Keseluruhan alternatif ini merupakan hasil diskusi (*knowledge transfer*) dari seluruh pihak manajemen eksekutif atau semua pihak yang sungguh-sungguh memiliki pemahaman akan visi dan misi serta strategi perusahaan.

c. Sayap kiri, merupakan daftar kriteria-kriteria indikator yang baik (*Good Performance Indicators*)

   Rancangan ini memungkinkan penetapan kriteria oleh perancang matriks atau oleh perusahaan tersebut jika perusahaan ingin menentukan kriteria indikator yang baik.

d. Sayap bawah, diisi dengan alternatif indikator (*Possible Indicator)* yang ingin diukur perusahaan.



Gambar 2.11. Matriks Prioritas

(Sumber: Christine Chandra, 2001)

Perusahaan dapat mendaftar keseluruhan indikator-indikator yang mungkin dilakukan pengukuran untuk masing-masing perspektif *Balanced Scorecard* yang cocok dengan jenis usaha.

Ruang atau persilangan antara 2 sayap disebut kuadran yang digunakan untuk memberikan nilai hubungan (*relationship*) keduanya. Terdapat 3 kuadran dalam matriks prioritas, yang terdiri dari:

a. Kuadran I, digunakan untuk menghubungkan alternatif-alternatif tujuan strategis yang telah didefinisikan dengan kriteria-kriteria tujuan strategis yang baik sesuai dengan yang telah ditetapkan oleh perusahaan.
b. Kuadran II, digunakan untuk menghubungkan alternatif-alternatif indikator dengan tujuan strategis terpilih.
c. Kuadran III, digunakan untuk menghubungkan antara alternatif-alternatif indikator dengan kriteria-kriteria indikator yang baik sesuai dengan yang telah ditetapkan oleh perusahaan.

Nilai hubungan tersebut dinyatakan dalam bentuk simbol, yaitu:

● = 9, artinya tingkat hubungannya sangat erat (sangat dominan)
◐ = 6, artinya tingkat hubungannya agak erat (dominan)
○ = 3, artinya tingkat hubungannya agak jauh (kurang dominan)
□ = 0, bila keduanya mempunyai hubungan yang sangat jauh atau yang bahkan tidak mempunyai hubungan sedikitpun.

Kolom Total dibagi menjadi 3 yaitu :

a. Total (1) digunakan untuk menjumlahkan nilai yang diperoleh masing-masing alternatif tujuan strategis
b. Total (2) digunakan untuk menjumlahkan nilai yang diperoleh masing-masing indikator bila dihubungkan dengan tujuan strategis terpilih
c. Total (3) digunakan untuk menjumlahkan nilai yang diperoleh masing-masing indikator atas dasar pertimbangan '*Good Performance Indicators*'

Keterangan penggunaan matriks prioritas:

a. Satu matriks hanya dapat digunakan untuk memilih indikator dari satu perspektif saja. Oleh karena itu diperlukan 4 buah matriks prioritas untuk dapat mennetukan indikator keempat perspektif *Balanced Scorecard*
b. Kolom sayap atas dan sayap kiri merupakan kolom standar yang berisi kriteria-kriteria untuk "*good strategic objective*" dan "*good indicator*". Yang dimaksud kolom standar adalah bahwa kedua kolom ini akan selalu sama untuk keempat perspektif.

Secara rinci prosedur penggunaan matriks prioritas dapat dijelaskan sebagai berikut:

a. Langkah Pertama

   Menetapkan kriteria tujuan strategis dan kriteria indikator yang baik atau perusahaan dapat menggunakan kriteria yang telah ditawarkan oleh penulis
b. Langkah Kedua

   Menuliskan semua tujuan strategis yang ingin dicapai oleh perusahaan pada kolom sayap kanan dan alternatif-alternatif indikator yang mungkin untuk satu perspektif pada kolom sayap bawah
c. Langkah Ketiga

   Merupakan tahap pemilihan tujuan strategis. Tahap ini dilakukan dengan menentukan tujuan strategis prioritas berdasarkan kriteria yang telah ditetapkan (kuadran I). Dengan menentukan hubungan antara setiap alternatif tujuan strategis terhadap setiap kriteria maka total nilai yang diperoleh untuk masing-masing alternatif dituliskan pada kolom TOTAL (I). Tujuan strategis terpilih adalah yang mendapat total nilai yang paling tinggi
d. Langkah Keempat

   Setelah prioritas tujuan strategis terpilih maka tahap selanjutnya adalah pemilihan indikator. Seperti yang telah dijelaskan sebelumnya, bahwa ada 2 pertimbangan untuk pemilihan indikator ini yaitu kesesuaian dengan Tujuan Strategis terpilih (kuadran II) yang diperoleh dengan menentukan nilai hubungan antara tujuan strategis yang telah terpilih dengan seluruh alternatif indikator. Pemilihan indikator ini adalah berdasarkan tingkat kepentingan atau

kedekatan masing-masing indikator dengan tujuan strategis terpilih. Indikator yang paling sesuai dengan tujuan strategis adalah indikator yang memperoleh total nilai paling tinggi pada kolom TOTAL 2. Selain itu, terdapat pula pertimbangan kesesuaian dengan kriteria *Good Performance Indicators.* Hal ini diperoleh dengan menentukan nilai hubungan untuk seluruh alternatif indikator dengan kriteria '*Good Performance Indicators'*. Indikator yang paling baik berdasarkan kriteria tersebut adalah indikator yang memperoleh total nilai paling tinggi pada kolom TOTAL 3.

Kelebihan-kelebihan yang dapat ditawarkan dari metode pemilihan indikator dengan menggunakan matriks prioritas adalah:

a. Matriks ini sangat sederhana (tidak membutuhkan perhitungan yang rumit atau teknologi), sehingga dapat dengan mudah dipelajari dan digunakan oleh siapapun.
b. Tahapan-tahapan penggunaan matriks mengikuti suatu prosedur yang sangat teratur dan terarah sehingga tidak akan menyulitkan atau membingungkan dalam penggunaanya.
c. Matriks Prioritas mempunyai tingkat fleksibilitas yang tinggi sehingga dapat digunakan oleh semua perusahaan dengan jenis usaha baik produksi maupun pemberi jasa.
d. Matriks Prioritas telah mencakup berbagai aspek yang dibutuhkan dalam pemilihan indikator, dimana indikator terpilih adalah selaras dengan tujuan strategis yang ingin dicapai, serta selaras dengan visi dan misi perusahaan, indikator terpilih memenuhi kriteria indikator yang baik, bagi anak perusahaan, maka indikator yang terpilih juga selaras dengan visi dan misi induk perusahaan, matriks prioritas dapat menentukan indikator masing-masing untuk keempat perspektif yang dibutuhkan dalam penerapan *Balanced Scorecard* (Finansial, Pelanggan, Proses Bisnis Internal, Pertumbuhan dan Pembelajaran)

Namun kekurangan yang dimiliki oleh Matriks Prioritas ini, antara lain:

a. Dalam pengaplikasian Matriks Prioritas, dibutuhkan pemikiran, komitmen, kesepakatan dan kerja sama dari seluruh pihak manajemen sehingga dalam menentukan tujuan strategis dan segala penilaian hubungannya untuk mendapatkan indikator prioritas menjadi tidak subyektif.
b. Penentuan hubungan serta perhitungan total nilai dalam Matriks Prioritas sangat lama dan cukup membosankan.
c. Satu matriks hanya dapat digunakan untuk memilih indikator dari satu perspektif saja sehingga dibutuhkan 4 buah matriks prioritas.
d. Matriks Prioritas hanya dapat digunakan untuk memilih tujuan strategis dan indikator produk (*lag indicators*), tidak mencakup jika dibutuhkan dalam hal pemilihan indikator proses (*lead indicators*) dan hal kuantifikasi indikator terpilih.

3. PENGUMPULAN DATA

3.1. Profil Departemen Teknologi Informasi Bank D

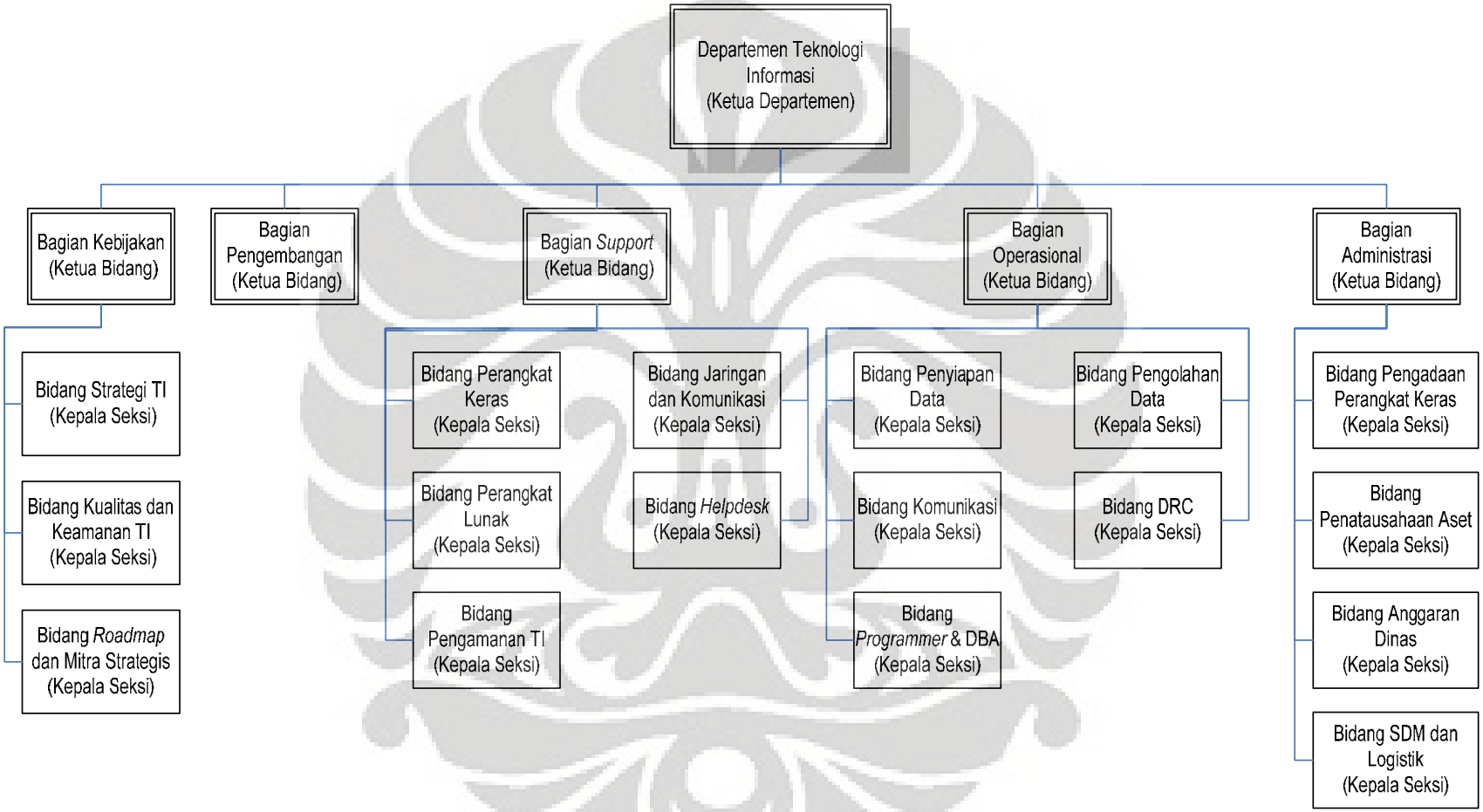
Departemen Teknologi Informasi Bank D adalah salah satu satuan kerja yang merupakan unit pendukung teknologi informasi pada Bank D. Visi Departemen Teknologi Informasi Bank D adalah menjadi satuan kerja pengelola teknologi informasi Bank D yang sangat kompeten dan dapat diandalkan.

Dalam pencapaian visi tersebut, Bank D memiliki misi yaitu menyediakan dukungan dan sumber daya teknologi informasi yang berkualitas tinggi secara efektif dan efisien untuk meningkatkan kinerja pelaksanaan tugas Bank D.

Sasaran strategis dari Departemen Teknologi Informasi Bank D antara lain:

a. Kepuasan pengguna terhadap sistem TI dan kualitas pelayanannya
b. Memelihara kondisi keuangan Bank D yang sehat dan akuntabel
c. Meningkatkan pengelolaan sistem TI
d. Menjaga ketersediaan sistem TI
e. Menjaga keamanan sistem TI
f. Meningkatkan pengetahuan TI pegawai Bank D, baik yang bersifat teknis maupun ketentuan
g. Meningkatkan efektivitas pelaksanaan *"good governance"*
h. Memperkuat institusi Bank D melalui penciptaan sinergi antara SDM, informasi, pengetahuan, dan rangan organisasi dengan strategi Bank D
i. Mengarahkan dan memantau efektivitas perubahan strategis Bank D.

Dalam mencapai sasaran strategis, Departemen Teknologi Informasi Bank D memiliki sumber daya manusia yang dapat diandalkan sesuai peran masing-masing pada organisasi. Gambar 3.1 di bawah ini merupakan struktur organisasi dari Departemen Teknologi Informasi Bank D.



Gambar 3.1. Struktur Organisasi Departemen Teknologi Informasi Bank D

(Sumber: Departemen Teknologi Informasi Bank D)

Tabel 3.1 berikut ini daftar tugas pokok dan output dari Departemen Teknologi Informasi Bank D yang merupakan dasar penilaian kinerja (Indikator Kinerja Utama) seluruh satuan kerja yang ada di Bank D.

Tabel 3.1. Daftar Tugas Pokok dan Output Departemen Teknologi Informasi

No.	Tugas Pokok	Output
1	Merumuskan arah dan strategis TI yang terpadu	Strategi dan Kebijakan TI
2	Melakukan pengamanan sistem TI	Keamanan sistem aplikasi dan infrastruktur TI
3	Melakukan perencanaan, pengembangan, pengawasan, dan pengujian kualitas sistem TI	Sistem aplikasi dan infrastruktur TI berkualitas yang siap untuk diimplementasikan
4	Melakukan pemeliharaan dan layanan bantuan teknis operasional TI	Kesinambungan operasional sistem aplikasi dan infrastruktur TI
5	Melakukan pemrosesan data	Ketersediaan data TI
6	Menyusun ketentuan yang berkaitan dengan tugas Departemen Teknologi Informasi	Ketentuan yang terkait TI
7	Melaksanakan pengadaan barang dan atau jasa TI	Ketersediaan barang dan/ atau jasa TI
8	Melakukan manajemen intern Departemen Teknologi Informasi	Manajemen direktorat yang efektif dan efisien

(Sumber: Departemen Teknologi Informasi Bank D)

Output yang dihasilkan Departemen Teknologi Informasi Bank D tentunya berpengaruh terhadap *stakeholders*. Tabel 3.2 berikut merupakan daftar output,

stakeholders dari masing-masing output, dan ekspektasi *stakeholders* terhadap masing-masing output.

Tabel 3.2. Output, *Stakeholders* Eksternal, dan Ekspektasi *Stakeholders* Departemen Teknologi Informasi

No.	Output	*Stakeholders*	Ekspektasi *Stakeholder*
1	Strategi dan Kebijakan TI	Dewan Gubernur, seluruh pegawai, seluruh Satker	Tersedianya strategi dan kebijakan TI yang terpadu, jelas, dan disosialisasikan
2	Keamanan sistem aplikasi dan infrastruktur TI	Dewan Gubernur, seluruh pegawai, seluruh Satker, masyarakat/ lembaga pengguna TI Bank D	Pengamanan sistem aplikasi dan infrastruktur TI yang handal
3	Sistem aplikasi dan infrastruktur TI berkualitas yang siap untuk diimplementasikan	Dewan Gubernur, seluruh pegawai, seluruh Satker, masyarakat/ lembaga pengguna TI Bank D	Sistem aplikasi dan infrastruktur TI yang berkualitas
4	Kesinambungan operasional sistem aplikasi dan infrastruktur TI	Dewan Gubernur, seluruh pegawai, seluruh Satker, masyarakat/ lembaga pengguna TI Bank D	Kesinambungan tersedianya sisitem dan infrastruktur yang berkinerja tinggi
5	Ketersediaan data TI	Dewan Gubernur, seluruh pegawai, seluruh Satker, masyarakat/ lembaga pengguna TI Bank D	Ketersediaan data yang lengkap, akurat, kini, dan utuh

Tabel 3.2. Output, *Stakeholders* Eksternal, dan kspektasi *Stakeholders* Departemen Teknologi Informasi (Sambungan)

No.	*Output*	*Stakeholders*	Ekspektasi *Stakeholder*
6	Ketentuan yang terkait TI	Dewan Gubernur, seluruh pegawai, seluruh Satker, masyarakat/ lembaga pengguna TI Bank D	Ketersediaan dan sosialisasi ketentuan TI yang mendukung operasional TI
7	Ketersediaan barang dan atau jasa TI	Dewan Gubernur, seluruh pegawai, seluruh Satker	Tersedianya barang dan atau jasa TI secara tepat waktu dan tepat guna
8	Manajemen direktorat yang efektif dan efisien	Dewan Gubernur, DKI, DSDM, Auditor	Perencanaan anggaran sesuai rencana, pemanfaatan SDM secara optimal

(Sumber: Departemen Teknologi Informasi Bank D)

3.2. Pemilihan Responden Penelitian

Pengembangan metode integrasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* Generasi ke-4 diilhami dari konsep *Balanced Scorecard for SOX* (Tomonori Tomura, 2006) dimana terdapat penambahan kontrol internal yang berasal dari manajemen risiko terhadap pembuatan *Balanced Scorecard* sebuah organisasi. Penelitian ini, merupakan aplikasi dari pengembangan metode penerapan *Balanced Scorecard* generasi ke-4 dengan mengambil studi kasus Bank D.

Oleh karena Bank D merupakan Bank pertama di Indonesia yang telah menerapkan *Balanced Scorecard* generasi ke-3 serta ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005, penelitian menggunakan penilaian dari ahli (*expertise judgement*) dalam dua bidang tersebut. Para ahli (*experts*) tersebut antara lain pegawai Departemen Teknologi Informasi Bank D yang berpengalaman dalam IKU Departemen Teknologi Informasi Bank D, pegawai yang berpengalaman

dalam ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005, serta perwakilan dari Tim Proyek Perluasan Lingkup Sertifikasi ISO/ IEC 27001:2005.

Responden dari penelitian ini sebagai berikut:

a. pegawai Departemen Teknologi Informasi Bank D yang berpengalaman dalam IKU Departemen Teknologi Informasi Bank D dan implementasi ISO/ IEC 17799:2005 dan ISO/ 27001:2005 yaitu Manajer IKU Departemen Teknologi Informasi Bank D dan *security officer* ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005
b. perwakilan dari Tim Proyek Perluasan Lingkup Sertifikasi ISO/ IEC 27001:2005 yaitu *project leader* Perluasan Lingkup Sertifikasi ISO/ 27001:2005.

Komposisi responden penelitian dapat dilihat pada tabel 3.3 berikut. Data responden secara lengkap dapat dilihat pada lampiran 1.

Tabel 3.3. Komposisi Responden Penelitian

Responden	**Jumlah**	**Persentase**
Pegawai Departemen Teknologi Informasi Bank D	3	75%
Project leader Perluasan Lingkup Sertifikasi ISO/ IEC 27001:2005	1	25%
Total	**4**	**100%**

Latar belakang pendidikan dan pengalaman responden di bidang Indikator Kinerja Utama Departemen Teknologi Informasi Bank D dan ISO/ IEC 17799:2005 dan ISO/ 27001:2005 adalah sebagai berikut:

a. Latar Belakang Pendidikan

   Dilihat dari latar belakang pendidikan, keempat responden dapat dianggap ahli karena memiliki latar belakang pendidikan di bidang teknologi informasi, telekomunikasi, dan *Balanced Scorecard* (lihat tabel 3.4).

Tabel 3.4. Latar Belakang Pendidikan Responden

Latar Belakang Pendidikan	Jumlah	Persentase
S1 dan S2 Telekomunikasi, Teknik Komputer, dan Teknologi Informasi	3	75%
S1 Teknik Industri	1	25%
Total	**4**	**100%**

b. Pengalaman (dalam tahun)

Pengalaman responden yang merupakan pegawai di Departemen Teknologi Informasi Bank D berkisar antara 11-14 tahun. Ditambah dengan pengalaman sebagai Manajer IKU Departemen Teknologi Informasi Bank D selama ±3 tahun. Di sisi lain, pengalaman seluruh responden dalam proyek implementasi ISO/ IEC 17799:2005 dan ISO/ 27001:2005 berkisar antara 1 sampai 3 tahun (selama implementasi ISO/ IEC 17799:2005 dan ISO/ 2700:2005 berjalan di Departemen Teknologi Informasi Bank D). Berdasarkan pengalaman tersebut, keempat responden dapat dianggap ahli.

Ditinjau dari pendidikan dan pengalaman para responden maka empat responden dapat dianggap cukup untuk menghasilkan penilaian yang validitas dan reabilitasnya baik serta objektif. Tidak ada jumlah responden minimum yang terbukti secara empiris mampu memberikan penilaian yang objektif untuk penentuan kriteria menurut konsep AHP. Menurut Saaty (komunikasi personal, 12 Oktober 2003) jika tidak ada orang yang dapat dianggap ahli dan menguasai subjek penelitian, maka jumlah responden yang banyak sekalipun tidak akan cukup. Akan tetapi jika 1 orang ahli saja dianggap menguasai semua bidang dalam hirarki, maka dapat dianggap cukup untuk menghasilkan penilaian yang baik. Semakin banyak jumlah responden, semakin tinggi objektivitasnya tetapi penilaian setiap ahli semakin tidak tercermin dalam penilaian kelompok sehingga reliabilitasnya berkurang (A. Iwan Setiawan, 2004, hal. 64).

3.3. Pengumpulan Data Tahap I

3.3.1. Langkah Pengumpulan Data

Pengumpulan data untuk menentukan kriteria pemilihan risiko dan indikator dilakukan dengan kuesioner. Langkah yang digunakan dalam pengumpulan data mengenai penentuan kriteria risiko dan Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) adalah sebagai berikut:

a. menyusun kuesioner ½ terbuka, sehingga dapat diperoleh masukan dari para ahli dalam menentukan risiko yang dijadikan penambahan untuk kontrol internal. Dalam penyusunan kuesioner tersebut dilakukan 2 tahap yaitu mengumpulkan kriteria risiko yang ditawarkan kepada responden dari ISO/ IEC 27001:2005 (ISO/IEC/TMB SAG-Security Secretariat, 2005, hal. 4) dan diskusi dengan pembimbing dan *project leader* Perluasan Lingkup Sertifikasi ISO/ IEC 27001:2005 serta mengumpulkan kriteria pemilihan indikator yang akan ditawarkan kepada responden dari kriteria pemilihan indikator yang telah diterapkan pada Bank D (PAMK, 2006). Menurut Saaty (komunikasi personal, 23 Juni 2003), kriteria pemilihan risiko dan indikator yang ditawarkan merupakan stimulus bagi responden dalam menentukan kriteria yang menurut mereka sesuai untuk memilih risiko dan indikator yang dihubungkan dengan IKU Departemen Teknologi Informasi Bank D (A. Iwan Setiawan, 2004, hal. 61).
b. menentukan skala penilaian yaitu skala *Likert* karena objektivitasnya dalam penilaian dan fleksibilitasnya untuk penambahan kriteria baru.
c. menyebarkan kuesioner untuk mendapatkan data penilaian kriteria pemilihan risiko dan indikator oleh responden berdasarkan skala *Likert.* Dalam menentukan kriteria tersebut, responden diminta memberikan nilai pada masing-masing kriteria yang ditawarkan. Selain itu, responden dapat menambahkan kriteria baru dan memberi skor pada kriteria tersebut dengan cara yang sama dengan penilaian pada kriteria yang ditawarkan.
d. Jika terdapat kriteria tambahan dari seorang responden, maka kriteria tersebut akan dikonfirmasikan responden yang bersangkutan. Bila kriteria tambahan tersebut tidak beririsan dengan kriteria yang telah ada, kriteria tambahan tersebut juga dinilai oleh responden lainnya berdasar skala *Likert.*

3.3.2. Pengumpulan Data Kriteria Pemilihan Risiko dan Indikator

Kuesioner yang telah disusun untuk menentukan kriteria pemilihan risiko dan indikator selanjutnya disebut Form Kuesioner Tahap I (Penentuan Kriteria Pemilihan Risiko dan Indikator Untuk Pengembangan *Balanced Scorecard* Generasi Ke-4 Direktorat Teknologi Informasi Bank D) yang dapat dilihat pada lampiran 2.

Pada kuesioner tersebut, alternatif kriteria yang dikumpulkan dari berbagai referensi tercantum pada tabel 3.5 dan tabel 3.6 sebagai berikut.

Tabel 3.5. Alternatif Kriteria Pemilihan Risiko

No.	Alternatif Kriteria Pemilihan Risiko
1	Risiko terjadi pada aset kritikal
2	Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol
3	Memiliki hubungan logis dengan Indikator Kinerja Utama Departemen Teknologi Informasi Bank D

Berikut ini adalah penjelasan setiap alternatif kriteria untuk pemilihan risiko:

a. Risiko terjadi pada aset kritikal

   Risiko yang dipilih terjadi pada aset kritikal perusahaan sesuai dengan kesepakatan pegawai Departemen Teknologi Informasi Bank D. Hal ini sesuai dengan langkah identifikasi risiko pada ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005.

b. Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol

   Hasil *risk assessment* berdasarkan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 menyatakan bahwa risiko belum memiliki tingkat pengendalian yang kuat dan/ atau dirasa perlu untuk mengkontrol risiko tersebut dengan pengendalian tambahan.

c. Memiliki hubungan logis dengan Indikator Kinerja Utama Departemen Teknologi Informasi BI

   Risiko harus memiliki hubungan logis dalam kaitannya dengan pelaksanaan tugas pokok Departemen Teknologi Informasi Bank D yang tertuang dalam penilaian kinerja yaitu IKU Departemen Teknologi Informasi Bank D.

Tabel 3.6. Alternatif Kriteria Pemilihan Indikator (IRU dan IPU)

No.	Alternatif Kriteria Pemilihan Indikator (IRU dan IPU)
1	Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol
2	Dapat diukur secara tepat
3	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini
4	Bersifat spesifik dan eksplisit
5	Merefleksikan data yang dapat diukur secara periodik
6	Biaya untuk mengidentifikasi dan memonitor ukuran indikator tidak melebihi nilai yang akan diketahui dari pengukuran tersebut
7	Dapat dicapai oleh organisasi
8	Realistis terhadap kondisi organisasi
9	Memiliki batas waktu
10	Mudah dimengerti

(Sumber: PAMK Bank D)

Berikut ini adalah penjelasan setiap alternatif kriteria untuk pemilihan indikator (IRU dan IPU):

a. Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol

   Indikator dapat mendukung sasaran strategis dari Departemen Teknologi Informasi Bank D yang telah ada dan pelaksanaannya dapat dikontrol.

b. Dapat diukur secara tepat

   Indikator dapat diekspresikan dengan penilaian kuantitatif sehingga dapat menggambarkan upaya pengukuran dampak dan pengendalian terhadap risiko secara tepat.

c. Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini

   Indikator perlu menggambarkan proses perbaikan antara satu periode pengukuran dengan periode pengukuran selanjutnya, untuk melihat ada atau tidaknya perbaikan pencapaian target pengukuran oleh perusahaan (*continuous improvement*).

d. Bersifat spesifik dan eksplisit

   Indikator bersifat spesifik dan tidak mengandung ambiguitas dalam pemahamannya di kemudian hari sehingga jelas yang diukur.

e. Merefleksikan data yang dapat diukur secara periodik

   Data yang diukur dalam indikator tersebut dapat tersedia dan dapat diukur secara periodik untuk memperlihatkan usaha mitigasi risiko secara berkala.

f. Biaya untuk mengidentifikasi dan memonitor ukuran IKU tidak melebihi nilai yang akan diketahui dari pengukuran tersebut

   Indikator bersifat *cost efficient* sehingga nilai manfaatnya melebihi biaya yang harus dikeluarkan untuk mengidentifikasi dan memonitor IKU sehingga tidak terdapat IKU yang tidak banyak memiliki nilai tambah.

g. Realistis terhadap kondisi organisasi

   Indikator dapat disesuaikan dengan kondisi organisasi agar menggambarkan pengukuran secara efektif dan target dari pengukuran dapat dicapai.

h. Memiliki batas waktu

   Indikator memiliki batas waktu pengukuran dan evaluasi.

i. Mudah dimengerti

   Indikator dapat dimengerti oleh Manajer IKU pada khususnya dan setiap pegawai Departemen Teknologi Informasi Bank D pada umumnya.

Karena skala *Likert* pada Form Kuesioner Tahap I digunakan untuk memilih kriteria yang sesuai untuk memilih risiko dan indikator (IRU dan IPU), maka

definisi yang digunakan adalah sangat setuju (5) sampai skala sangat tidak setuju (1). Tabel 3.7 memuat nilai dan definisi skala *Likert* yang digunakan.

Tabel 3.7. Skala *Likert* yang digunakan pada Form Kuesioner Tahap 1

Skala *Likert*	**Definisi**
5	Sangat setuju kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
4	Setuju kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
3	Ragu-ragu/ netral apakah setuju atau tidak kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
2	Tidak setuju kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
1	Sangat tidak setuju kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih

Form Kuesioner Tahap I diberikan secara langsung kepada empat responden yang telah ditentukan di atas. Dari keempat Form Kuesioner Tahap I yang diserahkan, seluruhnya diisi dan dikembalikan oleh responden. Hasil pengumpulan data penentuan kriteria pemilihan risiko dan indikator dari tiap responden dapat dilihat pada Tabel 3.8 dan tabel 3.9.

Tabel 3.8. Data Kriteria Pemilihan Risiko

No	**Alternatif Kriteria Pemilihan Risiko**	**Ahli 1**	**Ahli 2**	**Ahli 3**	**Ahli 4**
1	Risiko terjadi pada aset kritikal	5	5	5	4
2	Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol	4	4	5	4
3	Memiliki hubungan logis dengan Indikator Kinerja Utama Departemen Teknologi Informasi Bank D	3	4	4	2

Tabel 3.9. Data Kriteria Pemilihan Indikator

No	Alternatif Kriteria	Ahli 1	Ahli 2	Ahli 3	Ahli 4
1	Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	5	5	5	2
2	Dapat diukur secara tepat	5	4	5	4
3	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	4	4	5	4
4	Bersifat spesifik dan eksplisit	4	4	5	2
5	Merefleksikan data yang dapat diukur secara periodik	5	4	5	4
6	Biaya untuk mengidentifikasi dan memonitor ukuran indikator tidak melebihi nilai yang akan diketahui dari pengukuran tersebut	4	3	4	3
7	Realistis terhadap kondisi organisasi	5	4	5	4
8	Memiliki batas waktu	5	3	5	3
9	Mudah dimengerti	5	4	5	4

Pada proses pengumpulan data, tidak terdapat tambahan kriteria pemilihan risiko dan indikator (IRU dan IPU) dari responden. Oleh karena itu, langkah no.4 yaitu mengkonfirmasi kembali kriteria tambahan dan penilaian dari responden lainnya tidak perlu dilakukan.

3.4. Pengumpulan Data Tahap II

3.4.1. Langkah Pengumpulan Data

Pengumpulan data untuk membobotkan kriteria pemilihan indikator dan menentukan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D dilakukan dengan memberikan kuesioner tahap II kepada responden yang sama pada tahap I.

3.4.1.1. Pembobotan Kriteria

Kriteria pemilihan risiko tidak perlu diberi bobot karena kriteria tersebut merupakan kriteria masuknya sebuah risiko untuk dibuat indikatornya (IRU dan IPU). Pengumpulan data pembobotan kriteria pemilihan indikator (IRU dan IPU) dilakukan dengan langkah sebagai berikut:

a. mendaftar kriteria pemilihan indikator yang telah didapat dari hasil pengolahan data Form Kuesioner Tahap I
b. menentukan skala penilaian yaitu skala pada perbandingan berpasangan (*pairwise comparison*) dari metode *Analytical Hierarchy Process* karena cakupan area aplikasi dan objek yang dimungkinkan luas, layak digunakan dari sudut pandang riset ilmiah dan statistik, kemampuan objektivitasnya dalam penilaian, dan fleksibilitasnya untuk penambahan kriteria baru
c. menyebarkan kuesioner untuk mendapatkan data bobot kriteria pemilihan indikator oleh responden dengan memberikan nilai dari perbandingan tiap kriteria.

3.4.1.2. Penentuan IRU Dan IPU Serta Hubungannya Dengan IKU Departemen Teknologi Informasi Bank D

Langkah pengumpulan data untuk menentukan indikator (IRU dan IPU) dari tiap risiko serta hubungannya dengan IKU Departemen Teknologi Informasi Bank D sebagai berikut:

a. mengidentifikasi indikator (IRU dan IPU) yang telah ada dari implementasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005dan yang potensial (baru) dari risiko hasil *risk assessment* ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 yang telah diseleksi sesuai dengan kriteria pemilihan risiko dari tahap sebelumnya
b. menentukan skala penilaian yang berasal dari metode matriks prioritas karena kemudahan dan fleksibilitasnya
c. menyebarkan kuesioner untuk mendapatkan data evaluasi kemampuan indikator untuk mengukur risiko dan kemampuannya untuk memenuhi kriteria pemilihan indikator serta data nilai hubungan antara IRU dan IPU terpilih dengan IKU Departemen Teknologi Informasi Bank D

d. Jika ada tambahan IRU dan/ atau IPU dari salah satu responden, maka dilakukan evaluasi terhadap IRU dan/ atau IPU tersebut oleh responden lainnya. Evaluasi tersebut meliputi kemampuan IRU dan/ atau IPU untuk mengukur risiko yang terpilih, kemampuan IRU dan/ atau IPU untuk menjadi indikator berdasarkan persyaratan pada kriteria pemilihan indikator, dan hubungan antara IRU dan/ atau IPU dengan IKU Departemen Teknologi Informasi Bank D
e. IRU dan IPU yang memiliki nilai tertinggi pertama dan kedua berdasarkan tahap sebelumnya, dikonfirmasikan kepada responden. Hal ini memungkinkan adanya perbaikan terhadap IRU dan IPU agar lebih sesuai dengan risiko dan memenuhi kriteria pemilihan indikator.

3.4.2. Pengumpulan Data

Pada pengumpulan data, kuesioner yang disusun untuk selanjutnya disebut Form Kuesioner Tahap II (Pembobotan Kriteria Dan Penentuan Indikator Risiko Utama Dan Indikator Pengendalian Utama Untuk Pengembangan *Balanced Scorecard* Generasi ke-4 Departemen Teknologi Informasi Bank D) yang dapat dilihat pada lampiran 3. Dari keempat kuesioner yang diberikan, seluruh kuesioner diisi dan dikembalikan.

3.4.2.1. Pembobotan Kriteria

Daftar kriteria pemilihan indikator yang dibobotkan merupakan hasil dari pengolahan Form Kuesioner Tahap I. Selanjutnya, dari Form Kuesioner Tahap II yang diberikan, responden memberikan penilaian dari 1 – 9 berdasarkan tingkat kepentingan relatif dari kriteria yang dipasangkan karena pembobotan kriteria yang paling sesuai berdasarkan tingkat kepentingan (*importance*) dibandingkan dengan tingkat kemungkinan (*likelihood*) atau tingkat preferensi (*preference*) (A. Iwan Setiawan, 2004, hal. 90). Hal ini dikarenakan dari pembobotan tersebut ingin diketahui tingkat kepentingan dari tiap kriteria. Tabel 3.10 memuat definisi dari tiap nilai yang digunakan untuk melakukan perbandingan berpasangan.

Tabel 3.10. Skala Penilaian Perbandingan Berpasangan

Nilai	Definisi
1	Kedua elemen sama penting
3	Elemen yang satu sedikit lebih penting daripada elemen lainnya
5	Elemen yang satu lebih penting dibanding elemen lainnya
7	Satu elemen jelas lebih mutlak dibandingkan elemen lainnya
9	Satu elemen mutlak penting daripada elemen lainnya
2, 4, 6, 8	Nilai antara dua nilai pertimbangan yang berdekatan

(Sumber: A. Iwan Setiawan, 2004)

Data penilaian perbandingan berpasangan kriteria pemilihan indikator dari tiap responden dapat dilihat pada tabel 3.11 berikut.

Tabel 3.11 Data Perbandingan Berpasangan Kriteria Pemilihan Indikator

Kriteria	2				3			
	A1	A2	A3	A4	A1	A2	A3	A4
1	1.00	5.00	2.00	4.00	0.33	5.00	1.00	0.20
2					1.00	5.00	0.50	0.25
3								
4								
5								
6								
7								
8								
9								
Kriteria	**4**				**5**			
	A1	**A2**	**A3**	**A4**	**A1**	**A2**	**A3**	**A4**
1	4.00	5.00	5.00	6.00	3.00	5.00	2.00	0.50
2	0.17	5.00	3.00	5.00	0.17	5.00	3.00	0.17
3	5.00	3.00	6.00	4.00	1.00	3.00	4.00	1.00
4					0.25	0.33	0.33	0.20
5								
6								
7								
8								
9								

Tabel 3.11 Data Perbandingan Berpasangan Kriteria Pemilihan Indikator (Sambungan)

Kriteria	6				7			
	A1	A2	A3	A4	A1	A2	A3	A4
1	0.25	0.20	3.00	6.00	2.00	7.00	3.00	5.00
2	1.00	0.20	2.00	2.00	0.17	5.00	5.00	3.00
3	2.00	0.20	6.00	3.00	0.50	3.00	7.00	5.00
4	0.20	0.20	1.00	2.00	0.17	3.00	3.00	1.00
5	0.25	0.20	2.00	4.00	1.00	3.00	4.00	5.00
6					5.00	7.00	2.00	3.00
7								
8								

Kriteria	8			
	A1	A2	A3	A4
1	5.00	5.00	7.00	0.33
2	0.20	3.00	5.00	1.00
3	0.20	0.33	7.00	5.00
4	0.20	0.20	5.00	2.00
5	0.20	0.20	5.00	4.00
6	5.00	7.00	2.00	3.00
7	0.50	0.33	0.33	0.25
8				

3.4.2.2. Penentuan IRU Dan IPU Serta Hubungannya Dengan IKU Departemen Teknologi Informasi Bank D

Risiko hasil *risk assessment* ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 pada Bagian Kebijakan, Bagian Administrasi, dan Bagian Operasional Departemen Teknologi Informasi Bank D yang terpilih dapat dilihat pada tabel 3.12. Perincian risiko tersebut terdapat pada lampiran 4.

Tabel 3.12. Risiko Terpilih

No	Daftar Risiko Terpilih
1	Kurangnya pengamanan pada penggunaan *notebook* di luar ruang kerja/ tempat umum menyebabkan *notebook* rusak sehingga pekerjaan terganggu
2	Kurangnya kontrol penggunaan *notebook* di luar ruang kerja menyebabkan komponen atau keseluruhan *notebook* hilang sehingga pekerjaan terganggu

Tabel 3.12. Risiko Terpilih (Sambungan)

No	Daftar Risiko Terpilih
3	Tidak ada *user management* yang baik menyebabkan adanya akses oleh pihak tidak berwenang yang menyebabkan aplikasi Web Departemen Teknologi Informasi hilang atau rusak sehingga aktivitas tim *Roadmap* dan Mitra Strategis terganggu
4	Modifikasi aset yang tidak terotorisasi menyebabkan kinerja aplikasi Web Departemen Teknologi Informasi turun sehingga aktivitas tim *Roadmap* dan Mitra Strategis terganggu
5	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan internal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi
6	Rusaknya media penyimpanan informasi menyebabkan dokumen *softcopy* kajian/ laporan eksternal yang mengandung informasi rahasia menjadi tidak ada/ hilang/ tidak akurat saat dibutuhkan
7	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan eksternal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi
8	Kurangnya pengamanan fisik ruang kerja Direktur dan Deputi Direktur Departemen Teknologi Informasi yang menyebabkan akses pihak tak berwenang yang berdampak pada proses authorisasi
9	Kurangnya kontrol hak akses memungkinkan ruang kerja Direktur dan Deputi Direktur diakses pihak tak berwenang yang berdampak pada proses authorisasi
10	Belum berjalannya manajemen aset (inventarisasi, kepemilikan, otorisasi penggunaan, pemelihaaraan, penggunaan) dapat menyebabkan ruang pelatihan dan asetnya tidak berfungsi maksimal

Tabel 3.12. Risiko Terpilih (Sambungan)

No	Daftar Risiko Terpilih
11	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham tentang *setting policy & schedule back-up*
12	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham melakukan instalasi *agent* di aplikasi
13	Lemahnya mekanisme monitoring sistem menyebabkan kinerja PC Teleks menurun karena kebutuhan performa tidak terpenuhi
14	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan *Mainframe* mengalami *hardware failure*
15	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pembebanan Anggaran Pelaksanaan SOSA tidak akurat karena kesalahan pembuatan
16	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pengadaan Kunci Telegram Bank D tidak akurat karena kesalahan pembuatan
17	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen PKAT tidak akurat karena kesalahan pembuatan
18	Kurangnya *training* menyebabkan Informasi *softcopy* dokumentasi teknis tiap seksi dan kelompok tidak akurat karena kesalahan dalam pembuatan
19	Kurangnya *training* untuk mendukung pelaksanaan pekerjaan menyebabkan informasi *softcopy* SOP Seksi dan Bagian tidak akurat karena kesalahan pembuatan
20	Kurangnya kontrol pengamanan informasi menyebabkan *Tape / Catridge* hasil *back-up data* hilang ketika dalam perjalanan ke DRC
21	Kurangnya *training* menyebabkan informasi *softcopy* data dari satuan kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan

Tabel 3.12. Risiko Terpilih (Sambungan)

No	Daftar Risiko Terpilih
22	Tidak ada Aplikasi AntiVirus, Antimalware, Firewall,dll menyebabkan Informasi softcopy data satuan kerja yang telah diolah tidak tersedia karena virus
23	Ketidaktersediaan / Kurangnya / Gangguan AC menyebabkan pelaksanaan operasional di DRC, *strong room*, ruang *Mainframe*, dan ruang Server terganggu
24	Tidak adanya/ lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan *thermal control* tidak dapat digunakan karena komponen rusak
25	Pemeliharaan aset yang tidak baik menyebabkan *thermal control* tidak dapat digunakan karena kerusakan komponen
26	Pemeliharaan aset yang tidak baik menyebabkan *thermal control* tidak tersedia sehingga suhu ruangan DRC, *strong room*, ruang *Mainframe*, dan ruang server tidak dapat diketahui

(Sumber: *Risk Profile* Departemen Teknologi Informasi Bank D)

Alternatif IRU dan IPU yang dikumpulkan dari implementasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005, *guide for developing performance metric for information security* (Elizabeth Chew, et al., 2006) serta IRU dan IPU potensial sesuai dengan risiko terpilih dapat dilihat pada tabel 3.13 dan 3.14 di bawah ini. Perincian IRU dapat dilihat pada lampiran lampiran 5 dan perincian Indikator Pengendalian Utama (IPU) terdapat pada lampiran 6.

Tabel 3.13. Alternatif Indikator Risiko Utama

No.	Indikator Risiko Utama (IRU)
1	Pengukuran Tingkat Kerusakan *Notebook* Formula: (a / b) x 100% a= jumlah *notebook* yang rusak pada satuan kerja b= jumlah seluruh *notebook* yang menjadi tanggung jawab satuan kerja

Tabel 3.13. Alternatif Indikator Risiko Utama (Sambungan)

No.	Indikator Risiko Utama (IRU)
2	Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya Formula: (a / b) x 100% a= jumlah *notebook* atau komponennya yang hilang pada satuan kerja b= jumlah seluruh *notebook* yang menjadi tanggung jawab satuan kerja
3	Pengukuran Jumlah Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D Formula: (a + b) a= jumlah kejadian hilangnya aplikasi Web Departemen Teknologi Informasi Bank D b= jumlah kejadian rusaknya aplikasi Web Departemen Teknologi Informasi Bank D
4	Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja aplikasi Web Departemen Teknologi Informasi Bank D b= jumlah jam operasi aplikasi Web Departemen Teknologi Informasi Bank D
5	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi Formula: ((a + b) / c) x 100% a= jumlah kajian/ laporan internal pengembangan aplikasi yang diterapkan b= jumlah kajian/ laporan eksternal pengembangan aplikasi yang diterapkan c= jumlah kajian/ laporan internal dan eksternal pengembangan aplikasi
6	Pengukuran Gangguan Aktivitas tim *Roadmap* dan Mitra Strategis Formula: Jumlah aktivitas yang tidak sesuai dengan perencanaan terkait dengan kerusakan atau kehilangan aplikasi Web Departemen Teknologi Informasi Bank D

Tabel 3.13. Alternatif Indikator Risiko Utama (Sambungan)

No.	Indikator Risiko Utama (IRU)
7	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal Formula: ((a + b) / c) x 100% a= jumlah informasi kajian/ laporan internal dan eksternal yang hilang b= jumlah informasi kajian/ laporan internal dan eksternal yang tidak akurat c= jumlah informasi kajian/ laporan internal dan eksternal
8	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur Formula: ((a + b) / c) x 100%. a= jumlah aset pada ruang direktur dan deputi direktur yang hilang b= jumlah aset pada ruang direktur dan deputi direktur yang hilang c= jumlah seluruh aset pada ruag direktur dan deputi direktur
9	Pengukuran Tingkat Pemanfaatan Ruang Pelatihan Formula: (a / b) x 100% a= jumlah permintan penggunaan ruang pelatihan yang tidak terpenuhi b= jumlah permintaan penggunaan ruang pelatihan
10	Pengukuran Tingkat Kinerja *Robotic* Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja *robotic* b= jumlah jam operasi *robotic*
11	Pengukuran Tingkat Kinerja PC Teleks Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja PC Teleks b= jumlah jam operasi PC Teleks
12	Pengukuran Tingkat Kinerja *Mainframe* Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja *Mainframe* b= jumlah jam operasi *Mainframe*

Tabel 3.13. Alternatif Indikator Risiko Utama (Sambungan)

No.	Indikator Risiko Utama (IRU)
13	Pengukuran Tingkat Keakuratan Dokumen Pembebanan Anggaran Pelaksanaan SOSA Formula: (a / b) x 100% a= jumlah Dokumen Pembebanan Anggaran Pelaksanaan SOSA yang tidak akurat b= jumlah Dokumen Pembebanan Anggaran Pelaksanaan SOSA
14	Pengukuran Tingkat Keakuratan Dokumen Pengadaan Kunci Telegram Bank D Formula: (a / b) x 100% a= jumlah Dokumen Pengadaan Kunci Telegram Bank D yang tidak akurat b= jumlah Dokumen Pengadaan Kunci Telegram Bank D
15	Pengukuran Tingkat Keakuratan Dokumen PKAT Formula: (a / b) x 100% a= jumlah Dokumen PKAT yang tidak akurat b= jumlah Dokumen PKAT
16	Pengukuran Tingkat Keakuratan Dokumen Teknis Tiap Seksi dan Kelompok Formula: (a / b) x 100% a= jumlah SOP Seksi dan Bagian yang tidak akurat b= jumlah SOP Seksi dan Bagian
17	Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian Formula: (a / b) x 100% a= jumlah SOP Seksi dan Bagian yang tidak akurat b= jumlah SOP Seksi dan Bagian

Tabel 3.13. Alternatif Indikator Risiko Utama (Sambungan)

No.	Indikator Risiko Utama (IRU)
18	Pengukuran Tingkat Kehilangan *Tape / Catridge* hasil *back-up data* yang akan dikirim ke DRC Formula: (a / b) x 100% a= jumlah pengiriman *tape/ cartridge* hasil *back-up* data ke DRC dimana terjadi *tape/ cartridge* hasil *back-up* data yang hilang b= jumlah pengiriman *tape/ cartridge* hasil *back-up* data
19	Pengukuran Tingkat Keakuratan Data Satuan kerja Yang Telah Diolah Formula: (a / b) x 100% a= jumlah Data Satuan kerja Yang Telah Diolah yang tidak akurat b= jumlah Data Satuan kerja Yang Telah Diolah
20	Pengukuran Tingkat Serangan Virus Terhadap Data Satuan kerja Yang Telah Diolah Formula: jumlah terjadinya serangan virus yang ditemukan pada Data Satuan kerja Yang Telah Diolah
21	Pengukuran Tingkat Gangguan AC Formula: (a / b) x 100% a= jumlah jam terjadinya kerusakan pada AC b= jumlah jam operasi AC
22	Pengukuran Tingkat Kerusakan *Thermal Control* Formula: (a / b) x 100% a= jumlah jam terjadinya kerusakan pada AC b= jumlah jam operasi AC
23	Pengukuran Tingkat Ketersediaan *Thermal Control* Formula: (a / b) x 100% a= jumlah jam terjadinya kerusakan pada AC b= jumlah jam operasi AC

Tabel 3.14. Alternatif Indikator Pengendalian Utama

No	Indikator Pengendalian Utama (IPU)
1	Pengukuran Tingkat Pengamanan Personil Satuan kerja Formula: (a / b) * 100% a= jumlah Surat Menjaga Kerahasiaan Informasi yang telah ditandatangani oleh personil Unit b= Menghitung jumlah personil Unit Kerja
2	Pengukuran Tingkat Pengamanan Personil Pihak Ketiga Formula: (a / b) * 100% a= jumlah Surat Menjaga Kerahasiaan Informasi yang telah ditandatangani oleh personil Unit b= Menghitung jumlah personil Unit Kerja
3	Pengukuran Kelengkapan dan Kebenaran Data pada Database Aset Formula: ((100 - (a + b)) x 100% a= jumlah aset yang menjadi tanggung jawab satuan kerja tetapi tidak ada pada *database* b= jumlah asset pada *database* yang tidak digunakan lagi oleh satuan kerja
4	Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak Formula: (((a – b) / a) / c) x 100% a= jumlah perangkat lunak yang di-*install* pada PC/ *notebook* personil satuan kerja b= jumlah perangkat lunak pada PC/ *notebook* yang tidak terdaftar pada daftar perangkat lunak yang diizinkan untuk di-*install* di lingkup Departemen Teknologi Informasi c= jumlah PC/ *notebook* yang digunakan satuan kerja
5	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Satuan kerja Formula: ((100 – a) / 100) x 100% a = jumlah personil yang tidak diberikan hak akses ke ruangan Satuan kerja berdasarkan Ketentuan Kontrol Hak Akses Fisik tetapi sistem mengizinkan personil tersebut mengakses ruangan satuan kerja terkait

Tabel 3.14. Alternatif Indikator Pengendalian Utama (Sambungan)

No	Indikator Pengendalian Utama (IPU)
6	Pengukuran Pelaksanaan *Back-Up* Informasi Personil Satuan kerja Formula: (a / b) x 100% a= jumlah personil yang telah melakukan *back-up* sesuai jadwal b= jumlah personil satuan kerja yang aktif
7	Pengukuran Kesesuaian *Password* Personil Satuan kerja Formula: (a / b) x 100% a= jumlah personil yang telah menggunakan *password* sesuai ketentuan b= jumlah personil satuan kerja yang memiliki *user ID* dan *password* untuk *login* ke *active directory*
8	Pengukuran Pelaksanaan *Update Antivirus* Formula: (a / b) * 100% a= jumlah PC dan *notebook* satuan kerja atau Server, *Mainframe, Tandem* yang memiliki *updated Antivirus* b= jumlah PC dan *notebook* atau server, *Mainframe, Tandem* yang digunakan oleh satuan kerja
9	Pengukuran Pelaksanaan *Update Patch* Formula: (a / b) * 100% a= jumlah PC/ *notebook* personil satuan kerja atau server, *Mainframe, Tandem* yang telah memiliki *updated patch* b= jumlah PC/ *notebook* personil satuan kerja atau server, *Mainframe, Tandem* yang digunakan satuan kerja
10	Pengukuran Keefektifan Penanganan Insiden/ *Event* Formula: ((c – (a + b)) / c) x 100% a= jumlah insiden/ event yang dilaporkan yang belum ditangani sesuai dengan target waktu b= jumlah insiden/ event yang dilaporkan yang terjadi penundaan penanganan tindak lanjut c= jumlah insiden/ event yang dilaporkan

Tabel 3.14. Alternatif Indikator Pengendalian Utama (Sambungan)

No	Indikator Pengendalian Utama (IPU)
11	Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu Formula: ((c – (a + b)) / c) x 100% a= jumlah tamu yang tidak menandatangani atau mengisi waktu meninggalkan ruangan dalam buku/ aplikasi tamu pada hari yang sama b= jumlah personil satuan kerja yang tidak memparaf buku tamu setelah mengantarkan tamu keluar (hanya berlaku untuk buku tamu. Jika satuan kerja menggunakan aplikasi tamu, nilai b = 0) c= jumlah tamu yang berkunjung ke ruang satuan kerja
12	Pengukuran Identifikasi Pelabelan Aset *Removable Media* Formula: ((100 – a) / 100) x 100% a= jumlah asset *removable media* yang ditemukan menjadi tanggung jawab personil satuan kerja tetapi belum diberi label
13	Pengukuran kelengkapan data serah terima aset Formula: (a / b) x 100% a= form serah terima asset yang disimpan oleh *security officer* b= jumlah asset TI yang dialihkan /dipinjamkan/ dikembalikan berdasarkan permohonan peminjaman/ pengalihan oleh pihak lain. personil satuan kerja yang mutasi
14	Pengukuran Kesesuaian *Password Mainframe* dan *Tandem* Formula: (a / b) x 100% a= jumlah *password* super yang telah sesuai dengan kebijakan pengamanan b= jumlah *password* super yang digunakan untuk *login* ke dalam sistem *Mainframe* dan *Tandem*

Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D yang dihubungkan dengan IRU dan IPU di atas merupakan perspektif proses bisnis internal yang terdapat pada tabel 3.15. Perincian dari IKU Departemen Teknologi Informasi Bank D terdapat pada lampiran 7.

Tabel 3.15. Indikator Kinerja Utama Departemen Teknologi Informasi Bank D

No.	Indikator Kinerja Utama
3	**Meningkatkan pengembangan dan pengelolaan Sistem TI**
3.1	Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D Formula: (a / b) x 100% a= jumlah program kerja (PK) yang selesai sesuai tahapan (kesepakatan) b= jumlah PK yang disetujui Forum Manajemen TI-PK yang belum dimulai pada tahapan
3.2	Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan Formula: (a / b) x 100% a= jumlah PK yang selesai sesuai tahapan b= jumlah PK yang disetujui Forum Manajemen TI-PK yang belum dimulai pada tahapan
3.3	Peningkatan pemanfaatan infrastruktur TI yang telah diimplementasikan di Bank D Formula: Jumlah inovasi infrastruktur TI yang diimplementasikan Bank D
4	**Menjaga ketersediaan Sistem TI**
4.1	Persentase *downtime* sistem aplikasi kritikal dan *e-mail* Formula: (a / b) x 100% a= jumlah jam aplikasi kritikal tidak bisa dioperasikan b= jumlah jam operasi aplikasi kritikal
4.2	Persentase *downtime* jaringan Bank D-NET Formula: (a / b) x 100% a= jumlah jam jaringan Bank D-NET tidak bisa dioperasikan b= jumlah jam operasi jaringan Bank D-NET

Tabel 3.15. Indikator Kinerja Utama Departemen Teknologi Informasi Bank D (Sambungan)

No.	Indikator Kinerja Utama
4.3	Jumlah keberhasilan simulasi aplikasi kritikal Formula: Jumlah keberhasilan simulasi aplikasi kritikal (3 per semester)
5	**Menjaga keamananan Sistem TI**
5.1	Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang Ditindaklanjuti Formula: (a / b) x 100% a= jumlah rekomendasi yang ditindaklanjuti b= jumlah rekomendasi konsultan yang akan diselesaikan sesuai komitmen dalam periode pengukuran IKU
5.2	Maksimum waktu penanggulangan serangan virus yang menyebar secara Missal Formula: Jumlah hari penanggulangan terhadap serangan virus yang menyebar secara massal
5.3	Indeks hasil *assessment* atas kecukupan dan efektivitas ISMS Formula: Indeksasi hasil eksternal *assessment* dilakukan terhadap temuan ISMS berkategori major dan minor *non-conformity* dengan skala: 1. terdapat 1 atau lebih temuan major *non-conformity* 2. tidak terdapat temuan major *non-conformity* dengan lebih dari 15 temuan minor *non-conformity* 3. tidak terdapat temuan major *non-conformity* dengan 11-15 temuan minor *non-conformity* 4. tidak terdapat temuan major *non-conformity* dengan 5-10 temuan minor *non-conformity* 5. tidak terdapat temuan major *non-conformity* dengan maksimal 5 temuan minor *non-conformity* 6. tidak terdapat temuan major *non-conformity* dan minor *non-conformity*

Tabel 3.15. Indikator Kinerja Utama Departemen Teknologi Informasi Bank D (Sambungan)

No.	Indikator Kinerja Utama
6	**Meningkatkan pengetahuan TI pegawai Bank D, baik yang bersifat teknis maupun ketentuan TI**
6.1	Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil *mapping* Formula: Jumlah materi/ topik yang disosialisasikan
6.2	Peningkatan pemahaman peserta setelah sosialisasi Formula: (a / b) x 100% a= persentase jumlah peserta yang mengalami peningkatan pemahaman b= jumlah peserta

(Sumber: Departemen Teknologi Informasi Bank D)

Setelah mendapatkan IRU dan IPU yang tercantum pada tabel 3.13 dan 3.14 serta data IKU Departemen Teknologi Informasi Bank D pada tabel 3.15, dilakukan evaluasi kemampuan IRU dan IPU untuk mengukur risiko terpilih, kemampuan IRU dan IPU untuk menjadi indikator berdasarkan persyaratan pada kriteria pemilihan indikator dari tahap sebelumnya, dan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D menggunakan matriks prioritas.

Matriks prioritas yang digunakan terdiri dari 6 kuadran, yaitu:

1. Kuadran 1 yang berisi evaluasi antara risiko terpilih dengan IRU yang sesuai
2. Kuadran 2 yang berisi evaluasi antara risiko terpilih dengan IPU yang sesuai
3. Kuadran 3 yang berisi evaluasi antara IRU dengan kriteria pemilihan indikator
4. Kuadran 4 yang berisi evaluasi antara IPU dengan kriteria pemilihan indikator
5. Kuadran 5 yang berisi evaluasi hubungan antara IRU dengan IKU Departemen Teknologi Informasi Bank D
6. Kuadran 6 yang berisi evaluasi hubungan antara IPU dengan IKU Departemen Teknologi Informasi Bank D.

Skala yang digunakan pada matriks prioritas terdapat pada tabel 3.16 berikut.

Tabel 3.16. Skala Pada Matriks Prioritas

Lambang	Nilai	Definisi
●	9	Sangat Kuat
○	6	Sedang
▽	3	Rendah
(kosong)	0	Tidak terkait atau tidak memenuhi

(Sumber: Christine Chandra, 2001)

Selain dari IPU yang telah diidentifikasi di atas, terdapat tambahan IPU dari berbagai responden, dan tambahan IPU dari hasil *surveillance* ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005. IPU tambahan tersebut dimuat dalam tabel 3.17 berikut.

Tabel 3.17. Indikator Pengendalian Utama Tambahan

No.	Indikator Pengendalian Utama (IPU) Tambahan
1	Pengukuran *Form* Peminjaman Aset[a] Formula: (a / b) x 100% a= jumlah *form* peminjaman aset yang sesuai dengan pengembalian aset yang dipinjam b= jumlah *form* peminjaman aset
2	Pengukuran Tingkat Pemahaman[b] Formula: (a / b) x 100% a= jumlah personil dengan nilai di atas 75 skala 100 b= jumlah personil yang mengikuti *training*
3	Pengukuran Efektivitas Training[b] Formula: ((a + b) / c) x 100% a= jumlah personil dengan nilai ”baik” b= jumlah personil dengan nilai ”baik sekali” c= jumlah seluruh personil peserta *training*

Tabel 3.17. Indikator Pengendalian Utama Tambahan

No.	Indikator Pengendalian Utama (IPU) Tambahan
4	Pengukuran Analisis *Fault Logging* Akses Fisik[b] Formula: Jumlah *wrong acces* ke ruang satuan kerja sebanyak lebih dari 5 kali
5	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset[a] Formula: (a / b) x 100%. a= jumlah aktivitas pemeliharaan aktual yang terlambat lebih dari 3 hari daripada yang telah direncanakan b= jumlah aktivitas pemeliharaan
6	Audit *Security Log*[b] Formula: (a / b) x 100% a= jumlah aset yang mengalami *log-on failure* b= 3 aset secara *random*
7	Pengukuran *Form* Pengiriman *Tape Back-up*[a] Formula: (a / b) x 100% a= jumlah *tape back-up* yang tidak sesuai dengan form pengiriman b= jumlah *form* pengiriman *tape back-up*
8	Pengukuran Kesesuaian *User Account*[a] Formula: (a / b) x 100% a= jumlah *user account* tak dikenal oleh sistem yang mengakses *software*/ aplikasi b= jumlah *user account* yang diperbolehkan untuk mengakses *software*/ aplikasi
9	Pengukuran Utilisasi Aset[a] Formula: (a / b) x 100% a= jumlah kapasitas aset yang digunakan b= jumlah kapasitas aset yang tersedia

[a] Tambahan IPU dari Ahli

[b] Tambahan IPU dari *surveillance* ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005

Perincian IPU tambahan dapat dilihat lebih jelas pada lampiran 8. IPU tambahan di atas, dikonfirmasikan kembali kepada responden yang memberikan untuk diperjelas maksudnya agar tidak memiliki makna dan/ atau tujuan serupa dengan IPU yang telah diajukan. Selanjutnya, responden lain mengevaluasi IPU tambahan tersebut seperti IPU yang telah diajukan sebelumnya pada Form Kuesioner Tahap II yaitu menilai kemampuannya mengukur risiko terpilih, menilai kemampuan IPU tambahan dalam memenuhi kriteria pemilihan indikator, dan menilai hubungan antara IPU tambahan tersebut dan IKU Departemen Teknologi Informasi Bank D.

Data yang telah dikumpulkan dari keenam kuadran dapat dilihat pada lampiran 9. Hasil pengolahan dan analisis data dari Form Kuesioner Tahap I dan Form Kuesioner Tahap II dijelaskan pada bab selanjutnya.

4. PENGOLAHAN DATA DAN ANALISIS

4.1. Metode Integrasi ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005 Ke Dalam *Balanced Scorecard*

Pada penelitian pengembangan metode integrasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* generasi ke-4, didapatkan metode yang terdapat pada gambar 4.1.

Tiap proses beserta aspek ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 yang digunakan untuk mengembangkan *Balanced Scorecard* generasi ke-4 pada penelitian menggunakan penilaian para ahli yang memanfaatkan baik aspek kualitatif yaitu pendefinisian masalah maupun kuantitatif yaitu ekspresi penilaian (*judgment*) serta tingkat kepentingan (*importance*). Dalam aplikasi ke seluruh perspektif *Balanced Scorecard* dari Departemen Teknologi Informasi Bank D, dapat digunakan responden yang ahli dalam pengelolaan Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D dan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 seperti pada penelitian ini.

Penentuan kriteria pemilihan risiko dengan input dari langkah pertama implementasi ISMS yaitu rencana ISMS dan *deliverable* langkah ke-3 yaitu *risk profile,* sedangkan alternatif kriteria pemilihan indikator berasal dari Perencanaan Anggaran dan Manajemen Kinerja (PAMK) Bank D. Kriteria tersebut disesuaikan dengan kebutuhan Departemen Teknologi Informasi Bank D dengan fleksibilitas terhadap penambahan usulan kriteria. Oleh karena itu, skala *Likert* digunakan dalam penilaian karena tidak hanya objektif dan fleksibel terhadap penambahan kriteria, tetapi juga mudah diimplementasikan oleh Departemen Teknologi Informasi Bank D. Kriteria pemilihan risiko digunakan dalam menyeleksi risiko dari hasil *risk assessment* Bagian Kebijakan, Bagian Operasional, dan Bagian Administrasi; sedangkan kriteria pemilihan indikator digunakan untuk melihat kemampuan Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) sebagai metrik. Dalam

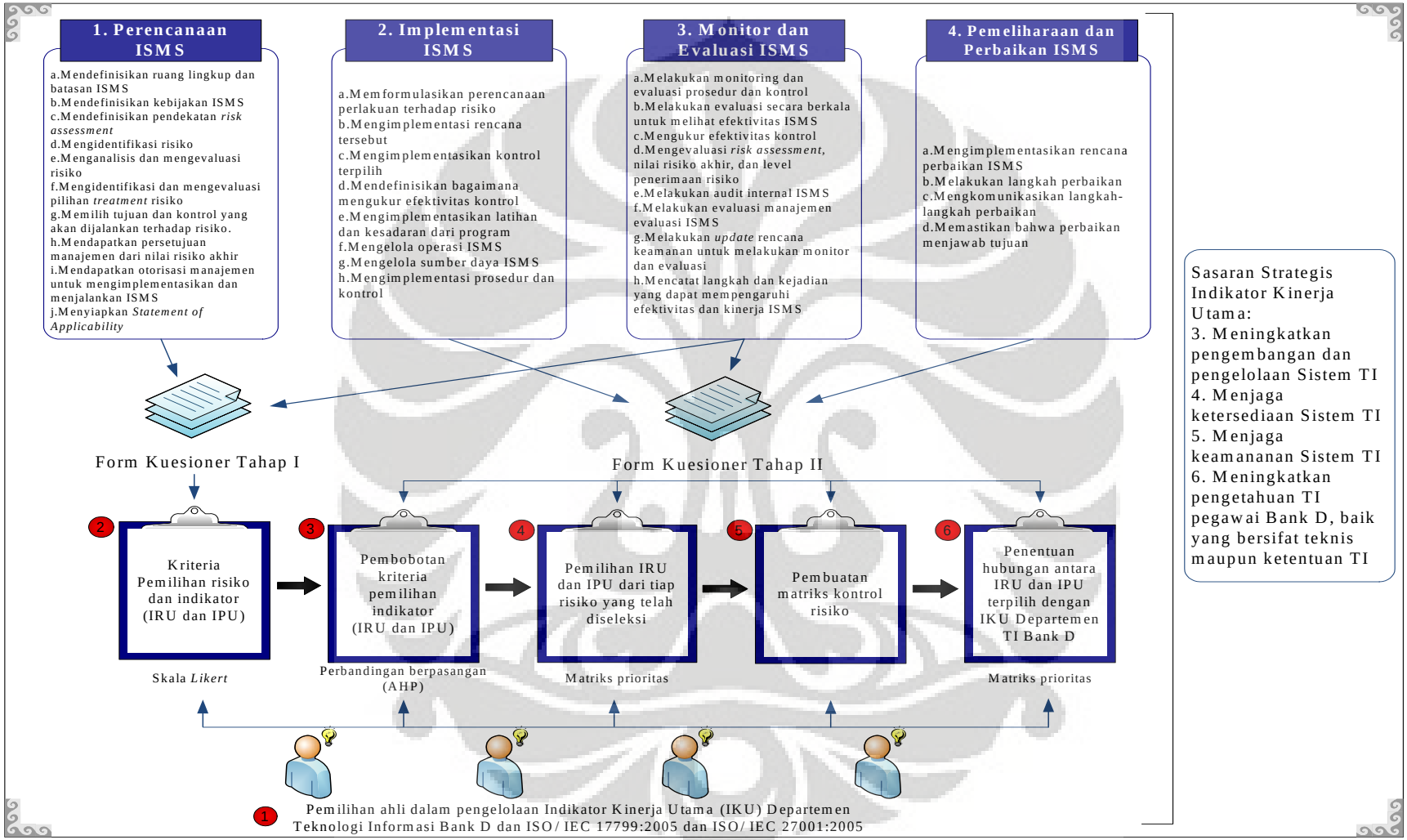
pengembangan selanjutnya, Departemen Teknologi Informasi Bank D dapat menggunakan kriteria pemilihan risiko dan indikator (IRU dan IPU) pada penelitian ini atau mengevaluasi kembali masing-masing kriteria serta menambahkan kriteria lain yang dianggap penting.

Setelah itu, dilakukan penentuan prioritas kriteria pemilihan indikator dengan membobotkan kriteria pemilihan indikator (IRU dan IPU) berdasarkan tingkat kepentingan. Pembobotan dilakukan dengan perbandingan berpasangan pada metode *Analytical Hierarchy Process* (AHP). Dari hasil pembobotan ini, dapat dilihat tingkat kepentingan dari tiap kriteria pemilihan indikator (IRU dan IPU) sehingga memudahkan Departemen Teknologi Informasi Bank D untuk mengambil keputusan mengenai IRU dan IPU yang sesuai untuk diterapkan.

Langkah penentuan IRU dan IPU dari tiap risiko menggunakan matriks prioritas memiliki input dari keempat langkah pada ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005. Dimulai dari penjelasan IRU dan IPU tersebut yang mengikuti format metrik ISMS, IPU yang berasal dari implementasi ISMS, dan tahap perbaikan dari konsep pemeliharaan dan perbaikan ISMS. IRU dan IPU ini akan dijadikan bahan pembuatan matriks kontrol risiko untuk pengembangan *Balanced Scorecard* generasi ke-4.

Matriks kontrol risiko merupakan persyaratan yang dibutuhkan dalam pengembangan *Balanced Scorecard* yang berasal dari hasil *risk assessment* Bagian Kebijakan, Bagian Operasional, dan Bagian Administrasi Departemen Teknologi Informasi Bank D serta hasil penentuan IRU dan IPU.

Penentuan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D dengan bantuan matriks prioritas merupakan dasar untuk mengidentifikasi dan menilai dukungan dari ISO/ IEC 17799:2005 dan ISO/IEC 27001:2005 terhadap IKU dari perspektif proses bisnis internal serta merupakan pengembangan *Balanced Scorecard* Departemen Teknologi Informasi Bank D dari generasi ke-3 ke generasi ke-4.



Gambar 4.1. Metode Integrasi ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005 Ke Dalam *Balanced Scorecard*

4.2. Penentuan Kriteria Pemilihan Risiko Dan Indikator (IRU dan IPU)

4.2.1. Langkah Pengolahan Data-15

Pengolahan data dilaksanakan dengan menggunakan penghitungan total nilai berdasarkan skala *Likert* dari setiap kriteria yang diajukan dan dari setiap kriteria tambahan dari responden. Nilai tersebut dijumlah dengan *software* Microsoft Excel 2007 dengan formula "sum(range)". Nilai maksimum untuk suatu kriteria adalah bila semua responden memilih nilai "5" untuk kriteria tersebut. Karena terdapat 4 responden dalam pengumpulan data, nilai maksimum tersebut adalah 20. Peneliti menetapkan bahwa kriteria yang terpilih menurut responden harus mempunyai skor total minimum 75% dari skor total maksimum yaitu 75% x 20 = 15 berdasarkan penelitian A. Iwan Setiawan (2004, hal 76) berikut ini:

a. Skor 15 merupakan skor yang logis. Contohnya jika 3 dari 4 responden memberikan skor 4 (Setuju) dan hanya 1 responden yang memberikan skor 3 (Ragu-ragu/ Netral) kepada suatu kriteria sehingga skor total adalah 15 maka kriteria itu dapat dianggap sesuai untuk memilih risiko serta Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU)
b. Dengan skor total minimum 15, jumlah kriteria indikator (IRU dan IPU) terpilih menurut responden adalah 8 sehingga dalam batas 7 ± 2 yang disarankan AHP.

4.2.2. Hasil Pengolahan Data Dan Analisis

Tabel 4.1 dan 4.2 memuat hasil penjumlahan dari keempat responden terhadap tiap kriteria risiko dan indikator (IRU dan IPU).

Tabel 4.1. Hasil Penjumlahan Kriteria Pemilihan Risiko

No	Kriteria	Jumlah
1	Risiko terjadi pada aset kritikal	19
2	Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol	17
3	Memiliki hubungan logis dengan Indikator Kinerja Utama Departemen Teknologi Informasi BD	13

Tabel 4.2. Hasil Penjumlahan Kriteria Pemilihan Indikator (IRU dan IPU)

No	Kriteria	Jumlah
1	Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	17
2	Dapat diukur secara tepat	18
3	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	17
4	Bersifat spesifik dan eksplisit	15
5	Merefleksikan data yang dapat diukur secara periodik	18
6	Biaya untuk mengidentifikasi dan memonitor ukuran indikator tidak melebihi nilai yang akan diketahui dari pengukuran tersebut	14
7	Realistis terhadap kondisi organisasi	17
8	Memiliki batas waktu	18
9	Mudah dimengerti	16

Berdasarkan langkah pengolahan data yang telah dijelaskan sebelumnya, maka kriteria pemilihan risiko dan indikator (IRU dan IPU) akan ditentukan dari total nilai dari kelima responden dimana kriteria tersebut harus memiliki total nilai minimum 15.

Kriteria risiko dan indikator (IRU dan IPU) yang terpilih menurut responden tercantum pada tabel 4.3 dan 4.4 sebagai berikut.

Tabel 4.3. Kriteria Risiko Terpilih

No	Kriteria Risiko Terpilih
1	Risiko terjadi pada aset kritikal
2	Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol

Tabel 4.4. Kriteria Indikator (IRU dan IPU) Terpilih

No	Kriteria Indikator (IRU dan IPU) Terpilih
1	Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol
2	Dapat diukur secara tepat
3	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini
4	Bersifat spesifik dan eksplisit
5	Merefleksikan data yang dapat diukur secara periodik
6	Realistis terhadap kondisi organisasi
7	Memiliki batas waktu
8	Mudah dimengerti

Pada kriteria risiko terpilih, risiko harus berasal dari aset kritikal yang sesuai dengan konsep ISO/ IEC 17799:2005 dan ISO/ IEC 27001: 2005 yang mengidentifikasi risiko dari aset kritikal yang diperlukan untuk menjalankan proses bisnis. Pemilihan risiko yang dikontrol merupakan upaya lanjutan dari hasil *risk assessment* karena risiko tersebut belum memiliki kontrol yang cukup.

Alternatif kriteria bahwa risiko memiliki hubungan logis dengan IKU Departemen Teknologi Informasi Bank D tidak terpilih karena risiko dari aset kritikal yang perlu dikontrol dinilai lebih penting. Hal ini dapat dilihat pada selisih jumlah penilaian yang besar antara kriteria "risiko terjadi dari aset kritikal" dengan jumlah nilai 19, "risiko yang bersangkutan perlu dikontrol" dengan jumlah nilai 17, dan "risiko memiliki hubungan logis dengan IKU Departemen Teknologi Informasi Bank D" dengan nilai 13. Pada kedua alternatif lainnya terdiri dari penilaian "sangat setuju" dan "setuju", sedangkan alternatif ke-tiga terdiri dari penilaian "ragu-ragu/ netral", "setuju", dan "tidak setuju".

Untuk kriteria pemilihan indikator (IRU dan IPU), yang terpilih antara lain alternatif bahwa baik IRU maupun IPU berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol, dapat diukur

secara tepat, mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini, bersifat spesifik dan eksplisit, merefleksikan data yang dapat diukur secara periodik, realistis terhadap kondisi organisasi, memiliki batas waktu, dan mudah dimengerti.

Alternatif kriteria "biaya untuk mengidentifikasi dan memonitor ukuran indikator tidak melebihi nilai yang akan diketahui dari pengukuran tersebut" dengan nilai 14 tidak terpilih karena meski dua responden menyatakan "setuju", dua responden lainnya menyatakan "ragu-ragu/ netral" dan "tidak setuju". Dengan demikian, kriteria mengenai biaya dinilai tidak mempengaruhi pemilihan indikator untuk IRU dan IPU dari tiap risiko.

Jumlah nilai tertinggi yaitu 18 didapat oleh kriteria:

a. "dapat diukur secara tepat" mengungkapkan bahwa sangat penting bagi IRU dan IPU untuk dapat diekspresikan dengan penilaian kuantitatif sehingga dapat menggambarkan upaya pengukuran dampak dan pengendalian terhadap risiko secara tepat. Kriteria ini sesuai dengan teori pembuatan indikator yang efektif untuk memonitor risiko operasional (Davies dan Haubenstock, 2002) dan karakteristik dari KRI yang efektif (James Lam et al., 2006)
b. "merefleksikan data yang dapat diukur secara periodik" yang berarti bahwa data yang diukur dalam indikator tersebut dapat tersedia dan dapat diukur secara periodik untuk memperlihatkan usaha mitigasi risiko secara berkala yang sesuai dengan teori pembuatan indikator yang efektif untuk memonitor risiko operasional (Davies dan Haubenstock, 2002)
c. "memiliki batas waktu" dimana indikator memiliki batas waktu pengukuran dan evaluasi yang jelas yang sesuai dengan karakteristik dari KRI yang efektif (James Lam et al., 2006).

Jumlah nilai 17 dimiliki oleh kriteria:

a. "berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol" sehingga indikator dapat mendukung sasaran strategis dari Departemen Teknologi Informasi Bank D yang telah ada dan

pelaksanaannya dapat dikontrol yang sesuai dengan karakteristik dari KRI yang efektif (James Lam et al., 2006)

b. ”mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini” sehingga indikator dapat menggambarkan proses perbaikan antara satu periode pengukuran dengan periode pengukuran selanjutnya, untuk melihat ada atau tidaknya perbaikan pencapaian target pengukuran oleh perusahaan (*continuous improvement*) yang berasal dari konsep SMART+C yaitu *Specific, Measurable, Achievable, Realistic, Time-bound*, dan *Continuously Improve*.
c. “realistis terhadap kondisi organisasi” dimana indikator dapat disesuaikan dengan kondisi organisasi sehingga menggambarkan pengukuran secara efektif dan target dari pengukuran dapat dicapai yang sejalan dengan karakteristik dari KRI yang efektif (James Lam et al., 2006).

Jumlah nilai 16 dimiliki oleh kriteria “mudah dimengerti” yang menyatakan bahwa indikator dapat dimengerti oleh Manajer Indikator Kinerja Utama (IKU) pada khususnya dan setiap pegawai Departemen Teknologi Informasi Bank D pada umumnya. Kriteria ini sesuai dengan teori pembuatan indikator yang efektif untuk memonitor risiko operasional (Davies dan Haubenstock, 2002) dan karakteristik dari KRI yang efektif (James Lam et al., 2006).

Jumlah nilai 15 adalah kriteria “bersifat spesifik dan eksplisit” dimana indikator bersifat spesifik dan tidak mengandung ambiguitas dalam pemahamannya di kemudian hari yang sesuai dengan cara membuat indikator yang baik menurut Patrick PC Ow (n.d.).

4.3. Pembobotan Kriteria Pemilihan Indikator (IRU dan IPU)

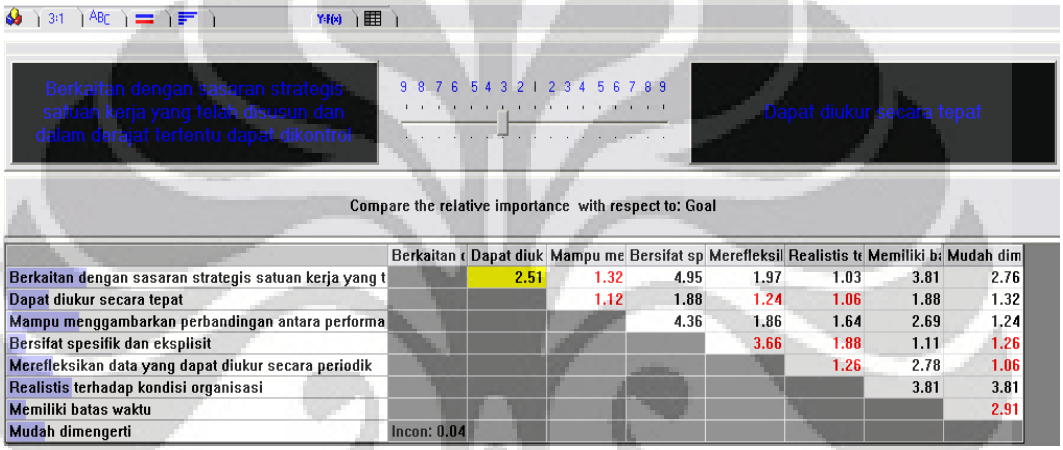
4.3.1. Langkah Pengolahan Data

Pengolahan data pembobotan kriteria indikator (IRU dan IPU) dilakukan dalam 2 tahap yaitu:

a. Menggabungkan penilaian perbandingan berpasangan tiap kriteria dari para ahli terhadap tingkat kepentingan relatif setiap kriteria. Penilaian kelompok dalam AHP dapat digabungkan menjadi satu penilaian yaitu rataan geometris

(Saaty, 1999, hal. 265) dari penilaian responden menggunakan *software* Microsoft Excel 2007 dengan formula "geomean(*range*)". Penilaian ini merupakan input untuk penghitungan bobot dari tiap kriteria indikator (IRU dan IPU).

b. Menghitung pembobotan dengan mode distributive untuk setiap kriteria dan rasio inkonsistensinya menggunakan Expert Choice 2000 dengan memasukkan hasil rataan geometris dari tahap sebelumnya seperti terdapat pada gambar 4.2.



Gambar 4.2. Penghitungan Menggunakan Expert Choice 2000

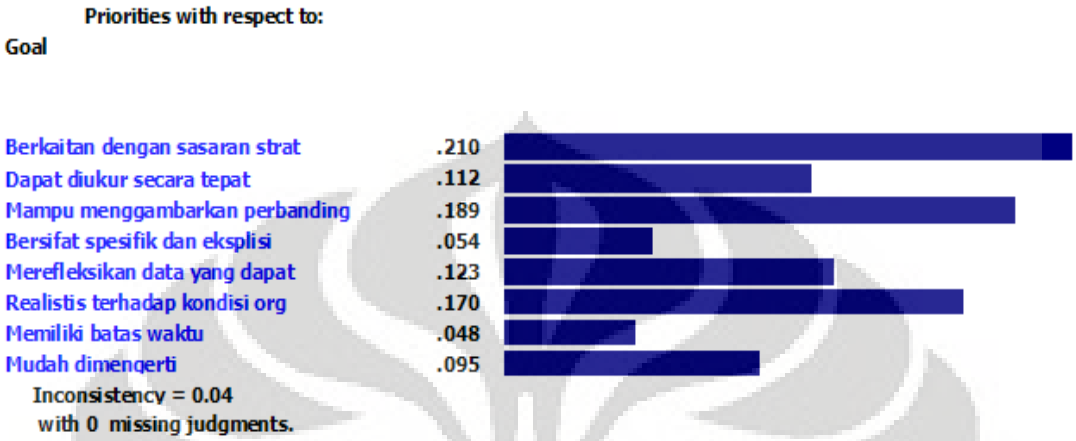
4.3.2. Hasil Pengolahan Data Dan Analisis

Hasil pengolahan rataan geometris dari penilaian tiap responden dapat dilihat pada tabel 4.5 berikut ini.

Tabel 4.5. Hasil Rataan Geometris Kriteria Indikator (IRU dan IPU)

Kriteria	2	3	4	5	6	7	8
	Ā	Ā	Ā	Ā	Ā	Ā	Ā
1	2.51	1/1.32	4.95	1.97	1/1.03	3.81	2.76
2		1/1.12	1.88	1/1.24	1/1.06	1.88	1.32
3			4.36	1.86	1.64	2.69	1.24
4				1/3.66	1/1.88	1.11	1/1.26
5					1/1.26	2.78	1/1.06
6						3.81	3.81
7							1/2.91
8							

Hasil pengolahan data tersebut dengan Expert Choice 2000 berupa pembobotan tiap kriteria pemilihan indikator (IRU dan IPU) yang dapat dilihat pada gambar 4.3 berikut.



Gambar 4.3. Hasil Pengolahan Data Menggunakan Expert Choice 2000

Mode pembobotan kriteria secara distributif merupakan cara dimana bobot semua alternatif jika dijumlahkan menjadi bernilai satu. *Distributive mode* digunakan ketika ada ketergantungan antara alternatif-alternatif dan unit prioritas yang didistribusikan ke alternatif-alternatif tersebut. Pada *distributive mode* bobot dari kriteria menunjukkan tingkat kepentingan yang diberikan pembuat keputusan kepada dominasi setiap alternatif relatif terhadap semua alternatif lainnya di dalam kriteria tersebut. Pada penelitian ini, bobot tiap kriteria juga merupakan faktor pengali dari kuadran 3 dan 4 pada matriks prioritas untuk memilih indikator (IRU dan IPU) yang memenuhi kriteria pemilihan indikator (IRU dan IPU) tersebut.

Dari seluruh kriteria, bobot yang paling tinggi yaitu 0.210 dimiliki oleh kriteria "berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol". Hal ini berarti bahwa sangat penting bahwa baik IRU maupun IPU bermanfaat dan mendukung keputusan serta langkah yang diambil oleh manajemen Bank D.

Selanjutnya, pentingnya indikator yang memperlihatkan perbaikan performa yang terdahulu dengan saat ini diperlihatkan dengan bobot kriteria 0.189 yang menempati posisi ke-2. Selanjutnya, berturut-turut urutan kepentingan pemilihan indikator (IRU dan IPU) yaitu "realistis terhadap kondisi organisasi" dengan bobot kriteria sebesar 0.170, "merefleksikan data yang dapat diukur secara periodik" dengan bobot kriteria 0.123, "dapat diukur secara tepat" dengan bobot kriteria 0.112, "mudah dimengerti" dengan bobot kriteria 0.095, "bersifat spesifik dan eksplisit" dengan bobot kriteria 0.054, dan memiliki batas waktu dengan bobot kriteria 0.048.

Rasio inkonsistensi dihitung dari tiap penilaian secara otomatis oleh *software* Expert Choice 2000 yaitu dengan menghitung inkonsistensi dari setiap pasangan penilaian dan mengalikannya dengan prioritas dari elemen dimana perbandingan dilakukan, dan selanjutnya ditambahkan ke seluruh elemen. Yang paling penting dalam pembobotan ini adalah untuk menghasilkan keputusan tepat, bukan hanya untuk meminimalkan rasio tersebut. Dalam kenyataan, tidak mudah ditemukan penilaian yang konsisten sempurna. Oleh karena itu, rasio 0.10 menjadi batas toleransi, dimana perbandingan berpasangan akan menjadi tidak konsisten jika bernilai lebih dari 0.10. Nilai inkonsistensi rasio pada perbandingan berpasangan kriteria pemilihan indikator (IRU dan IPU) adalah 0.04. Karena nilai ini lebih kecil 0.10, maka penilaian terhadap tingkat kepentingan kriteria indikator (IRU dan IPU) masih dalam batas toleransi sehingga penilaian konsisten.

4.4. Penentuan Risiko dan Indikator (IRU dan IPU)

4.4.1. Langkah Pengolahan Data

Pada pemilihan indikator (IRU dan IPU), dilakukan pengolahan data menggunakan *software* Microsoft Excel 2007 dengan tahap sebagai berikut:

a. Menjumlahkan kuadran 1 yang berisi penilaian responden terhadap keterkaitan antara risiko terpilih dan IRU dan memilih IRU dengan nilai tertinggi pertama dan ke-dua yang bernilai minimum 24

b. Menjumlahkan kuadran 2 yang berisi penilaian responden terhadap keterkaitan antara risiko terpilih dan IPU dan memilih IPU dengan nilai tertinggi pertama dan ke-dua yang bernilai minimum 24
c. Menjumlahkan kuadran 3 yang berisi penilaian responden terhadap IRU dan kemampuannya memenuhi kriteria pemilihan indikator dan mengalikan jumlah tersebut dengan bobot dari tiap kriteria pemilihan indikator (IRU dan IPU)
d. Menjumlahkan kuadran 4 yang berisi penilaian responden terhadap IPU dan kemampuannya memenuhi kriteria pemilihan indikator dan mengalikan jumlah tersebut dengan bobot dari tiap kriteria pemilihan indikator (IRU dan IPU)
e. Mengkonfirmasikan hasil dari langkah di atas kepada responden dan memperbaiki IRU dan IPU tersebut baik dari segi isi maupun diksi

4.4.2. Hasil Pengolahan Data Dan Analisis

Hasil pemilihan risiko Bagian Kebijakan, Bagian Operasional, dan Bagian Administrasi Departemen Teknologi Informasi dapat dilihat di bab sebelumnya, pada tabel 3.12 yang merupakan masukan untuk penyusunan Form Kuesioner Tahap II.

Selanjutnya, hasil pengolahan data kuadran 1 dan 2 untuk IRU dan IPU dari tiap risiko dengan nilai tertinggi pertama dan ke-dua yang bernilai minimum 24 dapat dilihat pada tabel 4.6 dan 4.7 berikut.

Nilai 24 ditentukan karena rata-rata nilai tersebut bernilai 6 yang berarti jika seluruh responden memberikan nilai terhadap IRU dan IPU tersebut, mereka menyatakan “hubungan sedang” antara risiko terpilih dan indikator (IRU dan IPU). Jika berada di bawah nilai 24, berarti hubungan antara risiko dan indikator (IRU dan IPU) rendah dan IRU serta IPU tidak cukup untuk menjadi pengukuran risiko yang bersangkutan.

Tabel 4.6. Hasil Penjumlahan Kuadran 1

No.	Risiko	Indikator Risiko Utama (IRU)	Total
1	Kurangnya pengamanan pada penggunaan *notebook* di luar ruang kerja/ tempat umum menyebabkan *notebook* rusak sehingga pekerjaan terganggu	Pengukuran Tingkat Kerusakan *Notebook*	33
2	Kurangnya kontrol penggunaan *notebook* di luar ruang kerja menyebabkan komponen atau keseluruhan *notebook* hilang sehingga pekerjaan terganggu	Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya	36
3	Tidak ada *user management* yang baik menyebabkan adanya akses oleh pihak tidak berwenang yang menyebabkan aplikasi Web Departemen Teknologi Informasi hilang atau rusak sehingga aktivitas tim Roadmap Mitra Strategis terganggu	Pengukuran Tingkat Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D	27
4	Modifikasi aset yang tidak terotorisasi menyebabkan kinerja aplikasi Web Departemen Teknologi Informasi turun sehingga aktivitas tim Roadmap Mitra Strategis terganggu	Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D	24
5	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan internal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi	24

Tabel 4.6. Hasil Penjumlahan Kuadran 1 (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Total
6	Rusaknya media penyimpanan informasi menyebabkan softcopy kajian/ laporan eksternal menjadi tidak ada/ hilang/ tidak akurat saat dibutuhkan	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal	30
7	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan eksternal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi	24
8	Kurangnya pengamanan fisik ruang kerja Direktur dan Deputi Direktur Departemen Teknologi Informasi yang menyebabkan akses pihak tak berwenang yang berdampak pada proses otorisasi	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur	27
9	Kurangnya kontrol hak akses memungkinkan ruang kerja Direktur dan Deputi Direktur diakses pihak tak berwenang yang berdampak pada proses otorisasi	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur	36
10	Belum berjalannya manajemen aset (inventarisasi, kepemilikan, otorisasi penggunaan, pemeliharaan, penggunaan) dapat menyebabkan ruang pelatihan dan asetnya tidak berfungsi maksimal	Pengukuran Tingkat Pemanfaatan Ruang Pelatihan	27

Tabel 4.6. Hasil Penjumlahan Kuadran 1 (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Total
11	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham tentang *setting policy & schedule backup*	Pengukuran Tingkat Kinerja *Robotic*	36
12	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham melakukan instalasi agent di aplikasi	Pengukuran Tingkat Kinerja *Robotic*	36
13	Lemahnya mekanisme monitoring sistem menyebabkan kinerja PC Teleks menurun karena kebutuhan performa tidak terpenuhi	Pengukuran Tingkat Kinerja PC Teleks	27
14	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan *mainframe* mengalami *hardware failure*	Pengukuran Tingkat Kinerja *Mainframe*	33
15	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pembebanan Anggaran Pelaksanaan SOSA tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan Dokumen Pembebanan Anggaran Pelaksanaan SOSA	33
16	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pengadaan Kunci Telegram Bank D tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan Dokumen Pengadaan Kunci Telegram Bank D	30

Tabel 4.6. Hasil Penjumlahan Kuadran 1 (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Total
17	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen PKAT tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan Dokumen PKAT	24
18	Kurangnya *training* menyebabkan Informasi *softcopy* dokumentasi teknis tiap seksi dan kelompok tidak akurat karena kesalahan dalam pembuatan	Pengukuran Tingkat Keakuratan Dokumen Teknis Tiap Seksi dan Kelompok	30
19	Kurangnya *training* untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi *softcopy* SOP Seksi dan Bagian tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian	27
20	Kurangnya kontrol pengamanan informasi menyebabkan Tape/ Catridge hasil backup data hilang ketika dalam perjalanan ke DRC	Pengukuran Tingkat Kehilangan Tape / Catridge hasil backup data yang akan dikirim ke DRC	36
21	Kurangnya training menyebabkan informasi softcopy data dari unit kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan	Pengukuran Tingkat Keakuratan Data Unit Kerja Yang Telah Diolah	27
22	Tidak ada Aplikasi *AntiVirus, Antimalware, Firewall,*dll menyebabkan Informasi *softcopy* data unit kerja yang telah diolah tidak tersedia karena virus	Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah	30

Tabel 4.6. Hasil Penjumlahan Kuadran 1 (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Total
23	Ketidaktersediaan / Kurangnya / Gangguan AC menyebabkan Pelaksanaan operasional di DRC, *strong room*, ruang *mainframe*, dan ruang *server* terganggu	Pengukuran Tingkat Gangguan AC	30
24	Tidak adanya / lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan *thermal control* tidak dapat digunakan karena komponen rusak	Pengukuran Tingkat Kerusakan *Thermal Control*	24
25	Pemeliharaan aset yang tidak baik menyebabkan *thermal control* tidak dapat digunakan karena kerusakan komponen	Pengukuran Tingkat Kerusakan *Thermal Control*	24
26	Pemeliharaan aset yang tidak baik menyebabkan suhu ruangan DRC, *strong room*, ruang *mainframe*, dan ruang *server* tidak dapat diketahui karena tidak terdapat *thermal control*	Pengukuran Tingkat Ketersediaan *Thermal Control*	27

Tabel 4.7. Hasil Penjumlahan Kuadran 2

No.	Risiko	Indikator Pengendalian Utama (IPU)	Total
1	Kurangnya pengamanan pada penggunaan *notebook* di luar ruang kerja/ tempat umum menyebabkan *notebook* rusak sehingga pekerjaan terganggu	Pengukuran *Form* Peminjaman Aset	30

Tabel 4.7. Hasil Penjumlahan Kuadran 2 (Sambungan)

No.	Risiko	Indikator Pengendalian Utama (IPU)	Total
2	Kurangnya kontrol penggunaan *notebook* di luar ruang kerja menyebabkan komponen atau keseluruhan *notebook* hilang sehingga pekerjaan terganggu	Pengukuran Kelengkapan dan Kebenaran Data pada *Database* Aset	30
		Pengukuran Form Peminjaman Aset	24
3	Tidak ada *user management* yang baik menyebabkan adanya akses oleh pihak tidak berwenang yang menyebabkan aplikasi Web Departemen Teknologi Informasi hilang atau rusak sehingga aktivitas tim Roadmap Mitra Strategis terganggu	Pengukuran Kesesuaian *User Account*	36
		Pengukuran Keefektifan Penanganan Insiden / *Event*	24
4	Modifikasi aset yang tidak terotorisasi menyebabkan kinerja aplikasi Web Departemen Teknologi Informasi turun sehingga aktivitas tim Roadmap Mitra Strategis terganggu	Pengukuran audit *security log*	36
		Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja	36
5	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan internal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Pengukuran Efektivitas *Training*	36
6	Rusaknya media penyimpanan informasi menyebabkan softcopy kajian/ laporan eksternal menjadi tidak ada/ hilang/ tidak akurat saat dibutuhkan	Pengukuran Pelaksanaan *Backup* Informasi Personil Unit Kerja	30
		Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset	30

Tabel 4.7. Hasil Penjumlahan Kuadran 2 (Sambungan)

No.	Risiko	Indikator Pengendalian Utama (IPU)	Total
7	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan eksternal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Pengukuran Tingkat Pemahaman	36
8	Kurangnya pengamanan fisik ruang kerja Direktur dan Deputi Direktur Departemen Teknologi Informasi yang menyebabkan akses pihak tak berwenang yang berdampak pada proses otorisasi	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja	33
		Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu	33
9	Kurangnya kontrol hak akses memungkinkan ruang kerja Direktur dan Deputi Direktur diakses pihak tak berwenang yang berdampak pada proses otorisasi	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja	33
		Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu	27
10	Belum berjalannya manajemen aset (inventarisasi, kepemilikan, otorisasi penggunaan, pemeliharaan, penggunaan) dapat menyebabkan ruang pelatihan dan asetnya tidak berfungsi maksimal	Pengukuran *Form* Peminjaman Aset	36
11	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham tentang *setting policy & schedule backup*	Pengukuran Efektivitas *Training*	33
		Pengukuran Tingkat Pemahaman	33

Tabel 4.7. Hasil Penjumlahan Kuadran 2 (Sambungan)

No.	Risiko	Indikator Pengendalian Utama (IPU)	Total
12	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham melakukan instalasi agent di aplikasi	Pengukuran Tingkat Pemahaman	33
		Pengukuran Efektivitas *Training*	33
13	Lemahnya mekanisme monitoring sistem menyebabkan kinerja PC Teleks menurun karena kebutuhan performa tidak terpenuhi	Pengukuran Utilisasi Aset	30
		Pengukuran Pelaksanaan *Update Antivirus*	24
		Pengukuran Pelaksanaan *Update Patch*	24
14	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan *mainframe* mengalami *hardware failure*	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset	30
		Pengukuran Keefektifan Penanganan Insiden / *Event*	27
15	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pembebanan Anggaran Pelaksanaan SOSA tidak akurat karena kesalahan pembuatan	Pengukuran Efektivitas *Training*	36
		Pengukuran Tingkat Pemahaman	36
16	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pengadaan Kunci Telegram Bank D tidak akurat karena kesalahan pembuatan	Pengukuran Efektivitas *Training*	36
		Pengukuran Tingkat Pemahaman	36

Tabel 4.7. Hasil Penjumlahan Kuadran 2 (Sambungan)

No.	Risiko	Indikator Pengendalian Utama (IPU)	Total
17	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen PKAT tidak akurat karena kesalahan pembuatan	Pengukuran Efektivitas *Training*	36
		Pengukuran Tingkat Pemahaman	36
18	Kurangnya *training* menyebabkan Informasi *softcopy* dokumentasi teknis tiap seksi dan kelompok tidak akurat karena kesalahan dalam pembuatan	Pengukuran Efektivitas *Training*	36
		Pengukuran Tingkat Pemahaman	36
19	Kurangnya *training* untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi *softcopy* SOP Seksi dan Bagian tidak akurat karena kesalahan pembuatan	Pengukuran Efektivitas *Training*	36
		Pengukuran Tingkat Pemahaman	36
20	Kurangnya kontrol pengamanan informasi menyebabkan Tape/ Catridge hasil backup data hilang ketika dalam perjalanan ke DRC	Pengukuran Form Pengiriman *Tape Backup*	33
		Pengukuran Identifikasi Pelabelan Aset *Removable Media*	24
21	Kurangnya *training* menyebabkan informasi softcopy data dari unit kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan	Pengukuran Efektivitas *Training*	36
		Pengukuran Tingkat Pemahaman	36

Tabel 4.7. Hasil Penjumlahan Kuadran 2 (Sambungan)

No.	Risiko	Indikator Pengendalian Utama (IPU)	Total
22	Tidak ada Aplikasi *AntiVirus, Antimalware, Firewall,*dll menyebabkan Informasi *softcopy* data unit kerja yang telah diolah tidak tersedia karena virus	Pengukuran Pelaksanaan *Update Antivirus*	36
23	Ketidaktersediaan / Kurangnya / Gangguan AC menyebabkan Pelaksanaan operasional di DRC, *strong room*, ruang *mainframe*, dan ruang *server* terganggu	Pengukuran Keefektifan Penanganan Insiden / *Event*	27
24	Tidak adanya / lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan *thermal control* tidak dapat digunakan karena komponen rusak	Pengukuran Keefektifan Penanganan Insiden / *Event*	30
25	Pemeliharaan aset yang tidak baik menyebabkan *thermal control* tidak dapat digunakan karena kerusakan komponen	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset	30
		Pengukuran Keefektifan Penanganan Insiden / *Event*	27
26	Pemeliharaan aset yang tidak baik menyebabkan suhu ruangan DRC, *strong room*, ruang *mainframe*, dan ruang *server* tidak dapat diketahui karena tidak terdapat *thermal control*	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset	30
		Pengukuran Keefektifan Penanganan Insiden / *Event*	27

Dari hasil penjumlahan kuadran 1 dan 2 yang termuat pada tabel 4.6 dan 4.7, dapat dilihat bahwa nilai total hubungan antara risiko dengan IRU dengan nilai tertinggi pertama dan ke-dua yang bernilai minimum 24 berkisar antara 24 sampai dengan 36. Nilai 24 merupakan nilai minimum yang dapat masuk sebagai alternatif IRU dan IPU terpilih seperti telah dijelaskan sebelumnya, sedangkan nilai 36 merupakan nilai maksimum yang berarti rata-rata tiap responden memberi nilai 9 yang berarti "hubungan kuat" antara risiko dengan IRU dan IPU". Hal ini berarti semakin mendekati angka 36, baik IRU maupun IPU semakin mampu menjadi indikator yang dapat menggambarkan pengukuran dari dampak risiko yang bersangkutan.

Pada alternatif IRU hanya terdapat 1 alternatif untuk setiap risiko, sedangkan pada alternatif IPU terdapat 1 hingga 3 alternatif IPU untuk setiap risiko. Hal ini berkaitan dari nilai yang telah diberikan responden sebelumnya sesuai dengan batas minimum 24. Selain itu, sifat IRU yang lebih spesifik terhadap dampak risiko menyebabkan hanya ada 1 IRU untuk tiap risiko yang dapat memiliki niai di atas 24. Di sisi lain, terdapat IRU yang dapat mengukur lebih dari 1 risiko. Contohnya adalah IRU "Pengukuran Tingkat Kerusakan *Thermal Control"* yang dinilai dapat mengukur dampak dari risiko "Tidak adanya / lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan *thermal control* tidak dapat digunakan karena komponen rusak" dan "Pemeliharaan aset yang tidak baik menyebabkan *thermal control* tidak dapat digunakan karena kerusakan komponen".

IPU merupakan pengukuran kontrol risiko yang dapat digunakan pada beberapa risiko. Selain itu, pada beberapa risiko, butuh pengendalian lebih dari satu sehubungan dengan kebutuhan dan perbedaan tujuan pengukuran itu sendiri. Contohnya adalah IPU "pengukuran tingkat pemahaman" dan "pengukuran efektivitas *training* untuk mengukur pengendalian risiko "Kurangnya *training* untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi *softcopy* SOP Seksi dan Bagian tidak akurat karena kesalahan pembuatan".

Setelah menjumlahkan kuadran 1 dan 2, dilanjutkan dengan mengolah data kuadran 3 dan 4 yang hasilnya dapat dilihat pada tabel 4.8 dan 4.9 di bawah

Tabel 4.8. Hasil Pengolahan Data Kuadran 3

No	Indikator Risiko Utama (IRU)	Total
1	Pengukuran Tingkat Kerusakan *Notebook*	19.09
2	Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya	18.17
3	Pengukuran Jumlah Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D	13.72
4	Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D	9.04
5	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi	10.03
6	Pengukuran Gangguan Aktivitas tim Roadmap dan Mitra Strategis	14.27
7	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal	7.67
8	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur	10.99
9	Pengukuran Tingkat Pemanfaatan Ruang Pelatihan	6.27
10	Pengukuran Tingkat Kinerja *Robotic*	12.06
11	Pengukuran Tingkat Kinerja PC Teleks	11.65
12	Pengukuran Tingkat Kinerja *Mainframe*	15.07
13	Pengukuran Tingkat Keakuratan Dokumen Pembebanan Anggaran Pelaksanaan SOSA	8.09
14	Pengukuran Tingkat Keakuratan Dokumen Pengadaan Kunci Telegram Bank D	2.61
15	Pengukuran Tingkat Keakuratan Dokumen PKAT	2.66
16	Pengukuran Tingkat Keakuratan Dokumen Teknis Tiap Seksi dan Kelompok	3.28

Tabel 4.8. Hasil Pengolahan Data Kuadran 3 (Sambungan)

No	Indikator Risiko Utama (IRU)	Total
17	Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian	3.97
18	Pengukuran Tingkat Kehilangan *Tape / Catridge* hasil *back-up data* yang akan dikirim ke DRC	6.56
19	Pengukuran Tingkat Keakuratan Data Satuan kerja Yang Telah Diolah	4.64
20	Pengukuran Tingkat Serangan Virus Terhadap Data Satuan kerja Yang Telah Diolah	7.87
21	Pengukuran Tingkat Gangguan AC	10.13
22	Pengukuran Tingkat Kerusakan *Thermal Control*	7.84
23	Pengukuran Tingkat Ketersediaan *Thermal Control*	10.24

Tabel 4.9. Hasil Pengolahan Data Kuadran 4

No	Indikator Pengendalian Utama (IPU)	Total
1	Pengukuran Tingkat Pengamanan Personil Unit Kerja	10.08
2	Pengukuran Tingkat Pengamanan Personil Pihak Ketiga	7.19
3	Pengukuran Kelengkapan dan Kebenaran Data pada Database Asset	10.34
4	Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak	9.62
5	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja	7.52
6	Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja	9.98
7	Pengukuran Kesesuaian *Password* Personil Unit Kerja	8.23
8	Pengukuran Pelaksanaan *Update Antivirus*	18.02
9	Pengukuran Pelaksanaan Update *Patch*	18.82
10	Pengukuran Keefektifan Penanganan Insiden / Event	13.13

Tabel 4.9. Hasil Pengolahan Data Kuadran 4 (Sambungan)

No	Indikator Pengendalian Utama (IPU)	Total
11	Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu	7.97
12	Pengukuran Identifikasi Pelabelan Aset *Removable Media*	5.87
13	Pengukuran kelengkapan data serah terima aset	9.30
14	Pengukuran Kesesuaian *Password Mainframe* dan *Tandem*	7.64
15	Pengukuran *Form* Peminjaman Aset	7.58
16	Pengukuran Tingkat Pemahaman	7.43
17	Pengukuran Efektivitas *Training*	10.70
18	Pengukuran *Analisis Fault Logging* Akses Fisik	10.94
19	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset	8.20
20	Pengukuran Audit *Security Log*	7.16
21	Pengukuran *Form* Pengiriman *Tape Backup*	10.66
22	Pengukuran Kesesuaian *User Account*	18.62
23	Pengukuran Utilisasi Aset	17.80

Dari hasil penjumlahan kuadran 3 dan 4, didapat jumlah dari tiap indikator (IRU dan IPU) terhadap kriteria pemilihan indikator. Penilaian ini akan mempengaruhi pemilihan IRU dan IPU jika terdapat lebih dari 1 alternatif IRU dan IPU dan untuk menilai kemampuan IRU dan IPU tersebut untuk memenuhi kriteria pemilihan indikator terpilih.

IRU dan IPU yang memiliki nilai tertinggi pertama dan ke-dua dari tiap risiko mengalami perbaikan dari segi isi agar memenuhi kriteria pemilihan indikator (IRU dan IPU) dengan lebih baik lagi. Isi dari IRU dan IPU tersebut meliputi nama pengukuran, tujuan, ruang lingkup, metode, frekuensi, sumber data dan prosedur pengumpulan data, serta target.

IRU dan IPU dari risiko terpilih terdapat pada tabel 4.10.

Tabel 4.10. IRU dan IPU Terpilih Untuk Tiap Risiko

No.	Risiko	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
1	Kurangnya pengamanan pada penggunaan *notebook* di luar ruang kerja/ tempat umum menyebabkan *notebook* rusak sehingga pekerjaan terganggu	Pengukuran Tingkat Kerusakan *Notebook*	Pengukuran *Form* Peminjaman Aset
2	Kurangnya kontrol penggunaan *notebook* di luar ruang kerja menyebabkan komponen atau keseluruhan *notebook* hilang sehingga pekerjaan terganggu	Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya	Pengukuran Kelengkapan dan Kebenaran Data pada *Database* Aset
3	Tidak ada *user management* yang baik menyebabkan adanya akses oleh pihak tidak berwenang yang menyebabkan aplikasi Web Departemen Teknologi Informasi hilang atau rusak sehingga aktivitas tim *Roadmap* Mitra Strategis terganggu	Pengukuran Jumlah Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D	Pengukuran Kesesuaian *User Account*
4	Modifikasi aset yang tidak terauthorisasi menyebabkan kinerja aplikasi Web Departemen Teknologi Informasi turun sehingga aktivitas tim *Roadmap* Mitra Strategis terganggu	Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D	Pengukuran audit *security log* Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja
5	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan internal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi	Pengukuran Efektivitas *Training*

Tabel 4.10. IRU dan IPU Terpilih Untuk Tiap Risiko (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
6	Rusaknya media penyimpanan informasi menyebabkan softcopy kajian/ laporan eksternal menjadi tidak ada/ hilang/ tidak akurat saat dibutuhkan	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal	Pengukuran Pelaksanaan *Backup* Informasi Personil Unit Kerja
			Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset
7	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan eksternal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi	Pengukuran Tingkat Pemahaman
8	Kurangnya pengamanan fisik ruang kerja Direktur dan Deputi Direktur Departemen Teknologi Informasi yang menyebabkan akses pihak tak berwenang yang berdampak pada proses authorisasi	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja
			Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu
9	Kurangnya kontrol hak akses memungkinkan ruang kerja Direktur dan Deputi Direktur diakses pihak tak berwenang yang berdampak pada proses otorisasi	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja
10	Belum berjalannya manajemen aset (inventarisasi, kepemilikan, otorisasi penggunaan, pemeliharaan, penggunaan) dapat menyebabkan ruang pelatihan dan asetnya tidak berfungsi maksimal	Pengukuran Tingkat Pemanfaatan Ruang Pelatihan	Pengukuran *Form* Peminjaman Aset

Tabel 4.10. IRU dan IPU Terpilih Untuk Tiap Risiko (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
11	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham tentang *setting policy & schedule backup*	Pengukuran Tingkat Kinerja *Robotic*	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman
12	Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham melakukan instalasi agent di aplikasi	Pengukuran Tingkat Kinerja *Robotic*	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman
13	Lemahnya mekanisme monitoring sistem menyebabkan kinerja PC Teleks menurun karena kebutuhan performa tidak terpenuhi	Pengukuran Tingkat Kinerja PC Teleks	Pengukuran Utilisasi Aset
14	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan *mainframe* mengalami *hardware failure*	Pengukuran Tingkat Kinerja *Mainframe*	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset
			Pengukuran Keefektifan Penanganan Insiden / *Event*
15	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pembebanan Anggaran Pelaksanaan SOSA tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan Dokumen Pembebanan Anggaran Pelaksanaan SOSA	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman
16	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen Pengadaan Kunci Telegram Bank D tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan Dokumen Pengadaan Kunci Telegram Bank D	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman

Tabel 4.10. IRU dan IPU Terpilih Untuk Tiap Risiko (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
17	Kurangnya *training* menyebabkan informasi *softcopy* Dokumen PKAT tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan Dokumen PKAT	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman
18	Kurangnya *training* menyebabkan Informasi *softcopy* dokumentasi teknis tiap seksi dan kelompok tidak akurat karena kesalahan dalam pembuatan	Pengukuran Tingkat Keakuratan Dokumen Teknis Tiap Seksi dan Kelompok	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman
19	Kurangnya *training* untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi *softcopy* SOP Seksi dan Bagian tidak akurat karena kesalahan pembuatan	Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman
20	Kurangnya kontrol pengamanan informasi menyebabkan *Tape/ Catridge* hasil *back-up* data hilang ketika dalam perjalanan ke DRC	Pengukuran Tingkat Kehilangan *Tape / Catridge* hasil *back-up* data yang akan dikirim ke DRC	Pengukuran Form Pengiriman *Tape Back-up*
21	Kurangnya training menyebabkan informasi *softcopy* data dari unit kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan	Pengukuran Tingkat Keakuratan Data Unit Kerja Yang Telah Diolah	Pengukuran Efektivitas *Training*
			Pengukuran Tingkat Pemahaman

Tabel 4.10. IRU dan IPU Terpilih Untuk Tiap Risiko (Sambungan)

No.	Risiko	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
22	Tidak ada Aplikasi *AntiVirus, Antimalware, Firewall*,dll menyebabkan Informasi *softcopy* data unit kerja yang telah diolah tidak tersedia karena virus	Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah	Pengukuran Pelaksanaan *Update Antivirus*
23	Ketidaktersediaan / Kurangnya / Gangguan AC menyebabkan Pelaksanaan operasional di DRC, *strong room*, ruang *mainframe*, dan ruang *server* terganggu	Pengukuran Tingkat Gangguan AC	Pengukuran Keefektifan Penanganan Insiden / *Event*
24	Tidak adanya / lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan *thermal control* tidak dapat digunakan karena komponen rusak	Pengukuran Tingkat Kerusakan *Thermal Control*	Pengukuran Keefektifan Penanganan Insiden / *Event*
25	Pemeliharaan aset yang tidak baik menyebabkan *thermal control* tidak dapat digunakan karena kerusakan komponen	Pengukuran Tingkat Ketersediaan *Thermal Control*	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset
			Pengukuran Keefektifan Penanganan Insiden / *Event*
26	Pemeliharaan aset yang tidak baik menyebabkan suhu ruangan DRC, *strong room*, ruang *mainframe*, dan ruang *server* tidak dapat diketahui karena tidak terdapat *thermal control*	Pengukuran Tingkat Ketersediaan *Thermal Control*	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset
			Pengukuran Keefektifan Penanganan Insiden / *Event*

Pemilihan IRU dan IPU, langkah yang dilakukan pada penelitian dibandingkan dengan teori (Immaneni, Mastro, dan Haubenstock; 2002), antara lain:

a. kedua penelitian mengambil risiko yang berasal dari hasil *risk assessment.* Konsep manajemen risiko yang digunakan oleh teori tersebut tidak dinyatakan secara eksplisit, sedangkan pada penelitian ini, *risk assessment* dilakukan sesuai ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005
b. indikator (IRU dan IPU) yang diidentifikasi sebagai alternatif IRU dan IPU pada penelitian ini berasal dari implementasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005, sedangkan pada teori tersebut IRU dan IPU berasal dari metrik yang telah ada dan hasil *subject expert matter* (SEM)
c. *design matrix* dan *gap assessment* pada teori tersebut merupakan matriks prioritas pada penelitian yang merupakan penilaian kemampuan indikator (IRU dan IPU) untuk mengukur risiko dan memenuhi kriteria pemilihan indikator
d. Tidak terdapat fase validasi IRU dan IPU menggunakan metode statistik karena keterbatasan waktu dan data dari penelitian
e. Dalam penelitian ini tidak dibuat *dashboard design* karena tidak seluruh IRU dan IPU telah diketahui hasil implementasinya dalam waktu yang tersedia untuk mengerjakan penelitian ini

Tabel 4.10 memperlihatkan IRU dan IPU terpilih dari tiap risiko. Risiko 1 sampai dengan 7 merupakan tanggung awab dari Bagian Kebijakan, 8 sampai 10 merupakan tanggung jawab Bagian Administrasi, dan risiko lainnya adalah tanggung jawab Bagian Operasional.

Pada pemilihan IRU hanya terdapat 1 IRU untuk setiap risiko, sedangkan terdapat risiko yang memiliki 2 IPU. Hal ini dikarenakan dari total nilai dan persetujuan responden, kedua IPU tersebut bernilai sama dan saling mendukung satu sama lain dari segi yang berbeda sehingga tidak mungkin dihilangkan salah satunya. Contohnya pada risiko "kurangnya *training* menyebabkan informasi *softcopy* data dari unit kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan", terdapat IPU "pengukuran efektivitas *training*" dan "pengukuran tingkat

pemahaman". Pengukuran efektivitas *training* mengukur kemampuan personil untuk mengaplikasikan *training* yang telah didapat pada pekerjaan sehari-hari, sedangkan pengukuran tingkat pemahaman merupakan tes terhadap pemahaman materi *training* segera setelah *training* dilaksanakan. Jika hanya dilakukan pengukuran tingkat pemahaman, maka kemungkinan yang terjadi adalah personil tidak mengaplikasikan hasil *training* dalam pekerjannya. Jika hanya dilakukan pengukuran efektivitas *training*, belum tentu personil benar-benar menyimak dan paham materi *training* yang mungkin mengakibatkan hasil pengukuran efektivitas *training* personil tersebut tidak optimal.

Pada alternatif IRU, hanya ada 1 alternatif yang tidak menjadi IRU terpilih yaitu "pengukuran gangguan aktivitas tim *roadmap* dan mitra strategis". Hal ini dikarenakan para ahli memberi nilai lebih besar untuk "pengukuran jumlah kehilangan atau kerusakan Web Departemen Teknologi Informasi Bank D" dan "pengukuran tingkat penurunan kinerja Web Departemen Teknologi Informasi Bank D" untuk risiko menyangkut aplikasi Web tersebut.

Pada pemilihan IPU, terdapat beberapa alternatif IPU yang tidak terpilih yaitu "pengukuran tingkat pengamanan personil unit kerja", "pengukuran tingkat pengamanan personil pihak ketiga", "pengukuran proses authorisasi penggunaan perangkat lunak", "pengukuran kesesuaian *password* personil unit kerja", "pengukuran pelaksanaan update *patch"*, "pengukuran identifikasi pelabelan aset *removable media"*, "pengukuran kelengkapan data serah terima aset", "pengukuran kesesuaian *password mainframe* dan *tandem"*, dan "pengukuran *analisis fault logging* akses fisik. IPU tersebut tidak terpilih karena tidak sesuai dengan usaha mitigasi dari masing-masing risiko.

4.5. Pembuatan Matriks Kontrol Risiko

Setelah IRU dan IPU untuk tiap risiko dan kontrol risiko terpilih, Matriks Kontrol Risiko Departemen Teknologi Informasi Bank D dibuat. Matriks tersebut dapat dilihat pada tabel 4.11.

Tabel 4.11. Matriks Kontrol Risiko

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
1	*Notebook*	Risiko Operasional	Kurangnya pengamanan pada penggunaan *notebook* di luar ruang kerja / tempat umum menyebabkan *notebook* mengalami kerusakan sehingga pekerjaan terkait strategi dan kebijakan TI tidak dapat dilakukan dengan menggunakan *notebook*	level 5	Level 6	Pengukuran Tingkat Kerusakan *Notebook*	- Pedoman pengelolaan *notebook* - SOP Pengelolaan PC dan *Notebook* - Peraturan Bank D mengenai Pengamanan Perangkat Keras Teknologi Informasi Di Luar Area Kantor - Implementasi Winzip untuk membatasi akses terhadap *File* atau proteksi dengan *password* - Standardisasi dan implementasi *cable lock*	Pengukuran Form Peminjaman Aset
2	*Notebook*	Risiko Operasional	Kurangnya kontrol atas penggunaan *notebook* di luar ruang kerja menyebabkan keseluruhan atau sebagian komponen *notebook* hilang sehingga aktivitas strategi dan kebijakan TI tidak dapat dilakukan dengan menggunakan *notebook*	level 4	Level 6	Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya	- Pedoman pengelolaan *notebook* - SOP Pengelolaan PC dan *Notebook* - Peraturan Bank D mengenai Pengamanan Perangkat Keras Teknologi Informasi Di Luar Area Kantor - Implementasi Winzip untuk membatasi akses terhadap *File* atau proteksi dengan *password* - Standardisasi dan implementasi *cable lock*	Pengukuran Kelengkapan dan Kebenaran Data pada Database Aset

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
3	Web Departemen Teknologi Informasi	Risiko Operasional	Tidak ada user management (pemberian, pencabutan, monitoring) yang baik (strong *password*, private *password*, change *password* regularly) menyebabkan aplikasi diakses oleh pihak yang tidak berwenang menyebabkan aplikasi Web Departemen Teknologi Informasi hilang atau rusak sehingga aktivitas RMS dapat terganggu	Level 2	Level 6	Pengukuran Tingkat Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D	- NDA - SE Pam TI - SOP Pengelolaan User	Pengukuran Kesesuaian User Account
4	Web Departemen Teknologi Informasi	Risiko Operasional	Modifikasi aset (komponen/ konfigurasi yang tidak terotorisasi menyebabkan kinerja aplikasi Web Departemen Teknologi Informasi turun sehingga aktivitas RMS dapat terganggu	Level 1	Level 6	Pengukuran Tingkat Penurunan Kinerja Web Departemen TI Bank D	- P3SA- SOP Pengelolaan user	- Pengukuran Audit Security Log - Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
5	Kajian/ Laporan internal yang mengandung informasi rahasia	Risiko Operasional	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan internal yang mengandung informasi rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Level 4	Level 6	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal	- sosialisasi awareness - SOP Monitoring pelaksanaan ketentuan P3SA	Pengukuran Tingkat Pemahaman
6	Kajian/ Laporan eksternal yang mengandung informasi rahasia	Risiko Operasional	Rusaknya media penyimpanan informasi (Harddisk, CD Back-up) menyebabkan dokumen softcopy kajian/laporan eksternal yang mengandung informasi rahasia menjadi tidak ada/hilang/tidak akurat saat dibutuhkan	Level 4	Level 8	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal	- SOP Back-Up Informasi '- Peraturan Bank D mengenai *back-up* dan *restore* - Memperbaiki proses *back-up* dengan sentralisasi pada *server*	- Pengukuran Pelaksanaan Backup Informasi Personil Unit Kerja - Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
7	Kajian/ Laporan eksternal yang mengandung informasi rahasia	Risiko Operasional	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan eksternal yang mengandung informasi rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Level 4	Level 6	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi	- sosialisasi awareness- SOP Monitoring pelaksanaan ketentuan P3SA	Pengukuran Tingkat Pemahaman
8	Ruang Direktur dan Deputi Direktur	Risiko Operasional	Kurangnya pengamanan fisik ruang kerja Direktur dan Deputi Direktur Departemen Teknologi Informasi memungkinkan terjadinya akses oleh pihak yang tidak berwenang, sehingga dapat berdampak pada proses otorisasi di Departemen Teknologi Informasi (misal: Informasi hilang/bocor).	Level 7	Level 7	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur	- Peraturan Bank D mengenai Penempatan aset TI serta perlindungannya - Peraturan Bank D mengenai Pengamanan kantor, ruangan dan fasilitas Teknologi Informasi - *Filing Cabinet* yang terkunci - Akses Ruang Kerja - Pengaturan Akses Fisik	- Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja - Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
9	Ruang Direktur dan Deputi Direktur	Risiko Operasional	Kurangnya kontrol dalam pemberian dan penarikan hak akses memungkinkan Ruang Direktur dan Deputi Direktur Departemen Teknologi Informasi diakses oleh pihak yang tidak berwenang, sehingga dapat berdampak pada proses otorisasi di Departemen Teknologi Informasi (misal: Informasi hilang/bocor).	Level 7	Level 7	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur	- Peraturan Bank D mengenai Pendaftaran dan Pencabutan Hak Akses Pengguna - Peraturan Bank D Evaluasi Hak Akses - Pengaturan Akses Fisik	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja
10	Ruang Pelatihan	Risiko Operasional	Belum berjalannya manajemen aset mencakup inventaris aset dan kepemilikannya, otorisasi penggunaan, pemeliharaan, dan mekanisme penggunaan sesuai fungsinya, dapat menyebabkan Ruang pelatihan (termasuk aset pelatihan) tidak dapat berfungsi dengan maksimal	Level 5	Level 5	Pengukuran Tingkat Pemanfaatan RuangPelatihan	- Kunci di ADepartemen Teknologi Informasi- Master kunci di satpam- Mekanisme penggunaan ruangan	Pengukuran Form Peminjaman Aset

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
11	Robotics	Risiko Operasional	Ketidaktersediaan / ketidaklengkapan SOP untuk melakukan kegiatan operasional (Contoh: SOP Pelaksanaan Back Up, SOP Monitoring, dll) menyebabkan Robotic tidak dapat menjalankan fungsinya dengan baik karena personil tidak paham melakukan setting policy dan schedule back up kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 6	Pengukuran Tingkat Kinerja Robotic	- SOP untuk menjalankan Robotics - Transfer Knowledge untuk pemahaman Robotics	- Pengukuran Tingkat Pemahaman - Pengukuran Efektivitas Training
12	Robotics	Risiko Operasional	Ketidaktersediaan / ketidaklengkapan SOP untuk melakukan kegiatan operasional (Contoh: SOP Pelaksanaan Back Up, SOP Monitoring, dll) menyebabkan Robotic tidak dapat menjalankan fungsinya dengan baik karena personil tidak paham melakukan instalasi agent di aplikasi kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 6	Pengukuran Tingkat Kinerja Robotic	- SOP untuk menjalankan Robotics - Transfer Knowledge untuk pemahaman Robotics	- Pengukuran Tingkat Pemahaman - Pengukuran Efektivitas Training

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
13	PC Teleks	Risiko Operasional	Lemahnya mekanisme monitoring sistem (event log, admin log, fault log, dll) menyebabkan kinerja aset menurun karena kebutuhan performa tidak terpenuhi sehingga operasional komunikasi serta pengiriman dan penerimaan berita teleks mengalami hambatan	Level 4	Level 10	Pengukuran Tingkat Kinerja PC Teleks	- Laporan monitoring performance server- Pedoman Audit Security Log- Koordinasi dengan SKTI dan PTTI untuk implementasi NMS	Pengukuran Utilisasi Aset
14	Mainframe	Risiko Operasional	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan mainframe mengalami hardware failure kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 6	Pengukuran Tingkat Kinerja Mainframe	- Preventive Maintenance - Koordinasi dengan SKTI dan PTTI untuk implementasi NMS	- Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset - Pengukuran Keefektifan Penanganan Insiden / Event
15	Dokumen Pembebanan Anggaran Pelaksanaan SOSA	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan informasi softcopy Dokumen Pembebanan Anggaran Pelaksanaan SOSA tidak akurat karena kesalahan dalam pembuatan	Level 4	Level 6	Pengukuran Tingkat Keakuratan Dokumen Pembebanan Anggaran Pelaksanaan SOSA	- Training - Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan Training)	- Pengukuran Efektivitas Training - Pengukuran Tingkat Pemahaman

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
16	Dokumen Pengadaan	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan informasi softcopy dokumen pengadaan kunci telegram bank indonesia tidak akurat karena kesalahan dalam pembuatan	Level 5	Level 6	Pengukuran Tingkat Keakuratan Dokumen Pengadaan Kunci Telegram Bank D	- Pemberian tugas kepada personel yang menguasai - Training terhadap personel - Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan training)	- Pengukuran Efektivitas Training - Pengukuran Tingkat Pemahaman
17	Dokumen PKAT	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi softcopy Dokumen PKAT tidak akurat karena kesalahan dalam pembuatan	Level 2	Level 3	Pengukuran Tingkat Keakuratan Dokumen PKAT	- Training- Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan training)	- Pengukuran Efektivitas Training- Pengukuran Tingkat Pemahaman
18	Dokumentasi Teknis Seksi dan Bagian	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi softcopy dokumentasi teknis tiap seksi dan kelompok tidak akurat karena kesalahan dalam pembuatan	Level 4	Level 4	Pengukuran Tingkat Keakuratan Dokumen Teknis Tiap Seksi dan Kelompok	- Pemberian tugas kepada personel yang menguasai - Training terhadap personel - Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan Training)	- Pengukuran Efektivitas Training - Pengukuran Tingkat Pemahaman

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
19	SOP Seksi dan Bagian	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi softcopy SOP Seksi dan Bagian tidak akurat karena kesalahan dalam pembuatan	Level 2	Level 10	Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian	- Pemberian tugas kepada personel yang menguasai - Training terhadap personel	- Pengukuran Efektivitas Training - Pengukuran Tingkat Pemahaman
20	*Tape / Catridge* hasil *back up data*	Risiko Operasional	Kurangnya kontrol pengamanan informasi dalam proses pembuatan, pencetakan, penyimpanan, distribusi/peminjaman dan pemusnahan informasi (dokumen pengadaan, event logs, admin log, fault log, dll) menyebabkan Tape / Catridge hasil back up data hilang ketika dalam perjalanan ke DRC	Level 2	Level 3	Pengukuran Tingkat Kehilangan Tape / Catridge hasil back-up data yang akan dikirim ke DRC	Daftar permintaan tape catridge yang dibawa	Pengukuran Form Pengiriman Tape Back-up
21	Data dari unit kerja yang telah diolah	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan informasi softcopy data dari unit kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan	Level 4	Level 10	Pengukuran Tingkat Keakuratan Data Unit Kerja Yang Telah Diolah	- Dokumen panduan (SOP) - Formulir kegiatan proses - Review SOP dan Formulir - Perbaikan data softcopy	- Pengukuran Efektivitas Training - Pengukuran Tingkat Pemahaman

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
22	Data dari unit kerja yang telah diolah	Risiko Operasional	Tidak Ada Aplikasi Pengamanan Sistem Informasi (AntiVirus, Antimalware, Firewall,dll) menyebabkan Informasi softcopy data dari unit kerja yang telah diolah tidak tersedia karena terserang virus	Level 4	Level 10	Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah	- Install anti-virus (Hanya untuk server dan PC Windows based)- Tes compatibility antara aplikasi dengan aplikasi- Back-up- SOP Penanganan Informasi- Server hardening	Pengukuran Pelaksanaan Update Antivirus
23	AC	Risiko Operasional	Ketidaktersediaan / Kurangnya / Gangguan sarana pendukung AC menyebabkan Pelaksanaan operasional di DRC, Strong Room, R.mainframe, dan R.Server terganggu karena gangguan sarana pendukung kegiatan operasional Bagian OTI mengalami hambatan	level 6	Level 8	Pengukuran Tingkat Gangguan AC	- Pengecekkan AC oleh petugas (DLP) yang dilakukan 3 kali dalam 1 hari dan ketika terjadi gangguan listrik - Pengukur Suhu dan Kelembaban (jumlah: 1) - Petugas (pihak ke-3) stand by 24 jam - Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	Pengukuran Keefektifan Penanganan Insiden / Event

Tabel 4.11. Matriks Kontrol Risiko (Sambungan)

No	Jenis Aset	Jenis Risiko	Uraian	Kecen-derungan	Dampak	IRU	Tindakan Pengendalian	IPU
24	*Thermal Control*	Risiko Operasional	Tidak adanya / lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan thermal kontrol tidak dapat digunakan karena kerusakkan komponen kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 8	Pengukuran Tingkat Kerusakan Thermal Control	- Pengecekkan output thermal kontrol - Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	Pengukuran Keefektifan Penanganan Insiden / Event
25	*Thermal Control*	Risiko Operasional	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan thermal kontrol tidak dapat digunakan karena kerusakkan komponen kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 8	Pengukuran Tingkat Ketersediaan Thermal Control	- Pengecekkan output thermal kontrol setiap hari - Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	- Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset - Pengukuran Keefektifan Penanganan Insiden / Event
26	*Thermal Control*	Risiko Operasional	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan suhu ruangan DRC, Strong Room, Ruang Mainframe, dan Ruang Server tidak dapat diketahui karena tidak terdapat thermal kontrol kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 8	Pengukuran Tingkat Ketersediaan Thermal Control	- Pengecekkan output thermal kontrol- Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	- Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset- Pengukuran Keefektifan Penanganan Insiden / Event

Matriks kontrol risiko ini terdiri dari jenis aset, jenis risiko, uraian, kecenderungan, dampak, Indikator Risiko Utama (IRU), tindakan pengendalian, dan Indikator Pengendalian Utama (IPU).

Tujuan dari pembuatan matriks kontrol risiko adalah mengidentifikasi IRU dan IPU dan rencana keseluruhan dari mitigasi risiko. Dokumen ini dapat menjadi dasar pembuatan atau perbaikan IRU dan IPU untuk risiko lain. Dengan demikian, bila satuan kerja lain ingin melakukan hal yang sama, bila ada evaluasi melalui siklus PDCA (*Plan, Do, Check, Action*) untuk pengembangan lebih lanjut, atau bila personil yang baru ingin memahami pengembangan *Balanced Scorecard* generasi ke-4 yang telah dilakukan, prosedur dan level risiko pada bisnis dapat dimengerti dengan cepat. Selain itu, matriks kontrol risiko memperlihatkan hubungan antara IRU dan IPU dari tiap risiko.

Matriks kontrol risiko (Tomonori Tomura, 2006, hal. 4) yang memperlihatkan penjelasan risiko secara detil dan IRU serta IPU terpilih serupa dengan dokumen *control plan* (Immaneni, Mastro, dan Haubenstock; 2002) yang memperlihatkan risiko, kecenderungan, dampak, tindakan pengendalian, dan metric. Namun, pada matriks komtrol risiko tidak terdapat kriteria penerimaan risiko karena telah terdapat pada langkah pertama implementasi ISMS.

Dasar penentuan kecenderungan, dampak, dan level risiko pada matriks kontrol risiko adalah hasil *risk assessment* Bagian Kebijakan, Bagian Operasional, dan Bagian Administrasi Departemen Teknologi Informasi Bank D dengan kriteria penentuan yang terdapat pada lampiran 10.

4.6. Penentuan Hubungan Antara IRU Dan IPU Dengan IKU Departemen Teknologi Informasi Bank D

4.6.1. Langkah Pengolahan Data

Pengolahan data untuk menentukan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D dilakukan sebagai berikut:

a. Menjumlahkan kuadran 3 yang berisi penilaian responden terhadap hubungan antara IRU dengan IKU Departemen Teknologi Informasi Bank D
b. Menjumlahkan kuadran 4 yang berisi penilaian responden terhadap hubungan antara IPU dengan IKU Departemen Teknologi Informasi Bank D

4.6.2. Hasil Pengolahan Data Dan Analisis

Hasil penjumlahan data kuadran 3 dan 4 dengan menggunakan *software* Microsoft Excel 2007 dengan formula "sum(*range)"* dapat dilihat pada tabel 4.12 berikut.

IKU Departemen Teknologi Informasi Bank D yang berkaitan terhadap beberapa IRU dan IPU memperlihatkan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D (Davies dan Haubenstock, 2002). Dengan demikian, konsep manajemen risiko telah sinergis dengan IKU Departemen Teknologi Informasi Bank D yang merupakan pengembangan *Balanced Scorecard* generasi ke-4 Departemen Teknologi Informasi Bank D (Tomonori Tomura, 2006).

IRU dan IPU tersebut dapat menjadi sarana untuk pengembangan *Balanced Scorecard* generasi ke-4 dengan memperlihatkan dukungan manajemen risiko terhadap IKU Departemen Teknologi Informasi Bank D. Hal ini dapat memberikan pemahaman bahwa implementasi ISMS dari ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 dan pengukuran kinerja sebenarnya bukanlah dua hal yang bertolak belakang. Implementasi ISMS juga tidak berarti menambah beban pekerjaan personil Departemen Teknologi Informasi Bank D bila dimanfaatkan untuk mendukung IKU Departemen Teknologi Informasi Bank D. Hal ini dikarenakan IRU dan IPU juga dapat menjadi *early warning* dari pencapaian IKU Departemen Teknologi Informasi Bank D. Sebagai contoh, pada IKU 4.2 yaitu persentase *downtime* sistem aplikasi kritikal dan *email*. Jika pengukuran tingkat kinerja *mainframe* sebagai IRU dan pengukuran tingkat pemeliharaan/ perbaikan aset sebagai IPU menunjukkan performa yang baik, maka persentase *downtime* sistem aplikasi kritikal dan *email* memperlihatkan pencapaian nilai kinerja yang baik.

Selain itu, IRU dan IPU dapat menjadi kandidat IKU. Untuk mengubah IRU dan IPU menjadi IKU, beberapa hal yang dapat dilakukan dan dipertimbangkan oleh Departemen Teknologi Informasi Bank D antara lain:

a. pemilihan IRU dan IPU yang dapat memenuhi kriteria pemilihan indikator
   hal ini berarti IRU dan IPU yang hendak dievaluasi untuk menjadi IKU sebaiknya dapat memenuhi seluruh kriteria pemilihan indikator dengan baik antara lain sejalan dengan sasaran strategis satuan kerja, dapat diukur secara tepat, mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini, bersifat spesifik dan eksplisit, merefleksikan data yang dapat diukur secara periodik, realistis terhadap kondisi organisasi, memiliki batas waktu, dan mudah dimengerti
b. proses validasi dan penentuan level pencapaian
   pada pengembangan selanjutnya, sebaiknya dilakukan penilaian korelasi antara indikator dan risiko, terutama indikator yang baru dibuat. Secara ideal, seharusnya validasi dilakukan dengan metode statistik. Namun, pada sebagian besar kasus, data historis tidak tersedia terutama pada kejadian risiko. Karena biasanya bisnis memiliki pemahaman yang baik dari level target dan batasan kontrol dari risiko, korelasi antara pemicu risiko dan indikator risiko memungkinkan kita untuk menetapkan level target dan batasan kontrol dari metrik. Validasi ini dapat digunakan untuk mengidentifikasi IRU dan/ atau IPU yang dapat mengurangi risiko operasional keamanan informasi dan menggambarkan peningkatan daya dukung terhadap teknologi informasi secara signifikan
c. desain *dashboard*
   dashboard didesain sedemikian rupa untuk melaporkan metrik kritikal bagi manajer, pemilik proses, dan *senior management. Dashboard* biasanya menggunakan gambar dan tabel untuk memperlihatkan risiko secara jelas dan menyeluruh. *Dashboard* dapat digunakan untuk melihat efektivitas IRU dan IPU untuk mengukur dampak dan kontrol risiko, sehingga dapat dilakukan evaluasi dan perbaikan terhadap IRU dan IPU yang sudah tidak efektif.

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
3.1	Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D	a.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal Dalam Pengembangan Aplikasi (6)	a.Pengukuran Pelaksanaan *Update Antivirus* (6)
			b.Pengukuran Tingkat Pemahaman (3)
			c.Pengukuran Efektivitas Training (3)
		b.Pengukuran Tingkat Kinerja *Robotic* (6)	d.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (3)
3.2	Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan	a.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal Dalam Pengembangan Aplikasi (6)	-
		b.Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian (6)	
		c.Pengukuran Tingkat Keakuratan Dok. Teknis Tiap Seksi dan Kelompok (3)	

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6 (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
3.3	Peningkatan pemanfaatan infrastruktur TI yang telah diimpl ementasikan di Bank D	a.Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D (12)	a.Pengukuran Utilisasi Aset (27)
		b.Pengukuran Tingkat Kerusakan *Notebook* (6)	b.Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja (15)
		c.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (6)	
		d.Pengukuran Tingkat Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D (6)	c.Pengukuran Keefektifan Penanganan Insiden / Event (9)
		e.Pengukuran Tingkat Kinerja *Robotic* (6)	d.Pengukuran *Form* Peminjaman Aset (6)
		f.Pengukuran Tingkat Kinerja PC Teleks (6)	e.Pengukuran Pelaksanaan *Update Antivirus* (3)
		g.Pengukuran Tingkat Kinerja *Mainframe* (6)	f.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (6)
		h.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	
		i.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (3)	
		j.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal Dalam Pengembangan Aplikasi (3)	

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6 (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
4.1	Persentase *downtime* sistem aplikasi kritikal dan *e-mail*	a.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (15)	a.Pengukuran Utilisasi Aset (15)
		b.Pengukuran Tingkat Kinerja *Mainframe* (12)	b.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (12)
		c.Pengukuran Tingkat Gangguan AC (9)	c.Pengukuran Pelaksanaan *Update Antivirus* (6)
		d.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (6)	d.Pengukuran Keefektifan Penanganan Insiden / *Event* (6)
		e.Pengukuran Tingkat Kinerja *Robotic* (6)	e.Pengukuran *Form* Peminjaman Aset (6)
		f.Pengukuran Tingkat Kerusakan *Thermal Control* (6)	f.Pengukuran Audit *Security Log* (3)
		g.Pengukuran Tingkat Ketersediaan *Thermal Control* (6)	g.Pengukuran Kesesuaian *User Account* (3)
4.2	Persentase *downtime* jaringan Bank D-NET	a.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (9)	a.Pengukuran Utilisasi Aset (21)
		b.Pengukuran Tingkat Gangguan AC (9)	b.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (15)
		c.Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D (6)	c.Pengukuran Keefektifan Penanganan Insiden / Event (12)

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6 (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
4.2	Persentase *downtime* jaringan Bank D-NET	d.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (6)	d.Pengukuran Kesesuaian *User Account* (9)
		e.Pengukuran Tingkat Kinerja *Mainframe* (6)	e.Pengukuran *Form* Peminjaman Aset (6)
		f.Pengukuran Tingkat Kerusakan *Thermal Control* (6)	f.Pengukuran Audit *Security Log* (6)
		g.Pengukuran Tingkat Ketersediaan *Thermal Control* (6)	g.Pengukuran *Form* Pengiriman *Tape Backup* (6)
4.3	Jumlah keberhasilan simulasi aplikasi kritikal	a.Pengukuran Tingkat Kinerja *Mainframe* (12)	-
		b.Pengukuran Tingkat Kinerja *Robotic* (6)	
		c.Pengukuran Tingkat Keakuratan Dok. Teknis Tiap Seksi dan Kelompok (6)	
		d.Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian (6)	
		e.Pengukuran Tingkat Kehilangan Tape / Catridge hasil backup data yang akan dikirim ke DRC	
5.1	Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti	a.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (21)	a.Pengukuran Keefektifan Penanganan Insiden / *Event* (18)

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6 (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
5.1	Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti	b.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (18)	b.Pengukuran Kesesuaian *User Account* (15)
		c.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi (15)	c.Pengukuran Pelaksanaan *Update Antivirus* (12)
		d.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (12)	d.Pengukuran Audit *Security Log* (6)
		e.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (12)	e.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (3)
		f.Pengukuran Tingkat Kerusakan *Notebook* (9)	f.Pengukuran *Form* Pengiriman *Tape Backup* (3)
		g.Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D (6)	g.Pengukuran Utilisasi Aset (3)
5.2	Maksimum waktu penanggulangan serangan virus yang menyebar secara massal	a.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (24)	a.Pengukuran Keefektifan Penanganan Insiden / *Event* (18)
		b.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (9)	b.Pengukuran Pelaksanaan *Update Antivirus* (9)

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6 (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
5.2	Maksimum waktu penanggulangan serangan virus yang menyebar secara massal	c.Pengukuran Tingkat Kinerja PC Teleks (3)	c.Pengukuran Efektivitas *Training* (3)
			d.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (3)
			e.Pengukuran Audit *Security Log* (3)
5.3	Indeks hasil *assessment* atas kecukupan dan efektivitas ISMS	a.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (18)	a.Pengukuran Pelaksanaan *Update Antivirus* (24)
		b.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (15)	b.Pengukuran Kelengkapan dan Kebenaran Data pada Database Asset (21)
		c.Pengukuran Tingkat Kerusakan *Notebook* (9)	c.Pengukuran Keefektifan Penanganan Insiden / *Event* (21)
		d.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi (9)	d.Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu (21)
		e.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (9)	e.Pengukuran Tingkat Pemahaman (21)
		f.Pengukuran Tingkat Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D (9)	f.Pengukuran Efektivitas *Training* (21)

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6 (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
5.3	Indeks hasil *assessment* atas kecukupan dan efektivitas ISMS	g.Pengukuran Tingkat Gangguan AC (9)	g.Pengukuran Kesesuaian *User Account* (21)
		h.Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D (6)	h.Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja (15)
		i.Pengukuran Tingkat Pemanfaatan R.Pelatihan (6)	i.Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja (15)
		j.Pengukuran Tingkat Keakuratan Dok. Pembebanan Anggaran Pelaksanaan SOSA (6)	j.Pengukuran *Form* Peminjaman Aset (15)
			k.Pengukuran Audit *Security Log* (15)
		k.Pengukuran Tingkat Keakuratan Dok. Pengadaan Kunci Telegram BD (6)	l.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (9)
		l.Pengukuran Tingkat Keakuratan Dok. PKAT (6)	m.Pengukuran *Form* Pengiriman *Tape Backup* (9)
		m.Pengukuran Tingkat Keakuratan Data Unit Kerja Yang Telah Diolah (6)	n.Pengukuran Utilisasi Aset (12)
		n.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	
		o.Pengukuran Tingkat Kerusakan *Thermal Control* (6)	
		p.Pengukuran Tingkat Ketersediaan *Thermal Control* (6)	
		q.Pengukuran Tingkat Kehilangan *Tape / Catridge* hasil backup data yang akan dikirim ke DRC (3)	

Tabel 4.12. Hasil Penjumlahan Kuadran 5 dan 6 (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
6.1	Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil *mapping*	a.Pengukuran Tingkat Kerusakan *Notebook* (9)	a.Pengukuran Tingkat Pemahaman (6)
		b.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (9)	b.Pengukuran Kelengkapan dan Kebenaran Data pada Database Aset (3)
		c.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	
6.2	Peningkatan pemahaman peserta setelah sosialisasi	a.Pengukuran Tingkat Kerusakan *Notebook* (18)	a.Pengukuran Kelengkapan dan Kebenaran Data pada Database Asset (9)
		b.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (15)	b.Pengukuran Pelaksanaan *Update Antivirus* (9)
		c.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (6)	c.Pengukuran Keefektifan Penanganan Insiden / *Event* (9)
		d.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (6)	d.Pengukuran Tingkat Pemahaman (6)
		e.Pengukuran Tingkat Keakuratan Dok. Pembebanan Anggaran Pelaksanaan SOSA (6)	e.Pengukuran Efektivitas *Training* (3)
		f.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	

5. PENUTUP

5.1. Kesimpulan

Penelitian ini bertujuan mendapatkan metode integrasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* generasi ke-4. Dengan demikian, penelitian ini lebih membahas mengenai metode pengembangan, sedangkan hasilnya merupakan implikasi dari aplikasi metode tersebut. Metode integrasi ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 ke dalam *Balanced Scorecard* Departemen Teknologi Informasi Bank D untuk menjadi *Balanced Scorecard* generasi ke-4 yaitu:

a. tiap proses pengembangan menggunakan penilaian para ahli Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D dan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005.
b. penentuan kriteria pemilihan risiko yang menggunakan skala *Likert* dalam penilaian. Kriteria pemilihan risiko digunakan dalam menyeleksi risiko dari hasil *risk assessment*, sedangkan kriteria pemilihan indikator digunakan untuk melihat kemampuan Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) sebagai metrik
c. penentuan prioritas kriteria pemilihan indikator dengan membobotkan kriteria pemilihan indikator (IRU dan IPU) berdasarkan tingkat kepentingan dengan perbandingan berpasangan pada metode *Analytical Hierarchy Process* (AHP)
d. langkah penentuan IRU dan IPU dari tiap risiko menggunakan matriks prioritas memiliki input dari keempat langkah pada ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005
e. matriks kontrol risiko merupakan persyaratan yang dibutuhkan dalam pengembangan *Balanced Scorecard* yang berasal dari hasil *risk assessment* Bagian Kebijakan, Bagian Operasional, dan Bagian Administrasi Departemen Teknologi Informasi Bank D serta hasil penentuan IRU dan IPU

f. penentuan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D dengan bantuan matriks prioritas merupakan dasar untuk mengidentifikasi dan menilai dukungan dari ISO/ IEC 17799:2005 dan ISO/IEC 27001:2005 terhadap IKU dari perspektif proses bisnis internal serta merupakan pengembangan *Balanced Scorecard* generasi ke-4 Departemen Teknologi Informasi Bank D.

Adapun hasil integrasi ISO/ IEC 17799:2005 dan ISO/IEC 27001:2005 ke dalam *Balanced Scorecard* menghasilkan IRU dan IPU yang bermanfaat antara lain untuk:

a. memperlihatkan hubungan antara IRU dan IPU dengan IKU Departemen Teknologi Informasi Bank D, yang merupakan pengembangan *Balanced Scorecard* generasi ke-4 Departemen Teknologi Informasi Bank D
b. memperlihatkan dukungan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 terhadap IKU Departemen Teknologi Informasi Bank D
c. menjadi *early warning* dari pencapaian IKU Departemen Teknologi Informasi Bank D sehingga memberikan pemahaman bahwa implementasi ISMS dapat meningkatkan daya dukung teknologi informasi Departemen Teknologi Informasi Bank D
d. menjadi kandidat IKU, dengan beberapa hal yang perlu dilakukan dan dipertimbangkan oleh Departemen Teknologi Informasi Bank D antara lain pemilihan IRU dan IPU yang dapat memenuhi kriteria pemilihan indikator, proses validasi dan penentuan level pencapaian, serta desain *dashboard* untuk melihat efektivitas IRU dan IPU.

5.2. Saran

Pengembangan *Balanced Scorecard* generasi ke-4 Departemen Teknologi Informasi Bank D dari perspektif proses bisnis internal dapat dikembangkan lebih lanjut meliputi seluruh perspektif *Balanced Scorecard*. Untuk itu, direkomendasikan penggunaan pemilihan ahli dari IKU Departemen Teknologi Informasi Bank D serta ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 dan menggunakan kriteria pemilihan

risiko dan indikator (IRU dan IPU) serta bobotnya pada penelitian ini atau mengevaluasi kembali masing-masing kriteria. Hal ini dimaksudkan agar penelitian selanjutnya dapat menjadi lebih mudah dan terarah mengingat pengembangan ini sangat mungkin untuk diimplementasikan pada Departemen Teknologi Informasi Bank D.

DAFTAR REFERENSI

Bandyopadhyay, Kakoli et al. (1999). A framework for integrated risk management in information technology. *Management Decision*, vol. 37, no.5, hal. 437.

Basel Committee on Banking Supervision. (2001). The internal rating – based approach (supporting document to the new basel capital accord), *Consultative Document.*

Brenner, Joel. (2007). ISO 27001: risk management and compliance. *Risk Management* ABI/INFORM Global, 54, hal. 24

Chandra, Christine. (2001). *Perancangan Metode Pemilihan Indikator: Studi Kasus Anak Perusahaan Pertamina*. Departemen Teknik Industri FT UI

Cheng, Eddy W.L. & Heng Li. (2001). *Analytic hierarchy process, an approach to determine measures for business success*. Measuring Business Excellence, vol.5, no. 3.

Crouhy, Michel, Galai, Dan, & Mark, Robert. (2001). *Risk Management*. McGraw-Hill.

Davies, Jonathan, $ Haubenstock, Michael. (2002). *Building effective indicators to monitor operational risk.* The RMA Journal.

Dube, D.P. (2005). *Information System Audit and Assurance,* New Delhi: Tata Mcgraw-Hill Publishing Company Ltd.

Epstein, Marc J. & Rejc, Adriana. (2005). *How to measure and improve the value of IT*. Strategic Finance.

Halim, Gunawan. (2001). Perbandingan Metode-Metode Pengurutan (rating) Pendukung Keputusan: Studi Kasus Metode Terpilih Pada PT Jasa Marga, Skripsi S1, Fakultas Teknik Universitas Indonesia.

Hansen, Don R., Mowen, Maryanne M. (2000), *Management Accounting* (5th ed.), Cincinati, Ohio : South Western College Publishing.

Hoffman, D. (2002). *Managing Operational Risk.* Canada: John Wiley and Sons, Inc.

Immaneni, Aravind, Mastro, Chris, & Haubenstock, Michael. (2004). *A structured building key risk*. Operational Risk: A Special Edition of *The RMA Journal*.

ISO/IEC/TMB SAG-Security Secretariat. (2005). *ISO/IEC 27001:2005, Information technology – Security techniques -- Information security management systems – Requirements.* Geneva: ISO/IEC/TMB SAG-Security Members.

IT Governance Institute. (2004). *Putting COSO's theory into practice.* IT Control Objectives for Sarbanes-Oxley. The Institute Of Internal Auditors.

John Simon, Steven. (2005). *Balanced Scorecard: A Tool to Improve IS Department Planning and Evaluation.* Journal of Information Technology Case and Application Research.

Kaplan, Robert S., & Norton, David P. (1996). *Balanced Scorecard: Translating Strategy Into action.* Boston, Massachusetts: Harvard Business School Press.

Kaplan, Robert S., & Norton, David P. (2004). *Strategy Maps: Converting Intangible Assets Into Tangible Outcomes.* Boston, Massachusetts: Harvard Business School Press.

Lam, James et al. (2006). *Developing key risk indicators and ERM reporting*. USA Emerging best practices. Inc. Cognos.

Ow, Patrick PC. (n.d.) Measuring Performance through KPIs.

Pöyhönen, Mari. & Hämäläinen, Raimo P. (1997). On the convergence of multiattribute weighting methods. Helsinki: Systems Analysis Laboratory, Helsinki University of Technology.

Saaty, Thomas L. (1999). Decision making for Leaders - the Analytic Hierarchy Process for Decisions in a Complex World. Pittsburgh: RWS Publications.

Saaty, Thomas L. (1999). The Seven Pillars of the Analytic Hierarchy Process. Kobe: Proceedings of the Fourth International Symposium on the Analytic Hierarchy Process,

Tomura, Tomonori. (2006). *Beyond sarbanes-oxley: improving corporate value with a 4th generation balanced scorecard approach.* www.bptrends.com.

Trochim, W.M.K. (29 Juni 2000). *General Issues in Scaling*. 30 Maret 2008. http://trochim.human.cornell.edu/kb/scalgen.htm.

Trochim, W.M.K. (29 Juni 2000). *Likert Scaling*. 30 Maret 2008. http://trochim.human.cornell.edu/kb/scallik.htm.

Vaughan, Emmet J. (1997). *Risk Management*. Canada: John Wiley & Sons.

Yuwono, Sony, Sukarno, Edy & Ichsan, Muhamad. (2003). *Petunjuk Praktis Penyusunan Balanced Scorecard*. Jakarta: PT Gramedia Pustaka Utama.

Lampiran 1: Data Diri Responden

1. Ahli 1

Nama	Noviadi S. Miraza
Direktorat/ Bagian/ Seksi	DTI/ Tim SKTI/ Bidang Roadmap dan Mitra Strategis
Lama Bekerja di Bank D	14 tahun
Pengalaman dalam Implementasi IKU DTI Bank D	2 tahun sebagai IKU Manajer
Pengalaman dalam Implementasi ISO/ IEC 27001: 2005	2 tahun sebagai *security officer*
Latar Belakang Pendidikan (Gelar, Jurusan, Institusi Pendidikan)	S1 Teknik Komputer Universitas Gunadarma

2. Ahli 2

Nama	Dwi Kurniawan
Direktorat/ Bagian/ Seksi	DTI/ Tim SKTI/ Bidang Pengawasan Kualitas dan Kebijakan Pengamanan Teknologi Informasi
Lama Bekerja di Bank D	14 tahun
Pengalaman dalam Implementasi IKU DTI Bank D	Penanggung jawab pencapaian beberapa target dari IKU DTI
Pengalaman dalam Implementasi ISO/ IEC 27001: 2005	2 tahun sebagai *Security officer*
Latar Belakang Pendidikan (Gelar, Jurusan, Institusi Pendidikan)	S1 Teknik Komputer Institut Teknologi Surabaya S2 MBA George Washington University

3. Ahli 3

Nama	Djarot Sumantri
Direktorat/ Bagian/ Seksi	DTI/ Bagian PTTI/ Seksi Pengamanan Teknologi Informasi
Lama Bekerja di Bank D	11 tahun
Pengalaman dalam Implementasi IKU DTI Bank D	3 tahun sebagai IKU Manajer
Pengalaman dalam Implementasi ISO/ IEC 27001: 2005	1 tahun sebagai *security officer*
Latar Belakang Pendidikan (Gelar, Jurusan, Institusi Pendidikan)	S1 Telekomunikasi Universitas Trisakti S2 MMIS Universitas Bina Nusantara

4. Ahli 4

Nama	Hadi Cahyono
Direktorat/ Bagian/ Seksi	*Project Leader* Proyek Perluasan Lingkup Sertifikasi ISO 27001
Lama Bekerja di Bank D	-
Pengalaman dalam Implementasi IKU DTI Bank D	-
Pengalaman dalam Implementasi ISO/ IEC 27001: 2005	1 tahun
Latar Belakang Pendidikan (Gelar, Jurusan, Institusi Pendidikan)	S1 Teknik Industri Universitas Indonesia

Lampiran 2: Form Kuesioner Tahap I

FORM KUESIONER TAHAP I
PENENTUAN KRITERIA PEMILIHAN RISIKO DAN INDIKATOR UNTUK PENGEMBANGAN *BALANCED SCORECARD* GENERASI KE-4 DEPARTEMEN TEKNOLOGI INFORMASI BANK D BERDASARKAN ISO/ IEC 17799:2005 DAN ISO/ IEC 27001:2005

DISTYA TARWORO ENDRI
0404070247

DEPARTEMEN TEKNIK INDUSTRI
FAKULTAS TEKNIK UNIVERSITAS INDONESIA
MEI 2008

Selamat Pagi / Siang / Sore,

Bapak/Ibu yang terhormat,

Saya, Distya Tarworo Endri, adalah mahasiswi Teknik Industri Universitas Indonesia yang sedang melakukan penelitian dalam rangka penyelesaian tugas akhir yaitu **"Pengembangan *Balanced Scorecard* Generasi Ke-4 Departemen Teknologi Informasi Bank D Berdasarkan ISO/ IEC 17799:2005 Dan ISO/ IEC 27001:2005 ".** Sampel yang digunakan adalah Bagian Kebijaka, Bagian Operasional, dan Bagian Administrasi Bank D. Hasil dari kuesioner ini akan digunakan sebagai bahan penentuan kriteria pemilihan risiko, Indikator Risiko Utama (IRU), dan Indikator Pengendalian Utama (IPU) dari Manajemen Risiko yang akan dihubungkan dengan Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D. Oleh karena itu, saya amat mengharapkan bantuan dari Bapak/ Ibu untuk menjawab pertanyaan sesuai pendapat Bapak/ Ibu. Pada kuesioner ini akan diberikan penjelasan mengenai *Balanced Scorecard* Generasi ke-4, metode pengumpulan dan pengolahan data, contoh hasil penelitian, petunjuk pengisian, daftar pertanyaan kuesioner, dan data diri responden.

Atas kerja sama serta bantuan Bapak/ Ibu, saya ucapkan terima kasih.

I. Penjelasan Balanced Scorecard Generasi Ke-4

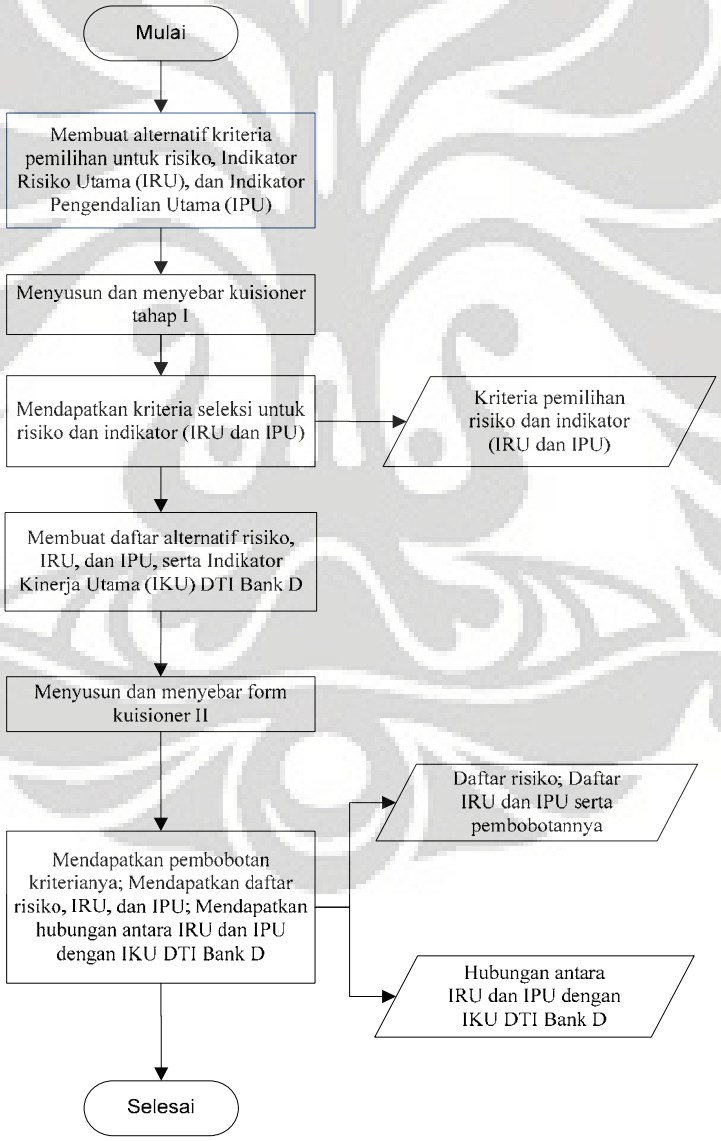
Menurut Tomonori Tomura (2006, hal. 1), *Balanced Scorecard* generasi ke-4 "*Beyond Sarbanes Oxley Tool*" *(balancing the profit earning strategy and the internal control strategy: Balanced Scorecard for SOX)* merupakan perbaikan dari *Balanced Scorecard* generasi sebelumnya. *Balanced Scorecard* terdahulu, antara lain:

1. Generasi pertama *"Multimodal Assessment Tool"* yaitu penambahan perspektif nonfinansial terhadap pengukuran kinerja – *learning and growth, internal business process*, dan *customers* – untuk merepresentasikan *stakeholder* mayor dalam bisnis.
2. Generasi ke-dua "*Top Down Management Tool*" yang merupakan permulaan dari konsep tujuan strategis dimana terdapat penambahan esensi dari strategi organisasi ke dalam tiap perspektif dari BSC pada generasi pertama.
3. Generasi ke-tiga yaitu "*Knowledge-creating and Strategic Communication Tool*" *(based on strategy map)* dimana dibuat *strategy map* yang dapat memberi gambaran tujuan kritikal organisasi dan hubungan antar *Key Performance Indicator* dari tiap perspektif.
4. Dalam hubungannya dengan *Sarbanes-Oxley Act, Balanced Scorecard* generasi ke-4 menambahkan pentingnya kontrol internal dalam sebuah organisasi. Kelebihannya dibandingkan *Balanced Scorecard* generasi sebelumnya antara lain meningkatkan

kontrol internal, pemahaman lebih lanjut terhadap entitas dari proses, dapat mendeteksi risiko pada proses internal lebih dini, sebagai alat bantu dalam membuat program audit internal yang efektif, meningkatkan transparansi dan akuntabilitas, memperlihatkan *gap* antara target dan kondisi saat ini pada proses internal, meningkatkan nilai organisasi, dan memastikan kontrol proses internal yang mudah dilacak serta dapat diperbaiki dengan *Kaizen* (perbaikan secara terus-menerus) pada periode selanjutnya.

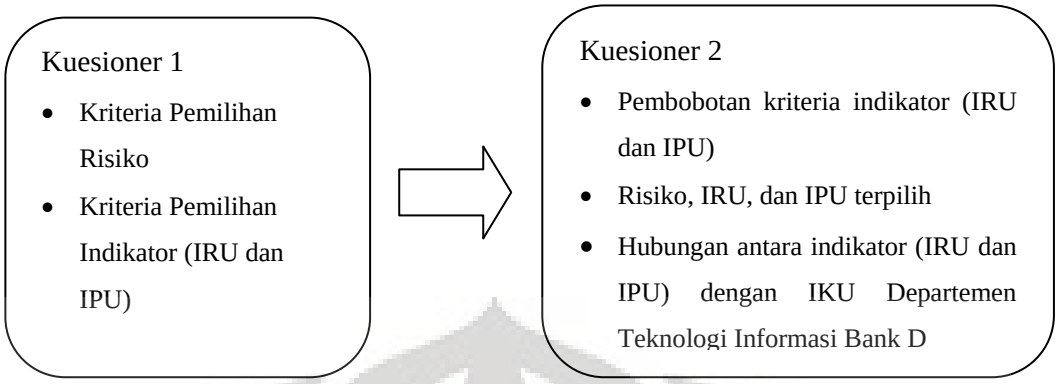
II. Metode Pengumpulan dan Pengolahan Data

Gambar 1 adalah metode pengumpulan dan pengolahan data yang akan dilakukan.



Gambar 1. Metode Penelitian

Penggambaran alur hasil data tiap kuesioner dijelaskan oleh gambar 2 sebagai berikut.



Gambar 2. Alur Hasil Data

III. Contoh Hasil Penelitian

Contoh di bawah ini dibuat untuk memberikan gambaran terhadap keseluruhan alur penelitian tanpa bermaksud mengarahkan jawaban dari pertanyaan wawancara. Asumsi yang digunakan dalam model ini antara lain:

1. Kriteria Penentuan Risiko
   a. Risiko dapat terjadi pada aset kritikal
   b. Hasil *risk assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol
   c. Risiko memiliki hubungan logis dengan IKU Departemen Teknologi Informasi Bank D yang berhubungan dengan proses bisnis internal Bank D yaitu mencakup IKU yang berada pada sasaran strategis no.3, 4, 5, dan 6.
2. Kriteria Penentuan Indikator (IRU dan IPU)
   a. *Specific*
   b. *Measurable*
   c. *Attainable*
   d. *Realistic*
   e. *Time Bound.*

Dengan menggunakan kriteria di atas, maka contoh hasil penelitian yaitu:

1. Risiko: **"Tidak ada aplikasi pengamanan sistem informasi (AntiVirus, Antimalware, Firewall, dll) menyebabkan informasi *softcopy* data dari unit kerja yang telah diolah tidak tersedia karena terserang virus"**.
2. Indikator Risiko Utama (IRU): **"Pengukuran Jumlah Serangan virus"**
3. Indikator Pengendalian Utama (IPU): **"Pengukuran Pelaksanaan *Update Antivirus"***
4. Indikator Kinerja Utama yang berhubungan: IKU 5.2 **"Maksimum waktu penanggulangan serangan virus yang menyebar secara massal**"

Penjelasan lebih detil dari contoh tersebut antara lain dapat dilihat pada uraian di bawah ini.

1. Risiko yang dipilih: **"Tidak ada aplikasi pengamanan sistem informasi (AntiVirus, Antimalware, Firewall, dll) menyebabkan informasi *softcopy* data dari unit kerja yang telah diolah tidak tersedia karena terserang virus"**.
2. Indikator Risiko Utama (IRU) yang dipilih: **"Pengukuran Jumlah Serangan virus"**

Metric	Pengukuran Jumlah Serangan Virus
Tujuan:	Untuk mengukur PC / Notebook Personil Unit Kerja, Server, Mainframe, dan Tandem yang telah terkena virus.
Ruang Lingkup:	Pengukuran ini berlaku untuk PC dan *notebook* Unit Kerja.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.10.4.1 Controls against malicious code ISO / IEC 27001:2005.
Metode:	• Menghitung jumlah PC dan *notebook* Unit Kerja Server,Mainframe, Tandem yang terserang virus ….....(a) • Menghitung jumlah PC dan Notebook / Server,Mainframe, Tandem yang digunakan oleh Unit Kerja ……....(b) • Formula pengukuran = (a / b) * 100%
Frekuensi	1 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	• Menghitung jumlah PC dan *notebook* / Server,Mainframe, Tandem yang terkena virus. • Menghitung presentase jumlah PC dan *notebook* / Server,Mainframe, Tandem secara keseluruhan.
Indikator	• 100% : Seluruh PC dan *notebook* / Server, Mainframe, Tandem tidak terserang virus • 97 – 99% : Diperlukan tindakan perbaikan segera untuk Mengatasi virus di PC dan Notebook Personil Unit Kerja / Server,Mainframe, Tandem. • < 97% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi berkoordinasi dengan Unit Kerja terkait.

3. Indikator Pengendalian Utama (IPU): **"Pengukuran Pelaksanaan *Update Antivirus*"**

Metric	Pengukuran Pelaksanaan *Update Antivirus*
Tujuan:	Untuk mengukur PC / Notebook Personil Unit Kerja, Server, Mainframe, dan Tandem yang telah ter-*update* antivirus yang terbaru.

Metric	Pengukuran Pelaksanaan *Update Antivirus*
Ruang Lingkup:	Pengukuran ini berlaku untuk PC dan *notebook* Unit Kerja.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.10.4.1 Controls against malicious code ISO / IEC 27001:2005.
Metode:	• Menghitung jumlah PC dan *notebook* Unit Kerja / Server,Mainframe, Tandem yang memiliki *updated Antivirus*.....(a) • Menghitung jumlah PC dan Notebook / Server,Mainframe, Tandem yang digunakan oleh Unit Kerja.....(b) • Formula pengukuran = (a / b) * 100%
Frekuensi	1 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	• Status antivirus pada PC dan *notebook* / Server,Mainframe, Tandem milik Unit Kerja dapat dilihat dari laporan McAffee EPO periode yang dihasilkan oleh PTTI. • Menghitung jumlah PC dan *notebook* / Server,Mainframe, Tandem dengan *antivirus* paling *update*. • Menghitung presentase jumlah PC dan *notebook* / Server,Mainframe, Tandem dengan *antivirus* paling *update* dengan jumlah PC dan *notebook* keseluruhan.
Indikator	• 100% : Seluruh PC dan *notebook* / Server, Mainframe, Tandem telah efektif ter-update antivirus terbaru • 97 – 99% : Diperlukan tindakan perbaikan segera untuk meng-*update* antivirus di PC dan Notebook Personil Unit Kerja / Server,Mainframe, Tandem. • < 97% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut yang meliputi berkoordinasi dengan Unit Kerja terkait.

4. Hubungan dengan Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D: IKU 5.2 **"Maksimum waktu penanggulangan serangan virus yang menyebar secara massal"**. Dalam hal ini, akan dilakukan pengumpulan dan pengolahan data tingkat lanjut untuk mengetahui seberapa erat kaitan antara IRU dan IPU dengan IKU tersebut dan perlu atau tidaknya mengevaluasi IKU yang telah ada.

IV. Petunjuk Pengisian

Bapak/Ibu dapat **melingkari nilai dari 1 – 5 (Skala Likert)** untuk menilai persetujuan terhadap kriteria yang sesuai untuk pemilihan risiko dan Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU). Selain itu, Bapak. Ibu **dapat menambahkan kriteria pada kolom yang telah disediakan**. Tabel 1 berikut memuat pengertian setiap nilai dari skala Likert.

Tabel 1 Skala Likert yang digunakan pada Kuesioner Tahap 1

Skala Likert	Pengertian
5	Sangat setuju Kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
4	Setuju Kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
3	Ragu-ragu/ netral apakah setuju atau tidak Kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
2	Tidak setuju Kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih
1	Sangat tidak setuju Kriteria tersebut digunakan untuk menilai risiko dan indikator yang akan dipilih

V. Daftar Pertanyaan Kuesioner

1. Kriteria Pemilihan Risiko

No.	Kriteria	Nilai				
1	Risiko terjadi pada aset kritikal	1	2	3	4	5
2	Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol	1	2	3	4	5
3	Memiliki hubungan logis dengan Indikator Kinerja Utama Departemen Teknologi Informasi Bank D	1	2	3	4	5
		1	2	3	4	5
		1	2	3	4	5
		1	2	3	4	5
		1	2	3	4	5
		1	2	3	4	5

Keterangan Alternatif Kriteria Pemilihan Risiko:

1. Risiko terjadi pada aset kritikal

   Risiko yang dipilih terjadi pada aset kritikal perusahaan sesuai dengan kesepakatan pegawai Departemen Teknologi Informasi Bank D. Hal ini sesuai dengan langkah identifikasi risiko pada ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005.

2. Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol

   Hasil *risk assessment* berdasarkan ISO/ IEC 17799:2005 dan ISO/ IEC 27001:2005 menyatakan bahwa risiko belum memiliki tingkat pengendalian yang kuat dan/ atau dirasa perlu untuk mengkontrol risiko tersebut dengan pengendalian tambahan.

3. Memiliki hubungan logis dengan Indikator Kinerja Utama Departemen Teknologi Informasi Bank D

   Risiko harus memiliki hubungan logis dalam kaitannya dengan pelaksanaan tugas pokok Departemen Teknologi Informasi Bank D yang tertuang dalam penilaian kinerja yaitu IKU Departemen Teknologi Informasi Bank D.

2. Kriteria Pemilihan Indikator (IRU dan IPU)

No.	Kriteria	Nilai				
1	Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	1	2	3	4	5
2	Dapat diukur secara tepat	1	2	3	4	5
3	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	1	2	3	4	5
4	Bersifat spesifik dan eksplisit	1	2	3	4	5
5	Merefleksikan data yang dapat diukur secara periodik	1	2	3	4	5
6	Biaya untuk mengidentifikasi dan memonitor ukuran IKU tidak melebihi nilai yang akan diketahui dari pengukuran tersebut	1	2	3	4	5
7	Realistis terhadap kondisi organisasi	1	2	3	4	5
8	Memiliki batas waktu	1	2	3	4	5
9	Mudah dimengerti	1	2	3	4	5
		1	2	3	4	5
		1	2	3	4	5
		1	2	3	4	5
		1	2	3	4	5

Keterangan Alternatif Kriteria Pemilihan Indikator (IRU dan IPU):

1. Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol

   Indikator dapat mendukung sasaran strategis dari Departemen Teknologi Informasi Bank D yang telah ada dan pelaksanaannya dapat dikontrol.
2. Dapat diukur secara tepat

   Indikator dapat diekspresikan dengan penilaian kuantitatif sehingga dapat menggambarkan upaya pengukuran dampak dan pengendalian terhadap risiko secara tepat.
3. Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini

   Indikator perlu menggambarkan proses perbaikan antara satu periode pengukuran dengan periode pengukuran selanjutnya, untuk melihat ada atau tidaknya perbaikan pencapaian target pengukuran oleh perusahaan (*continuous improvement*).
4. Bersifat spesifik dan eksplisit

   Indikator bersifat spesifik dan tidak mengandung ambiguitas dalam pemahamannya di kemudian hari sehingga jelas yang diukur.
5. Merefleksikan data yang dapat diukur secara periodik

   Data yang diukur dalam indikator tersebut dapat tersedia dan dapat diukur secara periodik untuk memperlihatkan usaha mitigasi risiko secara berkala.
6. Biaya untuk mengidentifikasi dan memonitor ukuran IKU tidak melebihi nilai yang akan diketahui dari pengukuran tersebut

   Indikator bersifat *cost efficient* sehingga nilai manfaatnya melebihi biaya yang harus dikeluarkan untuk mengidentifikasi dan memonitor IKU sehingga tidak terdapat IKU yang tidak banyak memiliki nilai tambah.
7. Realistis terhadap kondisi organisasi

   Indikator dapat disesuaikan dengan kondisi organisasi agar menggambarkan pengukuran secara efektif dan target dari pengukuran dapat dicapai.
8. Memiliki batas waktu

   Indikator memiliki batas waktu pengukuran dan evaluasi.
9. Mudah dimengerti

   Indikator dapat dimengerti oleh Manajer IKU pada khususnya dan setiap pegawai Departemen Teknologi Informasi Bank D pada umumnya.

VI. Data Diri Responden

Nama: _____

Departemen/ Bagian/ Seksi: _____

Lama Bekerja: _____

Pengalaman dalam Implementasi IKU Departemen Teknologi Informasi Bank D:

_____

Pengalaman dalam Implementasi ISO/ IEC 27001: 2005:

_____

Latar Belakang Pendidikan (Gelar, Jurusan, Institusi Pendidikan):

_____

_____

TERIMA KASIH

FORM KUESIONER TAHAP II

PEMBOBOTAN KRITERIA DAN PENENTUAN INDIKATOR RISIKO UTAMA DAN INDIKATOR PENGENDALIAN UTAMA UNTUK PENGEMBANGAN *BALANCED SCORECARD* GENERASI KE-4 DEPARTEMEN TEKNOLOGI INFORMASI BANK D

DISTYA TARWORO ENDRI

0404070247

DEPARTEMEN TEKNIK INDUSTRI

FAKULTAS

MEI 2008

Selamat Pagi / Siang / Sore,

Bapak/Ibu yang terhormat,

Saya, Distya Tarworo Endri, adalah mahasiswi Teknik Industri Universitas Indonesia yang sedang melakukan penelitian dalam rangka penyelesaian tugas akhir yaitu **"Pengembangan *Balanced Scorecard* Generasi Ke-4 Departemen Teknologi Informasi Bank D Berdasarkan ISO/ IEC 27001:2005 ".** Sampel yang digunakan adalah Tim SKTI, Bagian OTI, dan Bagian AdTI Departemen Teknologi Informasi Bank D. Hasil dari kuesioner ini akan digunakan sebagai bahan penentuan hubungan antara Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) dari Manajemen Risiko dengan Indikator Kinerja Utama (IKU) Departemen Teknologi Informasi Bank D. Oleh karena itu, saya amat mengharapkan bantuan dari Bapak/ Ibu untuk menjawab pertanyaan sesuai pendapat Bapak/ Ibu. Pada kuesioner ini akan diberikan penjelasan singkat, petunjuk pengisian, dan daftar pertanyaan kuesioner.

Atas kerja sama serta bantuan Bapak/ Ibu, saya ucapkan terima kasih.

VII. Penjelasan Singkat

Kuesioner pengembangan BSC Generasi ke-4 Tahap II ini merupakan lanjutan dari kuesioner tahap I yang bermaksud menentukan kriteria pemilihan risiko dan indikator. Dari kuesioner tahap I dihasilkan daftar kriteria pemilihan risiko dan indikator dimana terdiri dari 2 kriteria pemilihan risiko dan 9 kriteria pemilihan indikator seperti terlihat pada tabel 1 dan tabel 2. Kriteria yang telah didapat ini akan menjadi dasar pemilihan risiko dan indikator (IRU dan IPU).

Tabel 1. Daftar Kriteria Pemilihan Risiko

No.	Kriteria Pemilihan Risiko
1	Risiko terjadi pada aset kritikal
2	Hasil *Risk Assesment* menyatakan bahwa risiko yang bersangkutan harus dikontrol

Tabel 2. Daftar Kriteria Pemilihan Indikator

No.	Kriteria Pemilihan Indikator
1	Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol
2	Dapat diukur secara tepat
3	Mampu menggambarkan
4	Bersifat spesifik dan eksplisit
5	Merefleksikan data yang dapat diukur secara periodik
6	Dapat dicapai oleh organisasi
7	Realistis terhadap kondisi organisasi
8	Memiliki batas waktu
9	Mudah dimengerti

Lampiran 3: Form Kuesioner Tahap II (Sambungan)

Kuesioner tahap II terdiri dari 2 bagian yaitu pembobotan kriteria untuk indikator dan penentuan Indikator Risiko Utama dan Indikator Pengendalian Utama dari setiap risiko dan hubungan mereka dengan Indikator Kinerja Utama Bank D. Kriteria risiko yang terpilih tidak perlu lagi dibobotkan karena merupakan kriteria yang tidak memerlukan penilaian tetapi merupakan kriteria yang dapat menjadi dasar seleksi risiko.

Pembobotan kriteria menggunakan *pairwaise comparison* untuk memudahkan pengisian dan penilaian dari setiap tingkat kepentingan kriteria. Penentuan Indikator Risiko Utama dan Indikator Pengendalian Utama dari setiap risiko dan hubungan mereka dengan Indikator Kinerja Utama Bank D akan menggunakan matriks prioritas.

Dari kuesioner ini didapatkan bobot dari tiap kriteria pemilihan indikator yang terpilih, Indikator Risiko Utama dan Indikator Pengendalian Utama dari setiap risiko dan hubungan mereka dengan Indikator Kinerja Utama Bank D.

VIII. Petunjuk Pengisian

2.1 Bagian 1

Untuk Kuesioner tahap II bagian 1, Bapak/Ibu diminta untuk membobotkan kriteria risiko dan indikator (Indikator Risiko Utama dan Indikator Pengendalian Utama) dengan **membandingkan kepentingan antara satu kriteria dengan kriteria lainnya dengan membulatkan angka yang Bapak/ Ibu setujui**. Dalam melakukan pembandingan tersebut, diberikan **skala 1 – 9,** dimana definisi dari tiap skala tersebut adalah :

1 : Kedua elemen sama penting

3 : Elemen yang satu sedikit lebih penting daripada elemen lainnya

5 : Elemen yang satu lebih penting dibanding elemen lainnya

7 : Satu elemen jelas lebih mutlak dibandingkan elemen lainnya

9 : Satu elemen mutlak penting daripada elemen lainnya

2,4,6,8 : Nilai antara dua nilai pertimbangan yang berdekatan

Form Kuesioner Tahap II

Responden memilih 4, berarti menilai bahwa kriteria "realistis terhadap kondisi organisasi" lebih penting dibanding "dapat dicapai oleh organisasi"

Contoh:

No	Kriteria	Penilaian																	Kriteria
1	Dapat dicapai oleh organisasi	9	8	7	6	5	4	3	2	1	2	3	**4**	5	6	7	8	9	Realistis terhadap kondisi organisasi
2	Dapat dicapai oleh organisasi	9	8	7	6	5	4	**3**	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
3	Dapat dicapai oleh organisasi	9	8	7	6	5	4	3	2	**1**	2	3	4	5	6	7	8	9	Mudah dimengerti

Responden memilih 1 berarti menilai bahwa criteria "dapat dicapai oleh organisasi" memiliki kepentingan yang sama dengan "mudah dimengerti"

1.2 Bagian 2

Untuk Kuesioner tahap II bagian 1, Bapak/Ibu dapat **memberikan lambang sebagai berikut:**

● **(sangat kuat = 9),** ○ **(sedang = 6),** ▽**(rendah = 3), dan kosongkan bila tidak memiliki hubungan (0).**

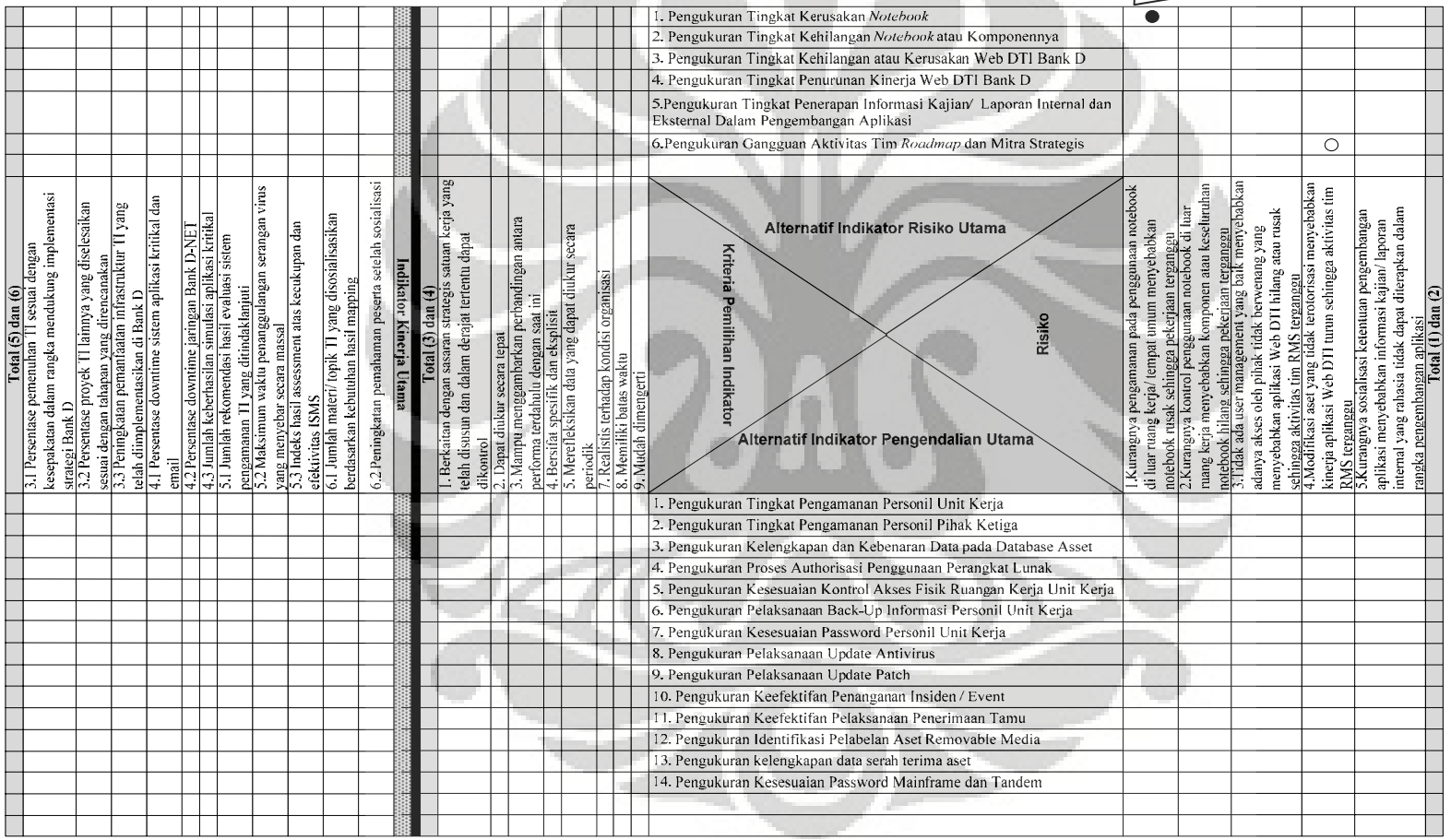
Lambang tersebut akan digunakan untuk menilai keterkaitan dari risiko, usulan Indikator Risiko Utama (IRU), dan Indikator Pengendalian Utama (IPU), dan hubungan mereka dengan Indikator Kinerja Utama Bank D yang akan menggunakan matriks prioritas. Dalam hal ini, **Bapak/ Ibu dapat menambahkan Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) selain dari yang telah diberikan. Indikator tersebut akan dipertimbangkan menjadi Indikator Risiko Utama (IRU) dan Indikator Pengendalian Utama (IPU) setelah meminta pendapat kembali dari responden lain.**

Contoh:

(Halaman Selanjutnya)

Lampiran 3: Form Kuesioner Tahap II (Sambungan)

Lambang ● berarti IRU tersebut merupakan indikator dengan korelasi tinggi untuk mengukur risiko



Universitas Indonesia

IX. Daftar Pertanyaan Kuesioner Bagian 1

Kriteria Pemilihan Indikator (IRU dan IPU)

No	Kriteria	Penilaian																	Kriteria
1	Berkaitan dengan sasaran strategis unit kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Dapat diukur secara tepat
2	Berkaitan dengan sasaran strategis unit kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini
3	Berkaitan dengan sasaran strategis unit kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Bersifat spesifik dan eksplisit
4	Berkaitan dengan sasaran strategis unit kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Merefleksikan data yang dapat diukur secara periodik
5	Berkaitan dengan sasaran strategis unit kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Realistis terhadap kondisi organisasi
6	Berkaitan dengan sasaran strategis unit kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
7	Berkaitan dengan sasaran strategis unit kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti
8	Dapat diukur secara tepat	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat

No	Kriteria	Penilaian																	Kriteria
																			ini
9	Dapat diukur secara tepat	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Bersifat spesifik dan eksplisit
10	Dapat diukur secara tepat	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Merefleksikan data yang dapat diukur secara periodik
11	Dapat diukur secara tepat	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Realistis terhadap kondisi organisasi
12	Dapat diukur secara tepat	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
13	Dapat diukur secara tepat	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti
14	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Bersifat spesifik dan eksplisit
15	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Merefleksikan data yang dapat diukur secara periodik
16	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Realistis terhadap kondisi organisasi
17	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
18	Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti
19	Bersifat spesifik dan eksplisit	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Merefleksikan data yang dapat diukur secara periodik
20	Bersifat spesifik dan eksplisit	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Realistis terhadap kondisi organisasi
21	Bersifat spesifik dan eksplisit	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
22	Bersifat spesifik dan eksplisit	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti

No	Kriteria	Penilaian																	Kriteria
23	Merefleksikan data yang dapat diukur secara periodik	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Realistis terhadap kondisi organisasi
24	Merefleksikan data yang dapat diukur secara periodik	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
25	Merefleksikan data yang dapat diukur secara periodik	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti
26	Dapat dicapai oleh organisasi	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Realistis terhadap kondisi organisasi
27	Dapat dicapai oleh organisasi	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
28	Dapat dicapai oleh organisasi	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti
29	Realistis terhadap kondisi organisasi	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Memiliki batas waktu
30	Realistis terhadap kondisi organisasi	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti
31	Memiliki batas waktu	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Mudah dimengerti

X. Daftar Pertanyaan Kuesioner Bagian 2

Penentuan Indikator Risiko Utama dan Indikator Pengendalian Utama

(Halaman Selanjutnya)

Total (5) dan (6)	Total (3) dan (4)	Kriteria Pemilihan Indikator / Alternatif Indikator Risiko Utama / Risiko / Alternatif Indikator Pengendalian Utama						Total (1) dan (2)
		1. Pengukuran Tingkat Kerusakan *Notebook*						
		2. Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya						
		3. Pengukuran Jumlah Kehilangan atau Kerusakan Web DTI Bank D						
		4. Pengukuran Tingkat Penurunan Kinerja Web DTI Bank D						
		5.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi						
		6.Pengukuran Gangguan Aktivitas Tim *Roadmap* dan Mitra Strategis						
		Kriteria Pemilihan Indikator / Alternatif Indikator Risiko Utama / Risiko / Alternatif Indikator Pengendalian Utama	1.Kurangnya pengamanan pada penggunaan *notebook* di luar ruang kerja/ tempat umum menyebabkan *notebook* rusak sehingga pekerjaan terganggu	2.Kurangnya kontrol penggunaan *notebook* di luar ruang kerja menyebabkan komponen atau keseluruhan *notebook* hilang sehingga pekerjaan terganggu	3.Tidak ada *user management* yang baik menyebabkan adanya akses oleh pihak tidak berwenang yang menyebabkan aplikasi Web DTI hilang atau rusak sehingga aktivitas tim RMS terganggu	4.Modifikasi aset yang tidak terotorisasi menyebabkan kinerja aplikasi Web DTI turun sehingga aktivitas tim RMS terganggu	5.Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan internal yang rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	
3.1 Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D	1. Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	1. Pengukuran Tingkat Pengamanan Personil Unit Kerja						
3.2 Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan	2. Dapat diukur secara tepat	2. Pengukuran Tingkat Pengamanan Personil Pihak Ketiga						
3.3 Peningkatan pemanfaatan infrastruktur TI yang telah diimplementasikan di Bank D	3. Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	3. Pengukuran Kelengkapan dan Kebenaran Data pada *Database* Aset						
4.1 Persentase downtime sistem aplikasi kritikal dan email	4. Bersifat spesifik dan eksplisit	4. Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak						
4.2 Persentase downtime jaringan Bank D-NET	5. Merefleksikan data yang dapat diukur secara periodik	5. Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja						
4.3 Jumlah keberhasilan simulasi aplikasi kritikal	6. Realistis terhadap kondisi organisasi	6. Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja						
5.1 Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti	7. Memiliki batas waktu	7. Pengukuran Kesesuaian *Password* Personil Unit Kerja						
5.2 Maksimum waktu penanggulangan serangan virus yang menyebar secara massal	8. Mudah dimengerti	8. Pengukuran Pelaksanaan *Update Antivirus*						
5.3 Indeks hasil assessment atas kecukupan dan efektivitas ISMS		9. Pengukuran Pelaksanaan *Update Patch*						
6.1 Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil mapping		10. Pengukuran Keefektifan Penanganan Insiden / *Event*						
6.2 Peningkatan pemahaman peserta setelah sosialisasi		11. Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu						
Indikator Kinerja Utama		12. Pengukuran Identifikasi Pelabelan Aset *Removable Media*						
		13. Pengukuran kelengkapan data serah terima aset						
		14. Pengukuran Kesesuaian *Password* Mainframe dan Tandem						

Total (5) dan (6)	Total (3) dan (4)	Alternatif Indikator Risiko Utama / Kriteria Pemilihan Indikator / Risiko / Alternatif Indikator Pengendalian Utama	6.Rusaknya media penyimpanan informasi menyebabkan *softcopy* kajian/ laporan eksternal menjadi tidak ada/ hilang/ tidak akurat saat dibutuhkan	7.Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan eksternal yang rahasia tidak dapat diterapkan dalam pengembangan aplikasi	8.Kurangnya pengamanan fisik r. kerja Direktur dan Deputi Direktur DTI yang menyebabkan akses pihak tak berwenang yang berdampak pada proses otorisasi	9.Kurangnya kontrol hak akses memungkinkan r.kerja Direktur dan Deputi Direktur diakses pihak tak berwenang yang berdampak pada proses authorisasi	10.Belum berjalannya manajemen aset (inventarisasi.kepemilikan, authorisasi penggunaan, pemelihaaraan, penggunaan) dapat menyebabkan r.pelatihan dan asetnya tidak berfungsi maksimal	Total (1) dan (2)
		7.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal						
		8.Pengukuran Tingkat Kehilangan dan Kerusakan Aset pada R.Direktur dan Deputi Direktur						
		9.Pengukuran Tingkat Pemanfaatan R.Pelatihan						
		5.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal Dalam Pengembangan Aplikasi						
3.1 Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D	Indikator Kinerja Utama	1. Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	1. Pengukuran Tingkat Pengamanan Personil Unit Kerja					
3.2 Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan		2. Dapat diukur secara tepat	2. Pengukuran Tingkat Pengamanan Personil Pihak Ketiga					
3.3 Peningkatan pemanfaatan infrastruktur TI yang telah diimplementasikan di Bank D		3. Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	3. Pengukuran Kelengkapan dan Kebenaran Data pada *Database* Aset					
4.1 Persentase downtime sistem aplikasi kritikal dan email		4. Bersifat spesifik dan eksplisit	4. Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak					
4.2 Persentase downtime jaringan Bank D-NET		5. Merefleksikan data yang dapat diukur secara periodik	5. Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja					
4.3 Jumlah keberhasilan simulasi aplikasi kritikal		6. Realistis terhadap kondisi organisasi	6. Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja					
5.1 Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti		7. Memiliki batas waktu	7. Pengukuran Kesesuaian *Password* Personil Unit Kerja					
5.2 Maksimum waktu penanggulangan serangan virus yang menyebar secara massal		8. Mudah dimengerti	8. Pengukuran Pelaksanaan *Update Antivirus*					
5.3 Indeks hasil assessment atas kecukupan dan efektivitas ISMS			9. Pengukuran Pelaksanaan *Update Patch*					
6.1 Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil mapping			10. Pengukuran Keefektifan Penanganan Insiden / *Event*					
6.2 Peningkatan pemahaman peserta setelah sosialisasi			11. Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu					
			12. Pengukuran Identifikasi Pelabelan Aset *Removable Media*					
			13. Pengukuran kelengkapan data serah terima aset					
			14. Pengukuran Kesesuaian *Password* Mainframe dan Tandem					

Alternatif Indikator Risiko Utama (lanjutan)

10. Pengukuran Tingkat Kinerja *Robotic*
11. Pengukuran Tingkat Kinerja PC Teleks
12. Pengukuran Tingkat Kinerja *Mainframe*
13. Pengukuran Tingkat Keakuratan Dok. Pembebanan Anggaran Pelaksanaan SOSA

Indikator Kinerja Utama (kolom kiri)

- Total (5) dan (6)
- 3.1 Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D
- 3.2 Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan
- 3.3 Peningkatan pemanfaatan infrastruktur TI yang telah diimplementasikan di Bank D
- 4.1 Persentase downtime sistem aplikasi kritikal dan email
- 4.2 Persentase downtime jaringan Bank D-NET
- 4.3 Jumlah keberhasilan simulasi aplikasi kritikal
- 5.1 Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti
- 5.2 Maksimum waktu penanggulangan serangan virus yang menyebar secara massal
- 5.3 Indeks hasil assessment atas kecukupan dan efektivitas ISMS
- 6.1 Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil mapping
- 6.2 Peningkatan pemahaman peserta setelah sosialisasi

Kriteria Pemilihan Indikator

- Total (3) dan (4)
1. Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol
2. Dapat diukur secara tepat
3. Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini
4. Bersifat spesifik dan eksplisit
5. Merefleksikan data yang dapat diukur secara periodik
6. Realistis terhadap kondisi organisasi
7. Memiliki batas waktu
8. Mudah dimengerti

Risiko (kolom kanan)

11. Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham tentang *setting policy & schedule backup*
12. Tidak tersedia/ lengkapnya SOP menyebabkan *robotic* tidak berfungsi dengan baik karena personil tidak paham melakukan instalasi *agent* di aplikasi
13. Lemahnya mekanisme monitoring sistem menyebabkan kinerja PC Teleks menurun karena kebutuhan performa tidak terpenuhi
14. Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan mainframe mengalami *hardware failure*
15. Kurangnya *training* menyebabkan informasi softcopy Dok. Pembebanan Anggaran Pelaksanaan SOSA tidak akurat karena kesalahan pembuatan

- Total (1) dan (2)

Alternatif Indikator Pengendalian Utama

1. Pengukuran Tingkat Pengamanan Personil Unit Kerja
2. Pengukuran Tingkat Pengamanan Personil Pihak Ketiga
3. Pengukuran Kelengkapan dan Kebenaran Data pada *Database* Aset
4. Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak
5. Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja
6. Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja
7. Pengukuran Kesesuaian *Password* Personil Unit Kerja
8. Pengukuran Pelaksanaan *Update Antivirus*
9. Pengukuran Pelaksanaan *Update Patch*
10. Pengukuran Keefektifan Penanganan Insiden / *Event*
11. Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu
12. Pengukuran Identifikasi Pelabelan Aset *Removable Media*
13. Pengukuran kelengkapan data serah terima aset
14. Pengukuran Kesesuaian *Password* Mainframe dan Tandem

																						14.Pengukuran Tingkat Keakuratan Dok. Pengadaan Kunci Telegram BD						
																						15.Pengukuran Tingkat Keakuratan Dok. PKAT						
																						16.Pengukuran Tingkat Keakuratan Dok. Teknis Tiap Sie. dan Kelompok						
																						17.Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian						
																						18.Pengukuran Tingkat Kehilangan *Tape / Catridge* hasil *backup* data yang akan dikirim ke DRC						
Total (5) dan (6)	3.1 Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D	3.2 Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan	3.3 Peningkatan pemanfaatan infrastruktur TI yang telah diimplementasikan di Bank D	4.1 Persentase downtime sistem aplikasi kritikal dan email	4.2 Persentase downtime jaringan Bank D-NET	4.3 Jumlah keberhasilan simulasi aplikasi kritikal	5.1 Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti	5.2 Maksimum waktu penanggulangan serangan virus yang menyebar secara massal	5.3 Indeks hasil assessment atas kecukupan dan efektivitas ISMS	6.1 Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil mapping	6.2 Peningkatan pemahaman peserta setelah sosialisasi	**Indikator Kinerja Utama**	**Total (3) dan (4)**	1. Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	2. Dapat diukur secara tepat	3. Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	4. Bersifat spesifik dan eksplisit	5. Merefleksikan data yang dapat diukur secara periodik	6. Realistis terhadap kondisi organisasi	7. Memiliki batas waktu	8. Mudah dimengerti	**Alternatif Indikator Risiko Utama** / **Kriteria Pemilihan Indikator** / **Risiko** / **Alternatif Indikator Pengendalian Utama**	16.Kurangnya *training* menyebabkan informasi softcopy Dok. Pengadaan Kunci Telegram Bank D tidak akurat karena kesalahan pembuatan	17.Kurangnya *training* menyebabkan informasi *softcopy* Dok. PKAT tidak akurat karena kesalahan pembuatan	18.Kurangnya *training* menyebabkan Informasi *softcopy* dokumentasi teknis tiap seksi dan kelompok tidak akurat karena kesalahan dalam pembuatan	19.Kurangnya *training* untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi *softcopy* SOP Seksi dan Bagian tidak akurat karena kesalahan pembuatan	20.Kurangnya kontrol pengamanan informasi menyebabkan *Tape / Catridge* hasil *backup* data hilang ketika dalam perjalanan ke DRC	**Total (1) dan (2)**
																						1. Pengukuran Tingkat Pengamanan Personil Unit Kerja						
																						2. Pengukuran Tingkat Pengamanan Personil Pihak Ketiga						
																						3. Pengukuran Kelengkapan dan Kebenaran Data pada *Database* Aset						
																						4. Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak						
																						5. Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja						
																						6. Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja						
																						7. Pengukuran Kesesuaian *Password* Personil Unit Kerja						
																						8. Pengukuran Pelaksanaan *Update Antivirus*						
																						9. Pengukuran Pelaksanaan *Update Patch*						
																						10. Pengukuran Keefektifan Penanganan Insiden / *Event*						
																						11. Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu						
																						12. Pengukuran Identifikasi Pelabelan Aset *Removable Media*						
																						13. Pengukuran kelengkapan data serah terima aset						
																						14. Pengukuran Kesesuaian *Password* Mainframe dan Tandem						

Total (5) dan (6)	Indikator Kinerja Utama	Total (3) dan (4)	Alternatif Indikator Risiko Utama / Kriteria Pemilihan Indikator / Alternatif Indikator Pengendalian Utama / Risiko	19. Pengukuran Tingkat Keakuratan Data Unit Kerja Yang Telah Diolah	20. Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah	21. Pengukuran Tingkat Gannguan AC	22.Pengukuran Tingkat Kerusakan *Thermal Control*	23.Pengukuran Tingkat Ketersediaan *Thermal Control*	Total (1) dan (2)
3.1 Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D		1. Berkaitan dengan sasaran strategis satuan kerja yang telah disusun dan dalam derajat tertentu dapat dikontrol	1. Pengukuran Tingkat Pengamanan Personil Unit Kerja	21.Kurangnya *training* menyebabkan informasi *softcopy* data dari unit kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan	22.Tidak ada Aplikasi AntiVirus, Antimalware, Firewall,dll menyebabkan Informasi *softcopy* data unit kerja yang telah diolah tidak tersedia karena virus	23.Ketidaktersediaan / Kurangnya / Gangguan AC menyebabkan Pelaksanaan operasional di DRC, Strong Room, R.mainframe, dan R.Server terganggu	24.Tidak adanya / lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan *thermal control* tidak dapat digunakan karena komponen rusak	25.Pemeliharaan aset yang tidak baik menyebabkan *thermal control* tidak dapat digunakan karena kerusakkan komponen	26.Pemeliharaan aset yang tidak baik menyebabkan suhu ruangan DRC, Strong Room, Ruang Mainframe, dan Ruang Server tidak dapat diketahui karena tidak terdapat *thermal control*	
3.2 Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan		2. Dapat diukur secara tepat	2. Pengukuran Tingkat Pengamanan Personil Pihak Ketiga						
3.3 Peningkatan pemanfaatan infrastruktur TI yang telah diimplementasikan di Bank D		3. Mampu menggambarkan perbandingan antara performa terdahulu dengan saat ini	3. Pengukuran Kelengkapan dan Kebenaran Data pada *Database* Aset						
4.1 Persentase downtime sistem aplikasi kritikal dan email		4. Bersifat spesifik dan eksplisit	4. Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak						
4.2 Persentase downtime jaringan Bank D-NET		5. Merefleksikan data yang dapat diukur secara periodik	5. Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja						
4.3 Jumlah keberhasilan simulasi aplikasi kritikal		6. Realistis terhadap kondisi organisasi	6. Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja						
5.1 Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti		7. Memiliki batas waktu	7. Pengukuran Kesesuaian *Password* Personil Unit Kerja						
5.2 Maksimum waktu penanggulangan serangan virus yang menyebar secara massal		8. Mudah dimengerti	8. Pengukuran Pelaksanaan *Update Antivirus*						
5.3 Indeks hasil assessment atas kecukupan dan efektivitas ISMS			9. Pengukuran Pelaksanaan *Update Patch*						
6.1 Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil mapping			10. Pengukuran Keefektifan Penanganan Insiden / *Event*						
6.2 Peningkatan pemahaman peserta setelah sosialisasi			11. Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu						
			12. Pengukuran Identifikasi Pelabelan Aset *Removable Media*						
			13. Pengukuran kelengkapan data serah terima aset						
			14. Pengukuran Kesesuaian *Password* Mainframe dan Tandem						

TERIMA KASIH

Lampiran 4: Perincian Risiko Terpilih

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
1	*Notebook*	Kebija-kan	Risiko Operasional	Kurangnya pengamanan pada penggunaan *notebook* di luar ruang kerja / tempat umum menyebabkan *notebook* mengalami kerusakan sehingga pekerjaan terkait strategi dan kebijakan TI tidak dapat dilakukan dengan menggunakan *notebook*	level 5	Level 6	S	- Pedoman pengelolaan *notebook* - SOP Pengelolaan PC dan *Notebook* - Peraturan Bank D mengenai Pengamanan Perangkat Keras Teknologi Informasi Di Luar Area Kantor - Implementasi Winzip untuk membatasi akses terhadap *File* atau proteksi dengan *password* - Standardisasi dan implementasi *cable lock*	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
2	*Notebook*	Kebija-kan	Risiko Operasional	Kurangnya kontrol atas penggunaan *notebook* di luar ruang kerja menyebabkan keseluruhan atau sebagian komponen *notebook* hilang sehingga aktivitas strategi dan kebijakan TI tidak dapat dilakukan dengan menggunakan *notebook*	level 4	Level 6	S	- Pedoman pengelolaan *notebook* - SOP Pengelolaan PC dan *Notebook* - Peraturan Bank D mengenai Pengamanan Perangkat Keras Teknologi Informasi Di Luar Area Kantor - Implementasi Winzip untuk membatasi akses terhadap *File* atau proteksi dengan *password* - Standardisasi dan implementasi *cable lock*	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
3	Web Departe-men Teknolo-gi Informasi	Kebija-kan	Risiko Operasional	Tidak ada user management (pemberian, pencabutan, monitoring) yang baik (strong *password*, private *password*, change *password* regularly) menyebabkan aplikasi diakses oleh pihak yang tidak berwenang menyebabkan aplikasi Web Departemen Teknologi Informasi hilang atau rusak sehingga aktivitas RMS dapat terganggu	Level 2	Level 6	R	- NDA - SE Pam TI - SOP Pengelolaan User	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
4	Web Departemen Teknologi Informasi	Kebija-kan	Risiko Operasional	Modifikasi aset (komponen/ konfigurasi yang tidak terotorisasi menyebabkan kinerja aplikasi Web Departemen Teknologi Informasi turun sehingga aktivitas RMS dapat terganggu	Level 1	Level 6	S	- P3SA- SOP Pengelolaan user	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
5	Kajian/ Laporan internal yang mengandung informasi rahasia	Kebija-kan	Risiko Operasional	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan internal yang mengandung informasi rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Level 4	Level 6	S	- sosialisasi awareness - SOP Monitoring pelaksanaan ketentuan P3SA	*Control*
6	Kajian/ Laporan eksternal yang mengandung informasi rahasia	Kebija-kan	Risiko Operasional	Rusaknya media penyimpanan informasi (Harddisk, CD Back-up) menyebabkan dokumen softcopy kajian/laporan eksternal yang mengandung informasi rahasia menjadi tidak ada/hilang/tidak akurat saat dibutuhkan	Level 4	Level 8	S	- SOP Back-Up Informasi '- Peraturan Bank D mengenai *back-up* dan *restore* - Memperbaiki proses *back-up* dengan sentralisasi pada *server*	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
7	Kajian/ Laporan eksternal yang mengandung informasi rahasia	Kebija-kan	Risiko Operasional	Kurangnya sosialisasi ketentuan pengembangan aplikasi menyebabkan informasi kajian/ laporan eksternal yang mengandung informasi rahasia tidak dapat diterapkan dalam rangka pengembangan aplikasi	Level 4	Level 6	S	- sosialisasi awareness- SOP Monitoring pelaksanaan ketentuan P3SA	*Control*
8	Ruang Direktur dan Deputi Direktur	Admi-nistrasi	Risiko Operasional	Kurangnya pengamanan fisik ruang kerja Direktur dan Deputi Direktur Departemen Teknologi Informasi memungkinkan akses pihak tidak berwenang, sehingga dapat berdampak pada proses otorisasi di Departemen Teknologi Informasi (misal: Informasi hilang/bocor).	Level 7	Level 7	T	- Peraturan Bank D mengenai Penempatan aset TI serta perlindungannya - Peraturan Bank D mengenai Pengamanan kantor, ruangan dan fasilitas Teknologi Informasi - *Filing Cabinet* yang terkunci - Akses Ruang Kerja - Pengaturan Akses Fisik	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
9	Ruang Direktur dan Deputi Direktur	Admi-nistrasi	Risiko Operasional	Kurangnya kontrol dalam pemberian dan penarikan hak akses memungkinkan Ruang Direktur dan Deputi Direktur diakses oleh pihak yang tidak berwenang, sehingga dapat berdampak pada proses otorisasi di Departemen Teknologi Informasi (misal: Informasi hilang/bocor).	Level 7	Level 7	T	- Peraturan Bank D mengenai Pendaftaran dan Pencabutan Hak Akses Pengguna - Peraturan Bank D Evaluasi Hak Akses - Pengaturan Akses Fisik	*Control*
10	Ruang Pelatihan	Admi-nistrasi	Risiko Operasional	Belum berjalannya manajemen aset mencakup inventaris aset dan kepemilikannya, otorisasi penggunaan, pemeliharaan, dan mekanisme penggunaan sesuai fungsinya, dapat menyebabkan Ruang pelatihan (termasuk aset pelatihan) tidak dapat berfungsi maksimal	Level 5	Level 5	S	- Kunci di ADepartemen Teknologi Informasi- Master kunci di satpam- Mekanisme penggunaan ruangan	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
11	Robotics	Operasional	Risiko Operasional	Ketidaktersediaan / ketidaklengkapan SOP untuk melakukan kegiatan operasional (Contoh: SOP Pelaksanaan Back Up, SOP Monitoring, dll) menyebabkan Robotic tidak dapat menjalankan fungsinya dengan baik karena personil tidak paham melakukan setting policy dan schedule back up kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 6	S	- SOP untuk menjalankan Robotics - Transfer Knowledge untuk pemahaman Robotics	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
12	Robotics	Operasional	Risiko Operasional	Ketidaktersediaan / ketidaklengkapan SOP untuk melakukan kegiatan operasional (Contoh: SOP Pelaksanaan Back Up, SOP Monitoring, dll) menyebabkan Robotic tidak dapat menjalankan fungsinya dengan baik karena personil tidak paham melakukan instalasi agent di aplikasi kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 6	S	- SOP untuk menjalankan Robotics - Transfer Knowledge untuk pemahaman Robotics	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
13	PC Teleks	Operasional	Risiko Operasional	Lemahnya mekanisme monitoring sistem (event log, admin log, fault log, dll) menyebabkan kinerja aset menurun karena kebutuhan performa tidak terpenuhi sehingga operasional mengalami hambatan	Level 4	Level 10	T	- Laporan monitoring performance server-Pedoman Audit Security Log-Koordinasi dengan SKTI dan PTTI untuk implementasi NMS	*Control*
14	Mainframe	Operasional	Risiko Operasional	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan mainframe mengalami hardware failure kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 6	S	- Preventive Maintenance - Koordinasi dengan SKTI dan PTTI untuk implementasi NMS	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
15	Dokumen Pembebanan Anggaran Pelaksanaan SOSA	Operasional	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan informasi softcopy Dokumen Pembebanan Anggaran Pelaksanaan SOSA tidak akurat karena kesalahan dalam pembuatan	Level 4	Level 6	S	- Training - Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan Training)	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
16	Dokumen Pengadaan	Operasional	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan informasi softcopy dokumen pengadaan kunci telegram bank indonesia tidak akurat karena kesalahan dalam pembuatan	Level 5	Level 6	S	- Pemberian tugas kepada personel yang menguasai - Training terhadap personel - Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan training)	*Control*
17	Dokumen PKAT	Operasional	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi softcopy Dokumen PKAT tidak akurat karena kesalahan dalam pembuatan	Level 2	Level 3	R	- Training- Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan training)	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
18	Dokumentasi Teknis Seksi dan Bagian	Operasional	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi softcopy dokumentasi teknis tiap seksi dan kelompok tidak akurat karena kesalahan dalam pembuatan	Level 4	Level 4	S	- Pemberian tugas kepada personel yang menguasai - Training terhadap personel - Melakukan Gap Analysis mengenai kompetensi personil dan review kompetensi secara keseluruhan (terhadap hasil pelaksanaan Training)	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
19	SOP Seksi dan Bagian	Operasional	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan Informasi softcopy SOP Seksi dan Bagian tidak akurat karena kesalahan dalam pembuatan	Level 2	Level 10	S	- Pemberian tugas kepada personel yang menguasai - Training terhadap personel	*Control*
20	*Tape / Catridge* hasil *back up data*	Operasional	Risiko Operasional	Kurangnya kontrol pengamanan informasi dalam proses pembuatan, pencetakan, penyimpanan, distribusi/peminjaman dan pemusnahan informasi (dokumen pengadaan, event logs, admin log, fault log, dll) menyebabkan Tape / Catridge hasil back up data hilang ketika dalam perjalanan ke DRC	Level 2	Level 3	R	Daftar permintaan tape catridge yang dibawa	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
21	Data dari unit kerja yang telah diolah	Operasional	Risiko Operasional	Kurangnya training untuk mendukung pelaksanaan pekerjaan menyebabkan informasi softcopy data dari unit kerja yang telah diolah tidak akurat karena kesalahan dalam pembuatan	Level 4	Level 10	S	- Dokumen panduan (SOP) - Formulir kegiatan proses - Review SOP dan Formulir - Perbaikan data softcopy	*Control*

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
22	Data dari unit kerja yang telah diolah	Operasional	Risiko Operasional	Tidak Ada Aplikasi Pengamanan Sistem Informasi (AntiVirus, Antimalware, Firewall,dll) menyebabkan Informasi softcopy data dari unit kerja yang telah diolah tidak tersedia karena terserang virus	Level 4	Level 10	S	- Install anti-virus (Hanya untuk server dan PC Windows based)- Tes compatibility antara aplikasi dengan aplikasi- Back-up- SOP Penanganan Informasi- Server hardening	*Control*
23	AC	Operasional	Risiko Operasional	Ketidaktersediaan / Kurangnya / Gangguan sarana pendukung AC menyebabkan operasional di DRC, Strong Room, R.mainframe, dan R.Server terganggu karena gangguan sarana pendukung kegiatan operasional mengalami hambatan	level 6	Level 8	T	- Pengecekkan AC oleh petugas (DLP) yang dilakukan 3 kali dalam 1 hari dan ketika terjadi gangguan listrik - Pengukur Suhu dan Kelembaban (jumlah: 1) - Petugas (pihak ke-3) stand by 24 jam - Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
24	*Thermal Control*	Operasional	Risiko Operasional	Tidak adanya / lemahnya mekanisme pelaporan insiden pengamanan informasi menyebabkan thermal kontrol tidak dapat digunakan karena kerusakkan komponen kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 8	S	- Pengecekkan output thermal kontrol - Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	*Control*
25	*Thermal Control*	Operasional	Risiko Operasional	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan thermal kontrol tidak dapat digunakan karena kerusakkan komponen kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 8	S	- Pengecekkan output thermal kontrol setiap hari - Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	*Control*

Lampiran 4: Perincian Risiko Terpilih (Sambungan)

No	Jenis Aset	Bagian	Jenis Risiko	Uraian	Kecen-derungan	Dampak	NRD	Tindakan Pengendalian	Jenis Pengendalian
26	*Thermal Control*	Operasional	Risiko Operasional	Pemeliharaan aset yang tidak dilakukan dengan baik menyebabkan suhu ruangan DRC, Strong Room, Ruang Mainframe, dan Ruang Server tidak dapat diketahui karena tidak terdapat thermal kontrol kegiatan operasional Bagian OTI mengalami hambatan	Level 4	Level 8	S	- Pengecekkan output thermal kontrol- Koordinasi dengan DLP untuk penambahan alat monitoring suhu (digital) untuk ruang kerja OTI	*Control*

Lampiran 5: Perincian Indikator Risiko Utama

IRU 1	Pengukuran Tingkat Kerusakan *Notebook*
Tujuan	Untuk mengukur jumlah *notebook* yang rusak pada satuan kerja
Ruang Lingkup	Pengukuran ini berlaku untuk semua *notebook* yang merupakan tanggung jawab Departemen Teknologi Informasi
Metode:	Formula: (a / b) x 100% a= jumlah *notebook* yang rusak pada satuan kerja b= jumlah seluruh *notebook* yang menjadi tanggung jawab satuan kerja
Frekuensi	3 bulan sekali
Sumber Data	Data berasal dari *trouble ticket* dari Bagian *Helpdesk* Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 2	Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya
Tujuan	Untuk mengukur jumlah kehilangan *notebook* atau komponennya
Ruang Lingkup	Pengukuran ini berlaku untuk semua *notebook* yang merupakan tanggung jawab Departemen Teknologi Informasi
Metode	Formula: (a / b) x 100% a= jumlah *notebook* atau komponennya yang hilang pada satuan kerja b= jumlah seluruh *notebook* yang menjadi tanggung jawab satuan kerja.
Frekuensi	3 bulan sekali
Sumber Data	Data berasal dari laporan yang didapat dari *security officer* dari

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 2	Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya
	tiap bagian pada Departmen Teknologi Informasi
Indikator	Dalam pengembangan

IRU 3	Pengukuran Jumlah Kehilangan atau Kerusakan Aplikasi Web DTI
Tujuan:	Untuk mengukur jumlah terjadinya aplikasi Web Departemen Teknologi Informasi Bank D yang hilang atau rusak
Ruang Lingkup:	Pengukuran ini berlaku untuk aplikasi Web Departemen Teknologi Informasi Bank D
Metode:	Formula: (a + b) a= jumlah kejadian hilangnya aplikasi Web Departemen Teknologi Informasi Bank D b= jumlah kejadian rusaknya aplikasi Web Departemen Teknologi Informasi Bank D.
Frekuensi	3 bulan sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 4	Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D
Tujuan:	Untuk mengukur lama terjadinya penurunan kinerja Web Departemen Teknologi Informasi Bank D
Ruang Lingkup:	Pengukuran ini berlaku untuk aplikasi Web Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja aplikasi Web Departemen Teknologi Informasi Bank D

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 4	Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D
	b= jumlah jam operasi aplikasi Web Departemen Teknologi Informasi Bank D.
Frekuensi	3 bulan sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 5	Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi
Tujuan:	Untuk mengukur tingkat penerapan dari kajian/ laporan pengembangan aplikasi baik internal maupun eksternal
Ruang Lingkup:	Pengukuran ini berlaku untuk laporan pada Departemen Teknologi Informasi Bank D
Metode:	Formula: ((a + b) / c) x 100% a= jumlah kajian/ laporan internal pengembangan aplikasi yang diterapkan b= jumlah kajian/ laporan eksternal pengembangan aplikasi yang diterapkan c= jumlah kajian/ laporan internal dan eksternal pengembangan aplikasi
Frekuensi	1 tahun sekali
Sumber Data	Penanggung jawab tiap bagian pada Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 6	Pengukuran Gangguan Aktivitas tim *Roadmap* dan Mitra Strategis
Tujuan:	Untuk Mengukur jumlah gangguan aktivitas pada tim *Roadmap* dan Mitra Strategis
Ruang Lingkup:	Pengukuran ini berlaku untuk tim *Roadmap* dan Mitra Strategis
Metode:	Formula: Jumlah aktivitas yang tidak sesuai dengan perencanaan terkait dengan kerusakan atau kehilangan aplikasi Web Departemen Teknologi Informasi Bank D
Frekuensi	6 bulan sekali
Sumber Data	Kepala Tim *Roadmap* dan Mitra Strategis
Indikator	Dalam pengembangan

IRU 7	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal
Tujuan:	Untuk mengukur tingkat terjadinya informasi kajian/ laporan internal dan eksternal berisi informasi rahasia yang hilang dan/ atau tidak akurat
Ruang Lingkup:	Pengukuran ini berlaku untuk laporan pada Departemen Teknologi Informasi Bank D
Metode:	Formula: ((a + b) / c) x 100% a= jumlah informasi kajian/ laporan internal dan eksternal yang hilang b= jumlah informasi kajian/ laporan internal dan eksternal yang tidak akurat c= jumlah informasi kajian/ laporan internal dan eksternal.
Frekuensi	1 tahun sekali

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 7	Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal
Sumber Data	Penanggung jawab laporan tiap bagian pada Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 8	Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur
Tujuan:	Untuk mengukur tingkat kehilangan dan kerusakan aset yang terdapat pada ruang direktur dan deputi direktur
Ruang Lingkup:	Pengukuran ini berlaku untuk laporan pada Departemen Teknologi Informasi Bank D
Metode:	Formula: ((a + b) / c) x 100%. a= jumlah aset pada ruang direktur dan deputi direktur yang hilang b= jumlah aset pada ruang direktur dan deputi direktur yang hilang c= jumlah seluruh aset pada ruag direktur dan deputi direktur.
Frekuensi	6 bulan sekali
Sumber Data	*Security Officer* Teknologi Informasi dan Pengamanan
Indikator	Dalam pengembangan

IRU 9	Pengukuran Tingkat Pemanfaatan Ruang Pelatihan
Tujuan:	Untuk mengukur tingkat pemanfaatan ruang pelatihan
Ruang Lingkup:	Pengukuran ini berlaku untuk laporan pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100%

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 9	Pengukuran Tingkat Pemanfaatan Ruang Pelatihan
	a= jumlah permintan penggunaan ruang pelatihan yang tidak terpenuhi b= jumlah permintaan penggunaan ruang pelatihan.
Frekuensi	1 tahun sekali
Sumber Data	Bagian Administrasi Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 10	Pengukuran Tingkat Kinerja *Robotic*
Tujuan:	Untuk mengukur lama terjadinya penurunan kinerja *robotic*
Ruang Lingkup:	Pengukuran ini berlaku untuk laporan pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja *robotic* b= jumlah jam operasi *robotic*
Frekuensi	6 bulan sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 11	Pengukuran Tingkat Kinerja PC Teleks
Tujuan:	Untuk mengukur lama terjadinya penurunan kinerja PC Teleks
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja PC Teleks b= jumlah jam operasi PC Teleks.

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 11	Pengukuran Tingkat Kinerja PC Teleks
Frekuensi	6 bulan sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 12	Pengukuran Tingkat Kinerja *Mainframe*
Tujuan:	Untuk mengukur lama terjadinya penurunan kinerja *Mainframe*
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah jam terjadinya penurunan kinerja *Mainframe* b= jumlah jam operasi *Mainframe*
Frekuensi	Dalam pengembangan
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 13	Pengukuran Tingkat Keakuratan Dokumen Pembebanan Anggaran Pelaksanaan SOSA
Tujuan:	Untuk mengukur tingkat terjadinya ketidakakuratan informasi pada Dokumen Pembebanan Anggaran Pelaksanaan SOSA
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah Dokumen Pembebanan Anggaran Pelaksanaan SOSA yang tidak akurat b= jumlah Dokumen Pembebanan Anggaran Pelaksanaan SOSA

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 13	Pengukuran Tingkat Keakuratan Dokumen Pembebanan Anggaran Pelaksanaan SOSA
Frekuensi	1 tahun sekali
Sumber Data	Penanggung jawab laporan dari tiap bagian pada Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 14	Pengukuran Tingkat Keakuratan Dokumen Pengadaan Kunci Telegram Bank D
Tujuan:	Untuk mengukur tingkat terjadinya ketidakakuratan informasi pada Dokumen Pengadaan Kunci Telegram Bank D
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah Dokumen Pengadaan Kunci Telegram Bank D yang tidak akurat b= jumlah Dokumen Pengadaan Kunci Telegram Bank D
Frekuensi	1 tahun sekali
Sumber Data	Penanggung jawab laporan dari tiap bagian pada Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 15	Pengukuran Tingkat Keakuratan Dokumen PKAT
Tujuan:	Untuk mengukur tingkat terjadinya ketidakakuratan informasi pada Dokumen Dokumen PKAT
Ruang Lingkup:	Pengukuran ini berlaku untuk dokumen PKAT Departemen

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 15	Pengukuran Tingkat Keakuratan Dokumen PKAT
	Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah Dokumen PKAT yang tidak akurat b= jumlah Dokumen PKAT.
Frekuensi	1 tahun sekali
Sumber Data	Penanggung jawab laporan dari tiap bagian pada Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 16	Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian
Tujuan:	Untuk mengukur tingkat terjadinya ketidakakuratan informasi pada SOP Seksi dan Bagian
Ruang Lingkup:	Pengukuran ini berlaku untuk SOP Seksi dan Bagian pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah SOP Seksi dan Bagian yang tidak akurat b= jumlah SOP Seksi dan Bagian.
Frekuensi	1 tahun sekali
Sumber Data	Penanggung jawab SOP dari tiap bagian pada Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 17	Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian
Tujuan:	Untuk mengukur tingkat terjadinya ketidakakuratan informasi pada SOP Seksi dan Bagian
Ruang Lingkup:	Pengukuran ini berlaku untuk SOP Seksi dan Bagian pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah SOP Seksi dan Bagian yang tidak akurat b= jumlah SOP Seksi dan Bagian.
Frekuensi	1 tahun sekali
Sumber Data	Penanggung jawab SOP dari tiap bagian pada Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 18	Pengukuran Tingkat Kehilangan *Tape / Catridge* hasil *back-up data* yang dikirim ke DRC
Tujuan:	Untuk mengukur kehilangan *tape/ cartridge* hasil *back-up data* yang dikirim ke DRC
Ruang Lingkup:	Pengukuran ini berlaku pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah pengiriman *tape/ cartridge* hasil *back-up* data ke DRC dimana terjadi *tape/ cartridge* hasil *back-up* data yang hilang b= jumlah pengiriman *tape/ cartridge* hasil *back-up* data.
Frekuensi	6 bulan sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 19	Pengukuran Tingkat Keakuratan Data Satuan kerja Yang Telah Diolah
Tujuan:	Untuk mengukur tingkat terjadinya ketidakakuratan informasi pada Data Satuan kerja Yang Telah Diolah
Ruang Lingkup:	Pengukuran ini berlaku pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah Data Satuan kerja Yang Telah Diolah yang tidak akurat b= jumlah Data Satuan kerja Yang Telah Diolah.
Frekuensi	6 bulan sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 20	Pengukuran Tingkat Serangan Virus Terhadap Data Satuan kerja Yang Telah Diolah
Tujuan:	Untuk mengukur jumlah terjadinya serangan virus yang berdampak pada Data Satuan kerja Yang Telah Diolah
Ruang Lingkup:	Pengukuran ini berlaku pada Departemen Teknologi Informasi Bank D
Metode:	Formula: jumlah terjadinya serangan virus yang ditemukan pada Data Satuan kerja Yang Telah Diolah.
Frekuensi	6 bulan sekali
Sumber Data	*Security Officer* Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 21	Pengukuran Tingkat Gangguan AC
Tujuan:	Untuk mengukur tingkat terjadinya gangguan AC pada DRC, *strong room*, ruang *Mainframe*, dan ruang *Server*
Ruang Lingkup:	Pengukuran ini berlaku pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah jam terjadinya kerusakan pada AC b= jumlah jam operasi AC
Frekuensi	1 tahun sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IRU 22	Pengukuran Tingkat Kerusakan *Thermal Control*
Tujuan:	Untuk mengukur tingkat kerusakan *thermal control* pada DRC, *strong room*, ruang *Mainframe*, dan ruang *Server*
Ruang Lingkup:	Pengukuran ini berlaku pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah jam terjadinya kerusakan pada AC b= jumlah jam operasi AC
Frekuensi	1 tahun sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Lampiran 5: Perincian Indikator Risiko Utama (Sambungan)

IRU 23	Pengukuran Tingkat Ketersediaan *Thermal Control*
Tujuan:	Untuk mengukur tingkat ketersediaan *thermal control* pada DRC, *strong room*, ruang *Mainframe*, dan ruang *Server*
Ruang Lingkup:	Pengukuran ini berlaku pada Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah jam terjadinya kerusakan pada AC b= jumlah jam operasi AC.
Frekuensi	1 tahun sekali
Sumber Data	Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Lampiran 6: Perincian Indikator Pengendalian Utama

IPU 1	Pengukuran Tingkat Pengamanan Personil Unit Kerja
Tujuan:	Untuk mengukur pengamanan Personil Unit Kerja yang menandatangani Surat Menjaga Kerahasian Informasi
Ruang Lingkup:	Pengukuran ini berlaku untuk semua personil Unit Kerja (pegawai Bank D, pegawai honorer Bank D dan personil *outsourcing* yang berafiliasi dengan Unit Kerja).
Metode:	Formula: (a / b) * 100% a= jumlah Surat Menjaga Kerahasiaan Informasi yang telah ditandatangani oleh personil Unit b= Menghitung jumlah personil Unit Kerja
Frekuensi	1 tahun sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: • Jumlah personil Unit Kerja yang aktif yang terdaftar pada *Database Asset* (Aset Personil) • Dokumen Surat Menjaga Kerahasiaan Informasi yang telah ditandatangani personil Unit Kerja disimpan oleh *Security Officer*.
Indikator	• 100% : Pengamanan personil telah mencakup seluruh personil Unit Kerja. • 97 – 99% : Diperlukan tindakan perbaikan segera untuk melengkapi pengamanan seluruh personil Unit Kerja. • < 97% : Perlu diidentifikasi alasan dan penyebab ketidaklengkapan serta dilakukan tindak lanjut secepatnya yang meliputi sosialisasi ke seluruh personil Unit Kerja untuk menanda-tangani Surat Menjaga Kerahasian Informasi

IPU 2	Pengukuran Tingkat Pengamanan Personil Pihak Ketiga.
Tujuan:	Untuk mengukur pengamanan Personil Pihak Ketiga yang bekerjasama dengan Unit Kerja atau yang ditempatkan di lingkungan Unit Kerja

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 2	Pengukuran Tingkat Pengamanan Personil Pihak Ketiga.
	terkait yang menandatangani Surat Menjaga Kerahasian Informasi
Ruang Lingkup:	Pihak ketiga yang dimaksud adalah: ▪ Tenaga kerja pihak ketiga yang sedang bekerjasama / ditempatkan di Unit Kerja terkait.
Metode:	Formula: (a / b) x 100% a= jumlah pihak ke-tiga yang masih aktif bekerja sama dengan satuan kerja dan telah menandatangani surat menjaga kerahasiaan informasi b= jumlah personil pihak ke-tiga yang termasuk ruang lingkup
Frekuensi	6 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: • Jumlah personil pihak ketiga Unit Kerja dapat diketahui dari masing-masing Unit Kerja. • Dokumen Surat Menjaga Kerahasiaan Informasi yang telah ditandatangani personil pihak ketiga Unit Kerja disimpan oleh masing-masing PIC Proyek.
Indikator	• 100% : Pengamanan personil telah mencakup seluruh personil pihak ketiga yang sedang berkerjasama di Unit Kerja terkait. • 97 – 99% : Diperlukan tindakan perbaikan segera untuk melengkapi pengamanan seluruh personil pihak ketiga. • < 97% : Perlu diidentifikasi alasan dan penyebab ketidaklengkapan serta dilakukan tindak lanjut secepatnya yang meliputi sosialisasi ke PIC proyek untuk menginformasikan ke pihak ketiga agar seluruh personil pihak ketiga segera menandatangani Surat Menjaga Kerahasian Informasi

IPU 3	Pengukuran Kelengkapan dan Kebenaran Data pada Database Asset
Tujuan:	Untuk mengukur ketepatan aset yang digunakan di Unit Kerja dan didaftarkan ke dalam database aset.
Ruang Lingkup:	Pengukuran ini berlaku untuk masing-masing klasifikasi aset yang digunakan atau menjadi tanggung jawab Unit Kerja.
Metode:	Formula: ((100 - (a + b)) x 100% a= jumlah aset yang menjadi tanggung jawab satuan kerja tetapi tidak ada pada *database* b= jumlah asset pada *database* yang tidak digunakan lagi oleh satuan kerja
Frekuensi	Setahun sekali
Sumber Data & Prosedur Pengumpulan Data	Pengumpulan data aset yang ada pada saat ini: • Observasi ke tiap personil Unit Kerja Pengumpulan data aset yang terdaftar pada database: • Akses ke Database *Asset* • Mengeluarkan report kompilasi jumlah aset. Pengukuran Kebenaran Data pada *Database Asset*: • Observasi ke tiap personil Unit Kerja disesuaikan antara kepemilikan aset terhadap data yang ada di *Database Asset*.
Indikator	Pengukuran Kelengkapan & Kebenaran Data pada *Database Asset*: • 96 – 100% : proses pelaporan aset baru Personil Unit Kerja sudah berjalan dengan efektif karena hanya terdapat deviasi kecil pada *Database Asset* • 90 – 95% : Diperlukan tindakan perbaikan untuk memastikan kelengkapan dan ketepatan data aset pada database sehingga proses registrasi berjalan dengan efektif. • < 90% : Proses registrasi aset perlu diperbaiki dan

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 3	Pengukuran Kelengkapan dan Kebenaran Data pada Database Asset
	dan perlu diperhatikan tindakan pencegahan sehingga database aset selalu ter-*update* berdasarkan aset yang digunakan di Unit Kerja.

IPU 4	Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak
Tujuan:	Untuk mengukur kesesuaian perangkat lunak yang digunakan di PC / Notebook masing-masing Personil Unit Kerja terhadap perangkat lunak yang diijinkan untuk digunakan.
Ruang Lingkup:	Pengukuran ini berlaku untuk aset perangkat lunak yang digunakan oleh Unit Kerja.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.6.1.4 Auhorization Process for Information Processing Facilites ISO / IEC 27001:2005.
Metode:	Formula: (((a – b) / a) / c) x 100% a= jumlah perangkat lunak yang di-*install* pada PC/ *notebook* personil satuan kerja b= jumlah perangkat lunak pada PC/ *notebook* yang tidak terdaftar pada daftar perangkat lunak yang diizinkan untuk di-*install* di lingkup Departemen Teknologi Informasi c= jumlah PC/ *notebook* yang digunakan satuan kerja.
Frekuensi	Setahun sekali

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 4	Pengukuran Proses Authorisasi Penggunaan Perangkat Lunak
Sumber Data & Prosedur Pengumpulan Data	Pengumpulan data aset perangkat lunak yang digunakan saat ini: • Observasi ke tiap PC / Notebook yang digunakan oleh personil Unit Kerja. • Melihat data *currently installed program* yang ada di *control panel* > *add / remove programs*. • Melakukan review apakah dari data tersebut terdapat penggunaan program yang tidak termasuk pada Daftar Perangkat Lunak yang Diijinkan untuk Di-*install* di Lingkup DTI.
Indikator	• 100% : Kontrol terhadap perangkat lunak di PC / Notebook personil Unit Kerja sudah sesuai dengan ketentuan instalasi software yang berlaku. • 97 – 99% : Diperlukan tindakan perbaikan segera untuk menyesuaikan perangkat lunak yang telah ter-*install* berdasarkan daftar perangkat lunak yang diijinkan. • < 97% : kontrol belum efektif dan perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi dilakukan sosialisasi agar instalasi perangkat lunak berdasarkan ketentuan yang ada

IPU 5	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja
Tujuan:	Untuk mengukur kesesuaian antara Personil yang dapat memasuki ruangan Unit Kerja berdasarkan daftar hak akses fisik yang diijinkan untuk memasuki ruang kerja Unit Kerja.
Ruang Lingkup:	Pengukuran ini berlaku untuk akses fisik ke ruangan kerja Unit Kerja.
Metode:	Formula: ((100 – a) / 100) x 100%

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 5	Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja
	a = jumlah personil yang tidak diberikan hak akses ke ruangan Satuan kerja berdasarkan Ketentuan Kontrol Hak Akses Fisik tetapi sistem mengizinkan personil tersebut mengakses ruangan satuan kerja terkait.
Frekuensi	6 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Mekanisme pengumpulan data meliputi: • Meminta Laporan dari DLP yang berisi daftar personil yang diberi akses oleh untuk memasuki ruang kerja Unit Kerja. • Melakukan review apakah terdapat pemberian hak akses fisik kepada personil yang seharusnya tidak diberikan hak akses fisik berdasarkan Ketentuan Kontrol Hak Akses Fisik.
Indikator	• 100% : Proses pemberian hak akses fisik dan pengamanan ruang kerja Unit Kerja sudah efektif sesuai dengan daftar hak akses yang diijinkan untuk memasuki ruang kerja Unit Kerja. • 97 – 99% : Diperlukan tindakan perbaikan segera untuk menyesuaikan daftar hak akses fisik berdasarkan ketentuan hak akses fisik yang diijinkan dengan berkoordinasi dengan satuan kerja terkait. • < 97% : kontrol belum efektif dan perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi dilakukan koordinasi dengan satuan kerja terkait untuk melakukan *updating* terhadap hak akses fisik ruangan Unit Kerja.

IPU 6	Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja
Ruang Lingkup:	Pengukuran ini berlaku untuk *back-up* informasi personil Unit Kerja.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 6	Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja
Metode:	Formula: (a / b) x 100% a= jumlah personil yang telah melakukan *back-up* sesuai jadwal b= jumlah personil satuan kerja yang aktif.
Frekuensi	3 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Pengumpulan data untuk pengukuran pelaksanaan *back-up:* • Mengumpulkan Form Dokumentasi *Back-Up* Informasi Personil Unit Kerja yang berisi informasi personil telah melaksanakan *back-up* sesuai dengan frekuensi pelaksanaan *back up* yang berlaku. • Menghitung jumlah personil yang telah melaksanakan *back-up* sesuai dengan frekuensi pelaksanaan *back up* yang berlaku. • Menghitung presentase jumlah personil yang telah melaksanakan *back-up* dengan jumlah personil Unit Kerja.
Indikator	Untuk pengukuran kelengkapan *back-up*: • 99 – 100% : *Back-up* terlaksana dengan baik • 95 – 99% : Diperlukan tindakan perbaikan segera untuk melengkapi proses back-up oleh Personil Unit Kerja. • < 95% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi dilakukan sosialisasi mengenai pelaksanaan *back-up* secara tepat waktu.

IPU 7	Pengukuran Kesesuaian Password Personil Unit Kerja
Tujuan:	Untuk mengukur kesesuaian penggunaan password oleh Personil Unit Kerja terhadap Kebijakan Pengamanan yang berlaku. Pengukuran kesesuaian password ini dapat dilakukan secara random ke seluruh Personil Unit Kerja secara periodik.
Ruang Lingkup:	Pengukuran ini berlaku untuk melihat apakah semua personil Unit Kerja telah menggunakan *password* sesuai peraturan yang berlaku. Password

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 7	Pengukuran Kesesuaian Password Personil Unit Kerja
	yang diukur hanya password untuk *log in* ke *Active Directory*.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.11.2.3 *User Password Management* ISO / IEC 27001:2005.
Metode:	Formula: (a / b) x 100% a= jumlah personil yang telah menggunakan *password* sesuai ketentuan b= jumlah personil satuan kerja yang memiliki *user ID* dan *password* untuk *login* ke *active directory.*
Frekuensi	6 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Mekanisme untuk melihat kesesuaian password yang telah sesuai dengan ketentuan adalah dengan *manual review* adalah sebagai berikut: • Meminta personil Unit Kerja untuk memasukkan *password* untuk *log in* ke *active directory.* • Meminta personil Unit Kerja untuk menunjukkan *alphabet, alphanumeric*, dan *special character* pertama yang digunakan sebagai *password*. • Memberikan tanda checklist (✔) pada Form Pengecekan Password pada kolom *alphabet* / *alphanumeric* / *special character* ketika personil menggunakannya. • Menghitung jumlah digit *password* yang dimasukkan oleh personil Unit Kerja dan mencatat jumlah digit *password* pada Form Pengecekan Password • Memeriksa apakah personil dapat *log in* ke active directory dengan menggunakan *password* yang telah dimasukkan. • Memberikan paraf pada Form Pengecekan Password pada akhir pemeriksaan oleh personil Unit Kerja dan pelaksana pemeriksa password. • Apabila dalam penggunaan *password*, jumlah digit kurang dari 8, tidak menggunakan alphabet / alphanumeric / special character maka personil tersebut belum menggunakan password sesuai ketentuan.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 7	Pengukuran Kesesuaian Password Personil Unit Kerja
Indikator	Untuk pengukuran kesesuaian *password*: • 100% : Seluruh personil Unit Kerja telah efektif menggunakan *password* sesuai dengan kebijakan pengamanan yang berlaku • 97 – 99% : Diperlukan tindakan perbaikan segera untuk menyesuaikan penggunaan *password* oleh Personil Unit Kerja. • < 97% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi dilakukan sosialisasi mengenai penggunaan *password* sesuai dengan kebijakan pengamanan yang berlaku.

IPU 8	Pengukuran Pelaksanaan *Update Antivirus*
Tujuan:	Untuk mengukur PC / Notebook Personil Unit Kerja, Server, Mainframe, dan Tandem yang telah ter-*update* antivirus yang terbaru.
Ruang Lingkup:	Pengukuran ini berlaku untuk PC dan *notebook* Unit Kerja.
Metode:	Formula: (a / b) * 100% a= jumlah PC dan *notebook* satuan kerja atau Server, *Mainframe*, *Tandem* yang memiliki *updated Antivirus* b= jumlah PC dan *notebook* atau server, *Mainframe*, *Tandem* yang digunakan oleh satuan kerja
Frekuensi	1 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	• Status antivirus pada PC dan *notebook* / Server,Mainframe, Tandem milik Unit Kerja dapat dilihat dari laporan McAffee EPO periode yang dihasilkan oleh PTTI. • Menghitung jumlah PC dan *notebook* / Server,Mainframe, Tandem dengan *antivirus* paling *update*.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 8	Pengukuran Pelaksanaan *Update Antivirus*
	• Menghitung presentase jumlah PC dan *notebook* / Server,Mainframe, Tandem dengan *antivirus* paling *update* dengan jumlah PC dan *notebook* keseluruhan.
Indikator	• 100% : Seluruh PC dan *notebook* / Server, Mainframe, Tandem telah efektif ter-update antivirus terbaru • 97 – 99% : Diperlukan tindakan perbaikan segera untuk meng-*update* antivirus di PC dan Notebook Personil Unit Kerja / Server,Mainframe, Tandem. • < 97% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi berkoordinasi dengan Unit Kerja terkait.

IPU 9	Pengukuran Pelaksanaan Update *Patch*
Tujuan:	Untuk mengukur PC / Notebook Personil Unit Kerja / Server, Mainframe, Tandem yang telah ter-*update* patch yang terbaru.
Ruang Lingkup:	Pengukuran ini berlaku untuk PC dan *notebook* Unit Kerja / Server,Mainframe, Tandem.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.12.4.1 Control of operational software ISO / IEC 27001:2005.
Metode:	Formula: (a / b) * 100% a= jumlah PC/ *notebook* personil satuan kerja atau server, *Mainframe*, *Tandem* yang telah memiliki *updated patch* b= jumlah PC/ *notebook* personil satuan kerja atau server, *Mainframe*, *Tandem* yang digunakan satuan kerja.
Frekuensi	1 bulan sekali
Sumber Data &	• Meminta Laporan *Updated Patch* periode yang berlaku dari PTTI.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 9	Pengukuran Pelaksanaan Update *Patch*
Prosedur Pengumpulan Data	• Menghitung jumlah PC dan *notebook* / Server,Mainframe, Tandem yang memiliki *patch* paling *update*. • Menghitung presentase jumlah PC dan *notebook* / Server,Mainframe, Tandem yang yang memiliki patch paling *update* dengan jumlah PC dan *notebook* keseluruhan.
Indikator	• 100% : Seluruh PC dan *notebook* / Server, Mainframe, Tandem telah efektif ter-update patch terbaru • 97 – 99% : Diperlukan tindakan perbaikan segera untuk meng-*update* patch di PC dan Notebook Personil Unit Kerja / Server,Mainframe, Tandem. • < 97% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi berkoordinasi dengan Unit Kerja terkait.

IPU 10	Pengukuran Keefektifan Penanganan Insiden / Event
Tujuan:	Untuk mengukur pelaksanaan proses tindakan pencegahan dan perbaikan yang dilakukan berdasarkan target waktu penanganannya.
Ruang Lingkup:	Pengukuran ini memberikan gambaran mengenai pelaksanaan proses penanganan insiden / *event* pengamanan informasi yang dilaporkan baik ke *Security Officers* maupun ke Helpdesk di Unit Kerja.
Metode:	Formula: ((c – (a + b)) / c) x 100% a= jumlah insiden/ event yang dilaporkan yang belum ditangani sesuai dengan target waktu b= jumlah insiden/ event yang dilaporkan yang terjadi penundaan penanganan tindak lanjut c= jumlah insiden/ event yang dilaporkan.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 10	Pengukuran Keefektifan Penanganan Insiden / Event
Frekuensi	3 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Sumber data dan Prosedur Pengukuran Keefektifan Penanganan Insiden / Event: • Jumlah insiden / *events* yang dilaporkan ke *Security Officers* pada periode tersebut dapat dilihat dari Log Tindakan Pencegahan dan Perbaikan. • Status pelaksanaan tindakan perbaikan / pencegahan atas insiden / events yang dilaporkan ke *Security Officers* dapat dilihat dari Log Tindakan Pencegahan dan Perbaikan.
Indikator	Untuk pengukuran efektifitas tindak lanjut insiden / *event*: • 99 - 100% : Penanganan insiden / *events* sudah cukup efektif • 97 – 99% : Diperlukan tindakan perbaikan segera untuk menangani keterlambatan tindak lanjut perbaikan. • < 97% : perlu diidentifikasi alasan dan penyebabnya atas trend keterlambatan penanganan insiden / *event* dan dilakukan tindakan pencegahan dan perbaikan lebih lanjut.

IPU 11	Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu
Tujuan:	Untuk mengukur pelaksanaan kontrol terhadap tamu yang memasuki are Unit Kerja melalui mekanisme penerimaan tamu
Ruang Lingkup:	Pengukuran ini memberikan gambaran mengenai pelaksanaan proses penerimaan tamu di Unit Kerja.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 11	Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu
Metode:	Formula: ((c – (a + b)) / c) x 100% a= jumlah tamu yang tidak menandatangani atau mengisi waktu meninggalkan ruangan dalam buku/ aplikasi tamu pada hari yang sama b= jumlah personil satuan kerja yang tidak memparaf buku tamu setelah mengantarkan tamu keluar (hanya berlaku untuk buku tamu. Jika satuan kerja menggunakan aplikasi tamu, nilai b = 0) c= jumlah tamu yang berkunjung ke ruang satuan kerja.
Frekuensi	1 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Sumber data dan Prosedur Pengukuran Keefektifan Penerimaan Tamu: • Jumlah tamu yang tidak menandatangani atau mengisi waktu meninggalkan ruangan pada Buku / Aplikasi Tamu pada hari yang sama dapat dilihat pada Buku Tamu atau cetakan log Tamu dari Aplikasi Tamu pada masing-masing Unit Kerja. • Jumlah personil Unit Kerja yang tidak memparaf Buku Tamu setelah mengantarkan tamu keluar meninggalkan ruangan dapat dilihat pada Buku Tamu Unit Kerja. • Jumlah total tamu yang memasuki ruangan Unit Kerja dapat dilihat pada Buku Tamu atau cetakan log Tamu dari Aplikasi Tamu.
Indikator	Untuk pengukuran efektifitas tindak lanjut penerimaan tamu: • 98 - 100% : Proses penerimaan tamu sudah cukup efektif • < 98% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya yang meliputi sosialisasi ke seluruh personil Unit Kerja

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 11	Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu
	untuk memperhatikan proses penerimaan tamu khususnya jika tamu akan meninggalkan ruangan.

IPU 12	Pengukuran Identifikasi Pelabelan Aset *Removable Media*
Tujuan:	Untuk mengukur jumlah pelabelan aset yang digunakan di Unit Kerja dan didaftarkan ke dalam database aset.
Ruang Lingkup:	Pengukuran ini berlaku untuk jenis *removable media* yang yang digunakan atau menjadi tanggung jawab Personil Unit Kerja.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.10.7.1 Management of Removable Media ISO / IEC 27001:2005.
Metode:	Formula: ((100 – a) / 100) x 100% a= jumlah asset *removable media* yang ditemukan menjadi tanggung jawab personil satuan kerja tetapi belum diberi label.
Frekuensi	Setahun sekali
Sumber Data & Prosedur Pengumpulan Data	Pengumpulan data aset *removable media* yang digunakan pada saat ini: • Observasi ke tiap personil Unit Kerja dan memeriksa apakah terdapat pelabelan aset dan disesuaikan dengan database aset.
Indikator	Pengukuran pelabelan aset *Removable Media*: • 97 – 100% : proses pelaporan aset baru personil Unit Kerja sudah berjalan dengan efektif karena hanya terdapat deviasi kecil pada aset yang belum diberi label. • 90 – 97% : Diperlukan tindakan perbaikan untuk segera memberikan label pada aset untuk melengkapi data aset pada database.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 12	Pengukuran Identifikasi Pelabelan Aset *Removable Media*
	• < 90% : Proses registrasi aset perlu diperbaiki dan dan perlu diperhatikan tindakan pencegahan sehingga aset *removable media* baru milik Personil Unit Kerja selalu diberi pelabelan.

IPU 13	Pengukuran kelengkapan data serah terima aset
Tujuan:	Untuk mengukur kelengkapan dan kebenaran data pemindahan / pengalihan aset ke pihak lain
Ruang Lingkup:	Pengukuran ini berlaku untuk mekanisme pengalihan aset TI yang dialihkan atau dipinjamkan ke pihak lain dari Personil Unit Kerja.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.8.3.2 Return of Asset ISO / IEC 27001:2005.
Metode:	Formula: (a / b) x 100% a= form serah terima asset yang disimpan oleh *security officer* b= jumlah asset TI yang dialihkan /dipinjamkan/ dikembalikan berdasarkan permohonan peminjaman/ pengalihan oleh pihak lain. personil satuan kerja yang mutasi.
Frekuensi	6 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Pengumpulan data kelengkapan serah terima meliputi: • Identifikasi dan memeriksa apakah terdapat aset TI yang telah dialihkan / dipindahkan melalui Personil Unit Kerja. • Memeriksa kelengkapan form serah terima Aset TI yang dikumpulkan
Indikator	Pengukuran kelengkapan dan kebenaran data serah terima: • 99 – 100% : proses serah terima aset TI oleh personil Unit Kerja sudah berjalan dengan efektif karena hanya terdapat deviasi kecil pada proses serah

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 13	Pengukuran kelengkapan data serah terima aset
	terima aset. • 97 – 99% : Diperlukan tindakan perbaikan untuk segera melengkapi form serah terima Aset TI. • < 97% : Perlu identifikasi alasan dan penyebab ketidaklengkapan proses serah terima aset TI dan perlu diperhatikan tindakan perbaikan meliputi sosialisasi ke Personil Unit Kerja sehingga proses serah terima berjalan lebih efektif.

IPU 14	Pengukuran Kesesuaian *Password* Mainframe dan Tandem
Tujuan:	Untuk mengukur apakah penggunaan *Password* Super – Super yang digunakan untuk *log in* ke dalam sistem *mainframe* dan tandem telah sesuai dengan Kebijakan Pengamanan yang berlaku.
Ruang Lingkup:	Pengukuran ini berlaku untuk melihat apakah semua *Password* Super – Super yang digunakan untuk *log in* ke dalam sistem *mainframe* dan tandem baik yang ada di *data center* maupun yang ada di DRC telah sesuai dengan Kebijakan Pengamanan yang berlaku.
Objektif:	Untuk memenuhi kesesuaian terhadap Annex A.11.2.3 *User Password Management* ISO / IEC 27001:2005.
Metode:	Formula: (a / b) x 100% a= jumlah *password* super yang telah sesuai dengan kebijakan pengamanan b= jumlah *password* super yang digunakan untuk *login* ke dalam sistem *Mainframe* dan *Tandem*.

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 14	Pengukuran Kesesuaian *Password* Mainframe dan Tandem
Frekuensi	3 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Mekanisme untuk melihat kesesuaian *password* yang telah sesuai dengan ketentuan adalah dengan *manual review* adalah sebagai berikut: • Melakukan review *Password* Super – Super yang digunakan untuk *log in* kedalam sistem mainframe dan tandem. Password yang digunakan harus memiliki *alphabet*, *alphanumeric*, *special character*, dan minimal 8 digit. • Memberikan tanda checklist (✔) pada Form Pengecekan Password pada kolom *alphabet* / *alphanumeric* / *special character* / panjang *password* apabila penggunaan password telah sesuai dengan Kebijakan Pengamanan. • Memberikan paraf pada kolom **Paraf Pemilik Password** di Form Pengecekan *Password* pada akhir pemeriksaan oleh personil Unit Kerja yang menjadi penanggung jawab *Password* Super – Super pada mainframe dan tandem. • Memberikan paraf pada kolom **Paraf Pelaksana Pengecekan** di Form Pengecekan *Password* pada akhir pemeriksaan oleh personil Unit Kerja yang menjadi pelaksana pengecekan *Password* Super – Super pada mainframe dan tandem. • Apabila dalam penggunaan *password*, jumlah digit kurang dari 8, tidak menggunakan alphabet / alphanumeric / special character maka *Password* Super – Super tersebut belum menggunakan *password* sesuai ketentuan.
Indikator	Untuk pengukuran kesesuaian *password*: • 100% : Seluruh *Password* Super – Super telah sesuai dengan Kebijakan Pengamanan yang berlaku • 97 – 99% : Diperlukan tindakan perbaikan segera untuk menyesuaikan penggunaan *Password* Super –

Lampiran 6: Perincian Indikator Pengendalian Utama (Sambungan)

IPU 14	Pengukuran Kesesuaian *Password* Mainframe dan Tandem
	Super terhadap Kebijakan Pengamanan yang berlaku. • < 97% : perlu diidentifikasi alasan dan penyebabnya serta dilakukan tindak lanjut secepatnya agar penggunaan *Password* Super – Super sesuai dengan Kebijakan Pengamanan yang berlaku.

Sasaran Strategis 3: Meningkatkan pengembangan dan pengelolaan Sistem TI

3.1 Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka mendukung implementasi strategi Bank D

IKU ini mengukur perbandingan tingkat penyelesaian proyek TI sesuai tahapan yang telah direncanakan sebelumnya untuk proyek-proyek TI terkait inisiatif Bank D setiap 3 bulan untuk mengukur tingkat penyelesaian proyek TI terkait inisiatif BI dan mengantisipasi proyek yang tidak tepat waktu.

Formula: (a / b) x 100%

a= jumlah program kerja (PK) yang selesai sesuai tahapan (kesepakatan)

b= jumlah PK yang disetujui Forum Manajemen TI-PK yang belum dimulai pada tahapan

Target:100%.

3.2 Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan

IKU ini mengukur perbandingan tingkat penyelesaian proyek TI sesuai tahapan yang telah direncanakan sebelumnya untuk proyek-proyek TI yang tidak terkait dengan inisiatif Bank D setiap 3 bulan untuk mengukur tingkat penyelesaian proyek TI dan mengantisipasi proyek yang tidak tepat waktu.

Formula: (a / b) x 100%

a= jumlah PK yang selesai sesuai tahapan

b= jumlah PK yang disetujui Forum Manajemen TI-PK yang belum dimulai pada tahapan

Target:75%.

3.3 Peningkatan pemanfaatan infrastruktur TI yang telah diimplementasikan di Bank D

IKU ini mengukur jumlah inovasi yang dilakukan terhadap pemanfaatan infrastruktur teknologi informasi setiap tahun untuk menilai adanya inovasi terhadap pemanfaatan infrastruktur teknologi informasi.

Formula: Jumlah inovasi infrastruktur TI yang diimplementasikan di Bank D

Target: 1 (satu) implementasi

Sasaran strategis 4: Menjaga ketersediaan sistem TI

4.1 Persentase *downtime* sistem aplikasi kritikal dan *e-mail*

IKU ini mengukur seberapa sering aplikasi kritikal dan *e-mail* tidak beroperasi setiap 3 bulan untuk mengetahui apakah aplikasi kritikal dan *e-mail* perlu ditingkatkan ketersediaan/ kehandalannya.

Formula:

a= jumlah jam aplikasi kritikal tidak bisa dioperasikan

b= jumlah jam operasi aplikasi kritikal

Aplikasi kritikal yang diukur: SID, LHBU, RTGS, S4, SOSA, SKN, dan e-*mail*. Masing-masing maksimal *downtime* adalah: SID 7%, LHBU 7%, RTGS 3%, S43%, SOSA 7%, SKN, 10%, dan *e-mail* 7%

Target: 7%.

Persentase *downtime* jaringan Bank D-NET

IKU ini mengukur ketersediaan jaringan Bank D-NET (intranet, ekstranet, dan internet) setiap 3 bulan untuk mengetahui apakah jaringan Bank D-NET perlu ditingkatkan ketersediannya.

Formula: (a / b) x 100%

a= jumlah jam jaringan Bank D-NET tidak bisa dioperasikan

b= jumlah jam operasi jaringan Bank D-NET

Target: 1%.

Jumlah keberhasilan simulasi aplikasi kritikal

IKU ini mengukur kesiapan aplikasi kritikal berdasarkan jumlah simulasi yang berhasil dilaksanakan setiap semester untuk mengetahui apakah aplikasi kritikal telah siap beroperasi dalam kondisi darurat atau tidak normal untuk meningkatkan ketersediaan keamanan TI.

Formula: Jumlah keberhasilan simulasi aplikasi kritikal (3 per semester)

Target: 6.

Sasaran strategis 5: Menjaga keamanan Sistem TI

5.1 Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti

IKU ini mengukur jumlah tindak lanjut penyelesaian rekomendasi hasil evaluasi terhadap sistem pengamanan TI yang dilakukan oleh pihak ketiga setiap tahun untuk menilai respon Departemen Teknologi Informasi terhadap peningkatan pengamanan TI.

Formula: (a / b) x 100%

a= jumlah rekomendasi yang ditindaklanjuti

b= jumlah rekomendasi konsultan yang akan diselesaikan sesuai komitmen dalam periode pengukuran IKU

Target: 100%.

5.2 Maksimum waktu penanggulangan serangan virus yang menyebar secara massal

IKU ini mengukur maksimum waktu penanggulangan serangan virus yang menyebar secara massal setiap semester untu menilai kehandalan dan kecepatan penanganan sistem pengamanan TI.

Formula: Jumlah hari penanggulangan terhadap serangan virus yang menyebar secara massal.

Target: 4 hari kerja.

5.3 Indeks hasil *assessment* atas kecukupan dan efektivitas ISMS

IKU ini mengukur konsistensi pelaksanaan ISMS berdasarkan ISO 27001 sehingga tidak terdapat temuan assessor ISO berkategori Major *non-conformity* yang dapat mengakibatkan pencabutan sertifikasi maupun temuan berkategori minor *non-conformity* yang dapat mengurangi efektivitas penerapan ISMS setiap semester untuk mempertahankan perolehan ISO 27001 atau ISMS serta mendorong kepatuhan pelaksanaan pengamanan TI.

Formula:

Indeksasi hasil eksternal *assessment* dilakukan terhadap temuan ISMS berkategori major dan minor *non-conformity* dengan skala:

1. terdapat 1 atau lebih temuan major *non-conformity*
2. tidak terdapat temuan major *non-conformity* dengan lebih dari 15 temuan minor *non-conformity*
3. tidak terdapat temuan major *non-conformity* dengan 11-15 temuan minor *non-conformity*
4. tidak terdapat temuan major *non-conformity* dengan 5-10 temuan minor *non-conformity*
5. tidak terdapat temuan major *non-conformity* dengan maksimal 5 temuan minor *non-conformity*
6. tidak terdapat temuan major *non-conformity* dan minor *non-conformity*

Target: 3

Sasaran strategis 6: Meningkatkan pengetahuan TI pegawai Bank D, baik yang bersifat teknis maupun ketentuan TI

6.1 Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil *mapping*

IKU ini menilai kecukupan/ banyaknya materi atau topik TI yang disosialisasikan kepada pegawai BI setiap tahun untuk mengetahui apakah materi/ topic TI yang disosialisasikan telah cukup beragam dalam rangka meningkatkan *IT literacy* pegawai BI.

Formula: Jumlah materi/ topik yang disosialisasikan

Target: 4.

6.2 Peningkatan pemahaman peserta setelah sosialisasi

IKU ini mengukur persentase peserta yang mengalami peningkatan pemahaman setelah mengikuti sosialisasi mengenai TI setiap tahun untuk menilai apakah sosialisasi TI telah dilaksanakan secara efektif sehingga dapat meningkatkan IT literacy pegawai BI.

Formula: (a / b) x 100%

a= persentase jumlah peserta yang mengalami peningkatan pemahaman

b= jumlah peserta

Target: 75%.

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan

IPU 15	Pengukuran *Form* Peminjaman Aset
Tujuan:	Untuk mengukur tingkat pengembalian asset yang dipinjam
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah *form* peminjaman aset yang sesuai dengan pengembalian aset yang dipinjam b= jumlah *form* peminjaman aset.
Frekuensi	6 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: *Form* peminjaman aset Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IPU 16	Pengukuran Tingkat Pemahaman
Tujuan:	Mengukur tingkat pemahaman personil satuan kerja yang mengikuti *training* dengan pembuatan tes materi *training* segera setelah pelaksanaannya

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 16	Pengukuran Tingkat Pemahaman
Ruang Lingkup:	Pengukuran ini berlaku untuk semua pegawai dan pegawai honorer Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah personil dengan nilai di atas 75 skala 100 b= jumlah personil yang mengikuti *training*.
Frekuensi	1 tahun sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: Hasil tes materi *training* Departemen Teknologi Informasi Bank D
Indikator	• 75 - 100% : Peserta *training* telah memahami materi yang diberikan • 97 – 99% : Diperlukan tindakan evaluasi terhadap peserta *training* atau pemberian materi

IPU 17	Pengukuran Efektivitas Training
Tujuan:	Mengukur hingga akhirnya dapat diperoleh hasil yang menggambarkan efektivitas *training* dalam meningkatkan performa bisnis organisasi untuk memperoleh informasi mengenai tingkat keefektifan dari *training* yang dilaksanakan terhadap performa bisnis organisasi dan memperoleh informasi

IPU 17	Pengukuran Efektivitas Training
	mengenai hal-hal yang perlu ditingkatkan terkait dengan variabel penilaian pelaksanaan *training*
Ruang Lingkup:	Pengukuran ini berlaku untuk semua pegawai dan pegawai honorer Departemen Teknologi Informasi Bank D
Metode:	Formula: ((a + b) / c) x 100% a= jumlah personil dengan nilai ”baik” b= jumlah personil dengan nilai ”baik sekali” c= jumlah seluruh personil peserta *training*.
Frekuensi	1 tahun sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: *Form* evaluasi aktivitas *training* dan form efektivitas *training* Departemen Teknologi Informasi Bank D
Indikator	• 75 - 100% : Peserta *training* telah mengimplementasikan materi yang diberikan • 97 – 99% : Diperlukan tindakan evaluasi terhadap peserta *training* atau pemberian materi

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 18	Pengukuran Efektivitas Training
Tujuan:	Mengukur hingga akhirnya dapat diperoleh hasil yang menggambarkan efektivitas *training* dalam meningkatkan performa bisnis organisasi untuk memperoleh informasi mengenai tingkat keefektifan dari *training* yang dilaksanakan terhadap performa bisnis organisasi dan memperoleh informasi mengenai hal-hal yang perlu ditingkatkan terkait dengan variabel penilaian pelaksanaan *training*
Ruang Lingkup:	Pengukuran ini berlaku untuk semua pegawai dan pegawai honorer Departemen Teknologi Informasi Bank D
Metode:	Formula: ((a + b) / c) x 100% a= jumlah personil dengan nilai ”baik” b= jumlah personil dengan nilai ”baik sekali” c= jumlah seluruh personil peserta *training.*
Frekuensi	1 tahun sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: *Form* evaluasi aktivitas *training* dan form efektivitas *training* Departemen Teknologi Informasi Bank D
Indikator	• 75 - 100% : Peserta *training* telah mengimplementasikan materi yang diberikan

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 18	Pengukuran Efektivitas Training
	• 97 – 99% : Diperlukan tindakan evaluasi terhadap peserta *training* atau pemberian materi

IPU 19	Pengukuran Analisis *Fault Logging* Akses Fisik
Tujuan:	Melakukan analisis atas usaha akses oleh pihak yang tidak berwenang yaitu *wrong access* ke ruang kerja Satuan kerja yang tercatat pada *Access Control System*. *Wrong Access* adalah usaha akses fisik yang tidak berhasil karena pihak yang berusaha akses tidak memiliki hak akses ke ruang kerja Satuan kerja
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: Jumlah *wrong acces* ke ruang satuan kerja sebanyak lebih dari 5 kali
Frekuensi	6 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: Data akses fisik Departemen Logistik dan Pengamanan Bank D
Indikator	Dalam pengembangan

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 20	Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset
Tujuan:	Mengukur kesesuaian tanggal aktivitas pemeliharaan aktual dengan tanggal pemeliharaan yang telah direncanakan setiap bulan untuk selanjutnya dianalisis setiap 3 bulan untuk perbaikan
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: Jumlah *wrong acces* ke ruang satuan kerja sebanyak lebih dari 5 kali
Frekuensi	3 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: Data aktivitas pemeliharaan Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 21	Pengukuran Audit *Security Log*
Tujuan:	Mengukur tingkat percobaan *log-on* yang *valid* maupun *invalid*, juga kejadian-kejadian terkait dengan penggunaan *resource*, seperti membuat, membuka, atau menghapus file pada PC, *notebook, server*, dan jaringan yang telah memiliki *security* log yang aktif
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah aset yang mengalami *log-on failure* b= 3 aset secara *random*.
Frekuensi	3 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: Data akses fisik Departemen Logistik dan Pengamanan Bank D
Indikator	Dalam pengembangan

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 22	Pengukuran *Form* Pengiriman *Tape Back-up*
Tujuan:	Mengukur kesesuaian antara *form* pengiriman *tape back-up* dengan aset
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah *tape back-up* yang tidak sesuai dengan form pengiriman b= jumlah *form* pengiriman *tape back-up.*
Frekuensi	1 tahun sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: Data *Form* Pengiriman *Tape Back-up* Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IPU 23	Pengukuran Kesesuaian *User Account*
Tujuan:	Mengukur *user account* yang tidak diperbolehkan mengakses *software*/ aplikasi karena bukan merupakan administrator

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 23	Pengukuran Kesesuaian *User Account*
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D
Metode:	Formula: (a / b) x 100% a= jumlah *user account* tak dikenal oleh sistem yang mengakses *software*/ aplikasi b= jumlah *user account* yang diperbolehkan untuk mengakses *software*/ aplikasi.
Frekuensi	3 bulan sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: Data akses dari Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

IPU 24	Pengukuran Utilisasi Aset
Tujuan:	Mengukur tingkat penggunaan aset untuk mengetahui kebutuhan penambahan kapasitas
Ruang Lingkup:	Pengukuran ini berlaku untuk Departemen Teknologi Informasi Bank D

Lampiran 8: Perincian Indikator Pengendalian Utama Tambahan (Sambungan)

IPU 24	Pengukuran Utilisasi Aset
Metode:	Formula: (a / b) x 100% a= jumlah kapasitas aset yang digunakan b= jumlah kapasitas aset yang tersedia.
Frekuensi	1 tahun sekali
Sumber Data & Prosedur Pengumpulan Data	Data yang digunakan: Data Bagian Operasional Departemen Teknologi Informasi Bank D
Indikator	Dalam pengembangan

Data Kuadran 1

Risiko	Indikator Risiko Utama (IRU)																										
	1					2					3					4					5					6				
	A1	A2	A3	A4	Σ	A1	A2	A3	A4	Σ	A1	A2	A3	A4	Σ	A1	A2	A3	A4	Σ	A1	A2	A3	A4	Σ	A1	A2	A3	A4	Σ
1	9	6	9	9	33	9				9					0					0					0					0
2	9		6		15	9	9	9	9	36					0					0					0					0
3					0					0	6	6	6	9	27	3				3					0	3			9	12
4					0					0	6		6		12	6	6	3	9	24					0	3	3	6		12
5					0					0					0					0		9	6	9	24					0
6					0					0					0					0					0					0
7					0					0					0					0					0					0
8					0					0					0					0					0					0
9					0					0					0					0					0					0
10					0					0					0					0					0					0
11					0					0					0					0					0					0
12					0					0					0					0					0					0
13					0					0					0					0					0					0
14					0					0					0					0					0					0
15					0					0					0					0					0					0
16					0					0					0					0					0					0
17					0					0					0					0					0					0
18					0					0					0					0					0					0
19					0					0					0					0					0					0
20					0					0					0					0					0					0
21					0					0					0					0					0					0
22					0					0					0					0					0					0
23					0					0					0					0					0					0
24					0					0					0					0					0					0

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

25					0				0					0					0					0				0
26					0				0					0					0					0				0
Jumlah					48				45					39					27					24				24

Data Kuadran 1

Risiko	**Indikator Risiko Utama (IRU)**																												
	7					**8**					**9**					**10**					**11**					**12**				
	A1	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**
1					0					0					0					0					0					0
2					0					0					0					0					0					0
3					0					0					0					0					0					0
4					0					0					0					0					0					0
5					0					0					0					0					0					0
6	6	9	9	6	30				3	3					0					0					0					0
7		9	9	6	24				3	3					0					0					0					0
8			6		6	9	9		9	27					0					0					0					0
9					0	9	9	9	9	36					0					0					0					0
10					0					0	6	6	9	6	27					0					0					0
11					0					0					0	9	9	9	9	36					0					0
12					0					0					0	9	9	9	9	36					0					0
13					0					0					0					0	3	6	9	9	27					0
14					0					0					0					0	3				3	9	6	9	9	33
15					0					0					0					0					0					0
16					0					0					0					0					0					0
17					0					0					0					0					0					0
18					0					0					0					0					0					0
19					0					0					0					0					0					0

20					0				0				0					0					0				0
21					0				0				0					0					0				0
22					0				0				0					0					0				0
23					0				0				0					0					0				0
24					0				0				0					0					0				0
25					0				0				0					0					0				0
26					0				0				0					0					0				0
Jumlah					60				69				27					72					30				33

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 1

Risiko	**Indikator Risiko Utama (IRU)**																										
	13					**14**					**15**					**16**					**17**					**18**				
	A1	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**	**A1**	**A2**	**A3**	**A4**	**Σ**
1					0					0					0					0					0					0
2					0					0					0					0					0					0
3					0					0					0					0					0					0
4					0					0					0					0					0					0
5					0					0					0					0					0					0
6					0					0					0					0					0					0
7					0					0					0					0					0					0
8					0					0					0					0					0					0
9					0					0					0					0					0					0
10					0					0					0					0					0					0
11					0					0					0					0					0					0
12					0					0					0					0					0					0
13					0					0					0					0					0					0
14					0					0					0					0					0					0
15	9	6	9	9	33					0					0					0					0					0
16					0	6	6	9	9	30					0	9				9	9				9					0
17					0					0		6	9	9	24					0	6			9	15					0

18					0					0					0	6	6	9	9	30					0					0
19					0					0					0					0		9	9	9	27					0
20					0					0					0					0					0	9	9	9	9	36
21					0					0					0					0					0					0
22					0					0					0					0					0					0
23					0					0					0					0					0					0
24					0					0					0					0					0					0
25					0					0					0					0					0					0
26					0					0					0					0					0					0
Jumlah					33					30					24					39					51					36

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 1

Risiko	**Indikator Risiko Utama (IRU)**																								
	19					**20**					**21**					**22**					**23**				
	A1	**A2**	**A3**	**A4**	**∑**	**A1**	**A2**	**A3**	**A4**	**∑**	**A1**	**A2**	**A3**	**A4**	**∑**	**A1**	**A2**	**A3**	**A4**	**∑**	**A1**	**A2**	**A3**	**A4**	**∑**
1					0					0					0					0					0
2					0					0					0					0					0
3					0					0					0					0					0
4					0					0					0					0					0
5					0					0					0					0					0
6					0					0					0					0					0
7					0					0					0					0					0
8					0					0					0					0					0
9					0					0					0					0					0
10					0					0					0					0					0
11					0					0					0					0					0
12					0					0					0					0					0
13					0					0					0					0					0
14					0					0					0					0					0
15					0					0					0					0					0

16					0					0					0					0					0
17					0					0					0					0					0
18					0					0					0					0					0
19					0					0					0					0					0
20					0					0					0					0					0
21	6	6	9	6	27					0					0					0					0
22					0	6	9	9	6	30					0					0					0
23					0					0															
24					0	9				9															
25					0					0	6				6	6	9	6	3	24	9		9		18
26					0					0					0			6	3	9	6	9	9	3	27
Jumlah					27					39					36					63					57

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 2

Risiko	Indikator Pengendalian Utama (IPU)																									
	1					2					3					4					5					6				
	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ
1	9				9		6			6	6				6				3	3					0	3				3
2	9				9		6			6	6	9	9	6	30		3			3					0	6	3			9
3					0		6			6					0			6		6					0		6			6
4					0		6			6					0			6		6	9	9	9	9	36					0
5	6	6			12	3	6			9	3				3					0			6		6			6		6
6	9				9					0			6	3	9			6		6					0	9	9	6	6	30
7	6				6					0			6	3	9			6		6					0		9	6		15
8			9		9		6	9		15					0					0	9	6	9	9	33					0
9			6		6		6	6		12					0					0	6	9	9	9	33					0
10	3				3					0		6			6			9		9					0					0
11			6		6			6		6					0					0					0					0
12			6		6			6		6					0					0					0					0

13	6				6					0					0					0					0					0
14					0					0					0					0					0					0
15	6	6			12					0					0					0					0					0
16	6	6			12					0					0					0					0					0
17		6			6	6				6	6			6	12					0					0	6				6
18		6			6					0					0					0					0					0
19		6			6					0					0					0					0					0
20		6		6	12	6				6			6		6	6				6					0			3		3
21	6				6					0	6				6					0	6				6					0
22	6				6	6				6					0			9		9					0					0
23					0					0					0					0	3				3					0
24					0					0					0					0					0					0
25	6				6					0	6				6					0					0					0
26					0					0					0	6				6					0					0
Jumlah					153					90					93					60					117					78

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 2

Risiko	**Indikator Pengendalian Utama (IPU)**																													
	7					**8**					**9**					**10**					**11**					**12**				
	E1	**E2**	**E3**	**E4**	**Σ**	**E1**	**E2**	**E3**	**E4**	**Σ**	**E1**	**E2**	**E3**	**E4**	**Σ**	**E1**	**E2**	**E3**	**E4**	**Σ**	**E1**	**E2**	**E3**	**E4**	**Σ**	**E1**	**E2**	**E3**	**E4**	**Σ**
1	3				3					0					0	6	6			12					0					0
2	6				6	3				3	3				3	6	6			12		3			3					0
3	6	6	6		18		6			6		6			6	6	6	6	6	24					0					0
4		6	9		15	3	6			9	3	6			9	3	3	6	6	18					0					0
5					0	9				9					0		6	6		12			6		6			9		9
6					0		6	9		15			6		6			6	3	9					0					0
7					0		6	9		15			6		6		6	6	3	15					0					0
8					0					0				3	3	6		6		12	6	9	9	9	33					0
9					0					0					0	6		6	3	15	6	6	6	9	27					0
10					0					0					0					0			6		6					0
11					0					0					0	6	6			12					0					0

12					0					0					0	9	6			15					0					0
13					0	6	6	6	6	24	6	6	6	6	24		6			6					0					0
14					0					0					0	6	9	6	6	27					0					0
15					0					0					0					0					0					0
16					0					0					0					0					0					0
17					0					0					0					0					0					0
18					0					0					0					0					0					0
19					0					0					0					0					0					0
20					0					0					0				3	3					0	6	6	6	6	24
21					0					0					0					0					0					0
22					0	9	9	9	9	36			9																	
23					0					0																				
24					0					0					0	9	6	6	9	30					0					0
25					0					0					0	6	6	6	9	27					0					0
26					0					0					0	6	6	6	9	27					0					0
Jumlah					42					117					66					309					75					33

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 2

Risiko	**Indikator Pengendalian Utama (IPU)**																													
	13					**14**					**15**					**16**					**17**					**18**				
	E1	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**
1	6				6					0	6	9	9	6	30					0					0					0
2	6	3	6	3	18					0	6	6	6	6	24					0					0					0
3					0					0					0					0					0					0
4					0					0					0				6	6					0					0
5					0					0					0					0	9	9	9	9	36					0
6					0					0					0					0					0					0
7					0					0					0	9	9	9	9	36					0					0
8					0					0					0					0					0					0
9					0					0					0					0					0					0

10			9		9					0	9	9	9	9	36					0					0					0
11					0					0	6	9	9	9	33	6	9	9	9	33					0					0
12					0					0	6	9	9	9	33	6	9	9	9	33					0					0
13					0		6			6					0					0					0					0
14					0					0					0					0				6	6					0
15					0					0					0	9	9	9	9	36	9	9	9	9	36					0
16					0					0					0	9	9	9	9	36	9	9	9	9	36					0
17					0					0					0	9	9	9	9	36	9	9	9	9	36					0
18					0					0					0	9	9	9	9	36	9	9	9	9	36					0
19					0					0					0	9	9	9	9	36	9	9	9	9	36					0
20					0					0					0					0					0					0
21					0					0					0	9	9	9	9	36	9	9	9	9	36		6	9	9	24
22					0					0					0					0					0					0
23					0					0																				
24					0					0																				
25					0					0					0					0					0					0
26					0					0					0					0					0					0
Jumlah					33					6					156					324					258					24

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 2

Risiko	Indikator Pengendalian Utama (IPU)																								
	19					20					21					22					23				
	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ	E5	E6	E7	E8	Σ	E9	E10	E11	E12	Σ	E13	E14	E15	E16	Σ
1					0					0					0					0					0
2					0					0					0					0					0
3				3	3					0					0	9	9	9	9	36					0
4					0	9	9	9	9	36					0					0					0
5				3	3					0					0					0					0
6	6	9	6	9	30				3	3					0					0					0
7					0				3	3					0					0					0

8					0					0					0					0					0
9					0					0					0					0					0
10					0					0					0					0					0
11					0					0					0					0					0
12					0					0					0					0					0
13					0					0				3	3					0	6	6	9	9	30
14	6	9	6	9	30					0					0					0					0
15					0					0					0					0					0
16					0					0					0					0					0
17					0					0					0					0					0
18					0					0					0					0					0
19					0					0					0					0					0
20					0					0	6	9	9	9	33				6	6				7	7
21					0					0					0					0					0
22					0					0															
23					0					0															
24					0					0					0					0					0
25	6	9	6	9	30				3	3					0					0					0
26	6	9	6	9	30				3	3					0					0					0
Jumlah					126					48					36					42					37

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 3

IRU	**Kriteria Pemilihan Indikator**																			
	1					**2**					**3**					**4**				
	0.21					0.112					0.189					0.054				
	E1	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**	**E1**	**E2**	**E3**	**E4**	**∑**
1	3	6			1.89	3	9	9	9	3.36		9	9		3.40	6	9			0.81
2		9			1.89		9	9	9	3.024	6	9	9		4.54		9			0.486
3		9			1.89	3	6	6		1.68		6	6	3	2.84		6			0.324
4		3		3	1.26	3	3	6		1.344		3	6		1.70		3			0.162
5		3		6	1.89		3	6		1.008		3	6		1.70		3	6	3	0.648

6		3		3	1.26	6	3	9		2.016	6	3	9		3.40	9	3	6		0.972
7		9			1.89	6		6	9	2.352					0.00	3	3	6		0.648
8		9		9	3.78	6	6	6		2.016					0.00	3	3	6		0.648
9		6			1.26		6	6		1.344		3			0.57		3	6		0.486
10		9			1.89	6		6	3	1.68		6	9	9	4.54					0
11		3			0.63	6		6	3	1.68		6	9	9	4.54					0
12	6	6			2.52	9		9	9	3.024		6	9	9	4.54	6				0.324
13		6			1.26	9		9	3	2.352		6			1.13	6		6		0.648
14		3			0.63			6		0.672					0.00					0
15		3			0.63	3		6		1.008					0.00					0
16		6			1.26			6		0.672					0.00	6				0.324
17		6			1.26			6		0.672					0.00					0
18	6	6			2.52			6	6	1.344					0.00	6		6		0.648
19		6			1.26	6		6		1.344					0.00					0
20		6			1.26	6	3	6		1.68		3	6		1.70		3			0.162
21		6			1.26	6	6	6		2.016		6			1.13		6			0.324
22		6			1.26		6	6												
23		6			1.26	9	6	6												

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 3

IRU	Kriteria Pemilihan Indikator																		Total
	5				6					7					8				
	0.123				0.17					0.048					0.095				
	E2	E3	E4	∑	E1	E2	E3	E4	∑	E5	E6	E7	E8	∑	E5	E6	E7	E8	∑	
1	9	9	9	4.428		9	9		3.06		9			0.432	6	6	6		1.71	19.09
2	9	9	9	3.321		9	9		3.06		9			0.432		9	6		1.425	18.17
3	6	9		2.214		6	9	3	3.06		6			0.288		3	9	3	1.425	13.72

4	3	6		1.107		3	6	3	2.04		3		3	0.288		3	6	3	1.14	9.04
5	3	6		1.107		3		6	1.53		3	6		0.432		3	6	9	1.71	10.03
6	3	9		2.214		3	9	3	2.55	9	3		3	0.72		3	6	3	1.14	14.27
7			9	1.107		3	6		1.53		3			0.144					0	7.67
8	6		9	2.583		3	6		1.53	6	3			0.432					0	10.99
9	3			0.369		3	6		1.53		3			0.144		6			0.57	6.27
10	6	6	6	2.214			6		1.02		3	6		0.432		3			0.285	12.06
11	6	6	6	2.214			6		1.02		3	6		0.432	3	3	6		1.14	11.65
12	6	6	6	2.214			6		1.02	3	3	6		0.576		3	6		0.855	15.07
13	6			0.738			6	3	1.53		3			0.144		3			0.285	8.09
14				0			6		1.02					0	3				0.285	2.61
15				0			6		1.02					0					0	2.66
16				0			6		1.02					0					0	3.28
17				0	6		6		2.04					0					0	3.97
18		6		0.738			6		1.02	3			3	0.288					0	6.56
19				0	6		6		2.04					0					0	4.64
20	3	6		1.107		3	6		1.53											
21	6	6		2.214		6	6		2.04											
22	6			0.738		6	6		2.04	3	6			0.432		6			0.57	7.84
23	6			0.738	9	6	6		3.57		6			0.288		6			0.57	10.24

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 4

IPU	Kriteria Pemilihan Indikator																			
	1					2					3					4				
	0.21					0.112					0.189					0.054				
	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ	E1	E2	E3	E4	Σ
1	3	6			1.89	9			9	2.02			6		1.13					0.00
2		6			1.26	9				1.01			6		1.13					0.00

3		6	6		2.52			9		1.01	6		9		2.84	9				0.49
4		6			1.26			9	3	1.34			9		1.70					0.00
5		6			1.26			9		1.01			9		1.70					0.00
6		6	6		2.52	9				1.01	6		9		2.84					0.00
7		6	6		2.52	9				1.01			6		1.13			6		0.32
8		6		6	2.52	9	6	9	6	3.36		6	9	3	3.40	3	6		6	0.81
9		6		6	2.52	9	6	9	6	3.36		6	9	3	3.40	3	6		6	0.81
10	3	6	9		3.78			6	9	1.68			9		1.70	3				0.16
11		6			1.26			6		0.67			6		1.13			6		0.32
12					0.00			6		0.67			9		1.70					0.00
13		6			1.26	6	6	6	3	2.35			9		1.70					0.00
14		6			1.26			6		0.67			6		1.13		6	6		0.65
15		6	6		2.52			6		0.67			6		1.13		6	6	3	0.81
16		6	6	3	3.15			6	6	1.34					0.00		3	3	3	0.49
17		6	6	6	3.78		3	6	6	1.68			6	6	2.27		3	6	6	0.81
18		6	3	3	2.52			6	6	1.34		6	6	6	3.40		3	3		0.32
19		6	6		2.52					0.00			6	6	2.27		6	6		0.65
20		6	6		2.52			3												
21		9		6	3.15	9														
22		9	9	6	5.04		3	6	9	2.02		6	9	6	3.97		9	9		0.97
23		6	6	6	3.78		3	9	9	2.35		3	9	9	3.97		6	9	6	1.13

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 4

IPU	Kriteria Pemilihan Indikator																				Total
	5					6					7					8					
	0.123					0.17					0.048					0.095					
	E1	E2	E3	E4	∑	E1	E2	E3	E4	∑	E5	E6	E7	E8	∑	E5	E6	E7	E8	∑	
1	6		6	9	2.58			6		1.02	9		6	3	0.86			6		0.57	10.08

2	6		6		1.48			6		1.02	9		6		0.72			6		0.57	7.19
3			9		1.11			9		1.53			6		0.29			6		0.57	10.34
4			9	3	1.48	6		9		2.55			6	3	0.43	3		6		0.86	9.62
5			9		1.11			6		1.02			6		0.29			6	6	1.14	7.52
6	6				0.74			6		1.02	9		6		0.72		6	6		1.14	9.98
7					0.00			9		1.53	6		6		0.58		6	6		1.14	8.23
8		6	9	9	2.95		6	6	3	2.55	6	6	3		0.72		6	6	6	1.71	18.02
9		6	9	9	2.95		6	9	3	3.06	6	6	6	3	1.01		6	6	6	1.71	18.82
10			9		1.11	6		9		2.55			6	9	0.72	6		6	3	1.43	13.13
11			9		1.11	6		6		2.04			6		0.29		6	6		1.14	7.97
12			9		1.11			9		1.53			6		0.29			6		0.57	5.87
13			6		0.74			9		1.53	6		6		0.58			9	3	1.14	9.30
14			9		1.11		3	6		1.53		3			0.14		6	6		1.14	7.64
15					0.00		3	3		1.02		3	3		0.29		6	6		1.14	7.58
16					0.00		3	3		1.02		3	3		0.29		6	6		1.14	7.43
17					0.00		3	3		1.02		3	3		0.29		3	3	3	0.86	10.70
18		6	6		1.48		3	3		1.02		3	3		0.29		3	3		0.57	10.94
19			3	3	0.74		3	3		1.02			6	3	0.43		3	3		0.57	8.20
20	3	3			0.74		3	3		1.02											
21	6			6	1.48		3			0.51											
22		6	9	6	2.58		3	9		2.04		3	9		0.58		6	9		1.43	18.62
23		6	9	6	2.58		3	9	3	2.55		3	9		0.58		3	6		0.86	17.80

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

Data Kuadran 5 Dan 6

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
3.1	Persentase pemenuhan TI sesuai dengan kesepakatan dalam rangka	a.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal Dalam	a.Pengukuran Pelaksanaan *Update Antivirus* (6)

	mendukung implementasi strategi Bank D	Pengembangan Aplikasi (6)	b.Pengukuran Tingkat Pemahaman (3)
			c.Pengukuran Efektivitas Training (3)
		b.Pengukuran Tingkat Kinerja *Robotic* (6)	d.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (3)
3.2	Persentase proyek TI lainnya yang diselesaikan sesuai dengan tahapan yang direncanakan	a.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal Dalam Pengembangan Aplikasi (6)	-
		b.Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian (6)	
		c.Pengukuran Tingkat Keakuratan Dok. Teknis Tiap Seksi dan Kelompok (3)	

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
3.3	Peningkatan pemanfaatan infrastruktur TI yang telah diimpl ementasikan di Bank D	a.Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D (12)	a.Pengukuran Utilisasi Aset (27)
		b.Pengukuran Tingkat Kerusakan *Notebook* (6)	b.Pengukuran Pelaksanaan *Back-Up* Informasi

		c.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (6)	Personil Unit Kerja (15)
		d.Pengukuran Tingkat Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D (6)	c.Pengukuran Keefektifan Penanganan Insiden / Event (9)
		e.Pengukuran Tingkat Kinerja *Robotic* (6)	d.Pengukuran *Form* Peminjaman Aset (6)
		f.Pengukuran Tingkat Kinerja PC Teleks (6)	e.Pengukuran Pelaksanaan *Update Antivirus* (3)
		g.Pengukuran Tingkat Kinerja *Mainframe* (6)	f.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (6)
		h.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	
		i.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (3)	
		j.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal Dalam Pengembangan Aplikasi (3)	
No.	**Indikator Kinerja Utama (IKU)**	**Indikator Risiko Utama (IRU)**	**Indikator Pengendalian Utama (IPU)**
4.1	Persentase *downtime* sistem aplikasi kritikal dan *e-mail*	a.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (15)	a.Pengukuran Utilisasi Aset (15)

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

		b.Pengukuran Tingkat Kinerja *Mainframe* (12)	b.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (12)
		c.Pengukuran Tingkat Gangguan AC (9)	c.Pengukuran Pelaksanaan *Update Antivirus* (6)
		d.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (6)	d.Pengukuran Keefektifan Penanganan Insiden / *Event* (6)
		e.Pengukuran Tingkat Kinerja *Robotic* (6)	e.Pengukuran *Form* Peminjaman Aset (6)
		f.Pengukuran Tingkat Kerusakan *Thermal Control* (6)	f.Pengukuran Audit *Security Log* (3)
		g.Pengukuran Tingkat Ketersediaan *Thermal Control* (6)	g.Pengukuran Kesesuaian *User Account* (3)
4.2	Persentase *downtime* jaringan Bank D-NET	a.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (9)	a.Pengukuran Utilisasi Aset (21)
		b.Pengukuran Tingkat Gangguan AC (9)	b.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (15)
		c.Pengukuran Tingkat Kinerja Departemen Teknologi Informasi Bank D (6)	Event (12)

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)

4.2	Persentase *downtime* jaringan Bank D-NET	d.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (6)	d.Pengukuran Kesesuaian *User Account* (9)
		e.Pengukuran Tingkat Kinerja *Mainframe* (6)	e.Pengukuran *Form* Peminjaman Aset (6)
		f.Pengukuran Tingkat Kerusakan *Thermal Control* (6)	f.Pengukuran Audit *Security Log* (6)
		g.Pengukuran Tingkat Ketersediaan *Thermal Control* (6)	g.Pengukuran *Form* Pengiriman *Tape Backup* (6)
4.3	Jumlah keberhasilan simulasi aplikasi kritikal	a.Pengukuran Tingkat Kinerja *Mainframe* (12)	-
		b.Pengukuran Tingkat Kinerja *Robotic* (6)	
		c.Pengukuran Tingkat Keakuratan Dok. Teknis Tiap Seksi dan Kelompok (6)	
		d.Pengukuran Tingkat Keakuratan SOP Seksi dan Bagian (6)	
		e.Pengukuran Tingkat Kehilangan Tape / Catridge hasil backup data yang akan dikirim ke DRC	
5.1	Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti	a.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (21)	a.Pengukuran Keefektifan Penanganan Insiden / *Event* (18)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
5.1	Jumlah rekomendasi hasil evaluasi sistem pengamanan TI yang ditindaklanjuti	b.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (18)	b.Pengukuran Kesesuaian *User Account* (15)
		c.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi (15)	c.Pengukuran Pelaksanaan *Update Antivirus* (12)
		d.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (12)	d.Pengukuran Audit *Security Log* (6)
		e.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (12)	e.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (3)
		f.Pengukuran Tingkat Kerusakan *Notebook* (9)	f.Pengukuran *Form* Pengiriman *Tape Backup* (3)
		g.Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D (6)	g.Pengukuran Utilisasi Aset (3)
5.2	Maksimum waktu penanggulangan serangan virus yang menyebar secara massal	a.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (24)	a.Pengukuran Keefektifan Penanganan Insiden / *Event* (18)
		b.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (9)	b.Pengukuran Pelaksanaan *Update Antivirus* (9)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
5.2	Maksimum waktu penanggulangan serangan virus yang menyebar secara massal	c.Pengukuran Tingkat Kinerja PC Teleks (3)	c.Pengukuran Efektivitas *Training* (3)
			d.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (3)
			e.Pengukuran Audit *Security Log* (3)
5.3	Indeks hasil *assessment* atas kecukupan dan efektivitas ISMS	a.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (18)	a.Pengukuran Pelaksanaan *Update Antivirus* (24)
		b.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (15)	b.Pengukuran Kelengkapan dan Kebenaran Data pada Database Asset (21)
		c.Pengukuran Tingkat Kerusakan *Notebook* (9)	c.Pengukuran Keefektifan Penanganan Insiden / *Event* (21)
		d.Pengukuran Tingkat Penerapan Informasi Kajian/ Laporan Internal dan Eksternal Dalam Pengembangan Aplikasi (9)	d.Pengukuran Keefektifan Pelaksanaan Penerimaan Tamu (21)
		e.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (9)	e.Pengukuran Tingkat Pemahaman (21)
		f.Pengukuran Tingkat Kehilangan atau Kerusakan Web Departemen Teknologi Informasi Bank D (9)	f.Pengukuran Efektivitas *Training* (21)

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
5.3	Indeks hasil *assessment* atas kecukupan dan efektivitas ISMS	g.Pengukuran Tingkat Gangguan AC (9)	g.Pengukuran Kesesuaian *User Account* (21)
		h.Pengukuran Tingkat Penurunan Kinerja Web Departemen Teknologi Informasi Bank D (6)	h.Pengukuran Kesesuaian Kontrol Akses Fisik Ruangan Kerja Unit Kerja (15)
		i.Pengukuran Tingkat Pemanfaatan R.Pelatihan (6)	i.Pengukuran Pelaksanaan *Back-Up* Informasi Personil Unit Kerja (15)
		j.Pengukuran Tingkat Keakuratan Dok. Pembebanan Anggaran Pelaksanaan SOSA (6)	j.Pengukuran *Form* Peminjaman Aset (15)
			k.Pengukuran Audit *Security Log* (15)
		k.Pengukuran Tingkat Keakuratan Dok. Pengadaan Kunci Telegram BD (6)	l.Pengukuran Tingkat Pemeliharaan/ Perbaikan Aset (9)
		l.Pengukuran Tingkat Keakuratan Dok. PKAT (6)	m.Pengukuran *Form* Pengiriman *Tape Backup* (9)
		m.Pengukuran Tingkat Keakuratan Data Unit Kerja Yang Telah Diolah (6)	n.Pengukuran Utilisasi Aset (12)
		n.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	
		o.Pengukuran Tingkat Kerusakan *Thermal Control* (6)	
		p.Pengukuran Tingkat Ketersediaan *Thermal Control* (6)	
		q.Pengukuran Tingkat Kehilangan *Tape / Catridge* hasil backup data yang akan dikirim ke DRC (3)	

Lampiran 9: Perincian Data Form Kuesioner Tahap II (Sambungan)

No.	Indikator Kinerja Utama (IKU)	Indikator Risiko Utama (IRU)	Indikator Pengendalian Utama (IPU)
6.1	Jumlah materi/ topik TI yang disosialisasikan berdasarkan kebutuhan hasil *mapping*	a.Pengukuran Tingkat Kerusakan *Notebook* (9)	a.Pengukuran Tingkat Pemahaman (6)
		b.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (9)	b.Pengukuran Kelengkapan dan Kebenaran Data pada Database Aset (3)
		c.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	
6.2	Peningkatan pemahaman peserta setelah sosialisasi	a.Pengukuran Tingkat Kerusakan *Notebook* (18)	a.Pengukuran Kelengkapan dan Kebenaran Data pada Database Asset (9)
		b.Pengukuran Tingkat Kehilangan *Notebook* atau Komponennya (15)	b.Pengukuran Pelaksanaan *Update Antivirus* (9)
		c.Pengukuran Tingkat Kehilangan dan Tingkat Keakuratan Informasi Kajian/ Laporan Internal dan Eksternal (6)	c.Pengukuran Keefektifan Penanganan Insiden / *Event* (9)
		d.Pengukuran Tingkat Kehilangan dan Kerusakan Aset Pada Ruang Direktur dan Deputi Direktur (6)	d.Pengukuran Tingkat Pemahaman (6)
		e.Pengukuran Tingkat Keakuratan Dok. Pembebanan Anggaran Pelaksanaan SOSA (6)	e.Pengukuran Efektivitas *Training* (3)
		f.Pengukuran Tingkat Serangan Virus Terhadap Data Unit Kerja Yang Telah Diolah (6)	

Lampiran 10: Kriteria Penentuan Kecenderungan, Dampak, dan Level Risiko

Kriteria Penentuan Kecenderungan Risiko

SKALA	katagori	KRITERIA PENGUKURAN	
		FREKUENSI TERJADI	KEMUNGKINAN/POTENSI TERJADI
1	Rendah	**Sangat jarang terjadi,** **misal hanya terjadi dalam kondisi sangat tak biasa/normal, atau terjadi sekali dalam kurun waktu 10 tahun atau lebih atau frekuensi terjadi 0,000001% dari total frekuensi kejadian selama periode tertentu.**	Sangat kecil kemungkinan terjadi dalam kondisi apapun. Kemungkinan terjadi dalam jangka waktu yang sangat lama (misal >20 th)
2	Rendah	**Jarang sekali terjadi,** **misal hanya terjadi dalam kondisi sangat tak normal, atau terjadi sesekali dalam kurun waktu antara 5-10 tahun, atau frekuensi terjadi 0,0001% dari total frekuensi kejadian selama periode tertentu.**	Kecil kemungkinan terjadi atau hanya sesekali terjadi dalam kondisi yang diluar kebiasaan atau di luar kondisi normal Kemungkinan terjadi dalam jangka waktu yang cukup lama (misal 15-20 tahun)
3	Rendah	**Jarang terjadi,** misal terjadi di luar kondisi kenormalan, atau sesekali terjadi dalam kurun waktu antara 3-5 tahun, atau frekuensi terjadi 0,001% dari total frekuensi kejadian selama periode tertentu	Kecil kemungkinan terjadi dalam kondisi normal atau hanya terjadi dalam kondisi yang di luar kebiasaan/normal Kemungkinan terjadi dalam jangka waktu yang relatif lama (misal 10-15 tahun)
4	Sedang	**Acap terjadi** misal sesekali terjadi dalam periode tertentu pengamatan	Relatif kecil kemungkinan terjadi dalam kondisi normal/biasa Kemungkinan terjadi dalam jangka waktu 5-10 tahun
5	Sedang	**Cukup acap terjadi** misal beberapa kali terjadi selama periode tertentu pengamatan	Mungkin terjadi (bisa ya bisa tidak) Kemungkinan terjadi dalam jangka waktu 3-5 tahun
6	Sedang	**Acapkali terjadi** misal beberapa kali terulang terjadi selama periode tertentu pengamatan	Cukup besar kemungkinan terjadi dalam berbegai kondisi Kemungkinan terjadi dalam jangka waktu 1-3 tahun
7	Tinggi	Sangat acap terjadi/Acap berulang misal cukup sering terulang terjadi kejadian selama periode tertentu pengamatan	Besar kemungkinan terjadi dalam berbagai kesempatan/kondisi normal Kemungkinan terjadi dalam jangka waktu tertentu (antara 6-12 bulan) untuk kegiatan berkala minimal triwulanan)
8	Tinggi	Cukup sering terjadi misal kejadian cukup sering terjadi selama periode tertentu pengamatan	Sangat besar kemungkinan terjadi Dipastikan kemungkinan terjadi dalam jangka waktu tertentu (3-6 bulan) atau sebagian besar terjadi pada setiap pelaksanaan kegiatan
9	Tinggi	Sering terjadi, terjadi pada sebagian besar kejadian selama periode tertentu pengamatan.	Dapat dipastikan terjadi Dipastikan kemungkinan terjadi dalam jangka yang sangat relatif pendek (1-3 bulan)
10	Tinggi	Sangat sering terjadi, selalu terjadi pada setiap kejadian selama periode pengamatan	Dipastikan terjadi setiap saat dalam berbagai kondisi/terjadi setiap kali pelaksanaan kegiatan, Kemungkinan terjadi dalam jangka yang sangat pendek (<1 bulan) khususnya untuk kejadian non rutin.

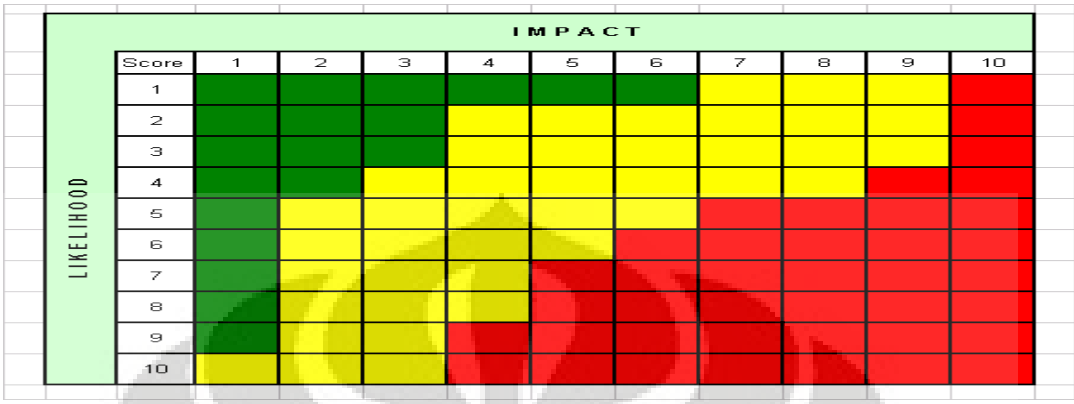
Lampiran 10: Kriteria Penentuan Kecenderungan, Dampak, dan Level Risiko (Sambungan)

Kriteria Penentuan Dampak Risiko

SKALA	KATAGORI	OPERASIONAL	FINANSIIL
1	Rendah	Tidak mengakibatkan gangguan operasional	kerugian/biaya s.d Rp300 juta
			Tidak terdapat kenaikan biaya secara overall
2		menimbulkan gangguan pada proses namun insignifikan	kerugian/biaya antara Rp 300 juta s.d Rp300 juta
			Kenaikan biaya antara 0,1 sampai 2%
3		menimbulkan gangguan yang relatif minor	kerugian/biaya antara Rp 600 juta s.d Rp1 milyar
			Kenaikan biaya 2-5%
4	Sedang	menimbulkan gangguan operasional yang berakibat penundaan dalam jangka waktu singkat	kerugian/biaya antara Rp1 milyar s.d Rp3 milyar
			Kenaikan biaya antara 5-7%%
5		menimbulkan gangguan yang timbulkan penundaan proses/kegiatan dalam jangka waktu tertentu	kerugian/biaya antara Rp3 milyar s.d Rp6 milyar
			Kenaikan biaya antara 7 sampai 10%
6		Timbulkan gangguan pada pelaksanaan proses utama yang berakibat pada pencapaian tujuan	kerugian/biaya antara Rp6 sampai Rp10 milyar
			Kenaikan biaya antara 10 sampai 15%
7	Tinggi	menimbulkan gangguan yang dapat mempengaruhi overall pencapaian tujuan/penyelenggaraan kegiatan	kerugian/biaya antara Rp10 milar s.d Rp30 milyar
			Kenaikan biaya antara 15 sampai 20%
8		menimbulkan kelumpuhan fungsional selama jangka waktu tertentu	kerugian/biaya antara Rp30 milyar s.d Rp60 milyar
			Kenaikan biaya antara 20% sampai 25%
9		menimbulkan kegagalan operasional sebagian besar fungsi utama	kerugian/biaya antara Rp60 milyar s.d Rp100 milyar
			Kenaikan biaya antara 25% sampai 30%
10		menimbulkan kelumpuhan secara overall pada pelaksanaan fungsi BI	kerugian/biaya > Rp100 milyar
			Kenaikan biaya >30%

Lampiran 10: Kriteria Penentuan Kecenderungan, Dampak, dan Level Risiko (Sambungan)

Penentuan Level Risiko



Keterangan:

Hijau = rendah

Kuning = sedang

Merah = tinggi