UNIVERSITAS INDONESIA

SIMULASI ANALISIS RISIKO DAN PENILAIAN PROSES BISNIS TERKAIT PENGAMANAN INFORMASI PADA INFRASTRUKTUR INTERNET

(Simulation of Risk Analysis and Business Process Assessment Related to Information Security on Internet Infrastructure)

SKRIPSI

Ridho Zamzam
0606043723

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INDUSTRI
DEPOK
DESEMBER 2008

UNIVERSITAS INDONESIA

SIMULASI ANALISIS RISIKO DAN PENILAIAN PROSES BISNIS TERKAIT PENGAMANAN INFORMASI PADA INFRASTRUKTUR INTERNET

(Simulation of Risk Analysis and Business Process Assessment Related to Information Security on Internet Infrastructure)

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar
SARJANA TEKNIK

Ridho Zamzam
0606043723

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INDUSTRI
DEPOK
DESEMBER 2008

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	: Ridho Zamzam
NPM	: 0606043723
Tanda tangan	:
Tanggal	:

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh	:
Nama	: Ridho Zamzam
NPM	: 0606043723
Program Studi	: Teknik Industri
Judul Skripsi	: Simulasi Analisis Risiko dan Penilaian Proses Bisnis terkait Pengamanan Informasi pada Infrastruktur Internet *(Simulation of Risk Analysis and Business Process Assessment Related to Information Security on Internet Infrastructure)*

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

DEWAN PENGUJI

Pembimbing	: Ir. Akhmad Hidayatno, MBT	(…….)
Penguji	: Dr. Ir. T. Yuri M. Zagloel, MEngSc	(…….)
Penguji	: Ir. Amar Rachman, MEIM	(…….)
Penguji	: Arian Dhini, ST, MT	(…….)

Ditetapkan di : ……

Tanggal : ……

UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih kepada:

1. Allah SWT. Atas rahmat-Nya, karya tulis ini dapat diselesaikan.
2. Keluarga tercinta, papah, mamah, kakak, gem, ayu, izam, dan seluruhn keluarga dan kerabat. Terima kasih atas doa dan dukungannya.
3. Dr. Ir. T. Yuri M. Zagloel, MEngSc., dan Ir. Fauzia Dianawati, MSi., selaku KaDep dan SekDep Teknik Industri Universitas Indonesia.
4. Ir. Akhmad Hidayatno MBT., dan Ir. Erlinda Muslim, MEE., selaku dosen pembimbing skripsi dan dosen pembimbing akademis. Terimakasih atas bimbingan, dukungan dan semangat yang diberikan.
5. Ir. Boy Nurtjahyo M., MSIE. Terimakasih atas bantuan yang begitu banyak, bimbingan, dukungan dan semangat yang diberikan.
6. Pak Amar, Pak Omar, Pak Yad, Ibu Betrianis, Ibu Isti, Ibu Dhini. Terima kasih atas semua masukan yang diberikan dalam penulisan skripsi ini.
7. Pak Fadjar, Pak Agung, dan seluruh rekan tim proyek Perluasan Lingkup Setifikasi ISO 27001-2005 : BI, trimakasih atas kerjasama, dukungan dan masukan dalam penulisan skripsi ini.
8. Pak Wayan Toni S selaku Kasi Operasi Akses Protokol Internet (DitJen PosTel), Pak Oki S, Pak Hadi P, Mbak Dwi Ely P. Trimakasih atas ketersediaan data, bantuan dan semangt yang diberikan selama penelitian.
9. Bapak Prof. Richardus Eko Indrajit, DrBA, MSc, MBA, MA/MSi, MPhil, Ir., dan Bapak Muhammad Salahuddien M, ST, selaku pimpinan dan wakil pimpinan, Pak Mantra, Pak Mizamil, Pak Bisyron, selaku manager, serta para staff ID-SIRTII. Terimakasih atas bantuan selama masa penelitian.
10. IE-ers satu angkatan, atas semangat dan dorongan kepada penulis selama ini.

Akhir kata, semoga karya tulis ini berguna dan bermanfaat bagi semua pihak, baik itu kalangan akademis dan praktisi ataupun instansi terkit lainnya.

Depok, 12 Desember 2008

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan dibawah ini:

Nama	: Ridho Zamzam
NPM	: 0606043723
Program Studi	: Teknik Industri
Departemen	: Teknik Industri
Fakultas	: Teknik
Jenis Karya	: Skripsi

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

Simulasi Analisis Risiko dan Penilaian Proses Bisnis terkait Pengamanan Informasi pada Infrastruktur Internet – *(Simulation of Risk Analysis and Business Process Assessment Related to Information Security on Internet Infrastructure)*

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada Tanggal : 12 Desember 2008

Yang menyatakan,

(Ridho Zamzam)

RIWAYAT HIDUP PENULIS

Nama : Ridho Zamzam
Tempat, Tanggal Lahir : Jakarta, 22 Februari 1984
Alamat : Jl. Nangka permai No. 1 RT 04/17 Perumnas 1 Bekasi Selatan 17144

Pendidikan

a.	Sekolah Dasar	:	SD Negeri Rawa Tembaga 1 (1990 – 1996)
b.	Sekolah Menengah Pertama	:	SMP BPS&K 3 Bekasi (1996 – 1999)
c.	Sekolah Menengah Umum	:	SMU Negeri 3 Bekasi (1999 – 2002)
d.	Diploma 3	:	Teknik Produksi, Jurusan Teknik Mesin, Politeknik Negeri Jakarta (2002 – 2005)
e.	Strata 1	:	Departemen Teknik Industri, Fakultas Teknik, Universitas Indonesia (2006 – 2008)

Pelatihan	:	• Manajerial Kewirausahaan Kota Bekasi dan Komputer Akuntansi, STIAMI (2002) • Mekatronik, FESTO, PNJ (2004) • *Injury Prevention Program* (K3), *Schlumberger* (2004) • *Injury Prevention Program* (K3), DISNAKERTRANS, TRAKINDO, PNJ (2004)
Organisasi	:	• OSIS, DKM/ ROHIS (1999 – 2001) • KIR, GALAKSI (2001 – 2002) • HMM , FIKRI (2003 – 2004)

ABSTRAK

Nama : Ridho Zamzam
Program Studi : Teknik industri
Judul : Simulasi Analisis Risiko dan Penilaian Proses Bisnis terkait Pengamanan Informasi pada Infrastruktur Internet.
(Simulation of Risk Analysis and Business Process Assessment Related to Information Security on Internet Infrastructure).

Skripsi ini membahas pemetaan proses bisnis dan penilaian kritikalitas pengamanan informasi dalam proses bisnis terkait manajemen risiko guna menunjang Sistem Manajemen Pengamanan Informasi (ISMS) berdasarkan ISO/IEC 27001:2005 dan ISO/IEC 17799:2005 sebagai panduan pengendaliannya. Penelitian ini bertujuan untuk memperoleh alternatif *risk treatment* dan model simulasi peramalan serta optimasi alokasi biaya berdasarkan analisa risiko dan proses penilaian *(dengan metode FRAAP - Facilitated Risk Analysis and Assessment Process)* terhadap proses bisnis yang terkait dengan *Information Security* pada Infrastruktur Internet. Hasil penelitian ini juga akan memperlihatkan prioritas alternatif *risk treatment* berdasarkan simulasi peramalan dan optimasi pengalokasian dana guna pengendalian risiko.

Kata kunci:
Simulasi, analisis risiko, proses penilaian risiko, proses bisnis, alternatif *risk treatment*, pengamanan informasi, ISMS, infrastruktur internet,

ABSTRACT

Name : Ridho Zamzam
Study Program : Industrial Engineering
Title : *Simulation of Risk Analysis and Business Process Assessment Related to Information Security on Internet Infrastructure*

The focus of this study is about business process mapping and criticality assessment of information security in business process related to risk management in order to support Information Security Management System (ISMS) base on ISO/IEC 27001:2005 and ISO/IEC 17799:2005 as a guide of control objectives. The purpose of this study is to obtain risk treatment alternatives and forecasting simulation model and also optimization of fund allocation base on risk analysis and business process assessment (with FRAAP method) that related to information security on internet infrastructure. The outcome of this study also showing risk treatment alternative priority base on forecasting simulation and optimization of fund allocation in order to controlling risk.

Key words:
Simulation, risk analysis, risk assessment process, business process, risk treatment alternative, information security, ISMS, internet infrastructure

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR SINGKATAN

AS/NZS	Australia/New Zealand Standard
CERT	*The Computer Emergency Response Team*
CIA	*confidentiality, integrity, availability*
FRAAP	*Facilitated Risk Analysis and Assessment Process*
ICOM	*Input, Control, Output, Mechanism*
ID-SIRTII	*Indonesia – Security Incident Response Team on Internet Infrastructure*
IDEF0	*Integration DEFinition language 0*
ISMS	*Information Security Management System*
ISO/IEC	*International Standard Organization/ International Electrotechnical Commission*
IT	*Information Technology*
NIST	*National Institute of Standards and Technology*
PDCA	*Plan-Do-Check-Action*
PMBOK	*Project Management Body of Knowledge*
PMI	*Project Management Institute*

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Teknologi Informasi saat ini telah menjadi sebuah perangkat kerja yang mutlak diperlukan dalam kegiatan operasional sebuah perusahaan. Hal ini terlihat dari banyaknya sistem aplikasi yang digunakan. Dengan demikian, keamanan informasi berbasis teknologi telah menjadi suatu hal yang penting.

Seiring dengan meningkatnya ketergantungan organisasi pada sistem informasi yang terotomatisasi, semakin meningkat pula tingkat kerentanan organisasi terhadap risiko-risiko seperti sabotase dan gangguan terhadap proses bisnis organisasi.

Faktor-faktor *Socio-Organizational* seperti karyawan perusahaan, kebijakan perusahaan dan *organizational culture* bersifat penting dalam memastikan keamanan sistem informasi karena sistem informasi meliputi teknologi yang dirancang, dipelihara, dipertahankan, dan digunakan oleh mereka yang berada dalam organisasi untuk memudahkan kerja, mendukung pembagian informasi dan proses-proses pekerjaan dan untuk melakukan transaksi bisnis. Sumber daya ini justru sering diabaikan guna meng-*cover* kelemahan-kelemahan perangkat keamanan sistem informasi. Sebaliknya, keamanan sistem informasi yang berdasar pada suatu pemahaman faktor organisasi menyediakan suatu pertahanan untuk melawan ancaman-ancaman ini.[1]

Manajemen risiko dapat dilakukan dengan bermacam metodologi dan pendekatan yang ditujukan untuk tujuan yang berbeda-beda pula. Salah satu organisasi yang memperhatikan bidang IT dalah *International Standard Organization*. Salah satu pedoman *ISO* yang paling *relevant* terhadap IT adalah ISO 27001:2005. Pedoman ini mendasari aktifitas manajemen risiko, *Information*

[1] Hu, Qing. Hart, Paul. and Cooke, Donna. *"The role of external and internal influences on information systems security – a neo-institutional perspective."* dalam *Journal of Strategic Information Systems 16 (2007) 153–172. Science Direct, Elsevier*. 2007, hal 154

Technology, Security Techniques, Information Security Management System – requirements, dan juga mendasari penelitian ini.

Information security risk management merupakan proses yang menyeluruh yang mengintegrasikan identifikasi dan analisa dari risiko-risiko dengan organisasi yang bersangkutan, penilaian *(assessment)* terhadap dampak potensial dalam bisnis, dan memutuskan tindakan apa yang dapat diambil untuk menghilangkan atau mengurangi risiko ke level yang dapat diterima.[2] Kegiatan ini mengacu pada *Standards and guidelines* yang ada tentang *information security management,* seperti pada (ISO, 2005[3]; NIST, 2008[4]) Sedangkan tujuan dari *Security risk analysis* itu sendiri adalah untuk mengidentifikasi dan mengukur risiko-risiko guna menunjang proses *decision-making.*[5] Atas dasar itu manajemen risiko berperan penting sebagai suatu pelindung terhadap asset informasi organisasi, yang juga berarti melindungi visi dan misi organisasi serta proses bisnis didalamnya dari ancaman risiko-risiko terkait keamanan sistem informasi.

Risiko sama sekali tidak dapat dihilangkan. Triknya adalah jangan mencoba untuk menghilangkan semua risiko, tetapi me-*manage*-nya. Rahasia dari *risk management* yang efektif adalah kemampuan untuk mengkualifikasi dan mengkuantifikasikan elemen risiko secara obyektif dan menguranginya pada level yang dapat diterima.[6]

Penanganan risiko informasi idealnya dilakukan dengan penuh pertimbangan secara menyeluruh, namun atas dasar prinsip efektifitas dan efisiensi alokasi sumber daya perusahaan, solusi yang paling baik adalah pelaksanaan penanganan risiko berdasarkan panduan prioritas. Untuk mencapai keadaan ini salah satu cara yang efektif adalah melalui simulasi. Simulasi yang baik dan dirancang atas dasar *input* yang baik pula akan menghasilkan *output* yang dapat diandalkan sebagai salah satu dasar alternatif pengambilan keputusan penanganan risiko.

---

[2] NIST (2002). *Risk management guide for information technology systems.* National Institute of Standards and Technology (NIST) Special Publication 800-30

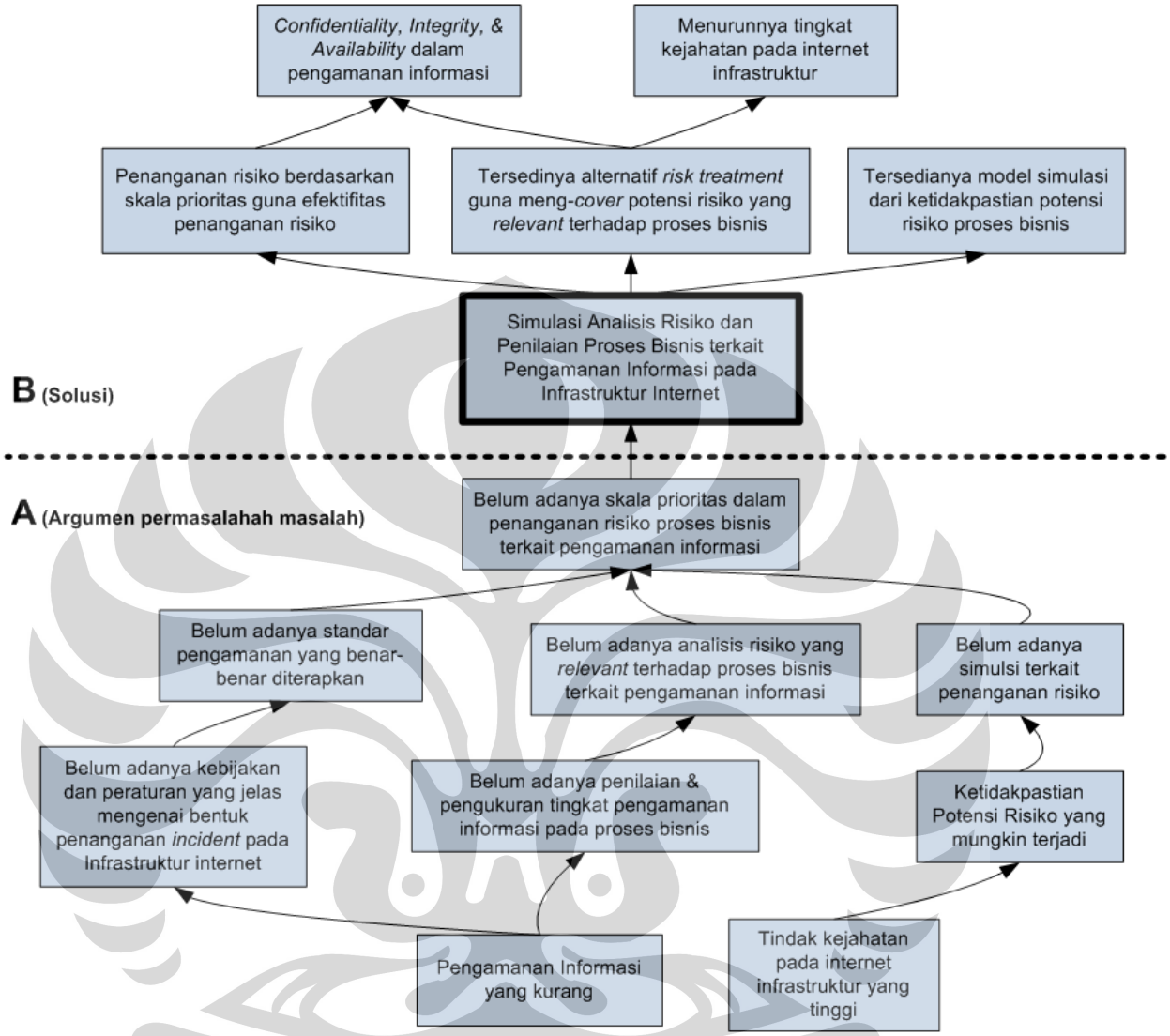
[3] ISO (2005). *Information technology-Security techniques-Information security management systems-Requirements, ISO/IEC 27001:2005*

[4] NIST (2008). *NIST Special Publications (800 Series).* Retrieved September 19, 2008.

[5] Bojanc, Rok. and Jerman-Blazic, Borka. "*An economic modeling approach to information security risk management."* dalam *International Journal of Information Management 28 (2008) 413-422. Science Direct, Elsevier.* 2008. Hal 414

[6] Merrit, James W. *Risk management.* Wang Global (703) 827-3534, from NIST. 2008. Hal 8.

1.2 DIAGRAM KETERKAITAN MASALAH



Gamabar 1.1 Diagram Keterkaitan Masalah

1.3 RUMUSAN MASALAH

Perlu adanya pemetaan proses bisnis terkait penilaian kritikalitas pengamanan informasi dalam proses bisnis. Penanganan risiko terkait pengamanan informasi terhadap proses bisnis menjadi sangat penting, guna menjaga setiap proses berfungsi sebagaimana mestinya atas dasar tuntutan akan efektifitas perusahaan. Untuk mencapai hal tersebut dan untuk meminimalkan terjadinya risiko pada proses bisnis, maka manajemen risiko yang tepat pada proses bisnis terkait *Information Security Management System* sangat diperlukan.

1.4 TUJUAN PENELITIAN

Penelitian ini bertujuan untuk memperoleh alternatif *risk treatment* dan model simulasi peramalan serta optimasi alokasi biaya dari alternatif *risk treatment* yang ada berdasarkan analisis risiko dan proses penilaian *(dengan metode FRAAP - Facilitated Risk Analysis and Assessment Process)* terhadap proses bisnis yang terkait dengan *Information Security* pada Infrastruktur Internet.

1.5 RUANG LINGKUP

Ruang lingkup penelitian ini adalah penelitian terhadap pengamanan informasi dan penilaian proses bisnis yang terkait dengan *Information Security Management System (ISMS)*. Penjabaran dan penilaian risiko yang terkait dengan proses bisnis hanya dilakukan pada satu bagian divisi/ bidang yang dianggap paling kritikal sesuai penilaian proses bisnis yang dilakukan sebelumnya. Sedangkan simulasi peramalan dan optimasi dilakukan hanya untuk memperlihatkan model alokasi biaya penanganan risiko dari alternatif *risk treatment* yang ada.

1.6 METODOLOGI PENELITIAN

Metodologi penelitian yang dilakukan terdiri dari beberapa tahap yaitu:

1. Pemilihan topik penelitian.
   Pada tahap ini, topik penelitian ditentukan dengan bantuan dari pembimbing skripsi mahasiswa, Teknik Industri – Universitas Indonesia.

2. Pemahaman dasar teori
   Pada tahap ini, disusun dan dipelajari teori-teori yang akan digunakan guna mendukung penelitian ini. Teori yang dibahas meliputi meliputi *Information Security*, Manajemen Risiko, metode IDEF0, Metode *FRAAP (Facilitated Risk Analysis and Assessment Process)*, dan model simulasi dan optimasi (OptQuest pada Crystal Ball).

3. Pengumpulan data tahap 1

Pada tahap ini, data yang diperlukan dikumpulkan, kemudian digunakan untuk melakukan pemetaan proses-proses bisnis.

Adapun data yang akan dikumpulkan antara lain:

- Data profil perusahaan, visi dan misi, serta gambaran umum struktur fungsional organisasi perusahaan.
- Peraturan-peraturan yang ada pada bagian atau divisi yang dijadikan ruang lingkup penelitian serta tugas dan fungsi operasional dari tiap bagian operational termasuk SOP tiap bagian.

Selain itu juga yang penting untuk dilakukan adalah wawancara guna mengetahui konfirmasi dari data-data yang sudah dikumpulkan serta perolehan informasi kegiatan operational secara teknis dari para staf, terkait tugas dan fungsi operasional.

4. Pengumpulan data tahap 2

   Pada tahap ini, data yang diperlukan adalah data historikal perusahaan seperti data mengenai risiko-risiko yang ada, baik yang pernah terjadi ataupun yang belum pernah terjadi, bentuk treatment yang diberikan, penilaian dampak dan probabilitas kejadiannya, yang kemudian dikumpulkan untuk nantinya akan dilakukan analisis dan penilaian risiko.

5. Pengolahan data

   Pada tahap ini, data yang telah dikumpulkan sebelumnya akan diolah menjadi peta proses bisnis dengan menggunakan metode IDEF0, kemudian dijabarkan risiko-risiko proses bisnis yang ada. Data identifikasi risiko, *assessments, treatments,* dan penentuan *risk handling* diolah dengan metode FRAAP.

6. Analisis

   Analisis dan simulasi dilakukan terhadap risiko-risiko yang relevant terhadap proses bisnis yang telah dipetakan sebelumnya, guna mendapatkan model simulasi peramalan dan optimasi alokasi biaya dari alternatif *risk treatment* yang ada guna pengendalian risiko.

7. Kesimpulan

   Menarik kesimpulan yang diperoleh dari keseluruhan proses penelitian.

1.7 SISTEMATIKA PENULISAN

Secara umum, pembahasan penelitian terdiri dari beberapa bab dengan sistemtika sebagai berikut:

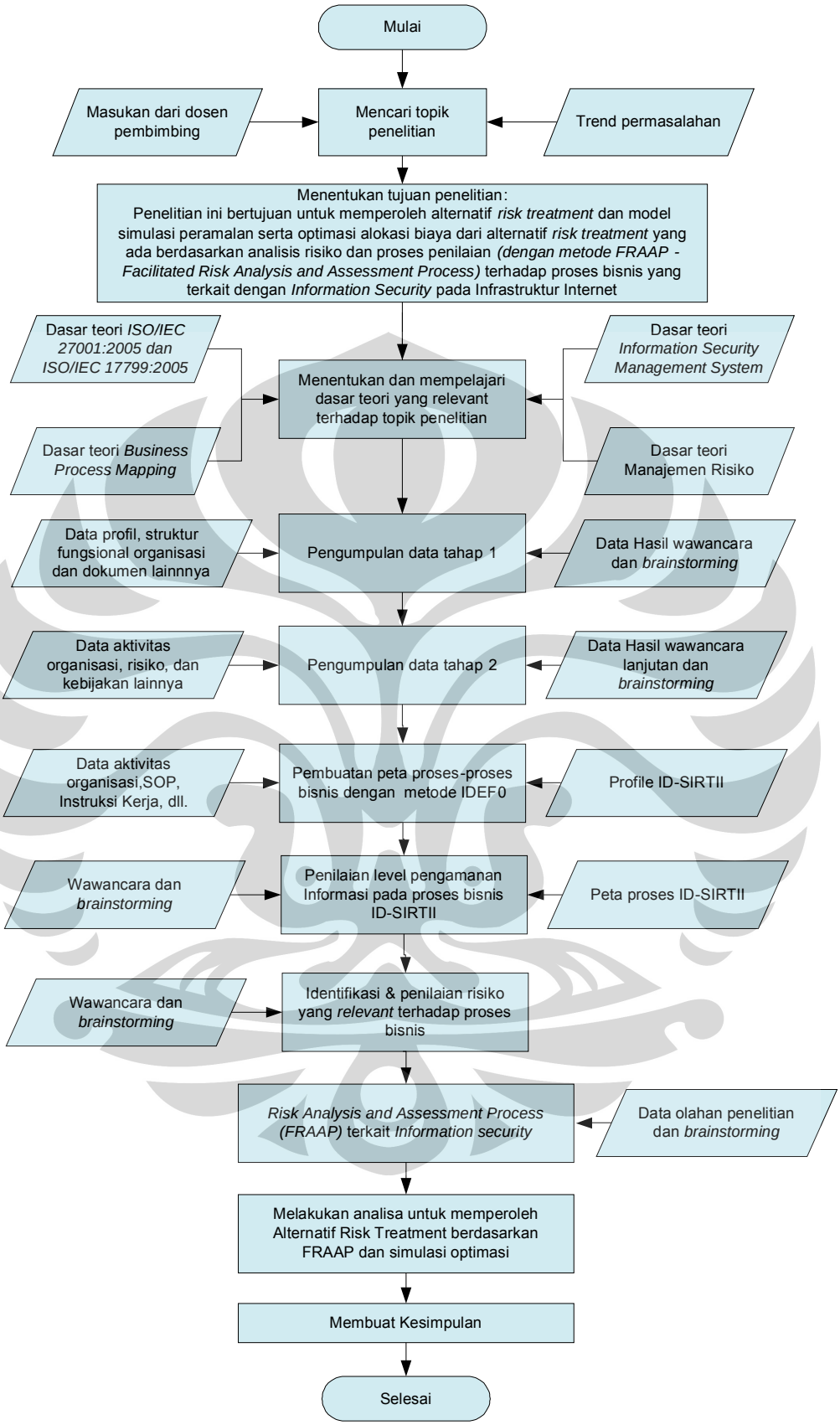
BAB 1. Merupakan pendahuluan yang menjelaskan mengenai latar belakang dilakukannya penelitian, diagram keterkaitan masalah, rumusan permasalahan, tujuan penelitian, ruang lingkup dan batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB 2. Merupakan landasan teori yang berhubungan dengan penelitian. Landasan teori yang dibahas meliputi *Information Security*, Manajemen Risiko, metode IDEF0, Metode *FRAAP (Facilitated Risk Analysis and Assessment Process)*, dan model simulasi dan optimasi (OptQuest pada Crystal Ball), serta teori-teori lainnya yang dapat membantu penelitian ini.

BAB 3. Berisi tentang pengumpulan dan pengolahan data. Pada bab ini akan dibahas mengenai data yang telah dikumpulkan selama penelitian. Data tersebut kemudian diolah. Dengan menggunakan metode IDEF0 dapat dilakukan pemetaan terhadap proses-proses bisnis, kemudian dilakuakn penilaian terhadap proses bisnis yang telah dipetakan tersebut. Dari hasil penilaian level pengamanan informasi yang dilakukan maka dapat diketahui proses bisnis yang paling kritikal yang kemudian dilakukan penilaian risiko dengan metode FRAAP.

BAB 4. Berisi tentang analisis data. Dari data penilaian risiko yang *relevant* terhadap proses bisnis yang didapat pada bab sebelumnya kemudian disusun rencana penanganan dan alternatif *risk treatment* dari potensi risiko yang ada. Setelah itu dengan bantuan *software* dibuatlah model simulasi peramalan dan optimasi alokasi dana guna penanganan risiko.

BAB 5. Merupakan kesimplan dari keseluruhan proses penelitian.



Gamabar 1.2 *Flow Process* Penelitian

BAB II
DASAR TEORI

2.1 *INFORMATION SECURITY*

Informasi adalah sebuah aset[7] seperti halnya aset-aset bisnis penting lainnya, yang sangat berharga bagi kelangsugan bisnis suatu organisasi.[8] Hal Ini menjadi sangat penting pada kondisi saat ini dimana lingkungan bisnis sudah semakin berkembang. *Information security* adalah suatu bentuk perlindungan informasi dari banyaknya ancaman-ancaman dalam rangka memastikan kelangsungan bisnis, memperkecil risiko bisnis, dan memaksimalkan peluang keuntungan bisnis.

Keamanan informasi dapat dicapai dengan menerapkan suatu control yang pas, termasuk kebijakan-kebijakan, proses-proses, prosedur-prosedur, struktur organisasi, serta fungsi software dan hardware yang baik. Kontrol ini perlu untuk dibentuk, diterapkan, dimonitor, dikaji ulang dan disempurnakan, dimana letak kepentingannya, untuk memastikan bahwa spesifik keamanan dan sasaran bisnis dari organisasi dapat dicapai. Ini harus dilaksanakan bersama dengan proses-proses bisnis manajemen lainnya.[9]

Information security atau pengamanan informasi dapat didefinisikan sebagai penjagaan terhadap kerahasiaan *(confidentiality)*, keutuhan *(integrity)*, dan ketersediaan *(availability)* dari suatu informasi; sebagai tambahan, atribut lainnya seperti *authenticity*, *accountability*, *non-repudiation*, dan *reliability* juga dapat dilibatkan. [10].

---

[7] Peltier, Thomas R. *Information Security Risk Analysis, second edition.* Auerbach Publications, Taylor & Francis Group. 2005. Hal 42

[8] ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*. 2005, Geneva, hal Viii

[9] *Ibid.*

[10] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management system – Requirements. AG meeting, 29-30 November* 2005, Geneva, hal 2

2.1.1 *ISO/IEC 17799:2005 (Information Technology – Security Techniques – Code of Practice for Information Security Management)*

Standard internasional ini menetapkan pedoman dan prinsip umum untuk memulai, menerapkan, memelihara, dan meningkatkan manajemen pengamanan informasi dalam sebuah organisasi. *Control objectives* dan pengendalian dalam standar internasional ini dimaksudkan untuk memenuhi kebutuhan yang diidentifikasikan dengan *risk assessment*. [11]

Struktur dari standar internasional ini terdiri dari 11 klausul kontrol pengamanan, yang terdiri dari 39 kategori pengamanan utama dan satu klausul pengantar yang memperkenalkan *risk assessment and treatment.*

Masing-masing area kontrol menyediakan panduan dan rekomendasi *(best practice)* dalam membuat suatu pengamanan informasi yang efektif. Kesebelas objektif kontrol tersebut dengan kategori pengamanan informasi dalam *ISO/IEC 17799:2005* yaitu;

1. (5) *Security policy*
   - (5.1) *Information security policy*
2. (6) *Organization of information security*
   - (6.1) *Internal organization*
   - (6.2) *External parties*
3. (7) *Asset management*
   - (7.1) *Responsibility for asset*
   - (7.2) *Information classification*
4. (8) *Human resources security*
   - (8.1) *Prior to employment*
   - (8.2) *During employment*
   - (8.3) *Termination or change of employment*
5. (9) *Physical and environmental security*
   - (9.1) *Secure areas*
   - (9.2) *Equipment security*

[11] ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*. 2005, Geneva, hal 1

6. (10) *Communications and operations management*
    - (10.1) *Operational procedure and responsibilities*
    - (10.2) *Third party service delivery management*
    - (10.3) *System planning and acceptance*
    - (10.4) *Protection against malicious and mobile code*
    - (10.5) *Back-up*
    - (10.6) *Network security management*
    - (10.7) *Media handling*
    - (10.8) *Exchange of information*
    - (10.9) *Electronic commerce service*
    - (10.10) *Monitoring*
7. (11) *Access control*
    - (11.1) *Business requirement for access control*
    - (11.2) *User access management*
    - (11.3) *User responsibilities*
    - (11.4) *Network access control*
    - (11.5) *Operation system access control*
    - (11.6) *Application and information access control*
    - (11.7) *Mobile computing and teleworking*
8. (12) *Information systems acquisition, development and mainenance*
    - (12.1) *Security requirement of information systems*
    - (12.2) *Correct processing in applications*
    - (12.3) *Cryptographic controls*
    - (12.4) *Security of system files*
    - (12.5) *Security in development and support processes*
    - (12.6) *Technical vulnerability management*
9. (13) *Information security incident management*
    - (13.1) *Reporting information security events and weaknesses*
    - (13.2) *Management of information security incident and improvements*
10. (14) *Business continuity management*

(14.1) *Information security aspects of business continuity management*

11. (15) *Compliance*
    (15.1) *Compliance with legal requirements*
    (15.2) *Compliance with security policies and standards, and technical compliance*
    (15.3) *Information systems audit considerations*

Yang menjadi *critical success factor* dalam implementasi pengamanan informasi dalam organisasi adalah;[12]

a) Kebijakan, tujuan dan kegiatan pengamanan informasi yang mencerminkan objektif bisnis.
b) Pendekatan dan kerangka untuk mengimplementasikan, memelihara, memonitor dan memperbaiki pengamanan informasi yang konsisten dalam budaya organisasi
c) Dukungan dan komitmen yang jelas dari seluruh level manajemen.
d) Pemahaman yang baik tentang kebutuhan pengamanan informasi, *risk assessment*, dan *risk management*.
e) Pemasaran/ sosialisasi yang efektif tentang pengamanan infrrmasi kepada semua manajer, peronil dan pihak lain untuk menumbuhkan *awareness*.
f) Distribusi panduan kebijakan pengamanan informasi, dan standar kepada seluruh *manager*, personil dan pihak lain.
g) Komitmen untuk mendanai kegiatan manajemen pengamanan informasi
h) Penyediaan *awareness, training* dan pendidikan yang mencukupi
i) Menetapkan proses manajemen insiden pengamanan informasi yang efektif
j) Implementasi dari system pengukuran yang digunakan untuk mengevaluasi performa dalam manajemen pengamanan informasi dan umpan balik untuk perbaikan.

[12] *Ibid.,* hal x

2.1.2 *ISO/IEC 27001:2005 (Information Technology – Security Techniques – Information Security Management System – Requirement)*

Standard internasional ini merupakan standar spesifikasi kebutuhan ISMS yang sebelumnya dikenal dengan BS 7799 part sertifikasi ISMS. Dalam implementasinya, organisasi bebas memilih kontrol yang sesuai dengan kondisi organisasinya, dari pilihan kontrol yang terdapat pada *Anex A – Control objectives and controls – ISO/IEC 27001:2005*, yang secara detilnya dijabarkan di *ISO/IEC 17799:2005* (dahulu BS 7799 part 1).

Standar internasional ini mencakup semua tipe organisasi baik itu perusahaan komersial, pemerintahan, ataupun *non-profit organizations*. Standar internasional ini menetapkan kebutuhan untuk mendirikan, menerapkan, mengoperasikan, *monitoring*, *reviewing*, memelihara dan memperbaiki dokumen ISMS dalam konteks risiko bisnis organisasi secara keseluruhan.[13]

Semua kebutuhan dalam standar ini generik, dan dimaksudkan agar bisa diaplikasikan ke semua organisasi, tanpa memperhitungkan tipe, ukuran, dan sifatnya. Kebutuhan implementasi ISMS berdasarkan ISO/IEC 27001:2005, dipenuhi pada klausul 4, 5, 6, 7, dan 8 (lihat tabel 2.1)

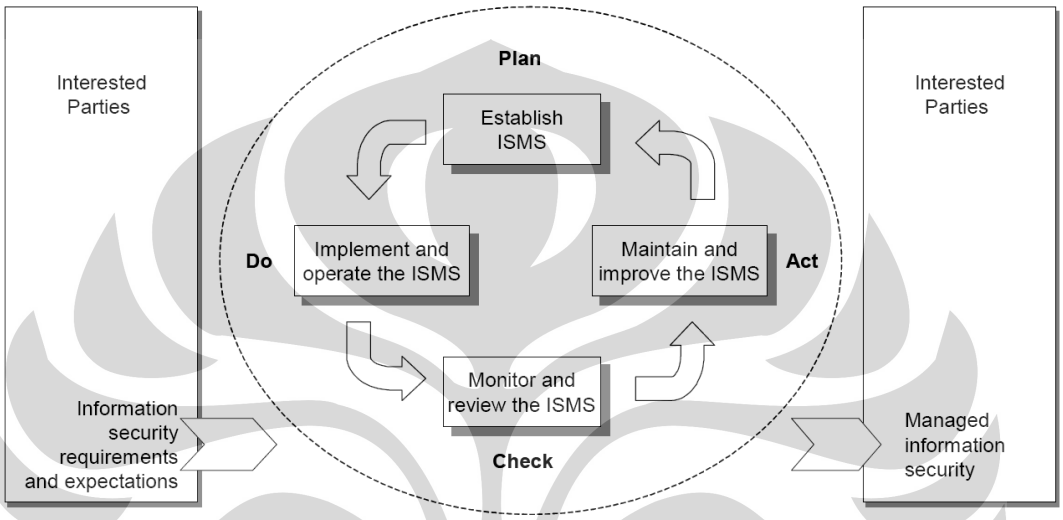
Tabel 2.1 Klausul ISMS dalam ISO/IEC 27001:2005

No Klausul	Klausul
4	*Information Security management System*
4.1	*General Requirement*
4.2	*Establishing & Managing ISMS*
4.3	*Documentation Requirements*
5	*Management Responsibilities*
5.1	*Management Commitment*
5.2	*Resource Management*
6	*Internal ISMS Audit*
7	*Management Review of ISMS*
7.1	*General*
7.2	*Review Input*
7.3	*Review Input*
8	*Review Output*
8.1	*Continual Improvement*
8.2	*Corrective Action*
8.3	*Preventive Action*

Sumber : ISO/IEC 27001:2005

[13] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management system – Requirements. AG meeting, 29-30 November* 2005, Geneva, hal 1

ISO/IEC 27001:2005 ini mendefinisikan kebutuhan-kebutuhan untuk menetapkan, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan memperbaiki *nformation Security Management System (ISMS)* sesuai dengan risiko proses bisnis organisasi. Konsep yang digunakan adalah PDCA *(Plan-Do-Check-Action)* yang merupakan struktur ISMS. Adapun penggambaran konsep PDCA dapat dilihat pada gambar berikut;



Gambar 2.1 Penerapan model PDCA untuk proses ISMS dalam ISO/IEC 27001:2005

Tabel 2.2 Definisi PDCA dalam ISO/IEC 27001:2005

***Plan** (establish the ISMS)*	Menetapkan kebijakan, sasaran utama, proses dan prosedur ISMS yang terkait dengan pengelolaan risiko dan memperbaiki pengamanan informasi untuk memberi hasil yang sesuai dengan kebijakan dan sasaran utama organisasi secara keseluruhan
***Do** (implement and operate the ISMS)*	Menerapkan dan menjalankan kebijakan, kendali, proses dan prosedur ISMS
***Check** (monitor and review the ISMS)*	Menilai dan, dimana dapat digunakan, mengukur performa proses terhadap kebijakan ISMS, sasaran utama dan pengalaman praktis dan pelaporan hasil untuk tinjauan manajemen
***Act** (maintain and improve the ISMS)*	Mengambil perbaikan dan aksi pencegahan, berdasarkan hasil dari audit internal ISMS dan tinjauan manajemen atau informasi lainnya yang terkait, untuk mencapai perbaikan ISMS yang berkesinambungan

Sumber : ISO/IEC 27001:2005

2.2 MANAJEMEN RISIKO

Risiko adalah ukuran kemungkinan dan konsekuensinya dari ketidakberhasilan penetapan sasaran/ tujuan *project.*[14] Banyak orang setuju bahwa risiko melibatkan pemikiran/ gagasan dari ketidakpastian. Menurut AS/NZS 4360:1995, risiko adalah kombinasi dari frekuensi, atau probabilitas dari perisiwa dan konsekuensi dari penetapan kejadian yang berbahaya *(hazardous events)*. Dengan kata lain risiko adalah kondisi dimana terdapat kemungkinan adanya penyimpangan kerugian dari keinginan hasil yang diharapkan atau pengharapan.

Manajemen risiko adalah proses menyeluruh yang digunakan untuk mengidentifikasi, mengendalikan dan meminimalisasi *impact* dari ketidakjelasan peristiwa. Sasaran utama dari *risk management program* adalah untuk mengurangi risiko yang dihasilkan beberapa aktifitas atau fungsi ke level yang dapat diterima dan mendapatkan persetujuan dari *senior management*.[15]

Manajemen risiko mencakup tiga proses; *risk assessment, risk mitigation*, dan *evaluation and assessment.*[16] Dijelskan pada bagian 3, draf NIST SP800-30 yang memaparkan *risk assessment process* meliputi *identification and evaluation of risks and risk impacts*, dan rekomendasi dari *risk-reducing measures*. Sedangkan *risk mitigation* dipaparkan pada bagian 4, berhubungan dengan prioritas, implementasi, dan pemeliharaan *risk-reducing measures* yang tepat yang telah direkomendasikan dalam *risk assessment process*. Dan pada bagian 5 dibahas proses evaluasi secara berkelanjutan dan kunci sukses untuk mengimplementasikan *risk management program*.

Ada beberapa kerangka manajemen risiko yang dapat diikuti selain dari perspektif PMI *(Project Management Insitute)* dalam panduannya *"A Guide to the Project Management Body of Knowledge"* dikenal dengan singkatan PMBOK (2004). Sebagai contoh, kerangka pemikiran yang muncul di Australia dan dikenal sebagai Australia/New Zealand Standard 4360:1999 yang dikembangkan oleh *Standard Association of Australia*, diadakan sebagai pedoman acuan utama

---

[14] Kerzner, Harold. *Project Management – Ninth Edition*. John Wiley. 2005. Hal 709

[15] Peltier, Thomas R. *Information Security Risk Analysis, second edition.* Auerbach Publications, Taylor & Francis Group. 2005. Hal 42

[16] NIST (2002). *Risk management guide for information technology systems*. National Institute of Standards and Technology (NIST) Special Publication 800-30 hal 4

manajemen risiko di Australia dan New Zealand. Berita baiknya adalah bahwa perbedaan kerangka yang ada mengikuti pesan mendasar yang sama. Dasar pandangan semua kerangka pemikiran yang ada adalah manajemen risiko yang efektif dibutuhkan organisasi untuk merencanakan dan sepakat dengan *proactively* risiko, identifikasi *events* risiko, mengembangkan strategi untuk perlakuannya, dan menanganinya ketika risiko itu timbul.[17]

Ada lima tahapan dalam kerangka *risk management*[18] yang sesuai dan diadopsi dari PMBOK, yaitu;

Step 1. Plan for risk. Persiapan untuk memanage risiko yang ada. Manajemen risiko yang efektif tidak terjaadi secara kebetulan. Ini merupakan hasil dari perencanaan dan pemikiran kedepan sebelumnya secara hati-hati.

Step 2. Identify risk. Secara rutin memeriksa keadaan internal dan eksternal organisasi untuk mengemukakan *risk events* yang mungkin mempengaruhi kegiatan dan yang sedang berjalan baik. Setelah proses ini, kembangkan pemikiran yang baik dari sesuatu hal yang buruk sesuai dengan *project* dan kegiatan yang dihadapi.

Step 4. Develop risk-handling strategies: Setelah *risk events* yang mungkin dihadapi (Step 2) dan konsekuensi yang terkait dengan risiko tersebut (Step 3) diketahui, kemudian kembangkan strategi untuk menanganinya.

Step 5. Monitor and control risks. Saat *project* dan kegiatan sedang berlangsung, anda harus memonitor besaran risiko organisasi untuk melihat jika timbul *events* yang tidak baik yang perlu untuk ditangani. Jika dalam usaha memonitoring ditemukan masalah dalam proses, maka harus diambil langkah untuk mengendalikannya.

[17] Frame, J Davidson. *Managing Risk in Organization – A Guide for Managers.* 2003. Jossey-Bass. Hal 14
[18] *Ibid.,* hal 14-15

2.3 IDEF0 *(Integration Definition for Function Modeling)*

IDEF0 adalah metode yang didesain untuk memodelkan *decision, action, and activities* dari organisasi atau system.[19] IDEF0 *(Integration DEFinition language 0)* didasari oleh SADT ™ *(Structured Analysis and Design Technique ™)*, dikembangkan oleh Douglas T. Ross and SoftTech, Inc. Dalam bentuk aslinya, IDEF0 termasuk didalamnya definisi dari bahasa permodelan secara grafis *(syntax and semantic)* dan deskripsi dari metodologi secara luas untuk mengembangkan model.[20]

Penggunaan *Draft Federal Information Processing Standards Publication 183*, membolehkan bentuk dari model IDEF0 terdiri dari fungsi-fungsi system *(action, processes operations),* terkait fungsi, dan objek-objek serta data pendukung analisis system dan desain, *enterprise analysis*, dan business process re-engineering.[21] Standar ini menggantikan IDEF0 yang didefinisikan oleh *U.S. Air Force Integrated Computer-Aided Manufacturing* (ICAM) *Function Modeling Manual* (IDEF0), Juni 1981, dan banyak digunakan oleh pengguna IDEF setelahnya

IDEF0 adalah sebuah metode keteknikan untuk menampilkan dan me-*manage* kebutuhan analisis, keuntungan analisis, kebutuhan definisi, analisis fungsional, desain system, perawatan, dan standar untuk *continuous improvement*. Model IDEF0 menyediakan sebuah *"blueprint"* dari fungsi-fungsi dan tampilannya yang harus di-*capture* dan dipahami dalam pembuatan keputusan *systems engineering* yang logis, mampu dihasilkan *(affordable)*, mampu diintegrasikan *(integratable)* dan mampu dicapai *(achievable)*.

Ketika digunakan secara sistematis, IDEF0 memberikan sebuah pendekatan *system engineering* untuk[22];

1. Melakukan analisis system dan desain di semua level, untuk penyusunan system dari *people, machines, material, computers* dan

[19] http://www.idef.com
[20] Draft Federal Information Processing Standards Publication 183. *Integration Definition for Function Modelling (IDEF0).* 1993. Hal vii.
[21] *Ibid.,* hal 1
[22] *Ibid.,* hal 7

informasi dari segala variasi – segala bentuk perusahaan, system, atau ruang lingkup tujuan.

2. Menghasilkan referensi dokumentasi secara bersamaan dengan pengembangan penyajian sebagai dasar untuk mengintegrasikan system yang baru atau memperbaiki system yang ada.
3. Mengkomunikasikan antara penganalisis, perancang, pengguna dan *manager*.
4. Memperbolehkan penyaatuan tujuan tim yang ingin dicapai dengan pembagian pemahaman.
5. Me-*manage project* yang besar dan kompleks dengan menggunakan pengukuran *qualitative*
6. Menyediakan sebuah referensi arsitektur untuk menganalisa perusahaan, *information engineering* dan manajemen sumber daya.

Model IDEF0 terdiri dari 3 tipe informasi [23]; diagram grafis, text, dan *glossary*. Tipe diagram tersebut saling berkaitan satu sama lainnya. Diagram grafis adalah komponen utama dari model IDEF0, terdiri dari kotak, tanda panah, kotak/panah yang saling terkait dan berhubungan erat.

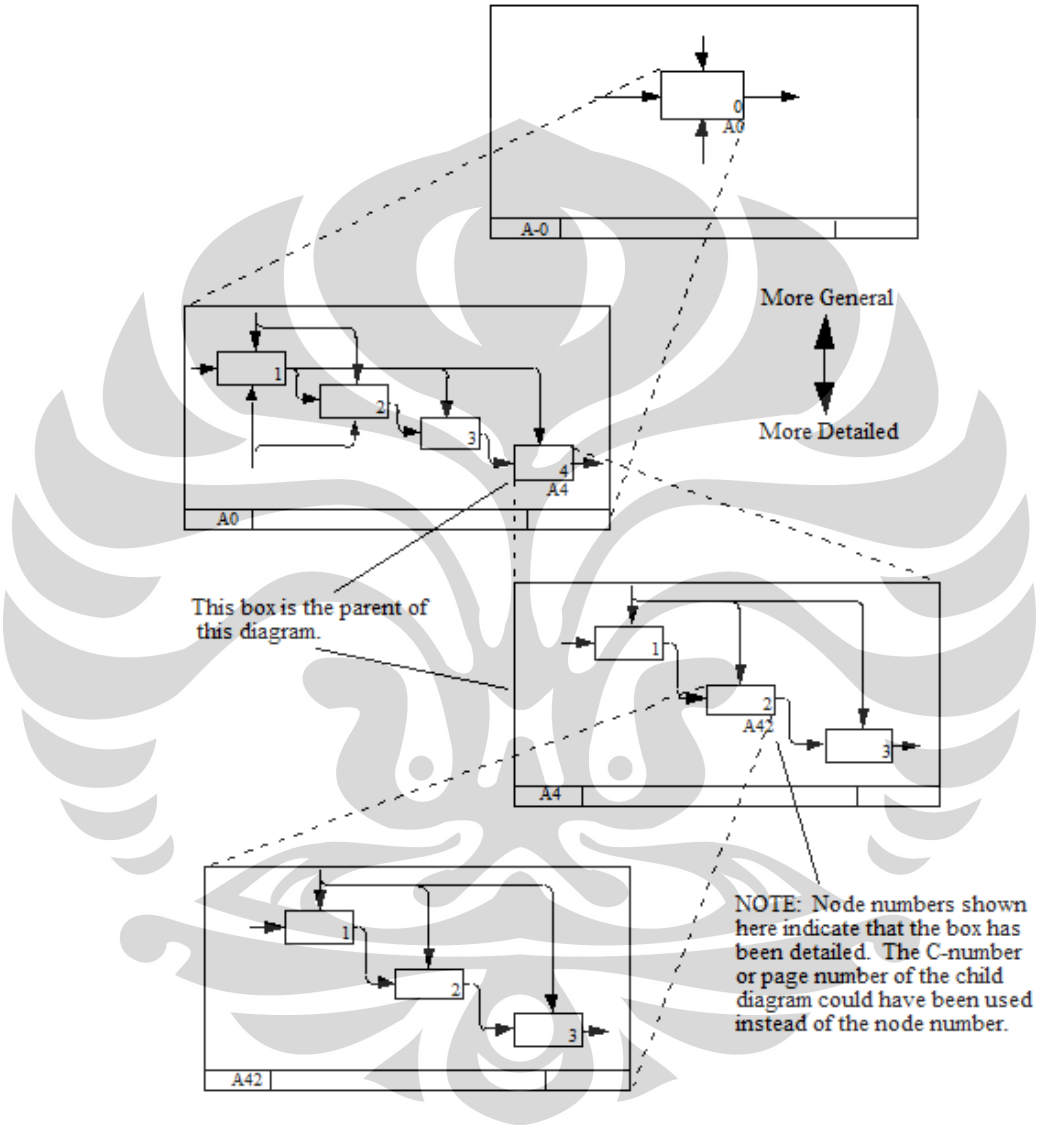
Pada diagram grafis, kotak merepresentasikan setiap fungsi utama dari subjek. Fungsi ini dijabarkan kedalam diagram yang lebih detail lagi, sampai subjek menjadi jelas pada setiap level yang diperlukan sehingga mendukung sasaran project yang jelas. Top-level dari diagram menyediakan deskripsi abstrak secara umum dari subjek yang direpresentasikan. Diagram ini diikuti oleh anak diagram yang menyediakan lebih detail tentang subjek.

Setiap model mempunyai sebuah *top-level context diagram*, yang subjek-nya direpresentasikan oleh kotak tunggal yang dikelilingi panah. Diagram ini disebut A-0 *(pronounced A minus zero)*. Karena kotak tunggal merepresentasikan seluruh object, maka deskripsi yang ditulis dalam kotak adalah general. Begitu juga dengan tampilan panah yang juga merepresentasikan tampilan eksternal subject secara lengkap.

Kecuali untuk A-0, diagram grafis terdiri dari minimum 3 dan maksimum 6 kotak. Kotak ini biasanya disusun secara diagonal dari pojok kiri atas ke kanan

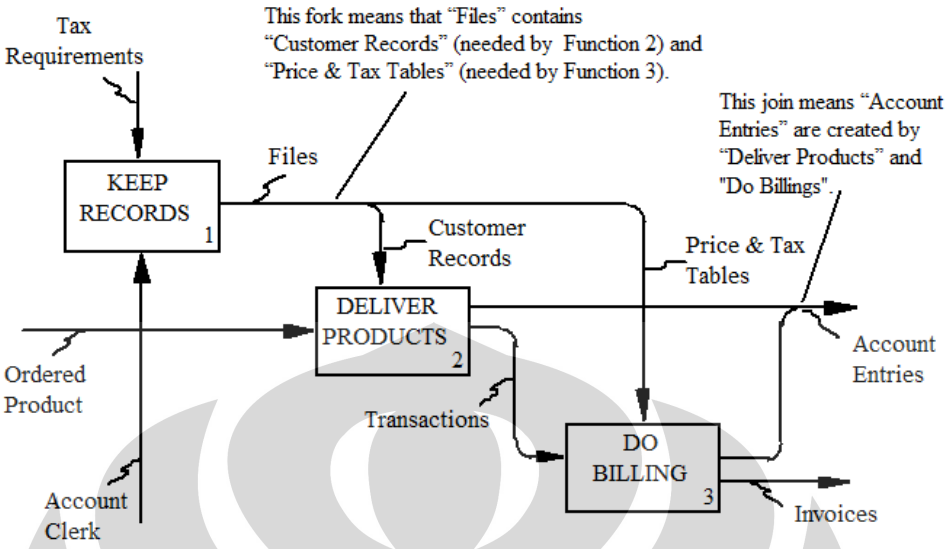
[23] *Ibid.,* hal 13

bawah, seperti susunan anak tangga. [24] Setiap panah keluaran memberikan beberapa atau semua dari *input, control, or mechanism* data atau objek ke kotak yang lainnya.

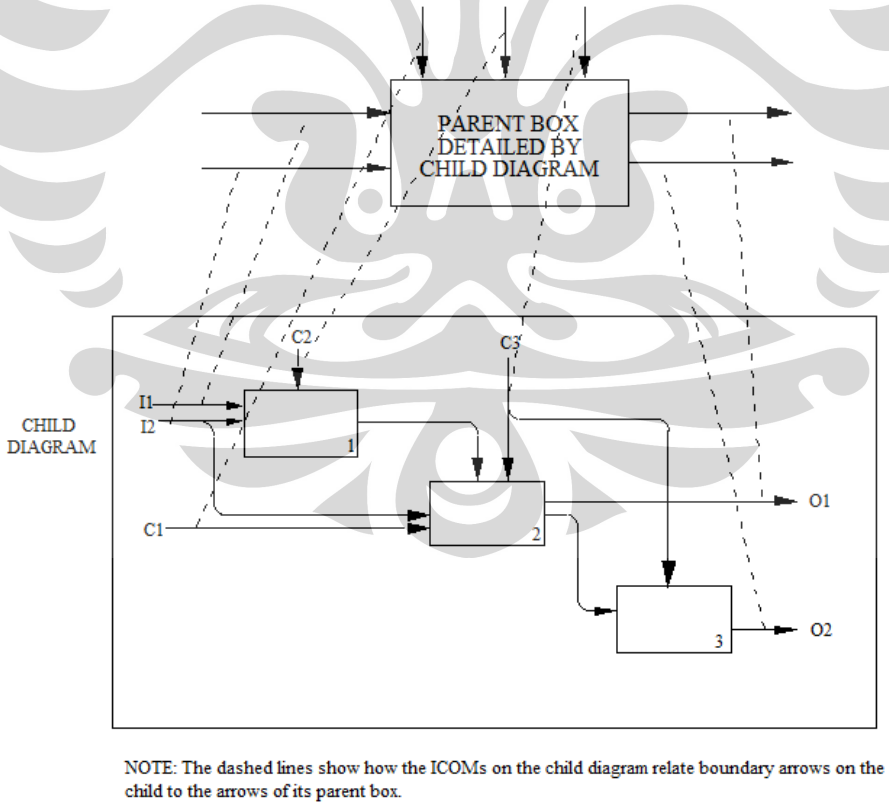


Gambar 2.2 *Decomposition Structure IDEF0*

[24] *Ibid.,* hal 21

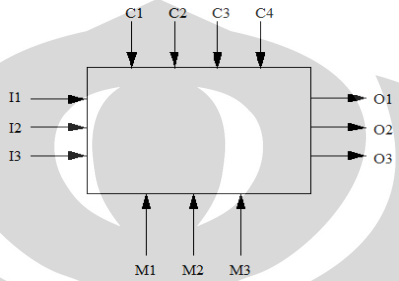


Gambar 2.3 *Connection between boxes*



Gambar 2.4 ICOM *codes and changing arrow roles*

Pengkodean ICOM mengaitkan panah pada diagram anak dengan panah yang terhubung pada kotak induknya. Notasi spesifiknya disebut kode ICOM, secara spesifik menyesuaikan penghubung.Huruf I, C, O atau M ditulis dekat dengan ujung panah yang tak terhubung pada anak diagram. Pengkodean ini mengidentifikasikan panah sebagai Input, Control, Output atau Mechanism pada kotak induk. Huruf ini diikuti nomor yang diberikan sesuai dengan posisi dimana panah pada kotak induk terlihat terhubung, penomoran dari kiri ke kanan atau atas ke bawah.



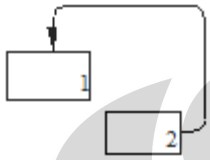
Gambar 2.5 Ilustrasi pengkodean ICOM

Aturan-aturan syntax diagram pada IDEF0, diantaranya[25];

1. Diagram utama sebaiknya mempunyai nomor *node* A-n, dimana n lebih besar dari atau sama dengan nol *(zero)*
2. Model sebaiknya mengandung diagram utama A-0, yang terdiri dari 1 kotak saja
3. Penomoran kotak dari kotak tunggal pada diagram utama A-0 sebaiknya 0
4. Yang bukan diagram utama sebaiknya paling tidak mempunyai 3 kotak dan tidak lebih dari 6 kotak
5. Setiap kotak yang bukan diagram utama sebaiknya dinomori pada pojok kanan bawah, diurutkan (dari kiri teratas ke kanan paling bawah pada diagram) dari 1 sampai tidak lebih dari 6
6. Setiap kotak yang ingin dijelaskan secara detail sebaiknya mempunyai penunjukan referensi detail (seperti nomor *node*, *C-number*, atau halaman lembaran) pada diagram anaknya
7. Panah sebaiknya digambarkan secara irisan garis lurus horizontal atau vertical. Garis irisan diagonal sebaiknya tidak digunakan

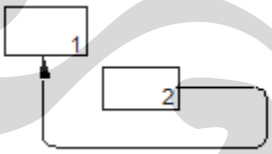
[25] *Ibid.,* hal 30

8. Setiap kotak sebaiknya mempunyai minimum 1 panah control dan 1 panah output
9. Kotak sebaiknya tidak mempunyai atau mempunyai panah input
10. Kotak sebaiknya tidak mempunyai atau mempunyai panah *non-call mechanism*
11. Kotak sebaiknya mempunyai 0 atau 1 *call arrows*
12. *Control feedback* sebaiknya ditunjukan diatas dan keatas

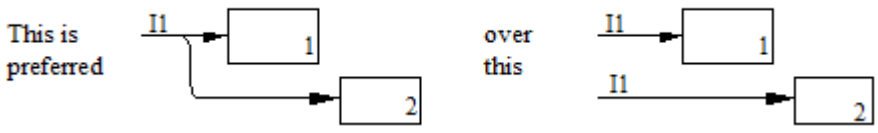


Input feedback sebaiknya ditunjukan dibawah dan kebawah

Mechanism feedback sebaiknya ditunjukan dibawah dan kebawah



13. Pangkal panah yang tidak terhubung sebaiknya diberi kode spesifikasi ICOM yang benar sesuai hubungannya dengan kotak induknya
14. Pangkal panah yang terbuka yang merepresentasikan data atau objek yang sama sebaiknya percabangannya disatukan untuk menunjukan semua tempat berpengaruh, walaupun hasil diagramnya tidak dapat dibaca. Sumber multiple yang merepresentasikan data atau objek yang sama sebaiknya disatukan kebentuk keluaran panah yang satu.



15. Penamaan kotak dan pemberian lebel panah sebaiknya tidak terdiri dari kata tunggal berikut; *function, activity, process, input, output, control or mechanism*

2.4 FACILITATED RISK ANALYSIS AND ASSESSMENT PROCESS (FRAAP)

Ada banyak teknik dan metode *risk assessment*.[26] *CERT (The Computer Emergency Response Team)*[27] mengemukakan mekanisme *risk assessment* yang dinamai OCTAVE *(Operational Critical Threat, Asset, and Vulnerability Evaluation).*[28] Beberapa metode *security risk assessment* yang pouler lainnya diantaranya adalah FFA *(Federal Aviation Administration) Security Risk Management, Facilitated Risk Analysis and Assessment Process (FRAAP)* yang dikembangkan oleh Peltier, Thomas R, CCTA *Risk Anylisis and Management Methode* (CRAMM) dikembangkan oleh UK Goverment's Central Computer and Telecomunications Agency (CCTA) dan National Security Agency's (NSAs), INFOSEC Assessment Methodology (IAM) Douglas, JL (2006) dalam *The security risk assessment handbook,* Auerbach Publication.

The Facilitated Risk Analysis and Assessment Process (FRAAP)[29] dikembangkan sebagai proses pendisiplinan dan efisien untuk memastikan bahwa *information security* - terkait risiko operasi bisnis betul-betul dipertimbangkan dan didokumentasikan. Proses termasuk penganalisaan sebuah system, aplikasi, *platform,* proses bisnis, atau segmen dari operasi bisnis secara bersaman.

FRAAP dibagi kedalam 3 fase, yang masing-masing fase dibagi kedalam bagian proses analisis risiko yang berbeda, yaitu;

- *Pre-FRAAP meeting, (prescreening, project scope statement, visual model, definitions, team member, meeting mechanics)*
- *The FRAAP session, (brainstorm to identify potensial threats to the integrity, confidentiality, and availability of information resources, risk level established, control selection)*
- *The Post-FRAAP, (summary)*

---

[26] Bojanc, Rok,. Jerman-Blazic, Borka,. *"An economic modeling approach to information security risk management."* dalam *International Journal of Information Management 28 (2008) 413-422. Science Direct, Elsevier.* 2008. Hal 416

[27] http://www.cert.org/octave/

[28] Albert, Chris., et all. *Defining Incident Management Process for CSIRTs.(CMU/SEI-2004-TR-015). 2004.Carnegie Mellon® Software Engineering Institute (SEI^{SM}).* Hal x

[29] Peltier, Thomas R. *Information Security Risk Analysis, second edition.* Auerbach Publications, Taylor & Francis Group. 2005. Hal 129-204

Modifikasi FRAAP yang mendekati original FRAAP dapat digunakan ketika penilaian risiko bisnis atau infrastuktur *information technology* diselenggarakan.[30]. Organisasi harus dapat menciptakan keamanan dan kenyamanan di lingkungan kerja bagi pekerjanya dan layanan yang diberikannya. *FRAAP (Facilitated Risk Analysis and Assessment Process)* dirancang agar dapat sefleksibel mungkin, sehingga bentuk dan modelnya dapat diubah sesuai dengan kebutuhan dari organisasi. [31]

2.5 MODEL SIMULASI DAN OPTIMASI (OptQuest pada Crystal Ball)

Simulasi adalah sebuah metode analitis yang bertujuan untuk mendapatkan suatu bentuk representasi sebuh system. Tujuan utama dari pembuatan model simulasi adalah untuk memudahkan pelaksanaan eksperimen, terutama jika manipulasi-manipulasi system pada kondisi nyata memerlukan biaya yang besar atau ada kendala-kendala lain yang sulit untuk direalisasikan.

Simulasi Monte Carlo adalah alat untuk memodelkan ketidakpastian. Secara khas, kita memulai dengan menentukan model *spreadsheet* dari situasi yang akan kita analisis, kemudian menggunakan Software Crystal Ball untuk memasukan asumsi statistical guna merepresentasikan banyak sumber penting yang tak pasti. Crystal Ball dikembangkan untuk membuat simulasi Monte Carlo dapat digunakan untuk *financial analysts* dan prnggunaan Excel lainnya pada *personal computer workstation* yang lebih baik daripada pengkodean dalam bahasa pemograman seperti C++ atau FORTRAN. [32] Dengan kata lain Smulasi Monte Carlo adalah sebuah system yang menggunakan random number untuk mengukur efek dari ketidakpastian dalam sebuah model *spreadsheet.*[33]

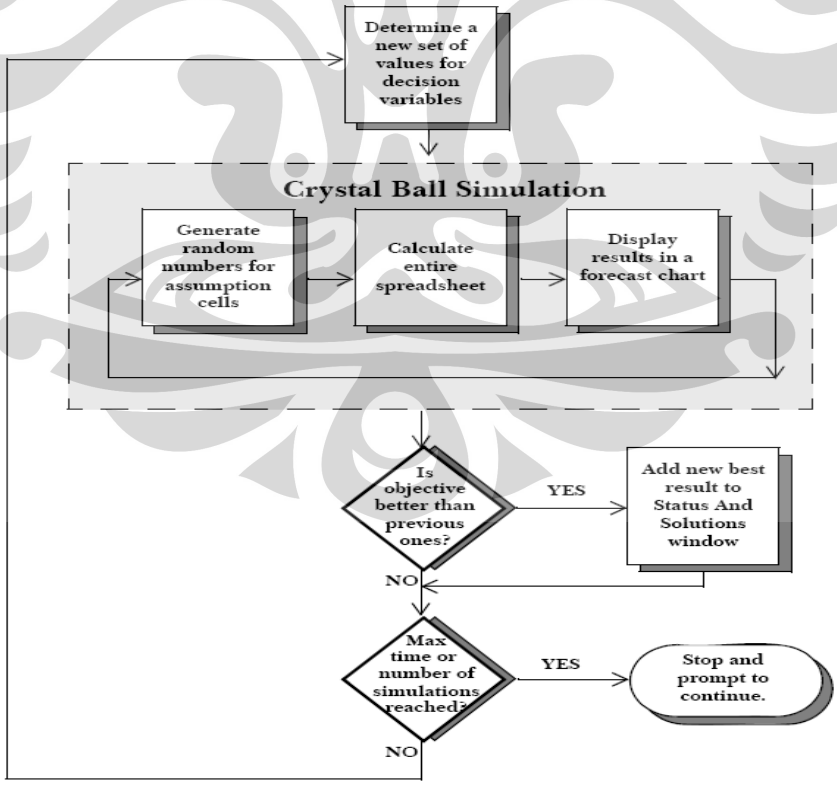
Dalam penggunaan Simulasi Monte Carlo yang dipaparkan dalam user manual Crystal Ball[34], *spreadsheet risk analysis* menggunakan *spreadsheet model* dan simulasi untuk menganalisis efek dari input terhadap output dari permodelan system.

---

[30] *Ibid.*, hal 205
[31] *Ibid.*, h al 221
[32] Charnes, Jhon. *Financial Modeling with Crystal Ball and Excel*. John Wiley & Sons, Inc., Hoboken, New Jersey. 2007. Hal 28
[33] *Ibid.*, hal 252
[34] Crystal Ball® 7.2.2 User Manual. Hal 11

Metode tradisional lain (seperti Solver pada Excel) bekerja baik ketika mencari solusi disekitar *starting point* dengan model yang datanya telah diketahui secara presisi. Metode ini menjadi lemah, pada saat mencari solusi global pada permasalahan yang sesungguhnya yang terdapat banyak nilai tak pasti yang *significant*. OptQuest memasukan *metaheuristic (a family of optimization approaches that includes genetic algorithms, simulated annealing, tabu search, scatter search, and their hybrids)*[35] untuk memandu dalam pencarian algoritma kearah solusi yang lebih baik.

Model OptQuest memiliki 3 elemen utama, yaitu variabel keputusan, batasan, dan tujuan. Variabel keputusan adalah variabel yang dapat dikendalikan, seperti jumlah produk yang akan diproduksi, besarnya investasi yang akan dikeluarkan, dan lain-lain. Batasan adalah nilai yang menjadi *constraint* atas hubungan beberapa variabel keputusan yang ada, seperti jumlah total investasi yang dianggarkan untuk beberapa proyek. Sedangkan tujuan adalah gambaran pencapaian yang diinginkan dari model secara matematis, contohnya adalah memaksimalkan keuntungan atau meminimalkan biaya.



Gambar 2.6 *Flow OptQuest*

[35] OptQuest ® 2.3 User Manual. Hal 11

BAB III
PENGUMPULAN DAN PENGOLAHAN DATA

3.1 PROFIL ID-SIRTII *(Indonesia – Security Incident Response Team on Internet Infrastructure)*

ID-SIRTII yang pada tahap awal diinisiasi oleh Ditjen Postel – Depkominfo (tahun 2005) merupakan sebuah lembaga tingkat nasional yang diharapkan akan mampu menangani berbagai permasalahan gangguan keamanan *(security incidents)* jaringan komputer berbasis internet. Gangguan kemanan pada jaringan internet ini dapat berupa peredaran *virus* dan *worm*, penyalahgunaan akses/ pembobolan jaringan *(cracking)* yang disertai pencurian dan perusakan data, penggunaan kartu kredit secara ilegal *(credit card fraud/ carding)*, pornografi, perjudian, *cyber terrorism, money laundering*, dan lain-lain.

Perbandingan kelembagaan dari beberapa lembaga CERT *(Computer Emergency Response Team)* pada skala nasional di berbagai negara diantaranya;

- US CERT – USA : sebagian oleh pemerintah (FBI) untuk fungsi keamanan dan sebagian oleh *Carnegie-Mellon University* (November 1988)
- AusCERT – Australia : *Queensland University – Brisbane* (October 1992) komersial tapi ada subsidi dari pemerintah.
- UK NISCC – UK : *UK Government – UK CIP Programe* (1992)
- MyCERT – Malaysia : *Malaysian Gov. NITC & GITIC* (Jan 1997)
- CanCERT – Canada : *EWA Canada Ltd* (1998)

Pengembangan sistem dan teknologi ID-SIRTII diawali dengan pengembangan 9 sensor inti pada ISP/IX besar di Indonesia. ID-SIRTII mampu meng-*cover* setidaknya 80% *internet traffic* besar nasional.

Berdasarkan Peraturan Mentri Komunikasi dan Informatika RI, No 26/PER/M.KOMINFO/5/2007 dijelaskan dalam pasal 2, bahwa maksud dilaksanakannya pengamanan pemanfaatan jaringan telekomunikasi berbasis

protokol internet adalah mendukung terciptanya pemanfaatan jaringan telekomunikasi berbasis protokol internet di Indonesia yang relatif bebas dari ancaman dan gangguan.

Sedangkan dalam pasal 3, dijelaskan tujuan pengamanan pemanfaatan jaringan telekomunikasi berbasis protocol internet adalah untuk;

a. terlaksananya dukungan proses penegakan hukum;
b. terciptanya pemanfaatan jaringan telekomunikasi berbasis protocol internet yang aman;
c. terlaksananya koordinasi dengan pihak-pihak terkait baik di dalam maupun luar negri.

3.1.1 Visi dan misi ID-SIRTII

Visi ID-SIRTII adalah mendorong iklim bebas ancaman dan gangguan infrastruktur internet di Indonesia, sehingga meningkatkan pemanfaatan Internet sebagai sarana untuk peningkatan daya saing bangsa.

Sedangkan misi ID-SIRTII adalah;

a. Mendorong peningkatan keamanan jaringan infrastruktur internet;
b. Mendorong peningkatan transaksi Internet yang aman dan legal;
c. Mendukung penegakan hukum di bidang keamanan jaringan Internet;
d. Meningkatkan kerjasama dengan mitra strategis baik didalam dan diluar negri dalam penanggulangan ancaman dan gangguan Internet.

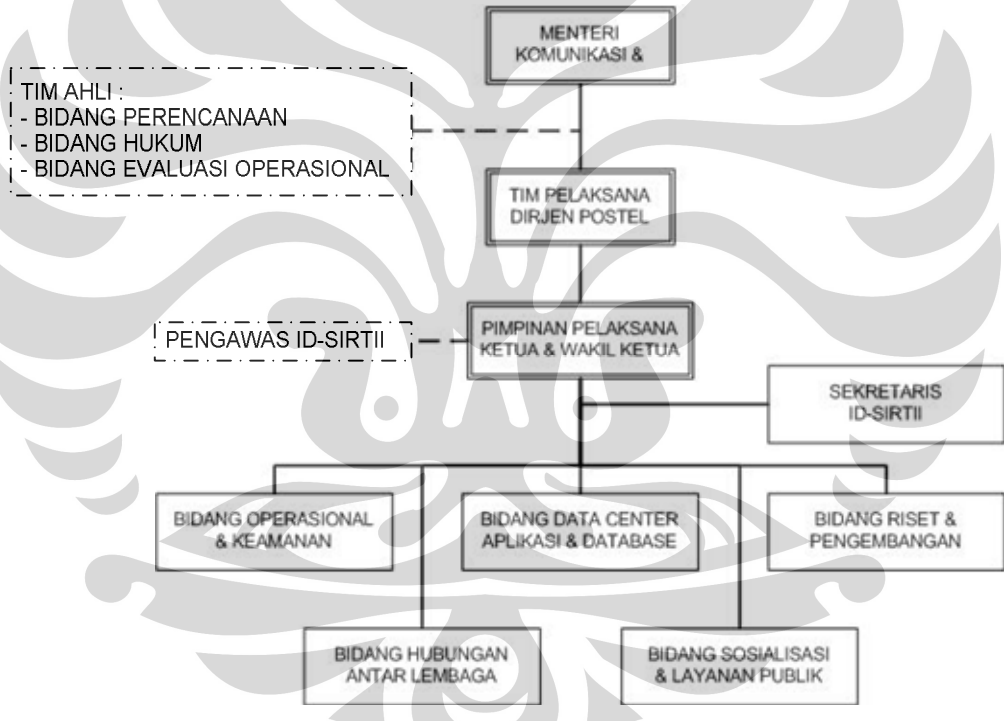
3.1.2 Target pencapaian ID-SIRTII

a. Terselenggaranya fasilitas pemantauan dan pencatatan untuk pembuktian serangan dan ganguan infrastruktur jaringan Internet di Indonesia;
b. Tersedianya bukti digital yang terpercaya yang dapat digunakan untuk mendukung proses hukum hingga di pengadilan;
c. Terciptanya koordinasi lembaga lokal dan internasional dalam mengatasi gangguan/ ancaman, serta menciptakan iklim yang mendukung stabilitas;
d. Tersedianya *internet early warning system*;
e. Terciptanya infrastruktur yang aman bagi berbagai aplikasi internet.

3.1.3 Struktur organisasi

Berdasarkan Peraturan Direktur Jendral Pos dan Telekomunikasi No. 226/DIRJEN/2007 tentang Susunan Organisasi, Tugas, Pengawas dan Standar Operasi dan Prosedur Pelaksana *Indonesia – Security Incident Response Team on Internet Infrastructure* (ID-SIRTII), pada pasal 1 dijelaskan pelaksanaan ID-SIRTII adalah petugas yang ditetapkan oleh Direktorat Jendral Pos dan Telekomunikasi untuk melaksanakan kegiatan dengan ruang lingkup Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Bagan struktur organisasi ID-SIRTII dapat dilihat pada gambar 3.1 berikut;



Gambar 3.1 Struktur Organisasi

3.2 PEMETAAN PROSES BISNIS

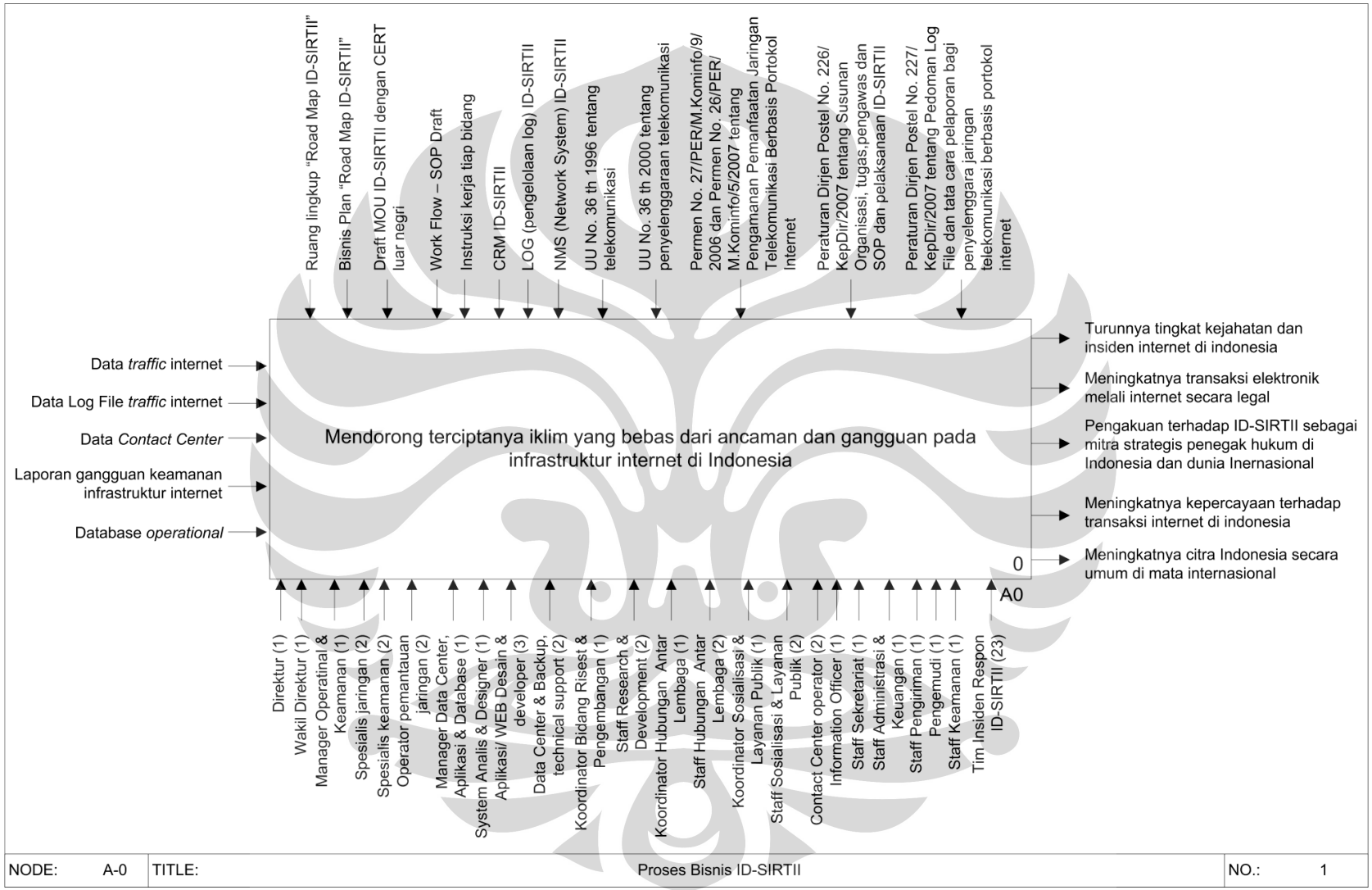
Sebelum melakukan pemetaan proses bisnis, penulis sebelumnya telah lebihdahulu melakukan riset pada object yang akan dipetakan, dalam hal ini adalah aktivitas, proses dan prosedur yang ada dalam ID-SIRTII. Data-data yang berhasil dikumpulkan saat riset berlangsung guna menunjang pemetaan proses bisnis diperkuat lagi dengan melakukan wawancara dengan bagian managerial dan staff operasional ID-SIRTII.

Metode yang digunakan dalam pemetaan proses bisnis ini adalah IDEF0, dimana dari data yang ada kemudian dikelompokan dan diterjemahkan kedalam pengkodean (ICOM) yang mengidentifikasikan panah sebagai Input, Control, Output, atau Mechanism pada kotak induk (A-0) sebagai diagram utama yang kemudian dijabarkan kembali menjadi diagram-diagram anak (A1, A2,… dst.).

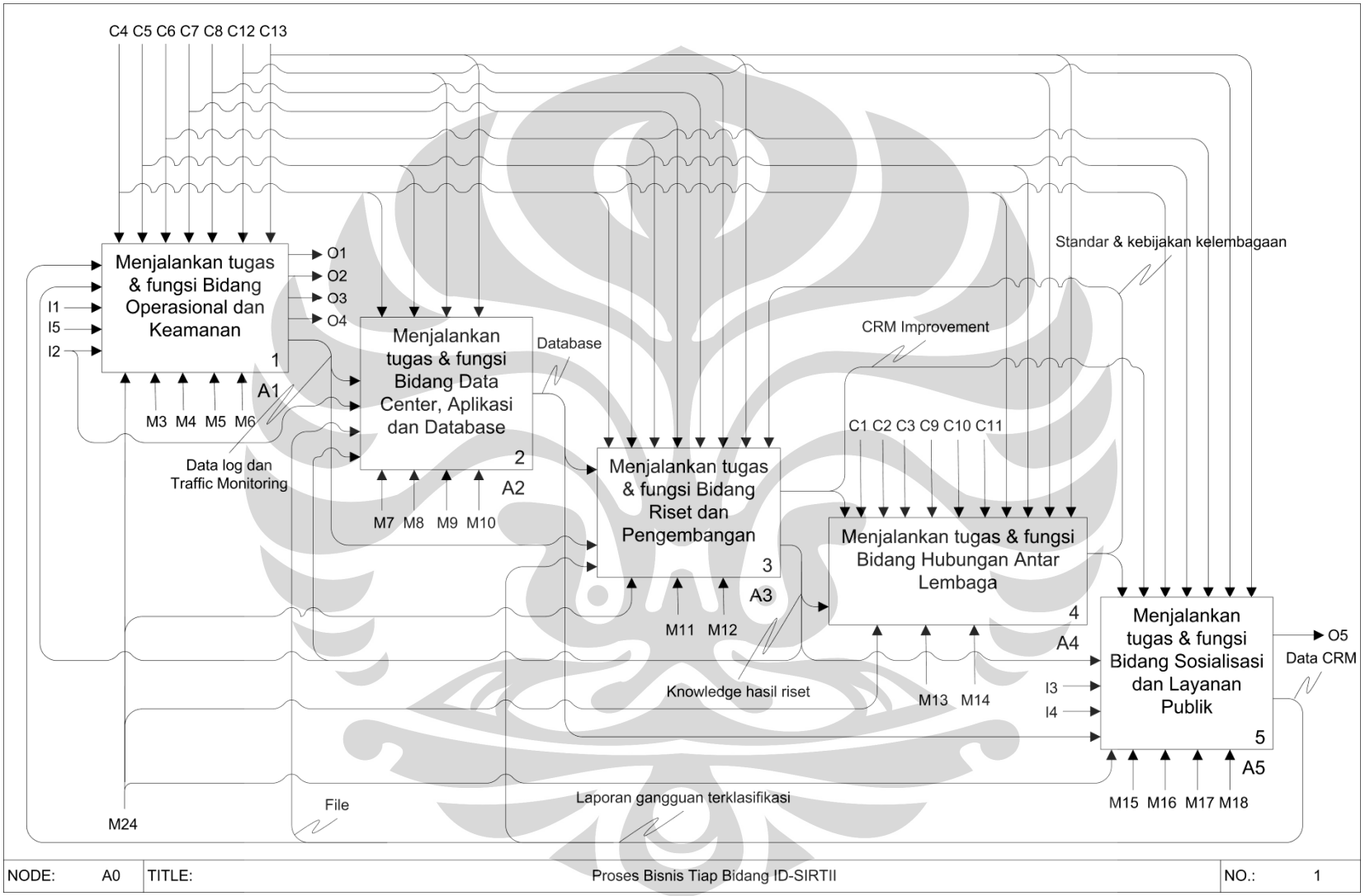
Pada diagram utama (A-0), aktivitas yang ditulis pada kotak adalah merupakan sasaran utama dalam organisasi, dalam hal ini dapat diartikan sebagai visi dari ID-SIRTII karena merupakan pencapaian secara umum dan general sehingga mampu menggambarkan keseluruhan aktivitas yang ada dan dituangkan kedalam diagram utama (A-0).

Dalam diagram utama digambarkan panah ***Input,*** yang merepresentasikan data masukan proses aktivitas ID-SIRTII dalam melakukan aktifitasnya seperti; data traffic, data log, data *contac center*, laporan gangguan dan database operasional. Panah ***C****ontrol* yang diberikan merepresentasikan kontrol-kontrol yang ada dalam melakukan aktivitas operasional ID-SIRTII seperti rung lingkup, *work flow, road map, draf* SOP, peraturan dan perundang-undangan, dan lain-lain. Sedangkan ***O****utput* adalah keluaran dari pencapaian misi ID-SIRTII, output ini dapat merepresentasikan indikator dari keberhasilan ID-SIRTII. Untuk panah ***M****echanism* merepresentasikan *resources* sumberdaya manusia yang ada guna menunjang aktivitas operasional.

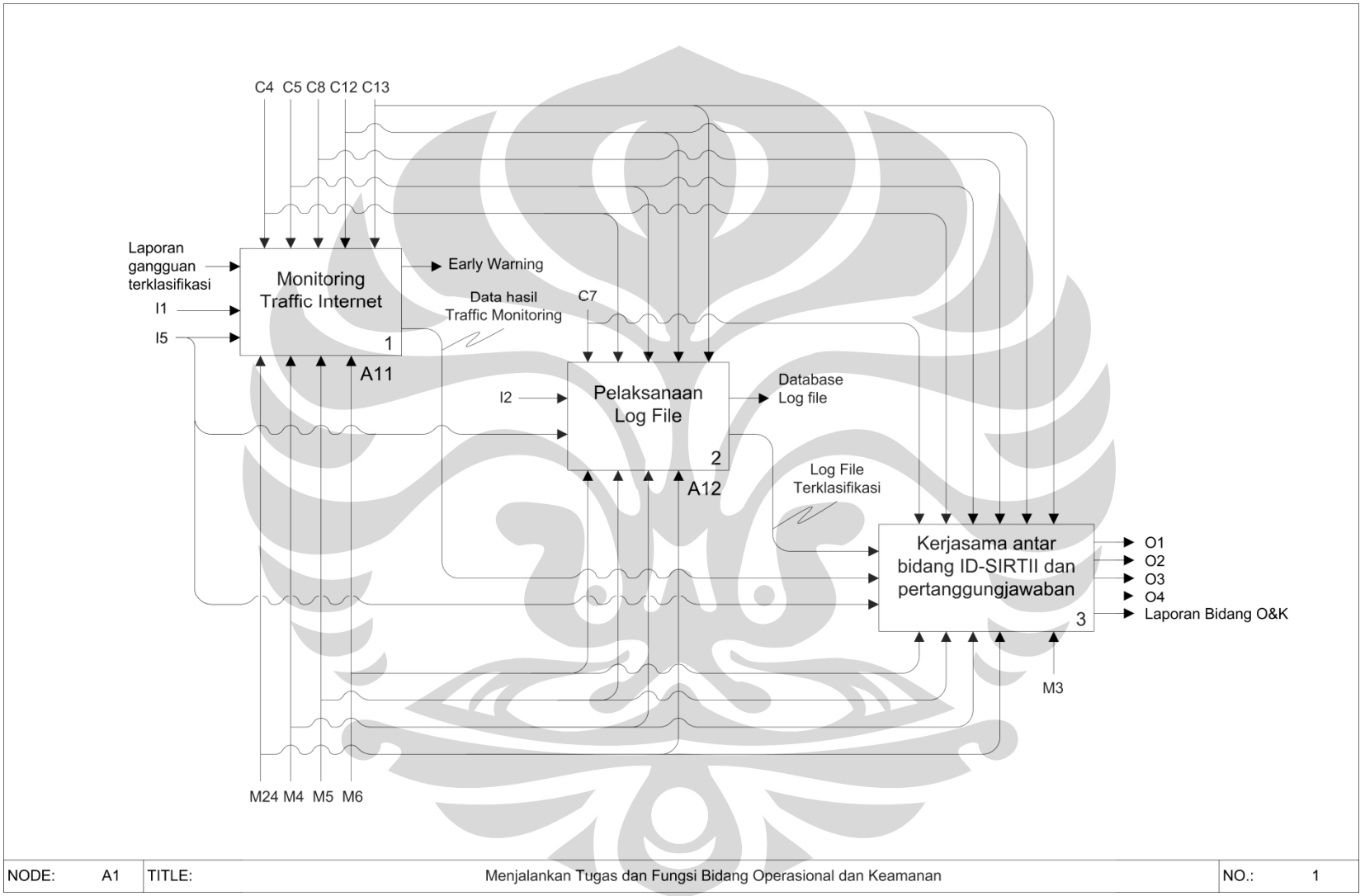
Penjabaran dari diagram utama dilakukan pada diagram-diagram anak yang merupakan penggambaran proses aktivitas turunan yang terintegrasi satu sama lain. Penjabaran dilakukan sesuai dengan konsep dan teori IDEF0 pada Draft Federal Information Processing Standards Publication 183.



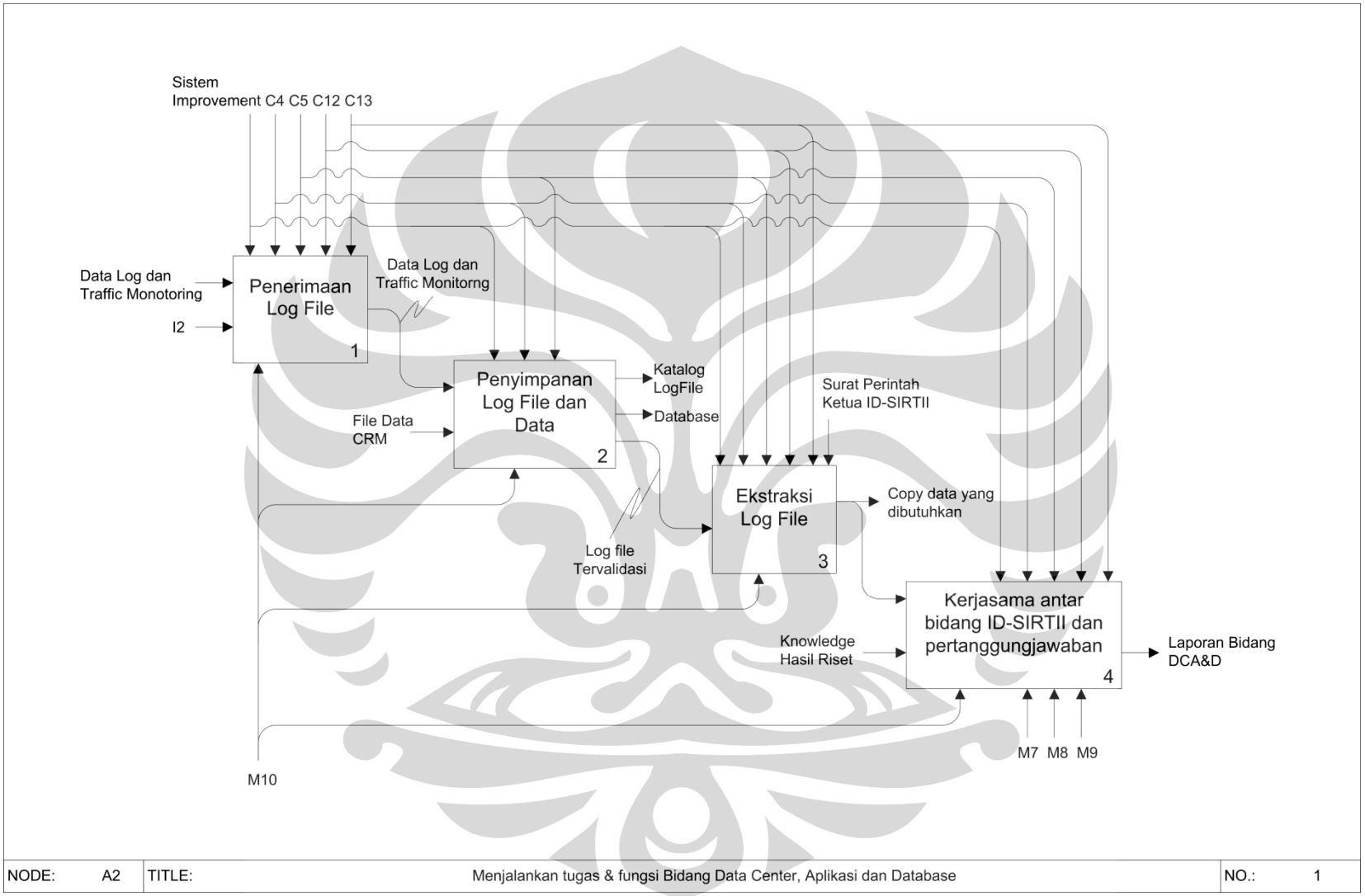
Gambar 3.2 Peta A-0, Proses Bisnis ID-SIRTII



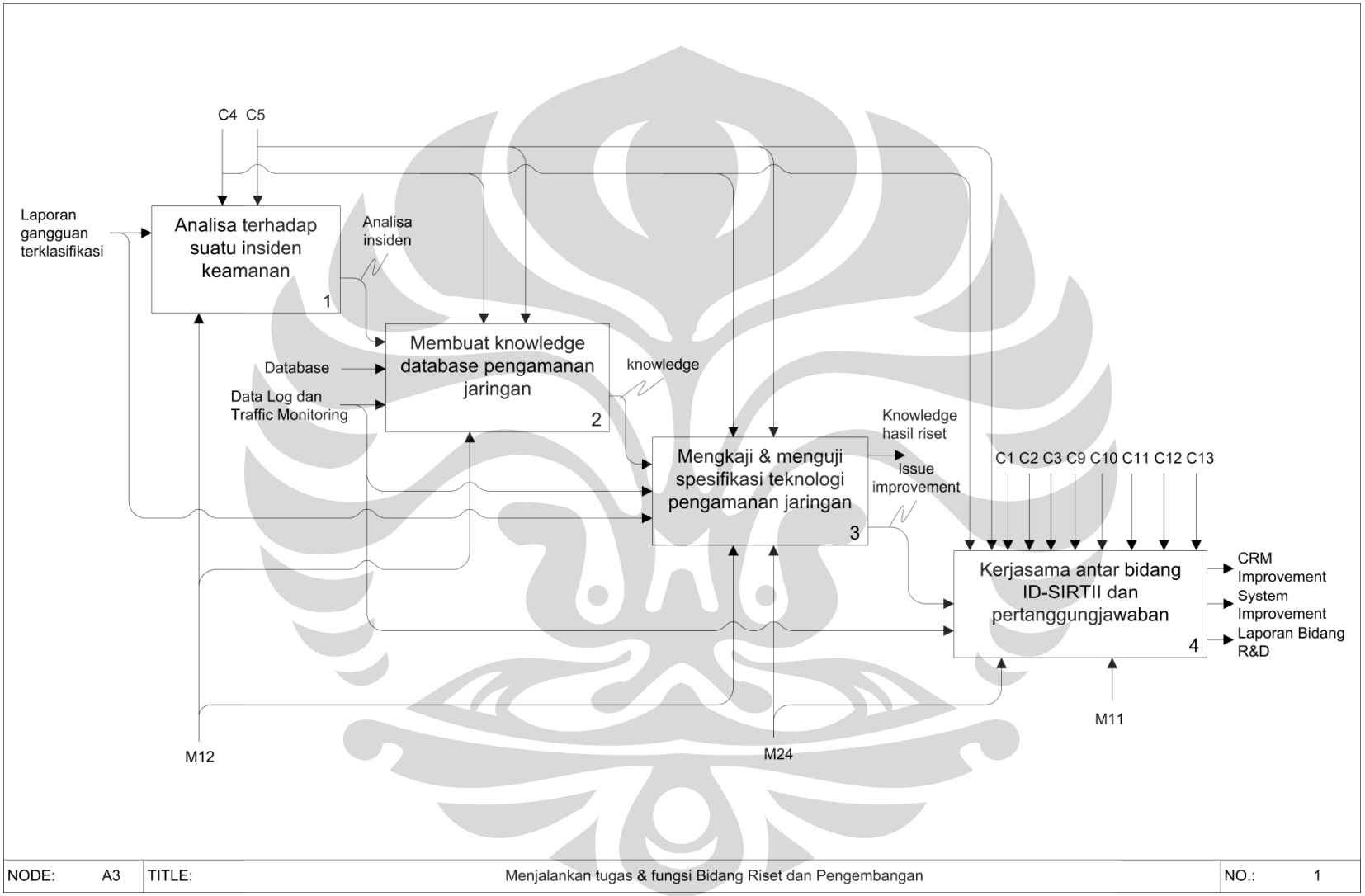
Gambar 3.3 Peta A0, Proses Bisnis Tiap Bidang ID-SIRTII



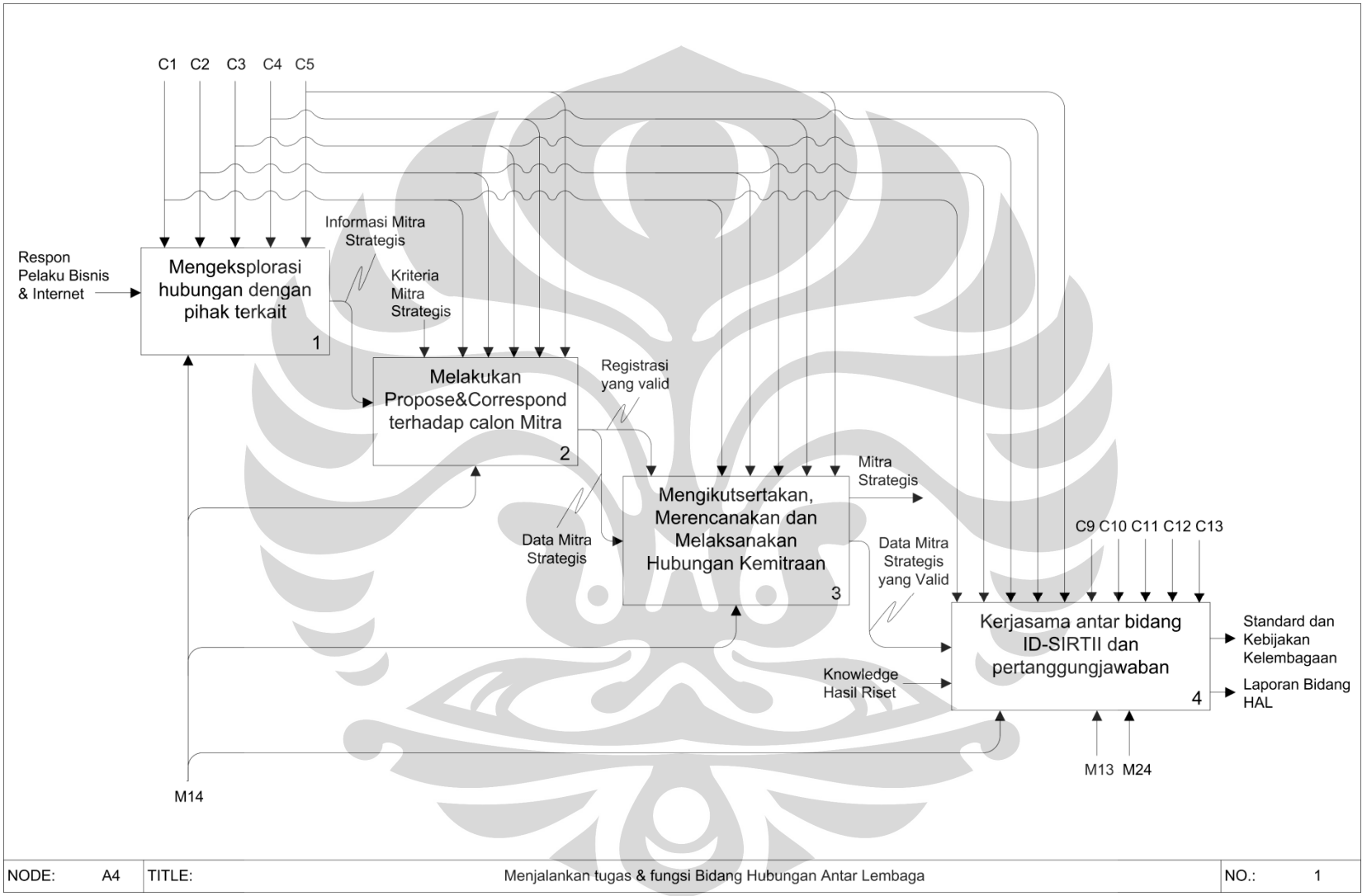
Gambar 3.4 Peta A1, Menjalankan Tugas dan Fungsi Bidang Operasional dan Keamanan



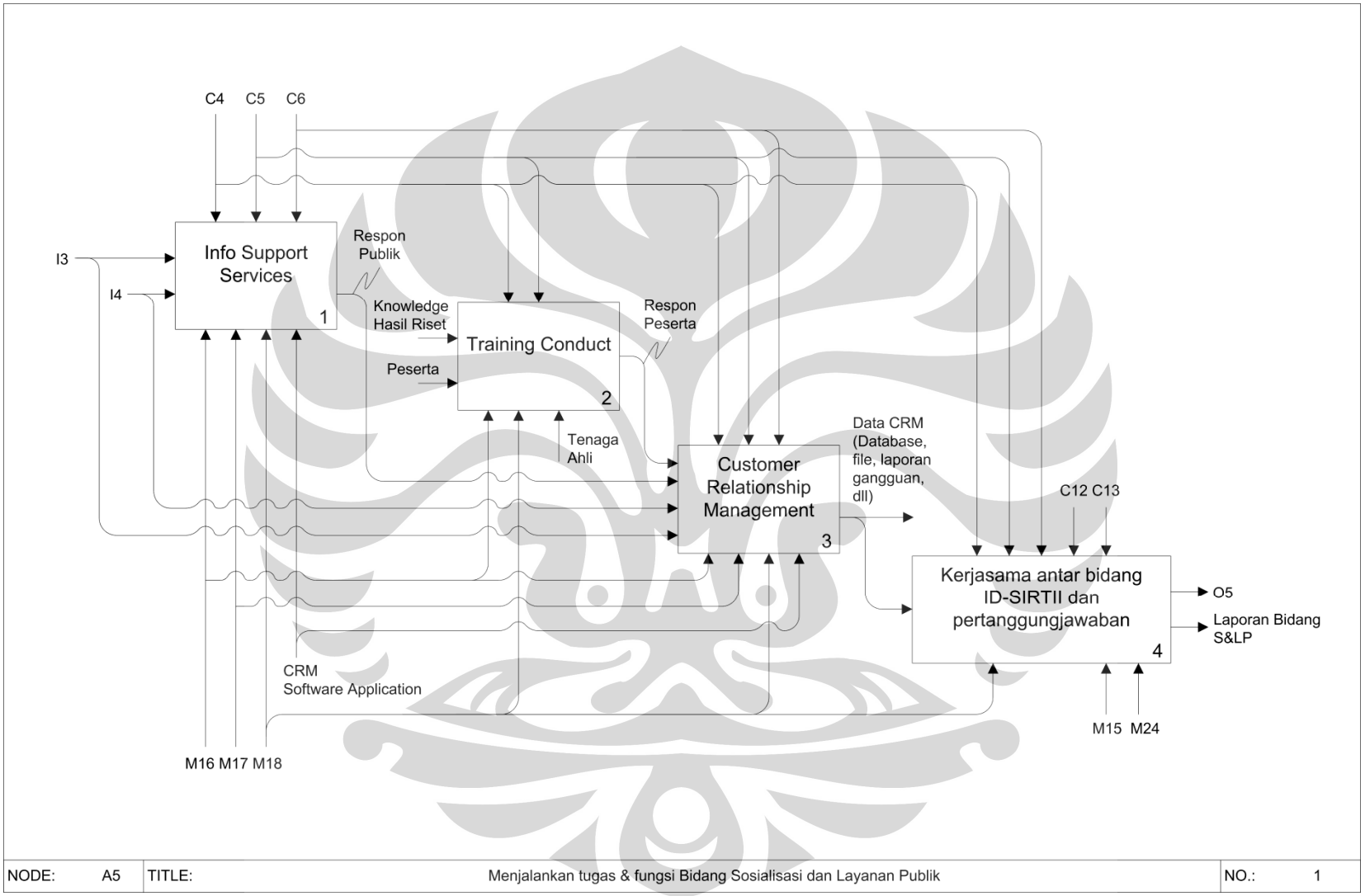
Gambar 3.5 Peta A2, Menjalankan tugas & Fungsi Bidang Data Center, Aplikasi dan Database



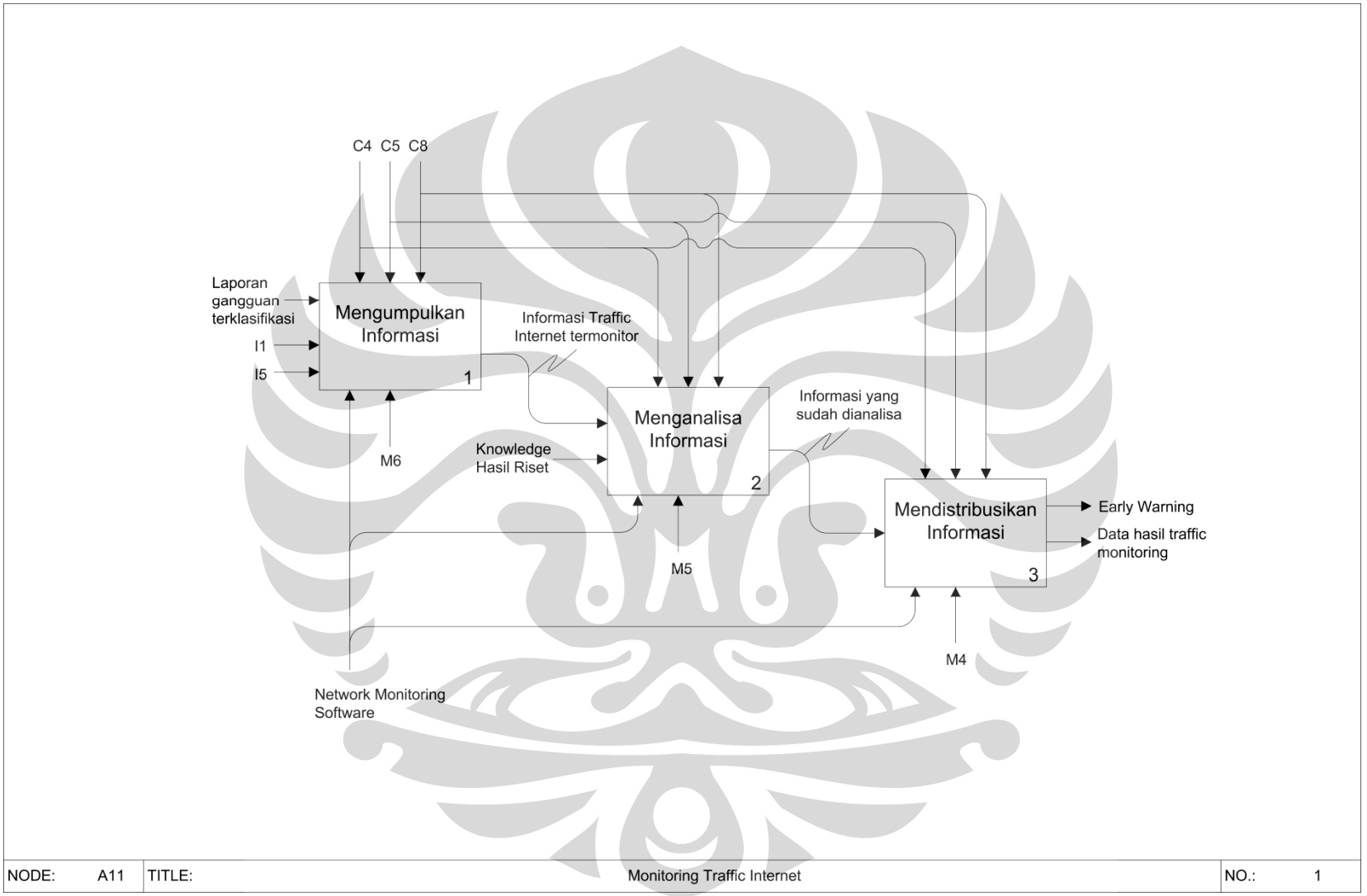
Gambar 3.6 Peta A3, Menjalankan tugas & fungsi Riset dan Pengembangan



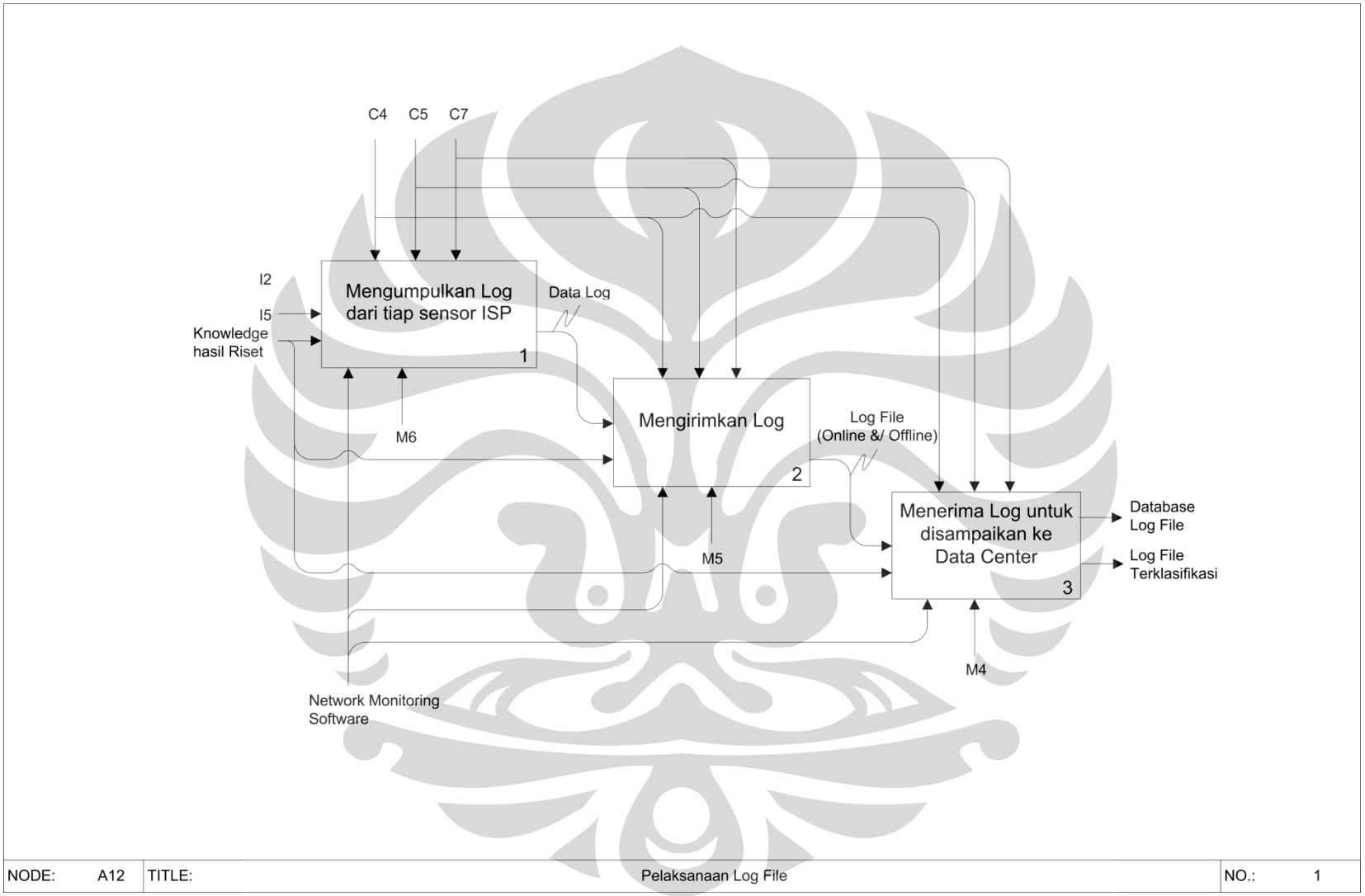
Gambar 3.7 Peta A4, Menjalankan tugas & fungsi Bidang Hubungan Antar Lembaga



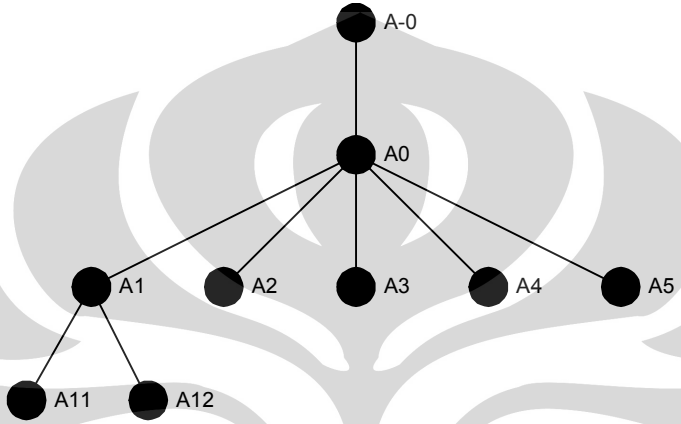
Gambar 3.8 Peta A5, Menjalankan tugas & fungsi Bidang Sosialisasi dan Layanan Publik



Gambar 3.9 Peta A11, Monitoring Trafic Internet



Gambar 3.10 Peta A12, Pelaksanaan Log File



Gambar 3.11 *Node Tree Diagram*

Referensi

A-0 ; Proses Bisnis ID-SIRTII

A0 ; Proses Bisnis Tiap Bidang ID-SIRTII

A1 ; Menjalankan Tugas dan Fungsi Bidang Operasional dan Keamanan

A2 ; Menjalankan tugas & Fungsi Bidang Data Center, Aplikasi dan Database

A3 ; Menjalankan tugas & fungsi Riset dan Pengembangan

A4 ; Menjalankan tugas & fungsi Bidang Hubungan Antar Lembaga

A5 ; Menjalankan tugas & fungsi Bidang Sosialisasi dan Layanan Publik

A11 ; Monitoring Trafic Internet

A12 ; Pelaksanaan Log File

3.3 PENILAIAN LEVEL PENGAMANAN INFORMASI PADA PROSES BISNIS ID-SIRTII

Penilaian level pengamanan informasi dilakukan pada setiap aktivitas proses bisnis di level 1 untuk mengetahui tingkat kritikalitas setiap aktivitas proses bisnis pada level 0 sebagai aktivitas utama dari proses bisnis. Hal ini dilakukan untuk mengetahui pada bagian mana pengamanan informasi dinilai paling kritikal untuk selanjutnya dilakuakan analisa, sekaligus menjadi batasan dalam penulisan penelitian ini.

Adapun penilaian dilakukan dengan menilai level pengamanan informasi untuk *Confidentiality, Integrity,* dan *Availability* terhadap *Vulnerability* dari setiap aktivitas proses bisnis level 1 dengan pertimbangan dampak citra *(public image)* yang akan terjadi jika hilangnya pengamanan informasi pada tiap aktivitas dalam proses bisnis yang dinilai.

Kritikalitas pengamanan informasi dinilai dengan memperhatikan sampai sebesar apa dampak yang akan terjadi pada kinerja organisasi, aset, ataupun individu jika dalam pengamanan informasi organisasi mengalami hilangnya kerahasiaan, integritas, dan ketersediaan. Untuk lebih mempertajam penilaian, kriteria penilaian juga memperhatikan besarnya dampak *public image* yang dialami organisasi jika terjadi *loss of Confidentiality, loss of Integrity, loss of availability* dalam pengamanan informasinya.

Pengukuran kritikalitas pengamanan informasi akan dapat terlihat jelas setelah penilaian *Confidentiality, Integrity,* dan *Availability* terhadap setiap aktivitas pada proses bisnis. Pada penelitian ini, penilaian dikelompokan pada 5 bidang yang ada dalam organisasi ID-SIRTII, yang dalam setiap bidangnya terdapat aktivitas-aktivitas utama yang dijadikan dasar penilaian kritikalitas pengamanan informasi. Setelah nilai *Confidentiality, Integrity,* dan *Availability* dirata-ratakan dalam tiap bidang, maka akan terlihat pada grafik nilai kritikalitas pengamanan informasi tiap bidang dalam organisasi.

Tabel 3.1 Kriteria Level Pengamanan Informasi

Score	Level	*Public Image* [36]	Level	*Impact* [37]
1	**Low**	*Little or no image impact*	**Low**	*The loss of confidentiality, integrity, or availability could be expected to have **limited adverse effects** on organizational operations, assets, or individuals.*
2	**Low to medium**	*Company business unit image damaged*	**Medium**	*The loss of confidentiality, integrity, or availability could be expected to have **serious adverse effects** on organizational operations, assets, or individuals.*
3	**Medium**	*Temporary blemish of company image*		
4	**Medium to high**	*Long-term blemish of company image*	**High**	*The loss of confidentiality, integrity, or availability could be expected to have **severe or catastrophic adverse effects** on organizational operations, assets, or individuals.*
5	**High**	*Total loss of public confidence and reputation*		

Sumber : Information Security Risk Analysis, second edition. Auerbach Publications, Taylor & Francis Group. 2005.

Tabel 3.2 Definisi Elemen Tingkat Pengamanan

Elemen	Definisi [38]
*Loss of **C**onfidentiality*	Kerahasiaan sistem dan data mengarah pada proteksi informasi dari penyikapan *(disclosure)* yang tidak berhak. Dampaknya mencakup dari bahaya *nonpublic*, personal, informasi pribadi, sampai hilangnya kompetisi keuntungan atau informasi rahasia perdagangan. Tersikapnya *Unauthorized, unanticipated,* atau *unintentional* dapat menyebabkan kehilangan kepercayaan publik, *competitive advantage*, *organization embarrassment*, atau tindakan hukum.
*Loss of **I**ntegrity*	Integritas sistem dan data mengarah pada kebutuhan proteksi informasi dari modifikasi yang tidak tepat. Integritas akan hilang jika perubahan data atau sistem dilakukan oleh yang tidak berhak baik itu disengaja atau tidak. Jika hal ini terjadi, pengguna sistem yang telah terkontaminasi atau data yang *corrupt* akan berakibat ketidaktepatan, penipuan/ kecurangan, atau kesalahan keputusan.
*Loss of **A**vailability*	Jika misi pada sistem yang kritikal tidak tersedia bagi penggunanya, misi organisasi mungkin akan dibuat-buat. Hilangnya fungsi system dan efektifitas operasional akan mengakibatkan kehilangan waktu produktif, olehkarena itu mengganggu *performance* tugas dari pengguna dalam mendukung misi organisasi.

Sumber : Information Security Risk Analysis, second edition. Auerbach Publications, Taylor & Francis Group. 2005

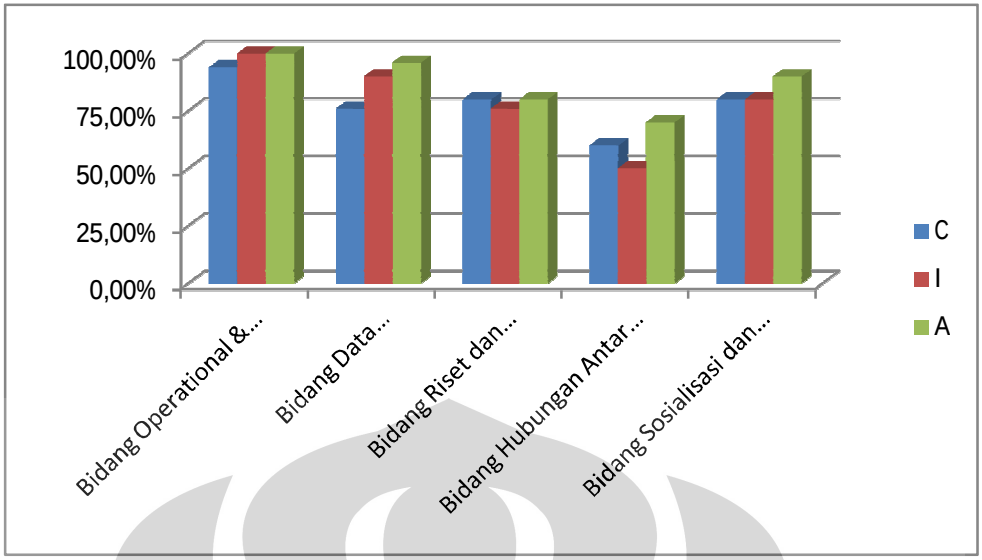
[36] Peltier, Thomas R. *Information Security Risk Analysis, second edition.* (New York: Auerbach Publications, Taylor & Francis Group, 2005), hal 292
[37] *Ibid.*, hal 53
[38] *Ibid.*, hal 44

3.3.1 Penilaian Tingkat Pengamanan pada Tiap Bidang

Pada tabel 3.3, penilaian dilakukan untuk mendapatkan rata-rata tingkat pengamanan di tiap aktivitas yang ada pada proses bisnis level 1 dengan mengacu pada (Tabel 3.1 Kriteria level pengamanan informasi) dan (Tabel 3.2 Definisi elemen tingkat pengamanan.)

Tabel 3.3 Penilaian kritikalitas pengamanan informasi

No.	Aktivitas	Lokasi dalam proses bisnis	Tingkat Pngamanan		
			C	I	A
1	Monitoring Traffic Internet	A1 (A11.1-3)	5	5	5
2	Pelaksanaan Log File	A1 (A12.1-3)	5	5	5
3	Kerjasama antar bidang ID-SIRTII dan pertanggungjawaban	A1	4	5	5
	Average		**4,67**	**5,00**	**5,00**
4	Penerimaan Log File	A2	5	5	5
5	Penyimpanan Log File	A2	5	5	5
6	Ekstraksi Log File yang dibutuhkan	A2	3	4	4
7	Kerjasama antar bidang ID-SIRTII dan pertanggungjawaban	A2	2	4	5
	Average		**3,75**	**4,50**	**4,75**
8	Analisa terhadap suatu insiden keamanan	A3	3	4	3
9	Membuat knowledge database pengamanan jaringan	A3	4	4	4
10	Mengkaji dan menguji spesifikasi teknologi pengamanan jaringan	A3	5	3	4
11	Kerjasama antar bidang ID-SIRTII dan pertanggungjawaban	A3	4	4	5
	Average		**4,00**	**3,75**	**4,00**
12	Mengeksplorasi hubungan dengan pihak terkait	A4	3	2	3
13	Melakukan propose& Correspond terhadap calon mitra	A4	3	2	3
14		A4	3	2	3
15	Kerjasama antar bidang ID-SIRTII dan pertanggungjawaban	A4	3	4	5
	Average		**3,00**	**2,50**	**3,50**
16	Info Support Services	A5	4	4	5
17	Training Conduct	A5	4	3	3
18	Customer Relationship Management	A5	5	5	5
19	Kerjasama antar bidang ID-SIRTII dan pertanggungjawaban	A5	3	4	5
	Average		**4,00**	**4,00**	**4,50**



Gambar 3.2 Kritikalitas Pengamanan Informasi pada Proses Bisnis di Tiap Bidang

3.4 IDENTIFIKASI DAN PENILAIAN RISIKO YANG *RELEVANT* TERHADAP PROSES BISNIS

Dalam identifikasi dan penilaian risiko yang *relevant* terhadap proses bisnis, penulis memprioritaskan untuk menilai risiko pada bidang yang level pengamanan informasinya paling kritikal. Berdasarkan penilaian level pengamanan informasi pada proses bisnis ID-SIRTI (sub-bab 3.3) maka penulis akan memprioritaskan identifikasi dan penilaian risiko proses bisnis pada Bidang Operasional dan Keamanan ID-SIRTII. Hal ini didasari atas nilai dari level pengamanan informasi pada proses bisnis bidang tersebut adalah yang paling kritikal dan sekaligus menjadi batasan dalam penulisan penelitian ini.

Penulis membagi identifikasi dan penilaian risiko yang ada kedalam 7 sasaran utama (*objectives)* Bidang Operasional dan Keamanan (sub-bab 3.4.1 s.d 3.4.7) dengan kriteria penilaian yang mengacu pada (Tabel 3.4 Kriteria penilaian risiko) untuk menilai level pengamanan dan (Tabel 3.4 Perlakuan terhadap risiko) untuk menentukan keputusan perlakuan terhadap risiko-risiko yang ada.

Tabel 3.4 Kriteria Penilaian Risiko

Nilai	Level Pengamanan	Definisi Kecenderungan[39]	Definisi Dampak[40]
1	Low	Sangat tidak mungkin bahwa ancaman akan terjadi selama 12 bulan kedepan	Mempengaruhi kelompok kerja atau department; Sedikit atau tidak berdampak pada proses bisnis
2	Low to medium	Tidak mungkin bahwa ancaman akan terjadi selama 12 bulan kedepan	Mempengaruhi satu/ lebih department; Sedikit penundaan dalam *meeting* pencapaian sasaran misi
3	Medium	Mungkin saja bahwa ancaman akan terjadi selama 12 bulan kedepan	Mempengaruhi dua/ lebih department/ unit bisnis; 4 s.d. 6 jam penundaan dalam *meeting* pencapaian sasaran misi
4	Medium to high	Mungkin ancaman akan terjadi selama 12 bulan kedepan	Mempengaruhi dua/ lebih unit bisnis; 1 s.d. 2 hari penundaan dalam *meeting* pencapaian sasaran misi
5	High	Sangat mungkin bahwa ancaman akan terjadi selama 12 bulan kedepan	Mempengaruhi usaha seluruh misi

Sumber : Information Security Risk Analysis, second edition. Auerbach Publications, Taylor & Francis Group. 2005

Setelah semua nilai *risk factor* didapat maka dapat ditentukan keputusan perlakuan terhadap risiko/ *threat* (potensi kejadian yang berdampak negatif terhadap sasaran bisnis atau *statement* misi dari perusahaan)[41]. Identifikasi pengendalian atau usaha perlindungan untuk setiap *risk factor* 6 atau lebih, nilai 4 atau 5 sebaiknya dimonitor secara berkala untuk memastikan *risk factor* tidak naik ke level yang tidak diinginkan, sedangkan nilai 3 atau lebih kecil tidak memerlukan *action* pada saat ini.[42] Berikut tabel 3.5 perlakuan terhadap risiko;

Tabel 3.5 Perlakuan terhadap Risiko

Risk factor	*Decision*
10 – 6	*Control & Safeguard*
4 – 5	*Control & Monitored*
2 – 3	*Do not require action at this time*

[39] *Ibid.*, hal 90
[40] *Ibid.*, hal 92
[41] *Ibid.*, hal 161
[42] *Ibid.*, hal 92

3.4.1 Pemantauan terhadap Jaringan Internet Indonesia pada Titik yang Sudah Terhubung dengan Jaringan ID-SIRTII

Tabel 3.6 Penilaian Risiko yang *Relevant* Terhadap Proses Bisnis (*objectives* 3.4.1)

No	Deskripsi Risiko/ *Threat*	Kecende-rungan	Dampak	*Risk factor*	*Decision*
1.	Keamanan jaringan internet yang kurang	3	5	8	*Control & Safeguard*
2.	Respon monitoring pada 5W (*incidents&responsibility*) + 1H (*action)* tidak tertangani dengan baik	3	5	8	*Control & Safeguard*
3.	Monitoring terganggu (*traffic moment* yang hilang/ tdk termonitor)	2	5	7	*Control & Safeguard*
4.	Gangguan pada 9 sensor yang sudah terpasang	2	5	7	*Control & Safeguard*
5.	Aktifitas monitoring tidak tertangani dengan baik	2	5	7	*Control & Safeguard*
6.	Penyimpanan informasi terganggu	1	4	5	*Control & Monitored*
7.	Klasifikasi Informasi tidak tersusun baik	1	4	5	*Control & Monitored*
8.	Distribusi Internal dan / Eksternal Informasi hasil tidak berjalan baik	1	4	5	*Control & Monitored*
9.	Personil tidak dapat melakukan tugasnya dengan efektif dan efisien	1	2	3	*Do not require action at this time*
10.	Personil tidak ada pada saat dibutuhkan	1	2	3	*Do not require action at this time*
11.	Informasi softcopy tidak tersedia ketika dibutuhkan karena kelalaian personil	1	2	3	*Do not require action at this time*

3.4.2 Mengoperasikan Sistem Pengumpulan Log File

Tabel 3.7 Penilaian Risiko yang *Relevant* Terhadap Proses Bisnis (*objectives* 3.4.2)

No	Deskripsi Risiko/ *Threat*	Kecende-rungan	Dampak	*Risk factor*	*Decision*
1.	Pengumpulan *log file* tidak maksimal	3	5	8	*Control & Safeguard*
2.	Pemanfaatan *content* log file tidak maksimal	3	5	8	*Control & Safeguard*
3.	Beban jaringan yg tinggi saat mengirim *log file* dengan kapasitas file yang besar secara online	3	5	8	*Control & Safeguard*
4.	*Effort* yg besar menggagalkan pengiriman *log file* secara *off-line*	2	5	7	*Control & Safeguard*
5.	Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP	2	5	7	*Control & Safeguard*
6.	Notifikasi pengiriman *log* tidak diterima	1	4	5	*Control & Monitored*
7.	Informasi *log file* telat diterima oleh data center akibat kelalaian personil	1	2	3	*Do not require action at this time*

3.4.3 Deteksi Dini terhadap Kemungkinan Adanya Gangguan atau Serangan

Tabel 3.8 Penilaian Risiko yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.3)

No	Deskripsi Risiko/ *Threat*	Kecende-rungan	Dampak	*Risk factor*	*Decision*
1.	Gangguan atau serangan tidak tertangangani dengan baik karena kelalaian personil	1	4	5	*Control & Monitored*
2.	Ketidaksiapan personil dalam melakuakan pendeteksian adanya gangguan	1	2	3	*Do not require action at this time*
3.	Ketidaksiapan sistem deteksi dalam melakuakan pendeteksian dini adanya gangguan atau serangan	1	2	3	*Do not require action at this time*

3.4.4 Menyusun Standar Prosedur Operasi (SOP) Pengamanan Jaringan dan Akses Jaringan Internet

Tabel 3.9 Penilaian Risiko yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.4)

No	Deskripsi Risiko/ *Threat*	Kecende-rungan	Dampak	*Risk factor*	*Decision*
1.	Prosedur pendeteksian terhadap gangguan dan serangan tidak berjalan	1	4	5	*Control & Monitored*
2.	Revisi SOP tidak dilakuakan secara berkala	2	1	3	*Do not require action at this time*
3.	Ketidaksiapan personil terhadap SOP hasil revisi	1	2	3	*Do not require action at this time*

3.4.5 Menyusun Standar Teknis Pelaksanaan Pemantauan Internet Sehari-hari Berdasarkan SOP yang Ada

Tabel 3.10 Penilaian Risiko yang *Relevant* Terhadap Proses Bisnis (*objectives* 3.4.5)

No	Deskripsi Risiko/ *Threat*	Kecende-rungan	Dampak	*Risk factor*	*Decision*
1.	Standar teknis monitoring tidak berjalan dengan baik	1	4	5	*Control & Monitored*
2.	Personil tidak siap dalam melakukan standar teknis yang sudah ditetapkan	1	3	4	*Control & Monitored*
3.	Standar teknis monitoring tidak efisien dan efektif	1	2	3	*Do not require action at this time*
3.	Standar teknis monitoring tidak direview secara berkala	1	2	3	*Do not require action at this time*

3.4.6 Melakukan Kerjasama dengan Bidang Data Center untuk Penyimpanan Data *Monitoring* dan *Log File*

Tabel 3.11 Penilaian Risiko yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.6)

No	Deskripsi Risiko/ *Threat*	Kecende-rungan	Dampak	*Risk factor*	*Decision*
1.	Kebocoran data akibat data tidak ter-enkripsi dengan baik oleh bagian Data Center saat pengiriman, penyimpanan dan ekstraksi data	1	4	5	*Control & Monitored*
2.	Koordinasi tentang penyimpanan data tidak berjalan dengan baik	1	4	5	*Control & Monitored*
3.	Verifikasi *log file* gagal dilakukan Data Center saat penyerahan dari Bidang Operasional & Keamanan	1	2	3	*Do not require action at this time*
4.	Validasi *log file* tidak valid saat pengiriman dari OK ke DC sistem *online*	1	2	3	*Do not require action at this time*

3.4.7 Melakukan Kerjasama dengan Bidang Layanan Publik, Menindaklanjuti Laporan Gangguan

Tabel 3.12 Penilaian Risiko yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.7)

No	Deskripsi Risiko/ *Threat*	Kecende-rungan	Dampak	*Risk factor*	*Decision*
1.	Laporan gangguan tidak tertangani dengan baik	2	5	7	*Control & Safeguard*
2.	Konsep layanan & materi layanan publik yang tidak sesuai dengan misi	1	4	5	*Control & Monitored*
3.	Ketidaksiapan personil bidang layanan publik terkait kinerja personil	1	2	3	*Do not require action at this time*

3.5 PENENTUAN PENANGANAN RISIKO

Penanganan risiko *(Risk handling)* termasuk methode spesifik dan teknik untuk menangani risiko-risiko yang ada, mengidentifikasi siapa yang bertanggung jawab terhadap risiko yang ada, menetapkan dan mengestimasi sumber yang berhubungan dengan penanganan risiko.[43] Pilihan dari *Risk handling* diantaranya; *Assumption, Avoidance, Control, Transfer* [44].

- *Assumption* : *(accept), Project manager* akan berkata, "Saya mengetahui adanya risiko dan menyadari konsekuensi yang mungkin terjadi. Saya mau menunggu dan melihat apa yang akan terjadi. Saya akan menerima risikonya ketika harus terjadi."
- *Avoidance* : *Project manager* akan berkata, "Saya tidak akan menerima opsi ini karena hasilnya berpotensi kurang baik. Saya akan merubah setiap rancangan untuk menghindarkan persoalan atau kebutuhan-kebutuhan persoalan yang pasti."
- *Control* : *(mitigation), Project manager* akan berkata, "Saya akan mengambil kebutuhan pengukuran yang penting-penting untuk mengendalikan risiko ini yang secara berkala dievaluasi dan merencanakan pengembangan secara berkala atau mengembalikan keadaan. Saya akan melakukan apa yang diharapkan."
- *Transfer* : *Project manager* akan berkata, "Saya akan berbagi risiko ini dengan yang lain melalui asuransi atau jaminan atau transfer seluruh resiko kepada mereka. Saya juga akan menyadari keterlibatan risiko melewati *interface* dari *hardware* dan/ atau *software* atau menggunakan pendekatan pembagian risiko lainnya.

Sebelum menentukan penanganan risiko yang tepat, setiap risiko yang telah ditetapkan untuk dilakukan *Control, Safeguard,*atau *Monitored* kemudian kembali di nilai (*assessment process)* terkait dengan *Infrastrukture FRAAP*. Hal ini dilakukan untuk lebih memperjelas penilaian *threat*/ risiko yang ada terhadap *alternative treatment* yang diusulkan guna menunjang keputusan pengendalian

[43] Kerzner, Harold. *Project Management – Ninth Edition.* John Wiley. 2005. Hal 742
[44] *Ibid*., hal 743

risiko nantinya; (*Assumption, Avoidance, Control,* atau *Transfer*). Penilaian berdasarkan tabel 3.13 berikut

Tabel 3.13 *Threat impact table*

Impact *(scale 1-3)*

Probability *(scale 1-3)*		**High**	**Medium**	**Low**
	High	**6**	**5**	**4**
	Medium	**5**	**4**	**3**
	Low	**4**	**3**	**2**

6 – 5 (High) ; 4 (Moderate) ; 3 – 2 (low)

Sumber : Information Security Risk Analysis, second edition. Auerbach Publications, Taylor & Francis Group. 2005

Infrastructure FRAAP akan megidentifikasi *threat (a potential cause of an unwanted incident, which may result in harm to a system or organization).* Dengan melakukan *Infrastruktur FRAAP*, organisasi akan dapat menentukan tingkat keamanan proses yang memperbolehkan penilaian risiko mendatang dapat dipahami bahwa dasar *controls*/ pengendaliannya ada pada tempatnya.[45]

Mengingat *FRAAP (Facilitated Risk Analysis and Assessment Process)* dapat dirancang sefleksibel mungkin sehingga bentuk dan modelnya dapat diubah sesuai dengan kebutuhan dari organisasi[46], maka selanjutnya penulis akan menganalisis dan menilai sekaligus mencoba menyimpulkan control yang dapat digunakan berdasarkan *Control* Objectives ISO/IEC 17799:2005 ; I*nformation technology – Security techniques – Code of practice for information security management* (*clauses 5 to 15; implementation advice and guidance on best practice)* yang juga terangkum pada Anex A – Controls ISO/IEC 27001:2005 ; *Information technology – Security techniques – Information security management systems – Requirements.*

[45] Peltier, Thomas R. *Information Security Risk Analysis, second edition.* Auerbach Publications, Taylor & Francis Group. 2005. Hal 207
[46] *Ibid.*, hal 221

Tabel 3.14 *FRAAP, Threat* yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.1 s.d 3.4.7 – *Control, Safeguard, & Monitored)*

No –	*Asset Classification–* / *– Object*	*Objectives –* / *– Threat/ Risk Definition*	*Security Level –* / *– Current Treatment*	*Risk Assessment (1 – 3)*			*Risk Level Expected –* / *Handling Type*	*Risk Treatment Alternative (Recommended)*	*Objectives controls; ISO/IEC 17799:2005 (Clauses 5 to 15) / Annex A – Controls ISO/IEC 27001:2005*	*PIC* / *Due Date*
				Prob.	*Impact*	*Risk Level*				
1.	Informasi	Pemantauan terhadap jaringan internet Indonesia pada titik yg sudah terhubung dgn jaringan ID-SIRTII ***(Objectives 3.4.1)- 1***	Strategic/ Fungsional/ Operasional	***Inherent (NRD)***			***Low***	***Device and infrastructure improvement***	A.9.2.1 Equipment sitting and protection, A.9.2.2 Supporting utilities, A.10.3.1 Capacity management, A.9.3.1 Securing offices, rooms, and facilities, A.15.1.1 s.d. A.1.6 (A.15.1 Compliance with legal requirements)	
				3	3	*High*				
	Bagian Operasional & Keamanan	Keamanan jaringan internet yang kurang	Pengadaan alat pemantau internet tahap 1-3	***Residual (NRA)***			*Control (Mitigation)*			
				1	3	***Medium***				
2.	Informasi	***… (Objectives 3.4.1)- 2***	Strategic/ Fungsional/ Operasional	***Inherent (NRD)***			***Low***	**Penyempurnaan regulasi dan sosialisasi SOP pengamanan informasi, Quality System**	A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures and responcibilities), A.13.2.1 s.d. A.13.2.3 (A.13.2. Management of information security incidents and improvements) A.15.1.1 s.d. A.1.6 (A.15.1 Compliance with legal requirements)	
				3	3	*High*				
	Bagian Operasional & Keamanan	Respon monitoring pada 5W *(incidents & responsibility)* + 1H (*action)* tidak tertangani dengan baik	Pembahasan regulasi dan Instruksi Kerja ID-SIRTII	***Residual (NRA)***			*Control (Mitigation)*			
				2	2	***Medium***				
3.	Informasi	***… (Objectives 3.4.1)- 3***	Fungsional/ Operasional	***Inherent (NRD)***			***Low***	***Maintenance & Improvement* pada *monitoring device (Office)***	A.10.10.2. Monitoring system use, A.9.3.1 Securing offices, rooms, and facilities, A.9.2.4 Equipment maintenance, A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures and responcibilities)	
				3	3	*High*				
	Bagian Operasional & Keamanan	Monitoring terganggu (*traffic moment* yang hilang/ tdk termonitor)	Memaksimalkan kapasitas device yang ada	***Residual (NRA)***			*Control (Mitigation)*			
				1	3	***Medium***				
4.	Informasi	***… (Objectives 3.4.1)-4***	Fungsional/ Operasional	***Inherent (NRD)***			***Low***	***Capacity & utilization Improvement* pada *device* sensor *(ISP)***	A.9.2.4 Equipment maintenance, A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures and responcibilities), A.10.2.3 Managing changes to third party services, A.9.3.1 Securing offices, rooms, and facilities	
				3	3	*High*				
	Bagian Operasional & Keamanan	Gangguan pada 9 sensor yang sudah terpasang	Memaksimalkan device sensor yang aktif	***Residual (NRA)***			*Control (Mitigation)*			
				1	3	***Medium***				

Tabel 3.15 *FRAAP, Threat* yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.1 s.d 3.4.7 – *Control, Safeguard, & Monitored)* lanjutan

No –	*Asset Classification–* / *– Object*	*Objectives –* / *– Threat/ Risk Definition*	*Security Level –* / *– Current Treatment*	*Risk Assessment (1 – 3)* Prob.	Impact	Risk Level	*Risk Level Expected –* / *Handling Type*	*Risk Treatment Alternative (Recommended)*	*Objectives controls; ISO/IEC 17799:2005 (Clauses 5 to 15) / Annex A – Controls ISO/IEC 27001:2005*	*PIC* / *Due Date*
5.	Informasi	***… (Objectives 3.4.1)- 5***	Strategic/ Fungsional/ Operasional	***Inherent (NRD)*** 3	3	*High*	***Low***	**Pelatihan, *workshop*, simulasi, & *knowledge shearing***	A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures and responcibilities), A.15.1.1 s.d. A.1.6 (A.15.1 Compliance with legal requirements), A.15.2.1 s.d. A.15.2.2 (A.15.2 Compliance with security policies and standards, and technical compliance)	
	Bagian Operasional & Keamanan	Aktifitas monitoring tidak tertangani dengan baik	Pemberdayaan dan memaksimalkan potensi SDM	***Residual (NRA)*** 1	3	***Medium***	*Control (Mitigation)*			
6.	Informasi	***… (Objectives 3.4.1)- 6***	Fungsional/ Operasional	***Inherent (NRD)*** 1	3	*Medium*	***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
	Bagian Operasional & Keamanan	Penyimpanan informasi terganggu	*Personal handling*	***Residual (NRA)*** 1	2	***Low***	*Assumption (Accept)*			
7.	Informasi	***… (Objectives 3.4.1)- 7***	Operasional	***Inherent (NRD)*** 1	3	*Medium*	***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
	Bagian Operasional & Keamanan	Klasifikasi Informasi tidak tersusun baik	SOP dan Instruksi Kerja	***Residual (NRA)*** 1	2	***Low***	*Assumption (Accept)*			
8.	Informasi	***… (Objectives 3.4.1)- 8***	Operasional	***Inherent (NRD)*** 1	3	*Medium*	***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
	Bagian Operasional & Keamanan	Distribusi Internal dan / Eksternal Informasi hasil tidak berjalan baik	SOP dan Instruksi Kerja	***Residual (NRA)*** 1	2	***Low***	*Assumption (Accept)*			

Tabel 3.16 *FRAAP, Threat* yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.1 s.d 3.4.7 – *Control, Safeguard, & Monitored)* lanjutan

No –	*Asset Classification–* / *– Object*	*Objectives –* / *– Threat/ Risk Definition*	*Security Level –* / *– Current Treatment*	*Risk Assessment (1 – 3)*			*Risk Level Expected –* / *Handling Type*	*Risk Treatment Alternative (Recommended)*	*Objectives controls; ISO/IEC 17799:2005 (Clauses 5 to 15) / Annex A – Controls ISO/IEC 27001:2005*	*PIC* / *Due Date*
				Prob.	*Impact*	*Risk Level*				
9.	Informasi	Mengoperasikan system pengumpulan log file ***(Objectives 3.4.2)- 1***	Fungsional/ Operasional	***Inherent (NRD)***			***Low***	***Device maintenance regularly***	A.10.10.2. Monitoring system use, A.9.3.1 Securing offices, rooms, and facilities, A.9.2.4 Equipment maintenance, A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures and responcibilities)	
				3	3	*High*				
	Bagian Operasional & Keamanan	Pengumpulan *log file* tidak maksimal	Memaksimalkan kinerja device yang aktif	***Residual (NRA)***			*Control (Mitigation)*			
				1	3	***Medium***				
10.	Informasi	***… (Objectives 3.4.2)- 2***	Strategic/ Fungsional/ Operasional	***Inherent (NRD)***			***Low***	**Regulasi dan standar pengamanan *Improvement***	A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures and responcibilities), A.13.2.2 Learning from information security incident, A.10.7.3 Information handling procedures,	
				3	3	*High*				
	Bagian Operasional & Keamanan	Pemanfaatan *content* log file tidak maksimal	Pembahasan regulasi dan Instruksi Kerja ID-SIRTII	***Residual (NRA)***			*Control (Mitigation)*			
				1	3	***Medium***				
11.	Informasi	***… (Objectives 3.4.2)- 3***	Strategic/ Fungsional/ Operasional	***Inherent (NRD)***			***Low***	**Penyempurnaan standar teknis. Penelitian dan pengembangan terkait penanganan beban log file**	A.10.3.1 Capacity management, A.10.3.2 System acceptance, A.12.1 s.d. A.12.6 (A.12 Information systems acquisition, development and maintenance), A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures & responcibilities)	
				3	3	*High*				
	Bagian Operasional & Keamanan	Beban jaringan yang tinggi saat mengirim log file dengan kapasitas file yang besar secara online	Memaksimalkan kapasitas device yang ada	***Residual (NRA)***			*Control (Mitigation)*			
				2	2	***Medium***				
12.	Informasi	***… (Objectives 3.4.2)- 4***	Fungsional/ Operasional	***Inherent (NRD)***			***Low***	***SDM Management***	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
				3	3	*High*				
	Bagian Operasional & Keamanan	*Effort* yang besar menggagalkan pengiriman *log file* secara *off-line*	*Personal handling*	***Residual (NRA)***			*Control (Mitigation)*			
				1	3	***Medium***				

Tabel 3.17 *FRAAP, Threat* yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.1 s.d 3.4.7 – *Control, Safeguard, & Monitored)* lanjutan

No –	*Asset Classification– / – Object*	*Objectives – / – Threat/ Risk Definition*	*Security Level – / – Current Treatment*	*Risk Assessment (1 – 3)* Prob.	Impact	Risk Level	*Risk Level Expected – / Handling Type*	*Risk Treatment Alternative (Recommended)*	*Objectives controls; ISO/IEC 17799:2005 (Clauses 5 to 15) / Annex A – Controls ISO/IEC 27001:2005*	*PIC / Due Date*
13.	Informasi	*… (Objectives 3.4.2)- 5*	Strategic/ Fungsional/ Operasional	***Inherent (NRD)*** 3	3	*High*	***Low***	**Penelitian dan pengembangan terkait utilisasi perangkat sensor yang terpasang pada ISP**	A.12.6.1 Control of technical vulnerabilities, A.15.1.1 s.d. A.1.6 (A.15.1 Compliance with legal requirements), A.15.2.1 s.d. A.15.2.2 (A.15.2 Compliance with security policies and standards, and technical compliance)	
	Bagian Operasional & Keamanan	Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP	Memaksimalkan kinerja device yang aktif	***Residual (NRA)*** 2	2	***Medium***	*Control (Mitigation)*			
14.	Informasi	*… (Objectives 3.4.2)- 6*	Operasional	***Inherent (NRD)*** 1	3	*Medium*	***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
	Bagian Operasional & Keamanan	Notifikasi pengiriman log tidak diterima	*Personal handling*	***Residual (NRA)*** 1	2	***Low***	*Assumption (Accept)*			
15.	Informasi	Deteksi dini terhadap kemungkinan adanya gangguan atau serangan ***(Objectives 3.4.3)- 1***	Operasional	***Inherent (NRD)*** 1	3	*Medium*	***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
	Bagian Operasional & Keamanan	Gangguan atau serangan tidak tertangani dengan baik karena kelalaian personil	*Personal handling*	***Residual (NRA)*** 1	2	***Low***	*Assumption (Accept)*			
16.	Informasi	Menyusun standar prosedur operasi (SOP) pengamanan jaringan dan akses jaringan internet ***(Objectives 3.4.4)- 1***	Operasional	***Inherent (NRD)*** 1	3	*Medium*	***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
	Bagian Operasional & Keamanan	Prosedur pendeteksian terhadap gangguan dan serangan tidak berjalan	Instruksi Kerja, *Personal handling*	***Residual (NRA)*** 1	2	***Low***	*Assumption (Accept)*			

Tabel 3.18 *FRAAP, Threat* yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.1 s.d 3.4.7 – *Control, Safeguard, & Monitored)* lanjutan

No –	*Asset Classification– / – Object*	*Objectives – / – Threat/ Risk Definition*	*Security Level – / – Current Treatment*	*Risk Assessment (1 – 3)* Prob.	Impact	Risk Level	*Risk Level Expected – / Handling Type*	*Risk Treatment Alternative (Recommended)*	*Objectives controls; ISO/IEC 17799:2005 (Clauses 5 to 15) / Annex A – Controls ISO/IEC 27001:2005*	*PIC / Due Date*
17.	Informasi	Menyusun standar teknis peaksanaan pemantauan internet sehari-hari berdasarkan SOP ***(Objectives 3.4.5)- 1***	Fungsional/ Operasional	***Inherent (NRD)***			***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
				1	3	*Medium*				
	Bagian Operasional & Keamanan	Standar teknis monitoring tidak berjalan dengan baik	SOP dan Instruksi Kerja	***Residual (NRA)***			*Assumption (Accept)*			
				1	2	***Low***				
18.	Informasi	***… (Objectives 3.4.5)- 2***	Operasional	***Inherent (NRD)***			***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management, A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
				1	3	*Medium*				
	Bagian Operasional & Keamanan	Personil tidak siap dalam melakukan standar teknis yang sudah ditetapkan	Instruksi Kerja, *Personal handling*	***Residual (NRA)***			*Assumption (Accept)*			
				1	2	***Low***				
19.	Informasi	Melakuakan kerjasama dengan bidang Data Center untuk penyimpanan data monitoring dan log file ***(Objectives 3.4.6)- 1***	Operasional	***Inherent (NRD)***			***Low***	-	A.11.1 s.d. A.11.7 (A.11 Access control), A.12.1 s.d. A.12.6 (A.12 Information systems acquisition, development and maintenance), A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures and responcibilities)	
				1	3	*Medium*				
	Bagian Operasional & Keamanan	Kebocoran data akibat data tidak ter-enkripsi dengan baik oleh bagian Data Center saat pengiriman, penyimpanan, dan ekstraks data	SOP, Instruksi Kerja & *Personal handling*	***Residual (NRA)***			*Assumption (Accept)*			
				1	2	***Low***				
20.	Informasi	***… (Objectives 3.4.6)- 2***	Operasional	***Inherent (NRD)***			***Low***	-	A.10.1.1. Documented operating procedures, A.10.1.2 Change management A.10.1.3 Segregation of duties, A.10.1.4 Separation of development, test & operational facilities	
				1	3	*Medium*				
	Bagian Operasional & Keamanan	Koordinasi tentang penyimpanan data tidak berjalan dengan baik	SOP dan Instruksi Kerja	***Residual (NRA)***			*Assumption (Accept)*			
				1	2	***Low***				

Tabel 3.19 *FRAAP, Threat* yang *Relevant* terhadap Proses Bisnis (*objectives* 3.4.1 s.d 3.4.7 – *Control, Safeguard, & Monitored)* lanjutan

No –	*Asset Classification–* / *– Object*	*Objectives –* / *– Threat/ Risk Definition*	*Security Level –* / *– Current Treatment*	*Risk Assessment (1 – 3)*			*Risk Level Expected –* / *Handling Type*	*Risk Treatment Alternative (Recommended)*	*Objectives controls; ISO/IEC 17799:2005 (Clauses 5 to 15) / Annex A – Controls ISO/IEC 27001:2005*	*PIC* / *Due Date*
				Prob.	*Impact*	*Risk Level*				
21.	Informasi	Melakukan kerjasama dengan bidang layanan public, menindaklanjuti laporan gangguan ***(Objectives 3.4.7)- 1***	Strategic/ Fungsional/ Operasional	***Inherent (NRD)***			***Low***	***CRM Implementation***	A.10.1.1 s.d. A.10.1.4 (A.10.1 Operational procedures & responcibilities), A.12.5 Security in development and support procedures, A.13.1 Reporting information security events and weaknesses, A.14.1. Information security aspects of business continuity management A.15.1.1 s.d. A.1.6 (A.15.1 Compliance with legal requirements),	
				3	3	*High*				
	Bagian Operasional & Keamanan	Laporan gangguan tidak tertangani dengan baik	SOP dan Instruksi Kerja	***Residual (NRA)***			*Control (Mitigation)*			
				1	3	***Medium***				
22.	Informasi	***… (Objectives 3.4.7)- 2***	Strategic/ Fungsional/ Operasional	***Inherent (NRD)***			***Low***	-	A.10.9.1 s.d. A.10.9.3 (A.10.9 Electronic commerce services) A.14.1.1 s.d A.14.1.5 (A.14.1 Information security aspects of business continuity management), A.15.1.1 s.d. A.1.6 (A.15.1 Compliance with legal requirements), A.15.2.1 s.d. A.15.2.2 (A.15.2 Compliance with security policies and standards, and technical compliance)	
				1	3	*Medium*				
	Bagian Operasional & Keamanan	Konsep layanan & materi layanan public yang tidak sesuai dengan misi	Pembahasan konsep, regulasi, *road map* dan Instruksi Kerja ID-SIRTII	***Residual (NRA)***			*Assumption (Accept)*			
				1	2	***Low***				

BAB IV
ANALISIS

Pada bab 4 ini, penulis akan menganalisis hasil identifikasi dan evaluasi penilaian risiko yang *relevant* terhadap proses bisnis terkait pengamanan informasi yang telah dijabarkan pada bab sebelumnya (tabel *FRAAP threat*, sub-bab 3.5). Penulis akan memulai dengan menyusun rencana penanggulangan resiko untuk setiap alternatif ***risk treatment*** yang membutuhkan penanganan (***risk handling*** yang tergolong pada tipe *Control/ Mitigation)*, kemudian mengaplikasikan ***software*** optimasi OptQuest pada Crystal Ball terhadap rencana penanggulangan risiko tersebut guna mendapatkan model simulasi peramalan dan optimasi pengalokasian dana dari alternatif *risk treatment* yang ada.

4.1 ANALISIS RISIKO TERKAIT RENCANA PENANGANAN RISIKO

4.1.1 Pengelompokan Risiko terkait Kebutuhan Penanganan Risiko

Setelah risiko dinilai dan ditentukan tipe penanganannya pada form *FRAAP*, tahap berikutnya yang dilakukan dalam penelitian ini adalah memisahkan setiap risiko yang tergolong pada tipe penanganan "*Control (Mitigation)*" untuk selanjutnya dilakukan penyusunan rencana penaggulangan risiko dengan memperhatikan dampak dari risiko-risiko yang ada.

Tujuan dari pengelompokan atau pemisahan risiko ini adalah untuk lebih meningkatkan efektifitas dari setiap usaha penanggulangan risiko yang ada. Diharapkan dengan semakin sedikitnya jumlah poin penaggulangan risiko, setiap poin tersebut dapat direalisasikan dengan usaha yang lebih besar dan terfokus sehingga diharapkan akan mendatangkan hasil berupa nilai risiko tertanggulangi yang optimal sesuai harapan.

Dari hasil tahapan *FRAAP* sebelumnya, didapat 11 poin risiko/ *threat* yang membutuhkan penanganan *(Control/ Mitigation)* untuk dikendalikan/ dikurangi risikonya ke tinggat risiko yang diharapkan.

Tabel 4.1 Alternatif *Risk Treatment* dalam Pengendalian Risiko yang Ada

No.	*Risk ID*	Deskripsi risiko*/ threat*	*Weakness Factor*	Alternatif *Risk Treatment*
1.	R1	Keamanan jaringan internet yang kurang	Keterbatasan *device* dan infrastruktur pengamanan jaringan internet	*Device and infrastructure improvement*
2.	R2	Respon monitoring pada 5W (*incidents & responsibility*) + 1H (*action)* tidak tertangani dengan baik	Regulasi, sosialisasi SOP pengamanan informasi dan *Quality System* masih belum sempurna	Penyempurnaan regulasi, sosialisasi SOP pengamanan informasi, *Quality System*
3.	R3	Monitoring terganggu (*traffic moment* yang hilang/ tdk termonitor)	Beban jumlah data *traffic* yang lewat terlalu besar sekitar atau lebih dari 300 ribu data *traffic*/ hari	*Maintenance & Improvement* pada *monitoring device (Office)*
4.	R4	Gangguan pada 9 sensor yang sudah terpasang	Penggunaan kapasitas sensor ISP yang berlebih dan terus menerus	*Capacity & utilization Improvement* pada *device* sensor *(ISP)*
5.	R5	Aktifitas monitoring tidak tertangani dengan baik	Keterbatasan kemampuan SDM yang ada	Pelatihan, *workshop, simulasi*, & *knowledge shearing*
6.	R6	Pengumpulan log file tidak maksimal	Fungsi sensor terpasang belum beroperasi baik secara maksimum	*Device maintenance regularly*
7.	R7	Pemanfaatan *content* log file tidak maksimal	Kebijakan pemanfaatan *content* log file masih dalam pembahasan	Regulasi dan standar pengamanan *Improvement*
8.	R8	Beban jaringan yg tinggi saat mengirim log file dengan kapasitas file yang besar secara online	Standar *format* log file, teknis dan strategi penanganan log file	Penyempurnaan standar teknis, Penelitian dan pengembangan terkait penanganan beban log file
9.	R9	*Effort* yg besar menggagalkan pengiriman log file secara *off-line*	*Eksternal factor* dari SDM yang ada,	*SDM management*
10.	R10	Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP	Strategi penanganan jaringan dan SDM yang ada masih terbatas	Penelitian dan pengembangan terkait *utilisasi* perangkat sensor yang terpasang pada ISP
11.	R11	Laporan gangguan tidak tertangani dengan baik	*Customer Relationship Management* belum berjalan baik	*CRM Implementation*

4.1.2 Potensi Kerugian dari Risiko yang Membutuhkan Pengendalian

Dari ke 11 poin risiko yang ada, berikut adalah potensi kerugian akibat *threat* terhadap *vulnerability* risiko yang mungkin terjadi setelah tahapan ke-3 dari pembangunan ID-SIRTII. Estimasi dan formulasi potensi kerugian dari risiko yang membutuhkan penanganan "*Control (Mitigation)*" dikalkulasikan berdasarkan informasi dan asumsi-asumsi yang dinilai berdasarkan objek yang sama yaitu potensi kerugian terhadap gangguan dan ancaman pada data *traffic* yang mungkin terjadi.

- Poin risiko 1, Keamanan jaringan internet yang kurang.
  Potensi *threat* terjadi pada sekitar 40% *traffic* pada 300 ISP&NAP di Jakarta tidak termonitor dengan baik oleh ke-9 sensor yang telah terpasang. Rata-rata 300.000 data *traffic*/ hari/ ISP&NAP di Jakarta dengan asumsi nilai Rp. 100,- s.d. Rp. 200,- /data *traffic* (karena terkait *traffic* 300 ISP&NAP besar ataupun kecil di Jakarta).
  - Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;
    (40%) x 300 (ISP&NAP) x 300.000 (data *traffic*/ hari/ ISP&NAP)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp. 1.314.000.000.000,- s.d. Rp. 2.628.000.000.000,- (dalam setahun)

- Poin risiko 2, Respon monitoring pada 5W (*incidents & responsibility*) + 1H (*action)* tidak tertangani dengan baik.
  Potensi *threat* terjadi pada sekitar 20% respon terhadap data *traffic* yang termonitor oleh 9 *sensor device*. Rata-rata 300.000 data *traffic* yang ter-*capture* tiap harinya oleh tiap sensor yang terpasang dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic*. (karena terkait *traffic* ISP&NAP besar yang termonitor oleh 9 sensor)
  - Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;
    (20%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp. 197.100.000.000,- s.d. Rp. 394.200.000.000,- (dalam setahun)

- Poin risiko 3, Monitoring terganggu (*traffic moment* yang hilang/ tidak termonitor). Potensi *threat* terjadi pada sekitar 40% *moment* data *traffic* yang hilang/ tidak termonitor dari 9 *sensor device* yang terpasang. Rata-rata 300.000 data *traffic* yang ter-*capture* tiap harinya dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic*.
  - Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;

    (40%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp. 394.200.000.000,- s.d. Rp 788.400.000.000,- (dalam setahun)

- Poin risiko 4, Gangguan pada 9 sensor yang sudah terpasang.
  9 sensor setidaknya mampu memonitor 80% data traffic pada ISP&NAP di Jakarta. Potensi *threat* terjadi pada sekitar 80% data *traffic* ISP&NAP besar di Jakarta yang ter-*capture* oleh sensor yang aktif tersebut. Rata-rata 300.000 data *traffic* yang ter-*capture* tiap harinya dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic.*
  - Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;

    (80%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp 788.400.000.000,- s.d. Rp 1.576.800.000.000,- (dalam setahun)

- Poin risiko 5, Aktifitas monitoring tidak tertangani dengan baik.
  SDM yang ada setidaknya mampu memonitor 60% data *traffic* pada ISP&NAP di Jakarta. Potensi *threat* terjadi pada sekitar 40% data *traffic* ISP&NAP yang tidak tertertangani oleh SDM yang ada. Rata-rata 300.000 data *traffic* yang harus dimonitoring oleh SDM yang ada tiap harinya dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic.*
  - Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;

    (40%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp. 394.200.000.000,- s.d. Rp 788.400.000.000,- (dalam setahun)

- Poin risiko 6, Pengumpulan log file tidak maksimal.

  Fungsi dari 9 sensor yang sudah terpasang pada ISP&NAP terdapat 2 sensor ditahun ini (2008) yang belum beroperasi maksimal. Rata-rata 300.000 data *traffic* /hari tidak dapat di-*capture* untuk pengumpulan log, dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic*.

  - Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;

    2 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp. 219.000.000.000,- s.d. Rp 438.000.000.000,- (dalam setahun)

- Poin risiko 7, Pemanfaatan *content* log file tidak berfungsi maksimal.

  Terdapat potensi kelemahan kebijakan waktu penyimpanan perekaman (logfile) yang seharusnya (3 bulan-kah, 1 tahun-kah atau lebih?) bagaimana dengan penyamaran IP,? dan bagaimana kebijakan dan aturan pemanfaatan *content* logfile tersebut bagi *professional - experts - police - attorney - government - academician - researcher – practitioner, advisory/ executive/ inspection board governance, internet service providers and related parties, institution and nation based response teams and other related bodies*...?

  Kelemahan kebijakan mengenai logfile tersebut berkaitan dengan nilai dari kapasitas *content* logfile yang mampu di-*capture* dan disimpan oleh ID-SIRTII guna pemanfaatannya, setidaknya 80% dapat dimanfaatkan sesuai kebijakan. Potensi kerugian akibat *threat* terhadap *vulnerability* risiko tersebut terdapat pada 20% kapasitas *content* yang ter-*capture* tidak berfungsi sebagaimana mestinya akibat kebijakan waktu penyimpanan, penyamaran IP pada logfile dan hal-hal lainnya yang berkaitan dengan kelemahan kebijakan penyimpanan log file.

  - Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;

    (20%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp. 197.100.000.000,- s.d. Rp 394.200.000.000,- (dalam setahun)

- Poin risiko 8, Beban jaringan yang tinggi saat mengirim log file dengan kapasitas file yang besar secara online.

  Threat terjadi pada sekitar 10% data *traffic* yang berpotensi *corrupt, delay* atau tidak tertertangani dengan baik akibat beban jaringan yang tinggi saat mengirim log file dengan kapasitas file yang besar secara *online*. Rata-rata 300.000 data *traffic* harian yang harus dikirim *online*. Potensi kerugian terjadi pada 10% kapasitas data *traffic* yang dikirim online yang dihitung dalam kurun waktu satu tahun, dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic*.

  Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;

  (10%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
  x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
  ≈ Rp. 98.550.000.000,- s.d. Rp 197.100.000.000,- (dalam setahun)

- Poin risiko 9, *Effort* yang besar menggagalkan pengiriman log file secara *off-line*.

  Threat terjadi pada sekitar 10% data *traffic* yang berpotensi hilang, *corrupt, delay* atau tidak tertertangani dengan baik oleh SDM yang ada sebagai dampak dari *Effort* yang tinggi saat mengirim log file secara *off-line*. Rata-rata 300.000 data *traffic* harian yang harus dikirim 2 kali dalam sebulan (setiap 14 hari kalender). Potensi kerugian terjadi pada 10% kapasitas data *traffic* yang dikirim *off-line* yang dihitung dalam kurun waktu satu tahun, dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic*.

  Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;

  (10%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
  x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
  ≈ Rp. 197.100.000.000,- s.d. Rp 394.200.000.000,- (dalam setahun)

- Poin risiko 10, Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP.

  Threat terjadi pada sekitar 40% data *traffic* berpotensi tidak tertertangani dengan baik akibat bertambahnya beban kinerja dan utilisasi yang diterima ISP. Rata-rata 300.000 data *traffic* harus ter-*capture* oleh 9 sensor tiap harinya, dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic*.

- Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;
  (40%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
  x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
  ≈ Rp. 394.200.000.000,- s.d. Rp 788.400.000.000,- (dalam setahun)

- Poin risiko 11, Laporan gangguan tidak tertangani dengan baik.
  Threat terjadi pada laporan gangguan internet disekitar 5% dari data *traffic* yang ter-*capture* oleh 9 sensor berpotensi tidak tertertangani dengan baik akibat *Customer Relationship Management* yang belum berjalan baik. Rata-rata 300.000 data *traffic* ter-*capture* oleh 9 sensor tiap harinya, dengan asumsi nilai Rp. 1000,- s.d. Rp. 2000,- /data *traffic*.
  - Ø Kalkulasi potensi kerugian terhadap *vulnerability* risiko tersebut adalah sebagai berikut;
    (5%) x 9 (*sensor device*) x 300.000 (data *traffic*/ hari/ sensor)
    x 365 (hari dalam setahun) x 1000 s.d. 2000 (Rp./ data *traffic*)
    ≈ Rp. 49.275.000.000,- s.d. Rp 98.550.000.000,- (dalam setahun)

4.1.3 Rencana Penanganan Risiko

Dari ke 11 poin risiko yang ada, berikut adalah rencana penanganan risiko yang merupakan *alternative risk treatment* yang disusun guna menanggulangi/ mengurangi potensi kerugian risiko yang mungkin terjadi.

Rencana penanganan risiko *(treatment cost)* adalah susunan estimasi biaya yang diusulkan penulis guna meng-*cover* potensi kerugian dari risiko yang ada *(risk cost)*. Sedangkan variable kendala (batasan *treatment cost*) pada simulasi optimalisasi alokasi biaya nantinya adalah rencana anggaran ID-SIRTII tahun 2009 yang meliputi rencana anggaran terkait SDM, rencana anggaran terkait lab simulasi, penelitian dan pengembangan, rencana anggaran terkait jaringan dan sewa *bandwidth*, dan rencana anggaran terkait perawatan, atau senilai total ≈ Rp.13.560.000.000,-

- Poin risiko 1, Keamanan jaringan internet yang kurang. *Weakness factor;* Keterbatasan *device* dan infrastruktur pengamanan jaringan internet. *Alternative risk treatment; Device and infrastructure improvement.*

  Ø Estimasi usulan rencana penanganganan;

  - Pengembangan infrastruktur (15% dari pengembangan tahun 2007 dan 2008 ≈ 15% x Rp. 14.897.478.000,-) ≈ Rp. 2.235.000.000,-
  - *Device* dan infrastruktur *maintenance* ≈ Rp. 200.000.000,-
  - *System improvement* ≈ Rp. 100.000.000,- +

    Total senilai ≈ Rp. 2.535.000.000,-

- Poin risiko 2, Respon monitoring pada 5W (*incidents & responsibility*) + 1H (*action)* tidak tertangani dengan baik. *Weakness factor;* Regulasi, sosialisasi SOP pengamanan informasi dan *Quality System* masih belum sempurna. *Alternative risk treatment;* Penyempurnaan regulasi dan sosialisasi SOP pengamanan informasi, *Quality System.*

  Ø Estimasi usulan rencana penanganganan;

  - Penyempurnaan regulasi (*study banding* dan simulasi perangkat monitoring *improvement*) ≈ Rp. 1.200.000.000,-
  - Sosialisasi (Seminar dan *workshop*) ≈ Rp. 200.000.000,-
  - Fasilitasi *Quality System training* ≈ Rp. 20.000.000,-
  - *Quality system training* (10 x $525) ≈ Rp. 65.000.000,- +

    Total senilai ≈ Rp. 1.485.000.000,-

- Poin risiko 3, Monitoring terganggu (*traffic moment* yang hilang/ tdk termonitor). *Weakness factor;* Beban jumlah data *traffic* yang lewat terlalu besar sekitar atau lebih dari 300 ribu data *traffic*/ hari. *Alternative risk treatment; Maintenance & Improvement* pada *monitoring device (Office).*

  Ø Estimasi usulan rencana penanganganan;

  - *Maintenance, improvement* & simulasi ≈ Rp. 1.500.000.000,-
  - Fasilitasi *device improvement* ≈ Rp. 50.000.000,-
  - Fasilitasi penelitian ≈ Rp. 50.000.000,- +

    Total senilai ≈ Rp. 1.600.000.000,-

- Poin risiko 4, Gangguan pada 9 sensor yang sudah terpasang. *Weakness factor;* Penggunaan kapasitas sensor ISP yang berlebih dan terus menerus. *Alternative risk treatment; Capacity & utilization Improvement* pada *device* sensor *(ISP).*

  Ø Estimasi usulan rencana penanganganan;

  - Fasilitasi penelitian dan pengembangan *device* sensor dan *utilization improvement* ≈ Rp. 100.000.000,-
  - *Capacity Improvement (bandwidth)* ≈ Rp. 1.100.000.000,- +
  - Total senilai ≈ Rp. 1.200.000.000,-

- Poin risiko 5, Aktifitas monitoring tidak tertangani dengan baik. *Weakness factor;* Keterbatasan kemampuan SDM yang ada. *Alternative risk treatment;* Pelatihan, *workshop* & Simulasi, *knowledge shearing.*

  Ø Estimasi usulan rencana penanganganan;

  - Fasilitasi pengembangan SDM ≈ Rp. 50.000.000,-
  - Penelitian, pelatihan & *workshop* SDM ≈ Rp. 300.000.000,-
  - Simulasi & *knowledge shearing* ≈ Rp. 1.550.000.000,- +
  - Total senilai ≈ Rp. 1.900.000.000,-

- Poin risiko 6, Pengumpulan log file tidak maksimal. *Weakness factor;* Fungsi sensor terpasang belum beroperasi baik secara maksimum. *Alternative risk treatment; Device maintenance regularly.*

  Ø Estimasi usulan rencana penanganganan;

  - Perawatan ≈ Rp. 100.000.000,-
  - Simulasi & penelitian system log file ≈ Rp. 350.000.000,- +
  - Total senilai ≈ Rp. 450.000.000,-

- Poin risiko 7, Pemanfaatan *content* log file tidak maksimal. *Weakness factor;* Kebijakan pemanfaatan *content* log file masih dalam pembahasan. *Alternative risk treatment;* Regulasi dan standar pengamanan *Improvement.*

  Ø Estimasi usulan rencana penanganganan;

  - Fasilitasi penyempurnaan regulasi
  - *Study banding* terkait standar pengamanan dan pemanfaatan *content* log file
  - Simulasi penanganan log file

  Total senilai ≈ Rp. 1.800.000.000,-

- Poin risiko 8, Beban jaringan yg tinggi saat mengirim log file dengan kapasitas file yang besar secara online. *Weakness factor;* Standar *format* log file, teknis dan strategi penanganan log file. *Alternative risk treatment;* Penyempurnaan standar teknis, Penelitian dan pengembangan terkait penanganan beban log file.

  Ø Estimasi usulan rencana penanganganan;

  - Penelitian, dan pengembangan teknis terkait strategi penanganan beban log file ≈ Rp. 200.000.000,-
  - Fasilitasi penyempurnaan standar teknis ≈ Rp. 50.000.000,-
  - *Capacity Improvement (bandwidth)* ≈ Rp. 700.000.000,- +

    Total senilai ≈ Rp. 950.000.000,-

- Poin risiko 9, *Effort* yg besar menggagalkan pengiriman log file secara *off-line*. *Weakness factor; Eksternal factor* dari SDM yang ada. *Alternative risk treatment; SDM management.*

  Ø Estimasi usulan rencana penanganganan;

  - *SDM management* (pengadaan, pelatihan dan pengembangan)

    Total senilai ≈ Rp. 1.900.000.000,-

- Poin risiko 10, Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP. *Weakness factor;* Strategi penanganan jaringan dan SDM yang ada masih terbatas. *Alternative risk treatment;* Penelitian dan pengembangan terkait *utilisasi* perangkat sensor yang terpasang pada ISP.

  Ø Estimasi usulan rencana penanganganan;

  - Pengembangan perangkat sensor & jaringan *(virtual device*),

    Penelitian dan simulasi terkait utilisasi perangkat sensor guna penanganan beban perangkat ISP ≈ Rp. 1.550.000.000,-
  - Fasilitasi pelatihan & pengembangan SDM ≈ Rp. 200.000.000,- +

    Total senilai ≈ Rp. 1.750.000.000,-

- Poin risiko 11, Pemasangan Laporan gangguan tidak tertangani dengan baik. *Weakness factor; Customer Relationship Management* belum berjalan baik. *Alternative risk treatment; CRM Implementation.*
  - Ø Estimasi usulan rencana penanganganan;
    - Sosialisasi (Seminar dan *workshop*) ≈ Rp. 100.000.000,-
    - Pelatihan & *workshop* CRM ≈ Rp. 300.000.000,-
    - Fasilitasi *CRM Implementation* ≈ Rp. 50.000.000,- +

      Total senilai ≈ Rp. 450.000.000,-

Tabel 4.2 Rekapitulasi Potensi Kerugian dan Rencana Penanganan Risiko

No.	*Risk ID*	Deskripsi risiko*/ threat*	Potensi kerugian *(Risk Cost) dalam setahun*	Alternatif *Risk Treatment*	Rencana penanganan *(Treatment Cost)*
1.	R1	Keamanan jaringan internet yang kurang	Rp. 1.314.000.000.000,- s.d. Rp. 2.628.000.000.000,-	*Device and infrastructure improvement*	Rp. 2.535.000.000,-
2.	R2	Respon monitoring pada 5W (*incidents & responsibility*) + 1H (*action)* tidak tertangani dengan baik	Rp. 197.100.000.000,- s.d. Rp. 394.200.000.000,-	Penyempurnaan regulasi, sosialisasi SOP pengamanan informasi, dan *Quality System*	Rp. 1.485.000.000,-
3.	R3	Monitoring terganggu (*traffic moment* yang hilang/ tdk termonitor)	Rp. 394.200.000.000,- s.d. Rp 788.400.000.000,-	*Maintenance & Improvement* pada *monitoring device (Office)*	Rp. 1.600.000.000,-
4.	R4	Gangguan pada 9 sensor yang sudah terpasang	Rp 788.400.000.000,- s.d. Rp 1.576.800.000.000,-	*Capacity & utilization Improvement* pada *device* sensor *(ISP)*	Rp. 1.200.000.000,-
5.	R5	Aktifitas monitoring tidak tertangani dengan baik	Rp. 394.200.000.000,- s.d. Rp 788.400.000.000,-	Pelatihan, *workshop,* simulasi, & *knowledge shearing*	Rp. 1.900.000.000,-
6.	R6	Pengumpulan log file tidak maksimal	Rp. 219.000.000.000,- s.d. Rp 438.000.000.000,-	*Device maintenance regularly*	Rp. 450.000.000,-
7.	R7	Pemanfaatan *content* log file tidak maksimal	Rp. 197.100.000.000,- s.d. Rp 394.200.000.000,-	Regulasi dan standar pengamanan *Improvement*	Rp. 1.800.000.000,-
.	R8	Beban jaringan yg tinggi saat mengirim log file dengan kapasitas file yang besar secara online	Rp. 98.550.000.000,- s.d. Rp 197.100.000.000,-	Penyempurnaan standar teknis, Penelitian dan pengembangan terkait penanganan beban log file	Rp. 950.000.000,-
9.	R9	*Effort* yg besar menggagalkan pengiriman log file secara *off-line*	Rp. 197.100.000.000,- s.d. Rp 394.200.000.000,-	*SDM management*	Rp. 1.900.000.000,-
10.	R10	Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP	Rp. 394.200.000.000,- s.d. Rp 788.400.000.000,-	Penelitian dan pengembangan terkait *utilisasi* perangkat sensor yang terpasang pada ISP	Rp. 1.750.000.000,-
11.	R11	Laporan gangguan tidak tertangani dengan baik	Rp. 49.275.000.000,- s.d. Rp 98.550.000.000,-	*CRM Implementation*	Rp. 450.000.000,-
				Total treatment cost	**Rp. 16.020.000.000,-**

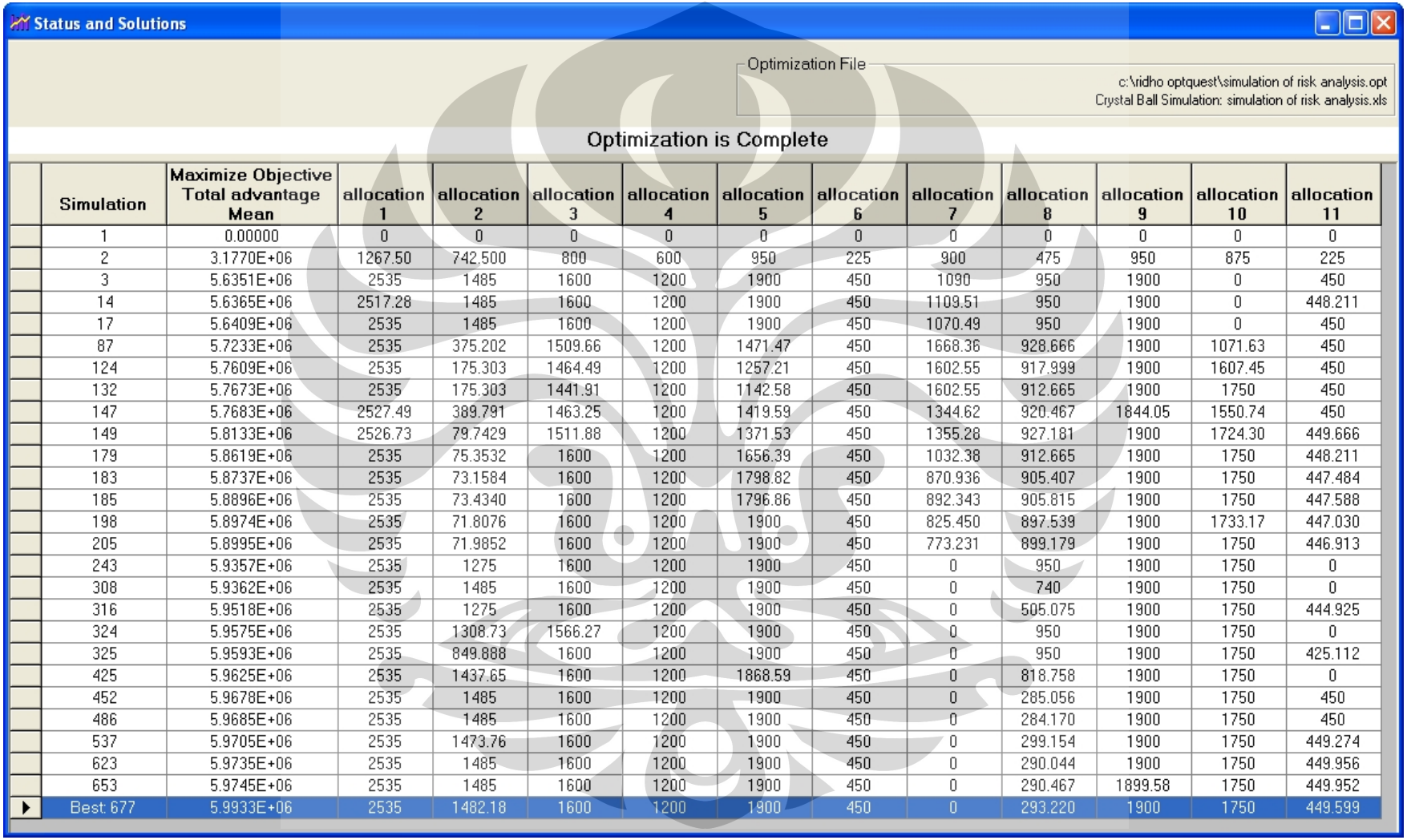
4.1.4 Simulasi Analisis Risiko

Total dari ke-11 point rencana penanganan risiko *(treatment cost)* yang disusunan berdasarkan estimasi biaya yang diusulkan adalah sebesar Rp. 16.020.000.000,-. Rencana penanganan risiko ini disusun guna meng-*cover* potensi kerugian/ risiko *(risk cost)* yang mungkin terjadi berdasarkan analisa risiko sebelumnya.

Mengingat *constraint* pada optimasi alokasi biaya nantinya adalah (*treatment cost allocation* $\leq$ *budget*), dimana budget adalah rencana anggaran ID-SIRTII tahun 2009 yang meliputi rencana anggaran terkait SDM, rencana anggaran terkait lab simulasi, penelitian dan pengembangan, rencana anggaran terkait jaringan dan sewa *bandwidth*, dan rencana anggaran terkait perawatan, atau senilai total $\approx$ Rp.13.560.000.000,-, maka dengan OptQuest pada Crystal Ball akan di *trial* besaran alokasi dana sesuai dengan kondisi *constraint* yang ada.

Variabel keputusan pada OptQuest adalah besar alokasi dana yang dialokasikan untuk *treatment* setiap poin risiko yang ada, dengan mempertimbangkan variabel tujuan yaitu memaksimalkan *advantage* yang diperoleh dengan mengalokasikan dana untuk setiap risiko yang ada.

Simulasi MonteCarlo berupa *forecast* akan berjalan pada *range* "potensi kerugian" *(risk cost)* di setiap poin risiko yang ada, sementara optimasi OptQuest berjalan guna mendapatkan alokasi dana yang sesuai untuk setiap poin risiko yang ada dengan tujuan memaksimalkan *advantage*. Dimana *advantage* didapat dari besarnya *risk coverage* setelah dikurangi *treatment cost allocation*, dan *risk coverage* itu sendiri adalah besarnya risiko yang ter-*cover* setelah dilakukan *risk treatment*, atau selisih nilai risiko sebelum dan sesudah dilakukan *risk treatment*.



Status and Solutions

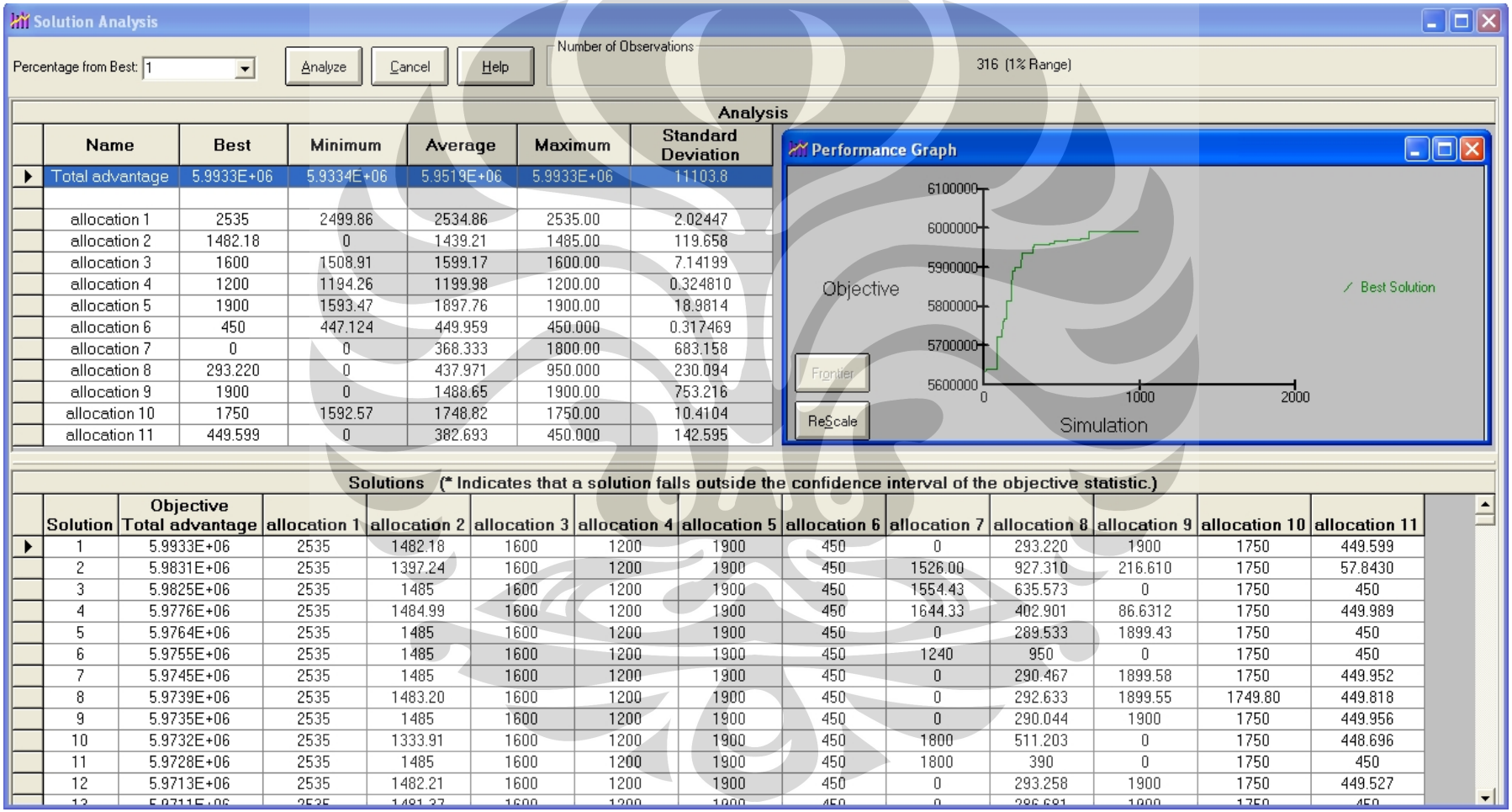
Optimization File

c:\ridho optquest\simulation of risk analysis.opt
Crystal Ball Simulation: simulation of risk analysis.xls

Optimization is Complete

Simulation	Maximize Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
1	0.00000	0	0	0	0	0	0	0	0	0	0	0
2	3.1770E+06	1267.50	742.500	800	600	950	225	900	475	950	875	225
3	5.6351E+06	2535	1485	1600	1200	1900	450	1090	950	1900	0	450
14	5.6365E+06	2517.28	1485	1600	1200	1900	450	1109.51	950	1900	0	448.211
17	5.6409E+06	2535	1485	1600	1200	1900	450	1070.49	950	1900	0	450
87	5.7233E+06	2535	375.202	1509.66	1200	1471.47	450	1668.36	928.666	1900	1071.63	450
124	5.7609E+06	2535	175.303	1464.49	1200	1257.21	450	1602.55	917.999	1900	1607.45	450
132	5.7673E+06	2535	175.303	1441.91	1200	1142.58	450	1602.55	912.665	1900	1750	450
147	5.7683E+06	2527.49	389.791	1463.25	1200	1419.59	450	1344.62	920.467	1844.05	1550.74	450
149	5.8133E+06	2526.73	79.7429	1511.88	1200	1371.53	450	1355.28	927.181	1900	1724.30	449.666
179	5.8619E+06	2535	75.3532	1600	1200	1656.39	450	1032.38	912.665	1900	1750	448.211
183	5.8737E+06	2535	73.1584	1600	1200	1798.82	450	870.936	905.407	1900	1750	447.484
185	5.8896E+06	2535	73.4340	1600	1200	1796.86	450	892.343	905.815	1900	1750	447.588
198	5.8974E+06	2535	71.8076	1600	1200	1900	450	825.450	897.539	1900	1733.17	447.030
205	5.8995E+06	2535	71.9852	1600	1200	1900	450	773.231	899.179	1900	1750	446.913
243	5.9357E+06	2535	1275	1600	1200	1900	450	0	950	1900	1750	0
308	5.9362E+06	2535	1485	1600	1200	1900	450	0	740	1900	1750	0
316	5.9518E+06	2535	1275	1600	1200	1900	450	0	505.075	1900	1750	444.925
324	5.9575E+06	2535	1308.73	1566.27	1200	1900	450	0	950	1900	1750	0
325	5.9593E+06	2535	849.888	1600	1200	1900	450	0	950	1900	1750	425.112
425	5.9625E+06	2535	1437.65	1600	1200	1868.59	450	0	818.758	1900	1750	0
452	5.9678E+06	2535	1485	1600	1200	1900	450	0	285.056	1900	1750	450
486	5.9685E+06	2535	1485	1600	1200	1900	450	0	284.170	1900	1750	450
537	5.9705E+06	2535	1473.76	1600	1200	1900	450	0	299.154	1900	1750	449.274
623	5.9735E+06	2535	1485	1600	1200	1900	450	0	290.044	1900	1750	449.956
653	5.9745E+06	2535	1485	1600	1200	1900	450	0	290.467	1899.58	1750	449.952
Best: 677	5.9933E+06	2535	1482.18	1600	1200	1900	450	0	293.220	1900	1750	449.599

Gambar 4.1 *Simulation Overview (Status and solution)*

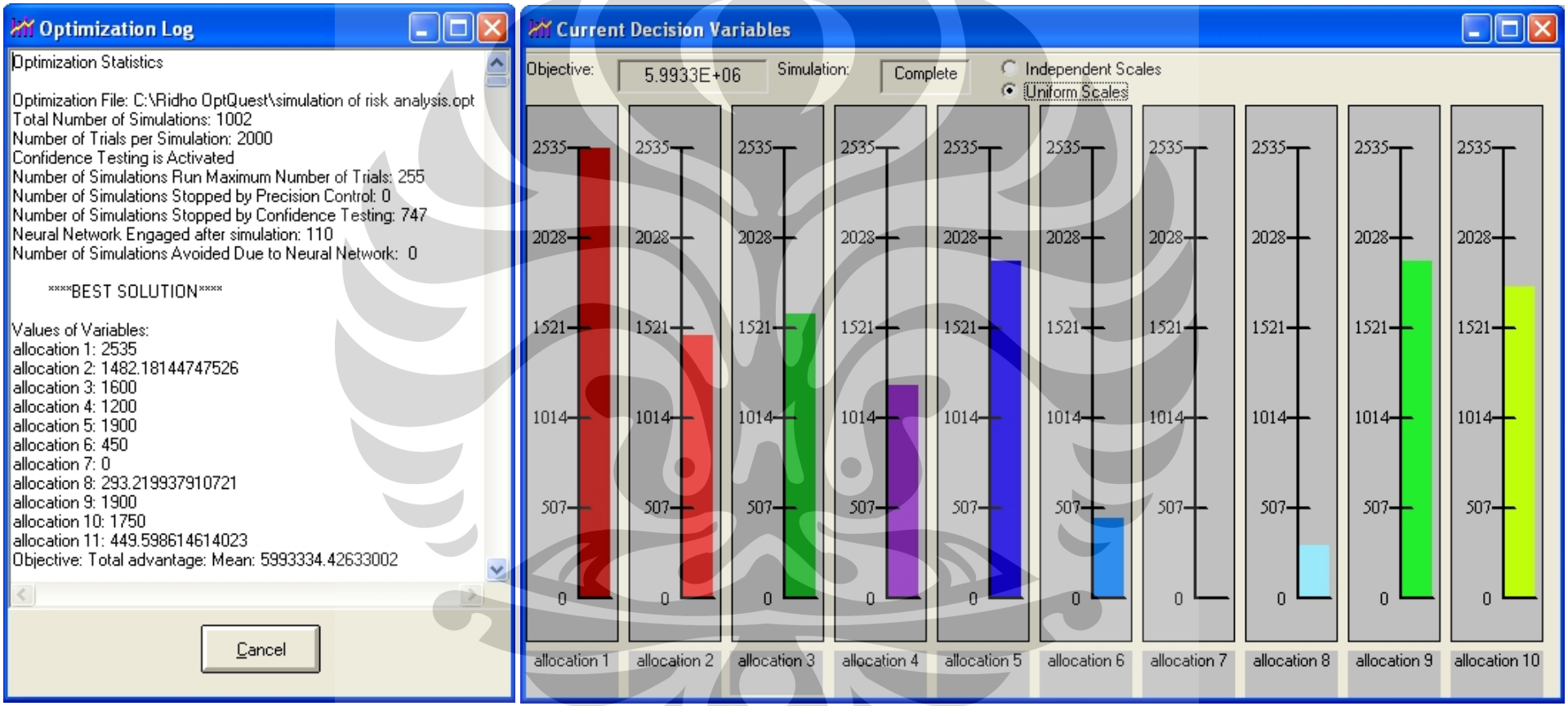


Name	Best	Minimum	Average	Maximum	Standard Deviation
Total advantage	5.9933E+06	5.9334E+06	5.9519E+06	5.9933E+06	11103.8
allocation 1	2535	2499.86	2534.86	2535.00	2.02447
allocation 2	1482.18	0	1439.21	1485.00	119.658
allocation 3	1600	1508.91	1599.17	1600.00	7.14199
allocation 4	1200	1194.26	1199.98	1200.00	0.324810
allocation 5	1900	1593.47	1897.76	1900.00	18.9814
allocation 6	450	447.124	449.959	450.000	0.317469
allocation 7	0	0	368.333	1800.00	683.158
allocation 8	293.220	0	437.971	950.000	230.094
allocation 9	1900	0	1488.65	1900.00	753.216
allocation 10	1750	1592.57	1748.82	1750.00	10.4104
allocation 11	449.599	0	382.693	450.000	142.595

Solutions (* Indicates that a solution falls outside the confidence interval of the objective statistic.)

Solution	Objective Total advantage	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
1	5.9933E+06	2535	1482.18	1600	1200	1900	450	0	293.220	1900	1750	449.599
2	5.9831E+06	2535	1397.24	1600	1200	1900	450	1526.00	927.310	216.610	1750	57.8430
3	5.9825E+06	2535	1485	1600	1200	1900	450	1554.43	635.573	0	1750	450
4	5.9776E+06	2535	1484.99	1600	1200	1900	450	1644.33	402.901	86.6312	1750	449.989
5	5.9764E+06	2535	1485	1600	1200	1900	450	0	289.533	1899.43	1750	450
6	5.9755E+06	2535	1485	1600	1200	1900	450	1240	950	0	1750	450
7	5.9745E+06	2535	1485	1600	1200	1900	450	0	290.467	1899.58	1750	449.952
8	5.9739E+06	2535	1483.20	1600	1200	1900	450	0	292.633	1899.55	1749.80	449.818
9	5.9735E+06	2535	1485	1600	1200	1900	450	0	290.044	1900	1750	449.956
10	5.9732E+06	2535	1333.91	1600	1200	1900	450	1800	511.203	0	1750	448.696
11	5.9728E+06	2535	1485	1600	1200	1900	450	1800	390	0	1750	450
12	5.9713E+06	2535	1482.21	1600	1200	1900	450	0	293.258	1900	1750	449.527

Gambar 4.2 *Simulation Overview (Solution analysis and performance graph)*



Gambar 4.3 *Simulation Overview (Optimization log and current decision variables)*

Tabel 4.3 *Worksheet Overview* (total ***advantage,*** ekstrim maksimum *risk cost*)

(dalam juta rupiah)		A	B	C	D	E	F	G	H	I
					C / F x 100%			D x B		H x (G – C)
No	**Deskripsi risiko**	**treatment cost**	**risk cost**	**treatment cost allocation**	**% allocation**	**lower bond**	**upper bond**	**risk coverage**	**decision**	**advantage**
1	1. Risiko terkait Keamanan jaringan internet yang kurang	2.535,00	2.628.000,00	2.535,00	100,00%	0	2.535,00	2.628.000,00	1	2.625.465,00
2	2. Risiko terkait Respon monitoring pada 5W (incidents & responsibility) + 1H (action) tidak tertangani dengan baik	1.485,00	394.200,00	1.482,18	99,81%	0	1.485,00	393.451,42	1	391.969,24
3	3. Risiko terkait Monitoring terganggu (traffic moment yang hilang/ tdk termonitor)	1.600,00	788.400,00	1.600,00	100,00%	0	1.600,00	788.400,00	1	786.800,00
4	4. Risiko terkait Gangguan pada 9 sensor yang sudah terpasang	1.200,00	1.576.800,00	1.200,00	100,00%	0	1.200,00	1.576.800,00	1	1.575.600,00
5	5. Risiko terkait Aktifitas monitoring tidak tertangani dengan baik	1.900,00	788.400,00	1.900,00	100,00%	0	1.900,00	788.400,00	1	786.500,00
6	6. Risiko terkait Pengumpulan log file tidak maksimal	450,00	438.000,00	450,00	100,00%	0	450,00	438.000,00	1	437.550,00
7	7. Risiko terkait Pemanfaatan content log file tidak maksimal	1.800,00	394.200,00	-	0,00%	0	1.800,00	-	0	-
8	8. Risiko Beban jaringan yg tinggi saat mengirim log file dengan kapasitas file yang besar secara online	950,00	197.100,00	293,22	30,87%	0	950,00	60.835,43	1	60.542,21
9	9. Risiko terkait Effort yg besar menggagalkan pengiriman log file secara off-line	1.900,00	394.200,00	1.900,00	100,00%	0	1.900,00	394.200,00	1	392.300,00
10	10. Risiko terkait Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP	1.750,00	788.400,00	1.750,00	100,00%	0	1.750,00	788.400,00	1	786.650,00
11	11. Risiko terkait Laporan gangguan tidak tertangani dengan baik	450,00	98.550,00	449,60	99,91%	0	450,00	98.462,18	1	98.012,58
								Total advantage		**7.941.389,03**

Total budget	**13.560,00**
Total treatment cost allocation	**13.560,00**
Surplus	**0,00**

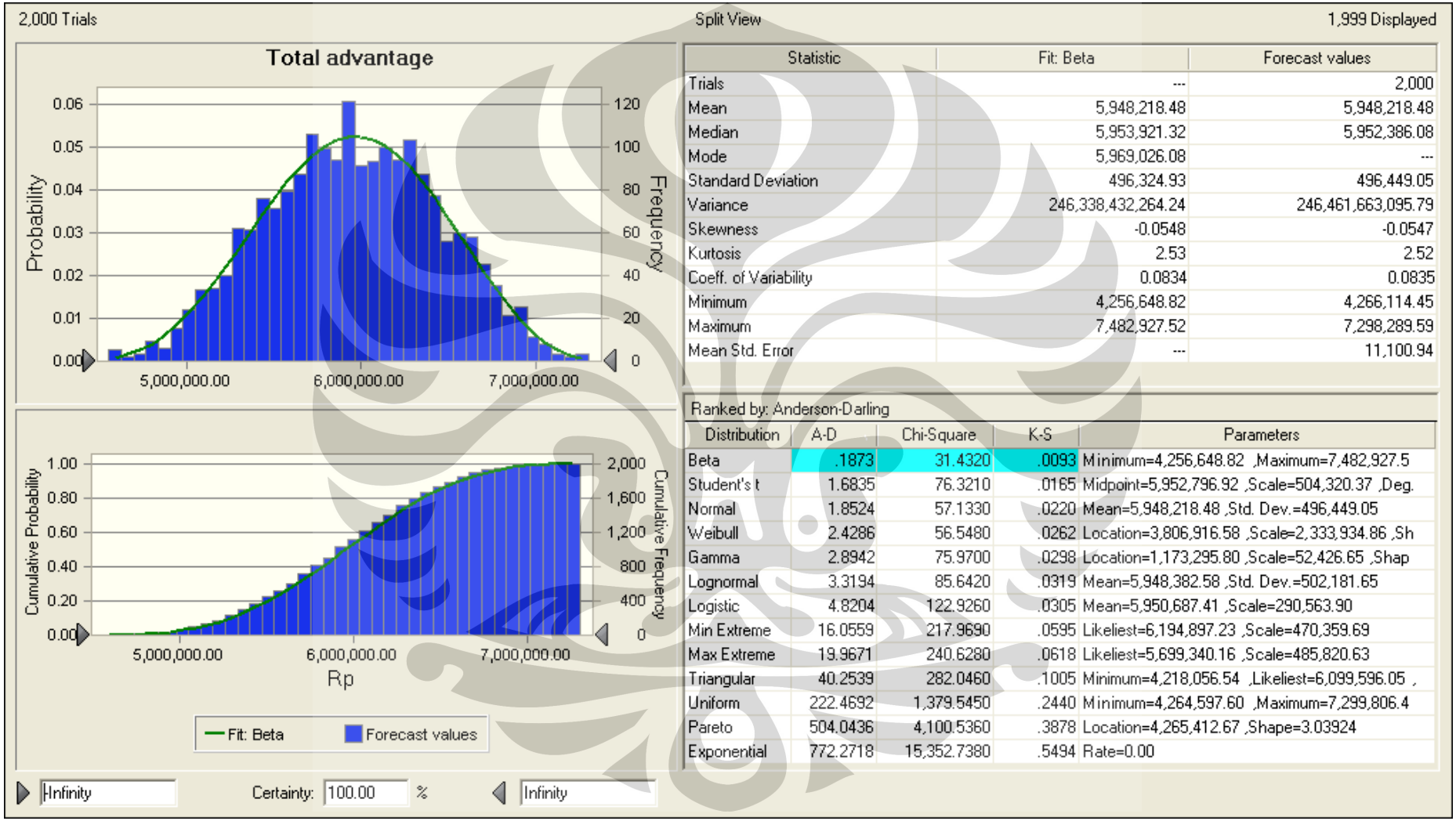
TOTAL ADVANTAGE MAKSIMUM (EKSTRIM) **7.941.389,03**

Tabel 4.4 *Worksheet Overview* (total ***advantage,*** ekstrim minimum *risk cost*)

(dalam juta rupiah)		A	B	C	D	E	F	G	H	I
					C / F x 100%			D x B		H x (G – C)
No	**Deskripsi risiko**	**treatment cost**	**risk cost**	**treatment cost allocation**	**% allocation**	**lower bond**	**upper bond**	**risk coverage**	**decision**	**advantage**
1	1. Risiko terkait Keamanan jaringan internet yang kurang	2.535,00	1.314.000,00	2.535,00	100,00%	0	2.535,00	1.314.000,00	1	1.311.465,00
2	2. Risiko terkait Respon monitoring pada 5W (incidents & responsibility) + 1H (action) tidak tertangani dengan baik	1.485,00	197.100,00	1.482,18	99,81%	0	1.485,00	196.725,71	1	195.243,53
3	3. Risiko terkait Monitoring terganggu (traffic moment yang hilang/ tdk termonitor)	1.600,00	394.200,00	1.600,00	100,00%	0	1.600,00	394.200,00	1	392.600,00
4	4. Risiko terkait Gangguan pada 9 sensor yang sudah terpasang	1.200,00	788.400,00	1.200,00	100,00%	0	1.200,00	788.400,00	1	787.200,00
5	5. Risiko terkait Aktifitas monitoring tidak tertangani dengan baik	1.900,00	394.200,00	1.900,00	100,00%	0	1.900,00	394.200,00	1	392.300,00
6	6. Risiko terkait Pengumpulan log file tidak maksimal	450,00	219.000,00	450,00	100,00%	0	450,00	219.000,00	1	218.550,00
7	7. Risiko terkait Pemanfaatan content log file tidak maksimal	1.800,00	197.100,00	-	0,00%	0	1.800,00	-	0	-
8	8. Risiko Beban jaringan yg tinggi saat mengirim log file dengan kapasitas file yang besar secara online	950,00	98.550,00	293,22	30,87%	0	950,00	30.417,72	1	30.124,50
9	9. Risiko terkait Effort yg besar menggagalkan pengiriman log file secara off-line	1.900,00	197.100,00	1.900,00	100,00%	0	1.900,00	197.100,00	1	195.200,00
10	10. Risiko terkait Pemasangan perangkat sensor membebani kinerja dan utilisasi ISP	1.750,00	394.200,00	1.750,00	100,00%	0	1.750,00	394.200,00	1	392.450,00
11	11. Risiko terkait Laporan gangguan tidak tertangani dengan baik	450,00	49.275,00	449,60	99,91%	0	450,00	49.231,09	1	48.781,49
								Total advantage		**3.963.914,52**

Total budget	**13.560,00**
Total treatment cost allocation	**13.560,00**
Surplus	**0,00**

TOTAL ADVANTAGE MINIMUM (EKSTRIM) **3.963.914,52**

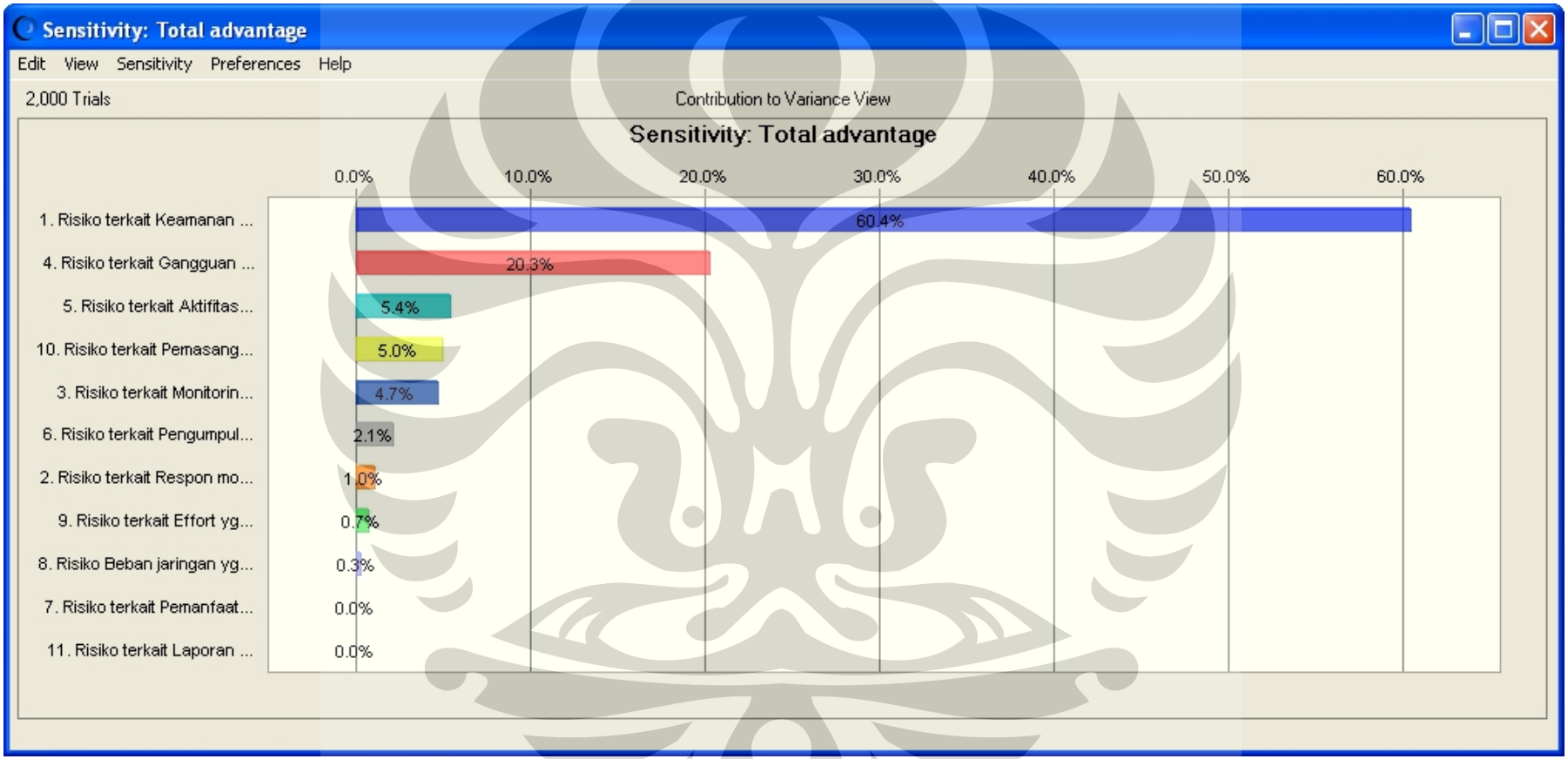


Statistic	Fit: Beta	Forecast values
Trials	---	2,000
Mean	5,948,218.48	5,948,218.48
Median	5,953,921.32	5,952,386.08
Mode	5,969,026.08	---
Standard Deviation	496,324.93	496,449.05
Variance	246,338,432,264.24	246,461,663,095.79
Skewness	-0.0548	-0.0547
Kurtosis	2.53	2.52
Coeff. of Variability	0.0834	0.0835
Minimum	4,256,648.82	4,266,114.45
Maximum	7,482,927.52	7,298,289.59
Mean Std. Error	---	11,100.94

Ranked by: Anderson-Darling

Distribution	A-D	Chi-Square	K-S	Parameters
Beta	.1873	31.4320	.0093	Minimum=4,256,648.82 ,Maximum=7,482,927.5
Student's t	1.6835	76.3210	.0165	Midpoint=5,952,796.92 ,Scale=504,320.37 ,Deg.
Normal	1.8524	57.1330	.0220	Mean=5,948,218.48 ,Std. Dev.=496,449.05
Weibull	2.4286	56.5480	.0262	Location=3,806,916.58 ,Scale=2,333,934.86 ,Sh
Gamma	2.8942	75.9700	.0298	Location=1,173,295.80 ,Scale=52,426.65 ,Shap
Lognormal	3.3194	85.6420	.0319	Mean=5,948,382.58 ,Std. Dev.=502,181.65
Logistic	4.8204	122.9260	.0305	Mean=5,950,687.41 ,Scale=290,563.90
Min Extreme	16.0559	217.9690	.0595	Likeliest=6,194,897.23 ,Scale=470,359.69
Max Extreme	19.9671	240.6280	.0618	Likeliest=5,699,340.16 ,Scale=485,820.63
Triangular	40.2539	282.0460	.1005	Minimum=4,218,056.54 ,Likeliest=6,099,596.05 ,
Uniform	222.4692	1,379.5450	.2440	Minimum=4,264,597.60 ,Maximum=7,299,806.4
Pareto	504.0436	4,100.5360	.3878	Location=4,265,412.67 ,Shape=3.03924
Exponential	772.2718	15,352.7380	.5494	Rate=0.00

Gambar 4.4 *Simulation Overview (Probability and forecast values)*



Gambar 4.5 Sensitivitas *(Forecast of Total Advantage)*

Dari hasil simulasi peramalan dan optimasi pengalokasian dana terhadap alternatif *risk treatment* yang dilakukan, maka didapat sensitivitas dari pengalokasian dananya. Prioritas alternatif *risk treatment* guna meng-*cover* dan memperkecil nilai risiko yang ada dan memaksimalkan nilai *advantage* adalah seperti yang ditunjukan pada table dibawah ini.

Tabel 4.5 Prioritas Alternatif *Risk Treatment*

No.	*Risk ID*	Alternatif *Risk Treatment*	Sensitivitas *Total Advantage*	*Treatment Allocation*
1.	R1	*Device and infrastructure improvement*	60,4 %	Rp. 2.535.000.000,-
2.	R4	*Capacity & utilization Improvement* pada *device* sensor *(ISP)*	20,3 %	Rp. 1.200.000.000,-
3.	R5	Pelatihan, *workshop, simulasi*, & *knowledge shearing*	5,4 %	Rp. 1.900.000.000,-
4.	R10	Penelitian dan pengembangan terkait *utilisasi* perangkat sensor yang terpasang pada ISP	5,0 %	Rp. 1.750.000.000,-
5.	R3	*Maintenance & Improvement* pada *monitoring device (Office)*	4,7 %	Rp. 1.600.000.000,-
6.	R6	*Device maintenance regularly*	2,1 %	Rp. 450.000.000,-
7.	R2	Penyempurnaan regulasi, sosialisasi SOP pengamanan informasi, *Quality System*	1,0 %	Rp. 1.482.000.000,-
8.	R9	*SDM management*	0,7 %	Rp. 1.900.000.000,-
9.	R8	Penyempurnaan standar teknis, Penelitian dan pengembangan terkait penanganan beban log file	0,3 %	Rp. 293.220.000,-
10.	R11	*CRM Implementation*	0,0 %	Rp. 449.600.000,-
11.	R7	Regulasi dan standar pengamanan *Improvement*	0,0 %	Rp. 0,-
Total treatment allocation (total budget)				**Rp. 13.560.000.000,-**

Hasil akhir, didapatlah alternatif *risk treatment* dan model simulasi peramalan serta optimasi alokasi biaya dari alternatif *risk treatment* yang ada, berdasarkan analisis risiko dan proses penilaian *(FRAAP)* terhadap proses bisnis yang terkait dengan *Information Security on Internet Infrastructure.*

BAB V
KESIMPULAN

- Dari hasil proses FRAAP *(Facilitated Risk Analysis and Assessment Process)*, terdapat 11 poin risiko yang memerlukan pengendalian risiko *(Control/ Mitigation)* dan telah didapat 11 alternatif *risk treatment* guna pengendalian risiko, dengan prioritas *treatmet* utama adalah *"device and infrastructure improvement"*, kedua *"capacity & utilization improvement* pada *device sensor (ISP)"*, ketiga "pelatihan, *workshop*, simulasi & *knowledge shearing*. (atau lebih lengkap pada, Tabel 4.5)
- Deskripsi model simulasi peramalan adalah sebagai berikut;
  Total alternatif *risk treatment cost* yang disusunan berdasarkan estimasi usulan biaya adalah sebesar Rp. 16.020.000.000,- guna meng-*cover* potensi kerugian/ risiko *(risk cost)* yang mungkin terjadi berdasarkan analisa risiko.
  Mengingat *constraint* pada simulasi optimasi alokasi biaya adalah *treatment cost allocation* $\leq$ *budget*, dimana budget adalah rencana anggaran senilai $\approx$ Rp.13.560.000.000,-, maka dengan software optimasi diperoleh model allokasi biaya dengan perkiraan perolehan rata-rata total keuntungan Rp. 5.993.300.000.000,- (*total advantage mean*, gambar 4.1) pada iterasi ke 667 dari 1002 simulasi yang dilakukan.
- Model *forecast simulation* yang dilakukan sebanyak 2000 trials dengan memasukan alokasi dana hasil optimasi, menunjukan nilai *forecast value* terhadap *advantage*, minimum Rp. 4.256.648.820.000,- dan maksimum *advantage* Rp. 7.482.927.500.000,- (nilai max dan min, Fit: Beta, Gambar 4.4), dengan rata-rata nilai *advantage* sebesar Rp. 5.948.218.480.000,-

DAFTAR REFERENSI

Albert, Chris., et al. (2004). *Defining Incident Management Process for CSIRTs.(CMU/SEI-2004-TR-015). Carnegie Mellon® Software Engineering Institute (SEI^{SM})*

Bojanc, Rok. and Jerman-Blazic, Borka. (2008). *"An economic modeling approach to information security risk management."* dalam *International Journal of Information Management 28 (2008) 413-422.* Science Direct, Elsevier

Crystal Ball® 7.2.2 User Manual

Charnes, Jhon. (2007). *Financial Modeling with Crystal Ball and Excel*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Draft Federal Information Processing Standards Publication 183. *Integration Definition for Function Modelling (IDEF0)*. 1993

Frame, J Davidson. (2003). *Managing Risk in Organization – A Guide for Managers.* Jossey-Bass

http://www.cert.org/octave/

http://www.idef.com

Hu, Qing. Hart, Paul. and Cooke, Donna. (2007). *"The role of external and internal influences on information systems security – a neo-institutional perspective."* dalam *Journal of Strategic Information Systems 16 (2007) 153–172.* Science Direct, Elsevier

ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*. 2005, Geneva

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management system – Requirements. AG meeting, 29-30 November* 2005, Geneva

Kerzner, Harold. (2005). *Project Management – Ninth Edition*. John Wiley.

Merrit, James W. *Risk management*. (1998). Wang Global (703) 827-3534, from NIST

NIST (2002). *Risk management guide for information technology systems*. National Institute of Standards and Technology (NIST) Special Publication 800-30

OptQuest ® 2.3 User Manual

Peltier, Thomas R. (2005). *Information Security Risk Analysis, second edition*. New York: Auerbach Publications, Taylor & Francis Group

Peraturan Direktur Jendral Pos dan Telekomunikasi No. 226/DIRJEN/2007

Peraturan Mentri Komunikasi dan Informatika RI, No 26/PER/M.KOMINFO/5/2007

LAMPIRAN 1

DATA RESPONDEN DAN VERIFIKASI DATA PENELITIAN

Lampiran 1: Data Responden dan Verifikasi Data Penelitian

Departement Teknik Industri

Fakultas Teknik Industri

DATA RESPONDEN DAN VERIFIKASI DATA PENELITIAN

Simulasi Analisis Risiko dan Penilaian Proses Bisnis

Terkait Pengamanan Informasi pada Infrastruktur Internet

"Simulation of Risk Analysis and Business Process Assessment

Related to Information Security on Internet Infrastructure"

NO	NAMA	JABATAN	TANDA TANGAN
1.	Wayan Toni S	Kasi Operasi Akses Protokol Internet	
2.	Dwi Ely P	Staf operasi API, Ditjen Postel	
3.	Oki S	Staf Operasi API, Ditjen Postel	
4	HADI PURNOMO	Staf operasi API, Ditjen Postel	
5	MIZAMIL	MANAJER Bidang Hubungan Antar Lembaga	
6.	IGN MANTRA	Manager operasi dan keamanan	
7.	Fandy Ardiyan	staff operasi dan keamanan	
8.	Nanda. L. Prasojo	Staf Database, Aplikasi dan Data Center	
9	Utama Andri A	Staff. operasional & keamanan	
10.	Tita Latifah.	Staf Database, Aplikasi & DC	

Atas segala bantuan dan semangat yang diberikan selama penelitian ini, saya mengucapkan banyak terimakasih. Semoga hasil penelitian dan penulisan tugas akhir ini berguna dan bermanfaat bagi semua pihak, baik itu kalangan akademis, praktisi ataupun instansi lain yang terkait.

Depok, 30 November 2008

30/11-'08

Ridho Zamzam

LAMPIRAN 2

SOLUTION ANALYSIS

(dalam juta rupiah)

Name	Best	Minimum	Average	Maximum	Standard Deviation
Total advantage	5,9933E+06	5,9334E+06	5,9519E+06	5,9933E+06	11103,8
allocation 1	2535	2499,86	2534,86	2535	2,02447
allocation 2	1482,18	0	1439,21	1485	119,658
allocation 3	1600	1508,91	1599,17	1600	7,14199
allocation 4	1200	1194,26	1199,98	1200	0,32481
allocation 5	1900	1593,47	1897,76	1900	18,9814
allocation 6	450	447,124	449,959	450	0,317469
allocation 7	0	0	368,333	1800	683,158
allocation 8	293,22	0	437,971	950	230,094
allocation 9	1900	0	1488,65	1900	753,216
allocation 10	1750	1592,57	1748,82	1750	10,4104
allocation 11	449,599	0	382,693	450	142,595

Solution Analysis

Number of Observation; 316 (1% range) from best

(dalam juta rupiah)

solution (* indicates that a solution falls outside the confidence interval of the objective statistic												
Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
1	5,9933E+06	2535	1482,18	1600	1200	1900	450	0	293,22	1900	1750	449,599
2	5,9831E+06	2535	1397,24	1600	1200	1900	450	1526	927,31	216,61	1750	57,843
3	5,9825E+06	2535	1485	1600	1200	1900	450	1554,43	635,573	0	1750	450
4	5,9776E+06	2535	1484,99	1600	1200	1900	450	1644,33	402,901	86,6312	1750	449,989
5	5,9764E+06	2535	1485	1600	1200	1900	450	0	289,533	1899,43	1750	450
6	5,9755E+06	2535	1485	1600	1200	1900	450	1240	950	0	1750	450
7	5,9745E+06	2535	1485	1600	1200	1900	450	0	290,467	1899,58	1750	449,952
8	5,9739E+06	2535	1483,2	1600	1200	1900	450	0	292,633	1899,55	1749,8	449,818
9	5,9735E+06	2535	1485	1600	1200	1900	450	0	290,044	1900	1750	449,956
10	5,9732E+06	2535	1333,91	1600	1200	1900	450	1800	511,203	0	1750	448,696
11	5,9728E+06	2535	1485	1600	1200	1900	450	1800	390	0	1750	450
12	5,9713E+06	2535	1482,21	1600	1200	1900	450	0	293,258	1900	1750	449,527
13	5,9711E+06	2535	1481,37	1600	1200	1900	450	0	286,681	1900	1750	450
14	5,9711E+06	2535	1478,09	1600	1200	1900	450	0	298,771	1899,47	1749,24	449,437
15	5,9707E+06	2535	1482,44	1600	1200	1900	450	0	293,182	1899,97	1749,96	449,453
16	5,9707E+06	2535	1485	1600	1200	1900	450	0	290,104	1899,94	1750	449,956
17	5,9706E+06	2534,89	1485	1600	1200	1900	450	0	290,392	1900	1750	449,72
18	5,9705E+06	2535	1473,76	1600	1200	1900	450	0	299,154	1900	1750	449,274
19	5,9703E+06	2535	1482,52	1600	1200	1900	450	0	291,942	1900	1750	449,667
20	5,9702E+06	2535	1484,96	1600	1200	1900	450	1800	0	390,092	1750	449,949

		solution (* indicates that a solution falls outside the confidence interval of the objective statistic										
Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
21	5,9701E+06	2535	1462,22	1600	1200	1900	450	0	311,67	1899,8	1750	448,786
22	5,9700E+06	2535	1483,65	1600	1200	1900	450	0	292,092	1899,56	1749,85	449,851
23	5,9693E+06	2535	1485	1600	1200	1900	450	1690	950	0	1750	0
24	5,9688E+06	2535	1379,46	1600	1200	1900	450	1419,68	878,939	0	1750	446,92
25	5,9685E+06	2535	1485	1600	1200	1900	450	0	284,17	1900	1750	450
26	5,9681E+06	2535	1458,88	1600	1200	1900	450	0	317,81	1900	1750	448,312
27	5,9678E+06	2535	1485	1600	1200	1900	450	0	285,056	1900	1750	450
28	5,9677E+06	2535	1482,58	1600	1200	1900	450	0	292,827	1899,94	1750	449,649
29	5,9676E+06	2535	1484,98	1600	1200	1900	450	0	296,418	1894,87	1749,22	449,512
30	5,9672E+06	2535	1484,14	1600	1200	1900	450	0	285,719	1900	1750	450
31	5,9669E+06	2535	1484,73	1600	1200	1900	450	0	296,816	1899,36	1750	440,282
32	5,9669E+06	2535	1441,2	1600	1200	1900	450	1700,93	416,575	82,4489	1750	449,913
33	5,9666E+06	2535	1456,43	1600	1200	1900	450	1248,2	916,329	0	1750	448,862
34	5,9666E+06	2535	1483,36	1600	1200	1900	450	1727,28	451,33	0	1750	449,941
35	5,9666E+06	2535	1469,26	1600	1200	1900	450	0	291,016	1900	1750	450
36	5,9665E+06	2535	1476	1600	1200	1900	450	0	298,179	1900	1750	449,342
37	5,9663E+06	2535	1462,62	1600	1200	1900	450	0	305,735	1900	1750	448,895
38	5,9658E+06	2535	1485	1600	1200	1900	450	0	287,922	1900	1750	450
39	5,9656E+06	2535	1437,13	1600	1200	1900	450	1719,94	867,806	0	1712,61	137,509
40	5,9652E+06	2535	1484,47	1600	1200	1900	450	0	299,006	1891,81	1750	449,716
41	5,9647E+06	2535	1482,23	1600	1200	1900	450	0	293,172	1900	1750	449,594
42	5,9646E+06	2535	1387,39	1600	1200	1900	450	1800	432,183	0	1750	449,795
43	5,9643E+06	2535	1385,5	1600	1200	1900	450	0	402,879	1898,67	1750	437,945
44	5,9642E+06	2535	1471,52	1600	1200	1900	450	0	300,129	1900	1750	449,205
45	5,9641E+06	2535	1484,77	1600	1200	1900	450	0	292,118	1898,4	1750	449,71

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
46	5,9641E+06	2535	1485	1600	1200	1900	450	0	795,716	1844,28	1750	0
47	5,9635E+06	2535	1216,61	1600	1200	1900	450	1800	671,041	0	1750	437,345
48	5,9635E+06	2535	1357,62	1600	1200	1900	450	0	404,502	1898,38	1750	435,926
49	5,9632E+06	2535	1375	1600	1200	1900	450	1800	950	0	1750	0
50	5,9630E+06	2535	1332,02	1600	1200	1900	450	0	404,536	1900	1750	446,923
51	5,9630E+06	2535	1483,64	1600	1200	1900	450	1713,02	443,005	14,8913	1750	449,949
52	5,9629E+06	2535	1485	1600	1200	1900	450	0	335,494	1854,51	1750	450
53*	5,9627E+06	2535	1413,73	1600	1200	1900	450	819,363	355,595	1362,41	1750	173,903
54*	5,9626E+06	2535	1485	1600	1200	1900	450	1800	840	0	1750	0
55	5,9625E+06	2535	1437,65	1600	1200	1868,59	450	0	818,758	1900	1750	0
56*	5,9621E+06	2535	1482,66	1600	1200	1900	450	178,386	341,29	1832,77	1750	289,894
57	5,9620E+06	2535	1483,95	1600	1200	1900	450	1270,17	874,961	12,211	1750	449,843
58	5,9619E+06	2535	1481,18	1600	1200	1900	450	0	296,797	1897,84	1750	449,191
59*	5,9618E+06	2534,98	1479,64	1600	1200	1900	450	0	295,069	1899,52	1749,43	449,484
60	5,9616E+06	2535	1446,9	1600	1200	1900	450	0	425,56	1858,02	1750	394,524
61*	5,9615E+06	2535	1477,47	1600	1200	1900	450	0	299,757	1899,46	1748,89	449,424
62*	5,9615E+06	2535	1484,99	1600	1200	1900	450	1644,33	402,886	86,6274	1750	450
63	5,9613E+06	2535	1481,33	1600	1200	1900	450	0	294,239	1900	1750	449,432
64	5,9613E+06	2535	1451,1	1600	1200	1900	450	1661,77	532,358	55,7174	1750	424,057
65*	5,9613E+06	2535	1482,97	1600	1200	1900	450	0	292,85	1899,98	1750	449,206
66*	5,9612E+06	2535	1444,85	1600	1200	1900	450	0	332,641	1899,65	1750	447,861
67	5,9611E+06	2535	1483,35	1600	1200	1900	450	0	325,602	1890,2	1750	424,155
68	5,9610E+06	2535	1474,55	1600	1200	1900	450	0	297,242	1900	1750	449,324
69	5,9610E+06	2535	1483,2	1600	1200	1900	448,913	0	293,526	1899,92	1750	449,441
70	5,9610E+06	2535	1435,02	1600	1200	1900	450	1800	418,598	0	1750	450

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
71	5,9608E+06	2535	1465,21	1600	1200	1900	450	0	459,527	1854,51	1750	345,757
72	5,9607E+06	2535	1469,61	1600	1200	1900	450	0	306,548	1900	1750	448,844
73*	5,9607E+06	2535	1482,18	1600	1200	1900	450	1601,76	553,809	37,6547	1750	449,599
74*	5,9605E+06	2535	1483,88	1600	1200	1900	450	0	291,815	1899,56	1749,88	449,868
75*	5,9605E+06	2535	1272,05	1600	1200	1900	450	483,797	313,159	1606,28	1750	449,714
76	5,9605E+06	2535	1485	1600	1200	1900	450	0	281,876	1900	1750	450
77	5,9602E+06	2535	1485	1600	1200	1900	450	0	289,035	1900	1750	449,958
78	5,9601E+06	2535	1485	1600	1200	1900	450	0	290,668	1899,37	1750	449,961
79*	5,9600E+06	2535	1484,71	1600	1200	1900	450	1712,67	442,088	14,9512	1750	450
80	5,9600E+06	2535	1474,85	1600	1200	1900	450	0	293,659	1900	1750	448,064
81*	5,9599E+06	2535	1394,2	1600	1200	1900	450	1580,61	950	156,371	1750	43,8243
82	5,9596E+06	2535	1349,21	1600	1200	1900	450	1800	525,794	0	1750	450
83*	5,9596E+06	2535	1481,38	1600	1200	1900	450	0	288,281	1900	1750	449,965
84*	5,9596E+06	2535	1482,18	1600	1200	1900	450	1800	393,22	0	1750	449,599
85*	5,9596E+06	2535	1426,2	1600	1200	1900	450	1586,16	934,597	116,096	1750	32,1468
86	5,9596E+06	2535	1485	1600	1200	1900	450	0	290,824	1899,18	1750	450
87	5,9595E+06	2535	1453,24	1600	1200	1900	450	0	319,757	1900	1750	448,011
88	5,9595E+06	2535	1485	1600	1200	1900	450	0	279,121	1900	1750	450
89	5,9595E+06	2535	1482,53	1600	1200	1900	450	0	285,442	1900	1750	450
90*	5,9593E+06	2535	1484,18	1600	1200	1900	450	1800	835,66	0	1750	5,1588
91	5,9593E+06	2535	849,888	1600	1200	1900	450	0	950	1900	1750	425,112
92	5,9593E+06	2535	1477,8	1600	1200	1900	450	0	291,673	1900	1750	449,497
93*	5,9589E+06	2535	1485	1600	1200	1900	450	0	950	1690	1750	0
94	5,9589E+06	2535	1485	1600	1200	1900	450	1711,79	443,158	15,1018	1750	449,952
95	5,9586E+06	2535	1485	1600	1200	1900	450	0	290	1900	1750	450

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
96*	5,9586E+06	2535	1485	1600	1200	1900	450	0	290,386	1899,38	1750	450
97*	5,9582E+06	2535	1285,41	1600	1200	1900	450	1800	499,846	0	1750	450
98*	5,9581E+06	2535	1438,66	1600	1200	1900	450	1693,69	950	0	1750	0
99	5,9580E+06	2535	1485	1600	1200	1900	450	0	283,273	1899,4	1750	450
100	5,9580E+06	2535	1485	1600	1200	1900	450	0	287,757	1900	1750	450
101*	5,9578E+06	2535	1484,18	1600	1200	1900	450	0	290,069	1899,64	1750	449,833
102	5,9576E+06	2535	1485	1600	1200	1900	450	0	260,706	1900	1750	450
103	5,9575E+06	2535	1308,73	1566,27	1200	1900	450	0	950	1900	1750	0
104*	5,9574E+06	2535	1485	1600	1200	1900	450	0	287,441	1899,68	1750	450
105	5,9573E+06	2535	1480,25	1600	1200	1900	450	0	290,353	1900	1750	449,841
106	5,9571E+06	2535	1481,63	1600	1200	1900	450	0	287,924	1900	1750	449,917
107	5,9569E+06	2535	1394,21	1600	1200	1882,18	450	0	404,366	1900	1750	444,24
108	5,9564E+06	2535	1471,27	1600	1200	1900	450	0	303,756	1900	1750	448,693
109	5,9564E+06	2535	1484,94	1600	1200	1900	450	0	650,803	1539,28	1750	449,972
110	5,9562E+06	2535	1485	1600	1200	1900	450	0	283,13	1900	1750	450
111	5,9560E+06	2535	1485	1600	1200	1900	450	0	284,738	1900	1750	450
112	5,9559E+06	2535	1485	1600	1200	1900	450	0	285,025	1899,62	1750	440,384
113	5,9556E+06	2535	1485	1600	1200	1900	450	0	286,681	1900	1750	450
114*	5,9555E+06	2535	1482,11	1600	1200	1900	450	1641,92	551,377	0	1750	449,589
115	5,9555E+06	2535	1485	1600	1200	1900	450	0	282,584	1900	1750	450
116*	5,9554E+06	2535	1482,38	1600	1200	1900	450	0	293,048	1899,93	1750	449,642
117*	5,9553E+06	2535	1450,61	1600	1200	1900	450	1665,35	538,07	73,1573	1750	397,812
118	5,9553E+06	2535	1485	1600	1200	1900	450	0	284,261	1899,53	1750	450
119	5,9551E+06	2535	1470,74	1600	1200	1900	450	0	306,974	1900	1750	447,282
120	5,9550E+06	2535	1262,36	1600	1200	1900	450	0	533,036	1900	1750	429,604

Lampiran 2: *Solution Analysis* (lanjutan)

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
121	5,9550E+06	2535	1485	1600	1200	1900	450	0	281,865	1900	1750	450
122	5,9550E+06	2535	1480,81	1600	1200	1900	447,177	0	313,014	1886,72	1750	447,285
123*	5,9550E+06	2535	1482,88	1600	1200	1900	450	0	283,683	1900	1750	449,796
124*	5,9548E+06	2535	1485	1600	1200	1900	450	0	249,309	1900	1750	450
125	5,9547E+06	2535	1465,82	1600	1200	1900	450	0	320,933	1889,62	1750	448,624
126*	5,9546E+06	2535	925	1600	1200	1900	450	1800	950	0	1750	450
127*	5,9545E+06	2535	1484,02	1600	1200	1900	450	0	291,452	1899,73	1750	449,802
128*	5,9542E+06	2535	1480,42	1600	1200	1900	450	0	293,531	1899,87	1749,78	449,517
129	5,9542E+06	2535	1249,21	1600	1200	1900	450	0	502,925	1900	1750	449,261
130	5,9540E+06	2535	1443,61	1585,67	1200	1900	450	0	487,21	1900	1750	288,332
131	5,9538E+06	2535	1455,47	1600	1200	1900	450	0	314,123	1900	1750	449,456
132	5,9535E+06	2535	1485	1600	1200	1900	450	0	286,33	1900	1750	450
133*	5,9531E+06	2535	1365,93	1600	1200	1900	450	1800	510,928	0	1750	448,145
134	5,9531E+06	2499,86	1412,57	1600	1200	1900	450	1571,11	831,121	203,899	1750	141,44
135	5,9530E+06	2535	1485	1600	1200	1900	450	0	283,555	1900	1750	450
136*	5,9530E+06	2535	1485	1600	1200	1900	450	0	286,109	1900	1750	450
137	5,9530E+06	2535	1481,36	1600	1200	1900	450	0	286,21	1900	1750	449,649
138*	5,9529E+06	2535	1457,8	1600	1200	1900	450	360	625,801	1231,43	1750	449,977
139	5,9529E+06	2535	1389,93	1597,77	1200	1900	450	0	402,099	1898,6	1750	436,603
140*	5,9528E+06	2535	1448,76	1600	1200	1900	450	1447,84	950	278,398	1750	0
141	5,9526E+06	2535	1447,58	1600	1200	1900	450	0	327,149	1900	1750	449,888
142*	5,9525E+06	2535	1480,95	1600	1200	1900	447,124	0	297,432	1900	1750	449,494
143	5,9524E+06	2535	1453,78	1600	1200	1900	450	0	310,473	1900	1750	448,07
144	5,9524E+06	2526,85	1481,14	1600	1200	1900	450	0	386,04	1874,29	1750	391,687
145*	5,9524E+06	2535	1484,55	1600	1200	1900	450	0	287,509	1899,74	1750	450

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
146	5,9521E+06	2535	1481,56	1600	1200	1900	450	0	290,167	1900	1750	449,971
147	5,9520E+06	2535	1485	1600	1200	1900	450	0	276,1	1900	1750	450
148	5,9520E+06	2535	1479,21	1600	1200	1900	450	0	295,68	1900	1750	449,314
149	5,9518E+06	2535	1275	1600	1200	1900	450	0	505,075	1900	1750	444,925
150	5,9518E+06	2535	1485	1600	1200	1900	450	0	291,327	1898,67	1750	450
151	5,9518E+06	2535	1470,1	1600	1200	1900	450	0	292,035	1900	1750	449,687
152	5,9517E+06	2535	1412,99	1600	1200	1900	450	0	755,225	1900	1750	6,21987
153	5,9517E+06	2535	1472,1	1600	1200	1847,75	450	0	377,519	1890,19	1750	437,441
154	5,9517E+06	2535	1275	1600	1200	1900	450	0	917,238	1900	1750	0
155	5,9516E+06	2535	1484,65	1600	1200	1900	450	0	277,865	1899,37	1750	435,612
156	5,9513E+06	2535	1336,45	1581,09	1200	1900	450	0	629,96	1900	1750	217,334
157	5,9513E+06	2535	1485	1600	1200	1900	450	0	290,066	1900	1750	449,934
158*	5,9512E+06	2535	1484,58	1600	1200	1900	450	0	290,096	1899,44	1749,96	449,963
159*	5,9511E+06	2535	1483,42	1600	1200	1900	450	0	292,495	1899,45	1749,76	449,882
160*	5,9511E+06	2535	1485	1600	1200	1900	450	1800	0	390	1750	450
161	5,9509E+06	2535	1485	1600	1200	1900	450	0	279,392	1900	1750	450
162*	5,9508E+06	2535	1483,65	1600	1200	1900	450	1713,01	442,948	14,893	1750	450
163	5,9507E+06	2535	1449,06	1600	1200	1865,69	450	0	785,915	1900	1750	0
164*	5,9507E+06	2535	1423,65	1600	1200	1900	450	1709,99	422,352	69,323	1750	449,654
165*	5,9505E+06	2535	1485	1600	1200	1900	450	0	797,686	1454,03	1750	388,281
166*	5,9504E+06	2535	1484,1	1600	1200	1900	450	0	290,526	1900	1750	449,64
167	5,9504E+06	2535	1482,83	1600	1200	1900	450	0	320,355	1899,85	1723,1	448,863
168*	5,9502E+06	2535	1483,39	1600	1200	1900	450	1800	349,777	17,6296	1750	449,94
169	5,9501E+06	2535	1485	1600	1200	1900	450	0	273,837	1900	1750	450
170*	5,9500E+06	2535	1482,48	1600	1200	1900	450	0	378,981	1840,07	1723,72	449,755

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
171*	5,9498E+06	2535	1461,4	1600	1200	1900	450	0	763,599	1900	1750	0
172	5,9497E+06	2535	1475	1600	1200	1900	450	0	296,853	1900	1750	449,564
173	5,9496E+06	2535	1381,35	1600	1200	1900	447,26	0	412,149	1892,46	1750	441,787
174*	5,9496E+06	2535	1483,96	1600	1200	1900	450	0	292,534	1899,69	1748,95	449,862
175	5,9495E+06	2535	1479,67	1600	1199,82	1900	450	0	331,875	1864	1750	449,638
176*	5,9492E+06	2535	1485	1600	1199,35	1900	450	0	290,976	1900	1750	449,67
177	5,9492E+06	2535	1485	1600	1200	1900	450	0	284,315	1900	1750	450
178*	5,9491E+06	2535	1484,59	1600	1200	1900	450	0	284,443	1900	1750	450
179	5,9491E+06	2535	1385,29	1600	1200	1900	450	0	372,179	1900	1750	447,698
180*	5,9487E+06	2535	1471,29	1600	1200	1900	450	1701,14	843,718	0	1750	72,321
181	5,9487E+06	2535	1293,74	1600	1200	1900	450	0	950	1900	1731,26	0
182	5,9485E+06	2535	1484,94	1600	1200	1900	450	0	302,757	1898,99	1750	437,079
183	5,9485E+06	2535	1457,23	1600	1200	1900	450	0	430,433	1854,65	1750	382,687
184*	5,9485E+06	2535	1482,18	1600	1200	1900	450	0	289,533	1900	1750	449,599
185	5,9485E+06	2535	1485	1600	1200	1900	450	0	256,436	1900	1750	450
186	5,9484E+06	2535	1475,19	1600	1200	1900	450	0	293,504	1900	1750	448,507
187	5,9483E+06	2535	1485	1600	1200	1900	450	0	286,051	1900	1750	450
188	5,9482E+06	2535	1455,14	1600	1200	1895,41	450	0	431,868	1857,55	1750	385,044
189*	5,9482E+06	2535	0	1600	1200	1900	450	1800	0	1875	1750	450
190	5,9482E+06	2535	1471,71	1600	1200	1900	450	0	291,556	1900	1750	449,855
191	5,9481E+06	2535	1474,37	1600	1200	1900	450	0	294,945	1900	1750	449,474
192	5,9481E+06	2535	1485	1597,37	1200	1863,86	450	0	778,762	1900	1750	0
193	5,9481E+06	2535	1454,84	1600	1200	1900	450	0	320,564	1900	1750	448,144
194	5,9481E+06	2535	1485	1600	1200	1900	450	0	505,075	1900	1750	234,925
195	5,9481E+06	2535	1478,42	1600	1200	1900	450	0	301,435	1889,6	1750	433,76

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
196*	5,9481E+06	2534,95	1482,29	1600	1200	1900	450	0	293,126	1900	1750	449,571
197*	5,9480E+06	2535	1477,95	1600	1200	1900	450	0	303,296	1895,39	1748,98	449,39
198*	5,9478E+06	2535	1482,18	1600	1200	1900	450	0	293,216	1900	1750	449,606
199	5,9477E+06	2535	1482,18	1600	1200	1900	450	453,089	374,643	1299,36	1750	449,599
200	5,9476E+06	2535	1443,26	1600	1200	1900	450	0	302,834	1899,5	1750	446,986
201*	5,9474E+06	2535	1485	1600	1200	1900	450	0	286,695	1900	1750	450
202	5,9473E+06	2535	1485	1600	1200	1900	450	0	268,627	1899,32	1750	438,495
203	5,9473E+06	2535	1314,14	1600	1200	1900	450	0	543,055	1900	1750	367,807
204*	5,9473E+06	2535	1484,68	1600	1200	1900	450	1800	390,085	0	1750	449,82
205	5,9473E+06	2535	1473,75	1600	1200	1900	450	0	300,043	1900	1750	450
206	5,9472E+06	2535	1485	1600	1200	1900	450	0	268,416	1900	1750	450
207	5,9468E+06	2535	1463,25	1600	1200	1900	450	0	313,154	1900	1750	448,595
208	5,9467E+06	2535	1485	1600	1200	1900	450	0	286,752	1900	1750	450
209	5,9466E+06	2535	1296,71	1577,36	1200	1900	450	0	943,494	1900	1750	0
210*	5,9466E+06	2535	1447,52	1600	1200	1900	450	1800	700,63	0	1750	63,7178
211	5,9465E+06	2535	1484,89	1600	1200	1900	450	0	290,264	1899,79	1750	448,593
212*	5,9462E+06	2535	1481,76	1600	1200	1900	450	0	293,911	1900	1749,76	449,568
213*	5,9457E+06	2535	1255,77	1600	1200	1900	450	1800	785,466	0	1669,89	363,866
214*	5,9457E+06	2535	1485	1600	1200	1900	450	1606,42	546,059	0	1750	450
215*	5,9454E+06	2535	1484,27	1600	1200	1900	450	1287,87	832,353	0	1750	449,86
216	5,9454E+06	2535	1155,32	1600	1200	1900	450	0	937,11	1900	1750	81,9233
217	5,9451E+06	2535	1473,21	1600	1200	1900	450	0	299,256	1900	1750	449,245
218*	5,9451E+06	2535	1482,18	1600	1200	1900	450	0	211,797	1900	1750	449,599
219	5,9449E+06	2535	1219,6	1600	1200	1900	450	0	577,246	1900	1750	428,151
220*	5,9448E+06	2535	1485	1600	1200	1900	450	290	0	1900	1750	450

solution (* indicates that a solution falls outside the confidence interval of the objective statistic												
Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
221*	5,9448E+06	2535	1485	1600	1200	1900	450	0	950	1240	1750	450
222	5,9448E+06	2535	1474,38	1600	1200	1900	450	0	296,375	1900	1750	449,233
223*	5,9447E+06	2535	1478,59	1600	1200	1900	450	0	296,344	1899,47	1749,56	449,66
224*	5,9445E+06	2535	1484,67	1600	1200	1900	450	0	285,179	1900	1750	450
225	5,9442E+06	2535	1482,97	1600	1200	1900	450	0	285,94	1900	1750	450
226*	5,9441E+06	2535	1482,2	1600	1200	1900	450	0	282,857	1900	1750	450
227*	5,9440E+06	2535	1421,67	1600	1200	1900	450	1536,52	883,424	110,327	1750	75,7778
228	5,9439E+06	2535	1481,17	1600	1200	1900	450	0	323,431	1888,84	1750	431,552
229	5,9439E+06	2535	1331,06	1600	1200	1900	450	0	616,923	1900	1750	222,97
230	5,9439E+06	2535	1275	1600	1200	1900	450	0	950	1900	1732,26	0
231	5,9439E+06	2535	1484,41	1600	1194,26	1900	450	0	351,407	1856,16	1750	438,773
232*	5,9434E+06	2535	1483,64	1600	1200	1900	450	1713,02	442,948	14,893	1750	450
233*	5,9432E+06	2534,67	1481,7	1600	1200	1900	450	0	294,127	1900	1750	449,507
234	5,9431E+06	2535	1358,22	1600	1200	1900	450	0	431,617	1900	1750	435,16
235*	5,9431E+06	2535	1481,93	1600	1200	1900	450	0	290,634	1900	1750	449,737
236	5,9431E+06	2535	1437,65	1600	1200	1900	450	0	362,234	1900	1750	425,112
237	5,9429E+06	2535	1484,07	1600	1200	1900	450	0	289,62	1900	1750	449,96
238*	5,9428E+06	2535	1485	1600	1200	1900	450	0	289,81	1899,61	1750	449,988
239*	5,9426E+06	2535	1297,31	1600	1200	1900	450	1609,76	626,101	28,5654	1750	449,787
240*	5,9424E+06	2535	1474,82	1600	1200	1900	450	0	301,078	1900	1750	449,102
241	5,9422E+06	2535	1482,61	1600	1200	1900	450	0	292,529	1899,85	1750	449,63
242	5,9419E+06	2535	1440,53	1600	1200	1867,95	450	0	816,529	1900	1750	0
243	5,9419E+06	2535	1320,87	1600	1200	1900	450	0	904,134	1900	1750	0
244*	5,9418E+06	2535	1449,49	1600	1200	1900	450	1291,3	950	0	1750	317,488
245*	5,9417E+06	2535	1484,84	1600	1200	1900	450	0	623,361	1567,01	1750	449,794

solution (* indicates that a solution falls outside the confidence interval of the objective statistic												
Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
246	5,9417E+06	2535	1453,53	1600	1200	1900	450	0	397,609	1871,99	1750	398,027
247*	5,9416E+06	2535	1471,23	1523,75	1200	1900	450	1362,86	917,249	0	1750	449,918
248*	5,9415E+06	2535	1361,47	1600	1200	1900	450	1800	457,048	0	1750	449,32
249*	5,9414E+06	2535	1485	1600	1200	1898,79	450	0	291,756	1899,52	1750	449,93
250*	5,9414E+06	2535	1485	1600	1200	1900	450	0	288,157	1900	1750	449,961
251	5,9412E+06	2535	1466,95	1600	1200	1900	450	0	345,968	1886,59	1750	423,283
252	5,9412E+06	2535	1362,64	1600	1200	1900	450	0	424,809	1890,7	1750	400,869
253*	5,9412E+06	2535	1482,94	1600	1200	1900	450	0	290,57	1899,71	1749,83	449,834
254	5,9411E+06	2535	1485	1600	1200	1900	450	0	296,247	1899,23	1750	436,905
255*	5,9411E+06	2534,94	1485	1600	1200	1900	450	0	290,426	1899,81	1750	449,825
256	5,9408E+06	2535	944,273	1600	1200	1900	450	0	950	1900	1750	330,727
257	5,9405E+06	2535	1485	1600	1200	1900	450	0	237,665	1900	1750	450
258	5,9405E+06	2535	1336,65	1600	1200	1885,75	450	0	521,178	1900	1750	322,267
259*	5,9403E+06	2535	1481,82	1600	1200	1791,74	450	505,678	233,746	1559,18	1750	449,529
260*	5,9403E+06	2535	1485	1600	1200	1900	447,347	0	293,22	1899,43	1750	450
261	5,9402E+06	2535	1485	1600	1199,73	1900	450	0	290,612	1899,7	1750	449,96
262*	5,9399E+06	2535	1483,07	1600	1200	1900	450	0	292,155	1899,98	1750	449,659
263*	5,9399E+06	2535	1474,29	1600	1200	1900	450	1474,41	945,601	0	1750	230,704
264*	5,9398E+06	2535	1455,49	1600	1200	1900	449,394	0	321,917	1900	1750	448,197
265	5,9397E+06	2535	1275	1600	1200	1900	450	0	899,179	1900	1750	0
266	5,9396E+06	2535	1260,66	1600	1200	1900	450	0	632,491	1789,7	1750	442,144
267*	5,9396E+06	2535	1484,07	1600	1200	1900	450	0	291,487	1900	1750	449,445
268*	5,9395E+06	2535	1381,62	1600	1200	1900	450	1800	437,655	0	1750	343,315
269	5,9392E+06	2535	1482,9	1600	1200	1900	450	0	288,4	1899,72	1750	446,348
270*	5,9392E+06	2535	1485	1600	1200	1900	450	0	280,542	1900	1750	450

solution (* indicates that a solution falls outside the confidence interval of the objective statistic

Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
271	5,9389E+06	2535	1482,72	1600	1200	1900	450	0	365	1900	1750	377,279
272*	5,9388E+06	2535	1395,67	1600	1200	1900	450	1550,75	731,469	152,965	1750	234,513
273	5,9388E+06	2535	1312,89	1600	1200	1900	450	0	899,04	1900	1750	0
274*	5,9387E+06	2535	1481,94	1600	1200	1900	450	0	286,073	1900	1750	449,478
275*	5,9386E+06	2535	1482,34	1600	1200	1900	450	0	285,608	1900	1750	450
276*	5,9384E+06	2535	1366,65	1600	1200	1900	450	1734,22	877,623	0	1750	146,5
277	5,9383E+06	2535	1407,11	1598,77	1200	1900	450	0	408,054	1900	1750	318,67
278*	5,9382E+06	2535	1472,58	1600	1200	1900	450	0	302,881	1900	1750	449,543
279*	5,9382E+06	2535	1473,76	1600	1200	1900	450	0	299,154	1900	1750	449,956
280*	5,9380E+06	2535	1483,65	1600	1200	1900	450	1713,04	442,942	14,8653	1750	450
281*	5,9379E+06	2535	1485	1600	1200	1900	450	0	279,126	1900	1750	450
282	5,9379E+06	2535	1449,88	1600	1200	1900	450	0	371,426	1900	1750	274,179
283	5,9377E+06	2535	1310,07	1600	1200	1864,93	450	0	950	1900	1750	0
284*	5,9375E+06	2535	1481,37	1600	1200	1900	450	0	290,044	1900	1750	449,956
285*	5,9373E+06	2535	1484,54	1600	1200	1900	450	1786,62	738,612	3,15577	1750	77,6113
286*	5,9371E+06	2535	1478,48	1600	1200	1900	450	0	301,523	1898,61	1750	444,389
287*	5,9371E+06	2535	1466,88	1600	1200	1900	450	0	294,705	1900	1750	449,146
288*	5,9369E+06	2535	1400,16	1508,91	1200	1900	450	1800	815,403	0	1750	200,529
289	5,9367E+06	2535	1477,7	1600	1200	1900	450	0	297,531	1900	1750	449,395
290*	5,9367E+06	2535	1484,99	1600	1200	1900	450	758,369	836,352	489,397	1750	449,99
291*	5,9367E+06	2535	1481,83	1600	1200	1900	450	0	286,834	1899,98	1750	449,984
292*	5,9365E+06	2535	1485	1600	1200	1900	450	0	285,783	1899,76	1750	450
293*	5,9364E+06	2535	1467,56	1600	1200	1900	450	1356,54	753,439	0	1750	450
294*	5,9364E+06	2535	1484,64	1600	1200	1900	450	0	290,406	1900	1750	449,931
295	5,9362E+06	2535	1485	1600	1200	1900	450	0	280,257	1900	1750	450

solution (* indicates that a solution falls outside the confidence interval of the objective statistic												
Solution	Objective Total advantage Mean	allocation 1	allocation 2	allocation 3	allocation 4	allocation 5	allocation 6	allocation 7	allocation 8	allocation 9	allocation 10	allocation 11
296	5,9362E+06	2535	1485	1600	1200	1900	450	0	740	1900	1750	0
297*	5,9361E+06	2535	1482,18	1600	1200	1900	450	1634,14	559,078	2,81E-15	1750	449,599
298	5,9357E+06	2535	1275	1600	1200	1900	450	0	950	1900	1750	0
299*	5,9356E+06	2535	1382,4	1600	1200	1900	450	1792,6	950	0	1750	0
300*	5,9356E+06	2535	1342,52	1600	1200	1900	450	0	386,512	1890,08	1750	448,176
301*	5,9355E+06	2535	1484,14	1600	1200	1900	450	0	290,653	1900	1750	449,846
302*	5,9353E+06	2535	1460,43	1600	1200	1900	450	0	689,659	1900	1750	7,04718
303*	5,9352E+06	2535	1485	1600	1200	1900	450	1800	505,927	0	1750	262,81
304*	5,9350E+06	2535	1399,88	1600	1200	1900	450	1541,81	934,501	248,813	1750	0
305*	5,9347E+06	2535	1478,49	1600	1200	1900	450	0	297,094	1900	1750	449,419
306*	5,9347E+06	2535	1450,57	1600	1200	1873,23	450	0	569,157	1900	1750	204,169
307*	5,9346E+06	2535	1162,69	1600	1200	1900	450	0	595,461	1900	1750	438,299
308	5,9343E+06	2535	1484,01	1600	1200	1900	450	0	285,08	1900	1750	449,691
309*	5,9342E+06	2535	1463,11	1600	1200	1900	450	0	308,519	1900	1750	448,704
310*	5,9341E+06	2535	1468,75	1600	1200	1899,99	450	0	511,147	1900	1592,57	402,545
311*	5,9340E+06	2535	1485	1600	1200	1900	450	0	295,446	1894,55	1750	450
312*	5,9339E+06	2535	1482,12	1600	1200	1900	449,769	0	293,55	1900	1750	449,565
313*	5,9338E+06	2535	1472,81	1600	1200	1900	450	0	286,182	1900	1750	449,115
314*	5,9338E+06	2535	868,707	1600	1200	1900	450	0	925,649	1898,18	1750	432,468
315*	5,9338E+06	2535	1479,9	1600	1200	1593,47	450	1255,54	146,045	1100,75	1750	449,29
316*	5,9334E+06	2535	1482,7	1600	1200	1893,77	450	0	309,406	1900	1750	340,178

LAMPIRAN 3

PERATURAN MENTRI KOMUNIKASI DAN INFORMATIKA
NOMOR 26/PER/M.KOMINFO/5/2007

TENTANG

PENGAMANAN PEMANFAATAN JARINGAN TELEKOMUNIKASI

BERBASIS PROTOKOL INTERNET

Lampiran 3: Peraturan Mentri Komunikasi dan Informatika
Nomor 26/PER/M.KOMINFO/5/2007

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA

NOMOR 26 /PER/M.KOMINFO/ 5 /2007

TENTANG

PENGAMANAN PEMANFAATAN JARINGAN TELEKOMUNIKASI BERBASIS PROTOKOL INTERNET

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KOMUNIKASI DAN INFORMATIKA,

Menimbang : a. bahwa perkembangan pemanfaatan jaringan telekomunikasi berbasis protokol internet selain membawa perubahan, kemudahan dan kemajuan diberbagai bidang kehidupan juga dapat memicu terjadinya penyalahgunaan pemanfaatan jaringan telekomunikasi tersebut;

b. bahwa dalam prakteknya penyalahgunaan jaringan telekomunikasi berbasis protokol internet dapat menimbulkan dampak negatif baik dalam lingkup nasional maupun internasional;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, maka perlu menetapkan Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet dengan Peraturan Menteri Komunikasi dan Informatika;

Mengingat : 1. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Nomor 3881);

2. Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 107, Tambahan Lembaran Negara Nomor 3980);

3. Peraturan Presiden Republik Indonesia Nomor 9 Tahun 2005 tentang Kedudukan, Tugas, Fungsi, Susunan Organisasi dan Tata Kerja Kementerian Negara Republik Indonesia;

4. Peraturan Presiden Republik Indonesia Nomor 10 Tahun 2005 Tentang Unit Organisasi dan Tugas Eselon I Kementerian Negara Republik Indonesia sebagaimana telah diubah dengan Peraturan Presiden Republik Indonesia Nomor 15 Tahun 2005;

Lampiran 3: Peraturan Mentri Komunikasi dan Informatika
Nomor 26/PER/M.KOMINFO/5/2007
(lanjutan)

5. Keputusan Menteri Perhubungan Nomor KM. 20 Tahun 2001 tentang Penyelenggaraan Jaringan Telekomunikasi sebagaimana telah diubah terakhir dengan Peraturan Menteri Komunikasi dan Informatika Nomor 40/PER/M.Kominfo/12/2006;

6. Keputusan Menteri Perhubungan Nomor KM. 21 Tahun 2001 tentang Penyelenggaraan Jasa Telekomunikasi sebagaimana telah diubah dengan Keputusan Menteri Perhubungan Nomor KM. 30 Tahun 2004;

7. Peraturan Menteri Komunikasi dan Informatika Nomor O1/P/M.Kominfo/4/2005 Tahun 2005 tentang Susunan Organisasi dan Tata Kerja Departemen Komunikasi dan Informatika;

8. Peraturan Menteri Komunikasi dan Informatika Nomor 03/P/M.Kominfo/5/2005 tentang Penyesuaian Kata Sebutan Pada Beberapa Keputusan/Peraturan Menteri Perhubungan yang Mengatur Materi Muatan Khusus di Bidang Pos dan Telekomunikasi;

MEMUTUSKAN :

Menetapkan : PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA TENTANG PENGAMANAN PEMANFAATAN JARINGAN TELEKOMUNIKASI BERBASIS PROTOKOL INTERNET.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan ini yang dimaksud dengan :

1. Protokol internet adalah sekumpulan protokol yang didefinisikan oleh *Internet Engineering Task Force* (*IETF*);

2. Jaringan telekomunikasi berbasis Protokol Internet adalah jaringan telekomunikasi yang digunakan penyelenggara jaringan dan jasa telekomunikasi dengan memanfaatkan protokol internet dalam melakukan kegiatan telekomunikasi;

3. Indonesia-*Security Incident Responses Team on Internet Infrastructure* yang selanjutnya disebut ID-SIRTII adalah Tim yang ditugaskan Menteri untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet;

4. Rekaman aktifitas transaksi koneksi (*Log File*) adalah suatu file yang mencatat akses pengguna pada saluran akses operator/ penyelenggara jasa akses berdasarkan alamat asal Protokol Internet (*source*), alamat tujuan (*destination*), jenis protokol yang digunakan, *Port* asal (*source*), *Port* tujuan (*destination*) dan waktu (*time stamp*) serta durasi terjadinya transaksi;

5. Monitoring Jaringan adalah fasilitas pemantau dan pendeteksi pola (*pattern*) akses dan transaksi yang berpotensi mengganggu atau menyerang jaringan untuk tujuan memantau kondisi jaringan, memberikan peringatan dini (*early warning*) dan melakukan tindakan pencegahan (*prevent*).

6. Penyelenggara akses internet (*Internet Service Provider/ISP*) adalah penyelenggara jasa multimedia yang menyelenggarakan jasa akses internet kepada masyarakat;

7. Penyelenggara jasa interkoneksi internet (*Network Access Point/NAP*) adalah penyelenggara jasa multimedia yang menyelenggarakan jasa akses dan atau ruting kepada ISP untuk melakukan koneksi ke jaringan internet global;

8. *Hot spot* adalah tempat tersedianya akses internet untuk publik yang menggunakan teknologi wireless;

9. *Internet Exchange Point* adalah titik dimana ruting internet nasional berkumpul untuk saling berinterkoneksi;

10. Pra bayar adalah sistem pembayaran diawal periode pemakaian melalui pembelian nomor perdana dan pulsa isi ulang *(voucher);*

11. Warung internet yang selanjutnya disebut Warnet adalah *reseller* dari ISP dan memiliki tempat penyediaan jasa internet kepada masyarakat;

12. Menteri adalah Menteri yang ruang lingkup tugas dan tanggung jawabnya di bidang telekomunikasi;

13. Direktur Jenderal adalah Direktur Jenderal Pos dan Telekomunikasi.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

Maksud dilaksanakannya pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet adalah mendukung terciptanya pemanfaatan jaringan telekomunikasi berbasis protokol internet di Indonesia yang relatif bebas dari ancaman dan gangguan.

Pasal 3

Tujuan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet adalah untuk :

a. terlaksananya dukungan proses penegakan hukum;

b. terciptanya pemanfaatan jaringan telekomunikasi berbasis protokol internet yang aman;

c. terlaksananya koordinasi dengan pihak-pihak terkait baik di dalam maupun luar negeri.

BAB III

RUANG LINGKUP

Pasal 4

Ruang lingkup pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet meliputi :

a. mensosialisasikan kepada seluruh pihak yang terkait untuk melakukan kegiatan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;

b. melakukan pemantauan, pendeteksian dini dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protokol internet di Indonesia;

c. membangun dan atau menyediakan, mengoperasikan, memelihara dan mengembangkan sistem database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet sekurang-kurangnya untuk :

   1. mendukung kegiatan sebagaimana dimaksud dalam butir b;
   2. menyimpan rekaman transaksi (*log file*);
   3. mendukung proses penegakan hukum.

d. melaksanakan fungsi layanan informasi atas ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;

e. menyediakan laboratorium simulasi dan pelatihan kegiatan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;

f. melakukan pelayanan konsultasi dan bantuan teknis;

g. menjadi *contact point* dengan lembaga terkait tentang pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet baik dalam negeri maupun luar negeri.

BAB IV

KELEMBAGAAN

Pasal 5

(1) Untuk melaksanakan ruang lingkup pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet sebagaimana dimaksud dalam Pasal 4, perlu dibentuk lembaga tersendiri.

(2) Lembaga sebagaimana dimaksud pada ayat (1) adalah Tim ID-SIRTII.

Pasal 6

(1) Tim ID-SIRTII terdiri atas Pelaksana dan Tim Ahli.

(2) Pelaksana bertugas untuk melaksanakan ruang lingkup sebagaimana dimaksud dalam Pasal 4.

(3) Tim Ahli bertugas untuk membantu Menteri dalam fungsi perencanaan, koordinasi, pengawasan dan pengendalian kegiatan ID-SIRTII.

Pasal 7

(1) Tim Ahli sebagaimana dimaksud dalam Pasal 6 ayat (3) ditetapkan dengan Keputusan Menteri tersendiri yang anggotanya terdiri dari unsur-unsur antara lain pemerintah, aparat penegak hukum, penyelenggara telekomunikasi, akademisi, dan praktisi.

(2) Tim Ahli terdiri dari :

a. bidang perencanaan;
b. bidang hukum; dan
c. bidang evaluasi operasional.

(3) Tim Ahli Bidang Perencanaan sebagaimana dimaksud pada ayat (2) huruf a mempunyai tugas dan fungsi sebagai berikut :

a. menyusun konsep dasar dan panduan kegiatan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet untuk setiap operator, pemeriksa dan aparat penegak hukum;

b. menyusun strategi sosialisasi konsep dan layanan ID-SIRTII;

c. mendorong terciptanya sinergi dalam implementasi ID-SIRTII;

d. apabila diperlukan, melakukan studi banding (*benchmarking*) tentang langkah-langkah pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet di negara lain;

e. menyusun rekomendasi kerjasama dengan lembaga sejenis dalam bidang antara lain strategi layanan, sumber daya manusia, teknologi dan pendanaan.

(4) Tim Ahli Bidang Hukum sebagaimana dimaksud pada ayat (2) huruf b mempunyai tugas dan fungsi sebagai berikut :

a. melakukan kajian hukum dan perundang-undangan di bidang keamanan jaringan internet di Indonesia;

b. mempersiapkan rekomendasi untuk penyusunan regulasi terkait;

c. mendorong koordinasi dan mempersiapkan konsep kerjasama di bidang hukum dengan lembaga penegak hukum di Indonesia (Kepolisian, Kejaksaan, Departemen Hukum dan HAM serta MA) dan di negara-negara lain yang terkait.

(5) Tim Ahli Bidang Evaluasi Operasional sebagaimana dimaksud pada ayat (2) huruf c mempunyai tugas dan fungsi sebagai berikut :

a. menyusun standar operasi dan prosedur pelaksanaan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;

b. menyusun kerangka acuan kebutuhan sarana dan prasarana serta kebutuhan biaya pembangunan, pengoperasian, pemeliharaan dan pengembangan sistem database pemantauan dan pengamanan transaksi internet;

c. menyusun panduan penilaian kinerja pelaksanaan ID-SIRTII;

d. menyusun rekomendasi kinerja pelaksanaan ID-SIRTII.

Pasal 8

(1) Pelaksana sebagaimana dimaksud dalam Pasal 6 ayat (2) dilaksanakan oleh Direktur Jenderal.

(2) Pelaksana ID-SIRTII sebagaimana dimaksud ayat (1) terdiri dari 2 (dua) kelompok yaitu :

a. Kelompok Pimpinan Pelaksana /Koordinator ID-SIRTII;

b. Kelompok Teknis Pelaksana ID-SIRTII.

(3) Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII sebagaimana dimaksud pada ayat (2) huruf a ditetapkan melalui seleksi.

(4) Penugasan pihak ketiga untuk Kelompok Teknis Pelaksana ID-SIRTII sebagaimana dimaksud pada ayat (2) huruf b ditetapkan melalui pelelangan umum.

(5) Pelaksanaan melalui seleksi dan pelelangan umum harus dilakukan sesuai dengan peraturan perundang-undangan yang berlaku.

Pasal 9

Tugas dan fungsi Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII adalah sebagai berikut :

1. Melakukan sosialisasi dengan pihak terkait baik di dalam negeriMelakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan maupun luar negeri untuk melakukan kegiatan pengamanan pemanfaatan jaringan dan mensosialisasikan keberadaan lembaga ID-SIRTII;

2. Melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancamam dan gangguan pada jaringan;

3. Berkoordinasi dengan pihak-pihak terkait baik di dalam maupun luar negeri didalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis IP;

4. Melakukan penyusunan dan kajian berkaitan dengan pengembangan sistem dan organisasi ID-SIRTII;

5. Mengoperasikan, memelihara dan mengembangkan sistem database sistem ID-SIRTII;

6. Menyusun katalog-katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan;

7. Memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis IP;

8. Menjadi *contact point* dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis IP;

9. Menyusun program kerja dalam rangka melaksanakan pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis IP;

10. Bertanggungjawab sebagai koordinator atas operasional lembaga ID-SIRTII sehari-hari;

11. Melaporkan hasil kegiatan kepada Direktur Jenderal Pos dan Telekomunikasi.

Pasal 10

Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII melaporkan hasil pelaksanaan tugasnya kepada Direktur Jenderal setiap 3 (tiga) bulan dan atau apabila diperlukan.

Pasal 11

(1) Kelompok Pimpinan Pelaksana/Koordinator Tim ID-SIRTII terdiri dari 3 (tiga) orang dengan komposisi 1 (satu) orang Ketua, 1 (satu) orang Wakil Ketua dan 1 (satu) orang Sekretaris;

(2) Sekretaris sebagaimana dimaksud pada ayat (1) diangkat dari unsur Pemerintah.

Pasal 12

(1) Ketua dan Wakil Ketua Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII sebagaimana dimaksud dalam Pasal 11 ayat (1) ditetapkan melalui seleksi.

(2) Sekretaris sebagaimana dimaksud dalam Pasal 11 ayat (2) adalah Pejabat di lingkungan Direktorat Jenderal Pos dan Telekomunikasi yang diangkat Direktur Jenderal.

Pasal 13

(1) Masa kerja Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII selain Sekretaris selama 3 (tiga) tahun dan dapat diangkat kembali untuk 1 (satu) kali masa kerja.

(2) Masa Kerja sebagaimana dimaksud pada ayat (1) berakhir pada saat penetapan Ketua dan Wakil Ketua Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII yang baru.

Pasal 14

Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII wajib menjaga kerahasiaan data dan informasi yang secara hukum dinyatakan rahasia.

Pasal 15

(1) Menteri memiliki kewenangan akses terhadap sistem Data Base ID-SIRTII.

(2) Untuk kepentingan operasional ID-SIRTII, Menteri mendelegasikan kewenangan akses kepada Direktur Jenderal.

(3) Direktur Jenderal dapat dibantu oleh Pelaksana ID-SIRTII untuk melaksanakan kewenangan, tugas dan fungsinya dengan mematuhi Standar Operasi dan Prosedur yang ditetapkan oleh Direktur Jenderal.

Pasal 16

(1) Dalam hal dipandang perlu Direktur Jenderal dapat mengangkat Pengawas dari unsur Pemerintah.

(2) Pengawas bertugas membantu Direktur Jenderal untuk melakukan pengawasan terhadap pelaksanaan tugas dan fungsi ID-SIRTII.

(3) Pengawasan terhadap pelaksanaan tugas dan fungsi ID-SIRTII sebagaimana dimaksud pada ayat (2) adalah sebagai berikut :

a. kepatuhan terhadap standar operasi dan prosedur dalam pengelolaan ID-SIRTII;

b. prosedur kerja antara ID-SIRTII dengan penyelenggara telekomunikasi dan aparat penegak hukum;

c. prosedur kerahasiaan dokumen dan atau data yang disimpan oleh ID-SIRTII.

Pasal 17

Untuk kelancaran pelaksanaan tugas ID-SIRTII sebagaimana dimaksud dalam Pasal 6 (1) dan Pasal 16 diberikan honorarium yang dibebankan kepada Anggaran Direktorat Jenderal Pos dan Telekomunikasi yang besarannya ditetapkan oleh Keputusan Direktur Jenderal sesuai dengan ketentuan yang berlaku.

Pasal 18

(1) Sistem database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet sebagaimana dimaksud dalam Pasal 4 huruf c, dapat dibangun atau diadakan secara bertahap sesuai kebutuhan masyarakat dan kemampuan keuangan negara.

(2) Dalam hal belum tersedia tempat untuk sistem database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, Direktur Jenderal dapat melakukan penyewaan tempat untuk kelangsungan operasional ID-SIRTII.

BAB V

KEWAJIBAN PENGAMANAN PEMANFAATAN JARINGAN TELEKOMUNIKASI BERBASIS PROTOKOL INTERNET

Pasal 19

(1) Setiap penyelenggara telekomunikasi yang menggunakan protokol internet wajib melakukan rekaman transaksi koneksi (*log file*).

(2) Rekaman transaksi koneksi sebagaimana dimaksud pada ayat (1) disimpan sekurang-kurangnya selama 3 (tiga) bulan.

(3) Laporan rekaman transaksi sebagaimana dimaksud pada ayat (1) disampaikan secara *online* kepada sistem database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet yang dimiliki oleh Pelaksana ID-SIRTII.

(4) Dalam hal fasilitas keterhubungan secara *online* sebagaimana dimaksud pada ayat (3) belum tersedia, penyelenggara telekomunikasi yang menggunakan protokol internet wajib menyampaikan rekaman transaksi secara *offline* dalam bentuk media penyimpanan digital (*storage media*) setiap 14 (empat belas) hari kalender kepada Pelaksana ID-SIRTII.

Pasal 20

(1) Pengelola Internet *Exchange Point* dan atau penyelenggara jasa interkoneksi internet (*Network Access Point/NAP*) yang beroperasi di Indonesia wajib mengaktifkan dan menyediakan fasilitas monitoring jaringan dan terhubung secara *online* kepada sistem database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet.

Lampiran 3: Peraturan Mentri Komunikasi dan Informatika
Nomor 26/PER/M.KOMINFO/5/2007
(lanjutan)

Pasal 21

(1) Pengelola *Warnet, Hotspot* dan sejenisnya wajib mendata setiap pengguna jasa internet dalam rangka pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, sekurang-kurangnya meliputi :

a. identitas pengguna jasa internet;

b. waktu mulai dan berakhirnya penggunaan akses internet;

(2) ISP yang menyelenggarakan jasa layanan pra bayar wajib mendata identitas pengguna.

(3) Data identitas pengguna jasa internet sebagaimana dimaksud pada ayat (1) dan ayat (2) wajib disimpan sekurang-kurangnya selama 1 (satu) tahun.

(4) Untuk keperluan proses peradilan pidana, data sebagaimana dimaksud pada ayat (1) dan ayat (2) wajib diserahkan kepada pihak yang berwenang.

Pasal 22

(1) Setiap penyelenggara telekomunikasi yang menggunakan protokol internet wajib melakukan penyelarasan waktu (*clock synchronization*) sesuai dengan server yang ditetapkan oleh Direktur Jenderal.

(2) Penetapan server sebagaimana dimaksud pada ayat (1) ditetapkan lebih lanjut dengan Keputusan Direktur Jenderal.

BAB VI

KETENTUAN PERALIHAN

Pasal 23

(1) Ketentuan sebagaimana dimaksud dalam Pasal 19 Pasal 20 Pasal 21 dan Pasal 22 Peraturan Menteri ini, berlaku sejak sistem database Pemantauan Dan Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet telah beroperasi.

(2) Direktur Jenderal menetapkan tanggal efektif operasional sistem database Pemantauan Dan Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

BAB VII

KETENTUAN PENUTUP

Pasal 24

Dengan berlakunya Peraturan Menteri ini, maka Peraturan Menteri Komunikasi dan Informatika Nomor :27/PER/M.KOMINFO/9/2006 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet dicabut dan dinyatakan tidak berlaku.

Lampiran 3: Peraturan Mentri Komunikasi dan Informatika
Nomor 26/PER/M.KOMINFO/5/2007
(lanjutan)

Pasal 25

Peraturan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di : J A K A R T A
Pada tanggal : 4 M E I 2007

MENTERI KOMUNIKASI DAN INFORMATIKA,

SOFYAN A. DJALIL

SALINAN Peraturan ini disampaikan kepada

1. Menteri Sekretaris Negara;
2. Menteri Hukum dan HAM;
3. Ketua Badan Pemeriksa Keuangan;
4. Ketua Mahkamah Agung;
5. Kepala Kejaksaan Agung;
6. Kepala Kepolisian RI;
7. Gubernur Bank Indonesia.

LAMPIRAN 4

PERATURAN DIREKTUR JENDRAL POS DAN TELEKOMUNIKASI
NOMOR 226/DIRJEN/2007

TENTANG

SUSUNAN ORGANISASI, TUGAS, PENGAWAS DAN STANDAR OPERASI DAN PROSEDUR PELAKSANA *INDONESIA – SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE* (ID-SIRTII)

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007

DEPARTEMEN KOMUNIKASI DAN INFORMATIKA RI
DIREKTORAT JENDERAL POS DAN TELEKOMUNIKASI
Menuju Masyarakat Informasi Indonesia
Jl. Medan Merdeka Barat No. 17 JAKARTA 10110 Tel. 021-3835815 Fax. 021-3835845 www.postel.go.id

PERATURAN DIREKTUR JENDERAL POS DAN TELEKOMUNIKASI

NOMOR : 226/DIRJEN/2007

TENTANG

SUSUNAN ORGANISASI, TUGAS, PENGAWAS DAN STANDAR OPERASI DAN PROSEDUR PELAKSANA *INDONESIA – SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE* (ID-SIRTII)

DENGAN RAHMAT TUHAN YANG MAHA ESA

DIREKTUR JENDERAL POS DAN TELEKOMUNIKASI,

Menimbang :

a. bahwa untuk melaksanakan ketentuan dalam Pasal 15 Ayat (3) Peraturan Menteri Komunikasi dan Informatika Nomor: 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet mengamanatkan bahwa Direktur Jenderal dapat dibantu oleh Pelaksana ID-SIRTII untuk melaksanakan kewenangan, tugas dan fungsinya dengan mematuhi Standar Operasi dan Prosedur yang ditetapkan oleh Direktur Jenderal;

b. bahwa berdasarkan pertimbangan butir a tersebut di atas, perlu menetapkan Peraturan Direktur Jenderal Pos dan Telekomunikasi tentang Susunan Organisasi, Tugas, Pengawas dan Standar Operasi dan Prosedur Pelaksana *Indonesia – Security Incident Response Team On Internet Infrastructure* (ID-SIRTII);

Mengingat :

1. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Nomor 3881);

2. Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 107, Tambahan Lembaran Negara Nomor 3980);

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

3. Peraturan Presiden Republik Indonesia Nomor 9 Tahun 2005 tentang Kedudukan, Tugas, Fungsi Susunan Organisasi dan Tata Kerja Kementerian Negara Republik Indonesia;

4. Peraturan Presiden Republik Indonesia Nomor 10 Tahun 2005 Tentang Unit Organisasi dan Tugas Eselon I Kementerian Negara Republik Indonesia sebagaimana telah diubah dengan Peraturan Presiden Republik Indonesia Nomor 7 Tahun 2007;

5. Keputusan Menteri Perhubungan Nomor: KM.20 Tahun 2001 tentang Penyelenggaraan Jaringan Telekomunikasi sebagaimana telah diubah dengan Peraturan Menteri Komunikasi dan Informatika Nomor: 40/P/M.Kominfo/12/2006;

6. Keputusan Menteri Perhubungan Nomor: KM.21 Tahun 2001 tentang Penyelenggaraan Jasa Telekomunikasi sebagaimana telah diubah dengan Keputusan Menteri Perhubungan Nomor: KM.30 Tahun 2004;

7. Peraturan Menteri Komunikasi dan Informatika Nomor: 01/P/M.Kominfo/4/2005 Tahun 2005 tentang Susunan Organisasi dan Tata Kerja Departemen Komunikasi dan Informatika;

8. Peraturan Menteri Komunikasi dan Informatika Nomor: 03/P/M.Kominfo/5/2005 tentang Penyesuaian Kata Sebutan pada Beberapa Keputusan/Peraturan Menteri Perhubungan yang Mengatur Materi Muatan Khusus di Bidang Pos dan Telekomunikasi;

9. Peraturan Menteri Komunikasi dan Informatika Nomor: 26/P/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

MEMUTUSKAN :

Menetapkan : PERATURAN DIREKTUR JENDERAL POS DAN TELEKOMUNIKASI TENTANG SUSUNAN ORGANISASI, TUGAS, PENGAWAS DAN STANDAR OPERASI DAN PROSEDUR PELAKSANA *INDONESIA – SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE* (ID-SIRTII).

2

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

BAB I

SUSUNAN ORGANISASI DAN TUGAS ID-SIRTII

Bagian Pertama

Susunan Organisasi

Pasal 1

Pelaksana ID-SIRTII adalah petugas yang ditetapkan oleh Direktur Jenderal Pos dan Telekomunikasi untuk melaksanakan kegiatan dengan ruang lingkup Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Pasal 2

(1) Pelaksana ID-SIRTII sebagaimana dimaksud dalam Pasal 1 meliputi :

a. Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII terdiri dari Ketua, Wakil Ketua dan Sekretaris;
b. Kelompok Teknis Pelaksana ID-SIRTII terdiri dari Manajer dan Staf.

(2) Manajer sebagaimana dimaksud pada ayat (1) membidangi :

a. bidang Operasional dan Keamanan;
b. bidang Data Center, Aplikasi dan Database;
c. bidang Riset dan Pengembangan;
d. bidang Hubungan Antar Lembaga; dan
e. bidang Sosialisasi dan Layanan Publik.

Pasal 3

Struktur Organisasi Pelaksana ID-SIRTII sebagaimana dimaksud dalam Pasal 2 tercantum dalam Lampiran Peraturan ini.

Bagian Kedua

Tugas Pelaksana ID-SIRTII

Pasal 4

Kelompok Pimpinan Pelaksana/Koordinator ID-SIRTII sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf a mempunyai tugas sebagai berikut :

3

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

1. Ketua :

   a. memimpin pelaksanaan tugas dan fungsi manajemen ID-SIRTII secara umum;
   b. melakukan kerjasama operasional baik di dalam maupun di luar negeri;
   c. menyusun laporan pelaksanaan tugas secara periodik setiap 3 (tiga) bulan sekali dan laporan pertanggungjawaban tahunan;
   d. bertanggung jawab atas pelaksanaan tugas kepada Direktur Jenderal Pos dan Telekomunikasi.

2. Wakil Ketua :

   a. membantu Ketua dalam melaksanakan fungsi manajemen ID-SIRTII;
   b. memimpin pelaksanaan tugas dan fungsi operasional sehari-hari;
   c. bertanggung jawab atas pelaksanaan tugas kepada Ketua.

3. Sekretaris :

   a. menjalankan fungsi-fungsi kesekretariatan;
   b. melakukan fungsi penghubung dalam implementasi kebijakan dan peraturan Pemerintah yang terkait dengan keamanan internet di lingkungan pelaksana ID-SIRTII;
   c. bertanggung jawab atas pelaksanaan tugas kepada Ketua;
   d. menyiapkan bahan penyusunan pedoman langkah-langkah teknis pelaksanaan pengamanan jaringan dan pengelolaan data pada lingkup:
      1) bidang Operasi dan Keamanan;
      2) bidang *Data Center*, Aplikasi dan *Database*;
      3) bidang Hubungan Antar Lembaga.

Pasal 5

Kelompok Teknis Pelaksana ID-SIRTII sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf b mempunyai tugas sebagai berikut :

1. Bidang Operasional dan Keamanan:

   a. melakukan pengumpulan *log file* dan pemantauan terhadap jaringan Internet Indonesia serta deteksi dini terhadap kemungkinan adanya gangguan atau serangan;

4

b. melakukan koordinasi dengan bidang *Data Center*, Aplikasi dan *Database* untuk penyimpanan data *log* dan Pemantauan;
c. melakukan koordinasi dengan bidang Sosialisasi dan Layanan Publik untuk menindaklanjuti laporan gangguan;
d. melakukan koordinasi dengan bidang Riset dan Pengembangan untuk merencanakan pengembangan jaringan;
e. memberikan layanan dalam mengatasi gangguan dan ancaman, jika diperlukan;
f. menyusun laporan pelaksanaan tugas dan pertanggungjawaban kepada Wakil Ketua.

2. Bidang Data Center, Aplikasi dan Database :

a. melakukan penyimpanan dan pengamanan data *log* dan hasil pemantauan jaringan;
b. mengoperasikan data center yang aman, baik dari gangguan fisik maupun gangguan lain;
c. menyediakan layanan data center yang aman untuk aplikasi pemerintahan dan swasta;
d. menyediakan layanan *Executive Information System* (EIS), *Decision Support System* (DSS);
e. menyediakan layanan *Business Analysis System* (BAS) dan *Risk Management System* (RMS);
f. merancang dan mengembangkan aplikasi (perangkat lunak) pendukung operasional;
g. melakukan koordinasi dengan bidang Operasional dan Keamanan untuk penyimpanan data *log* dan Pemantauan;
h. melakukan koordinasi dengan bidang Sosialisasi dan Layanan Publik untuk menindaklanjuti laporan gangguan;
i. melakukan koordinasi dengan bidang Riset dan Pengembangan untuk merencanakan pengembangan jaringan;
j. menyusun laporan pelaksanaan tugas dan pertanggungjawaban kepada Wakil Ketua.

3. Bidang Riset dan Pengembangan:

a. membuat *knowledge database* yang digunakan sebagai laboratorium uji coba sistem operasi, jaringan, aplikasi, ataupun perangkat, dalam segi keamanan maupun ketangguhan;

5

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

b. membuat *repository data*, informasi, *tools*, desain, konfigurasi, *database*, statistik, *white paper*, *best practice* dan hasil analisa insiden keamanan sebagai rujukan bagi bidang lain;
c. membantu bidang lain sebagai wadah riset dan pengembangan (R&D) secara umum;
d. menguji spesifikasi teknologi dan produk (perangkat lunak dan keras) yang digunakan;
e. merancang, mengembangkan teknologi, perangkat lunak/keras pendukung operasional;
f. mempelajari *roadmap* teknologi dan produk serta memberikan rekomendasi pemanfaatan;
g. evaluasi Standar Operasi dan Prosedur teknis (Jaringan, Data Center, *Contact Center*);
h. melakukan *Business Process Reenginering (Eliminated – Simplify – Integrate – Automate);*
i. menyusun laporan pelaksanaan tugas dan pertanggungjawaban kepada Wakil Ketua.

Bidang Hubungan Antar Lembaga :

a. menyusun dan menyelenggarakan sistem koordinasi antar instansi terkait di dalam negeri;
b. menyusun dan menyelenggarakan sistem koordinasi antar instansi sejenis di luar negeri;
c. menyusun dan menyelenggarakan pola kerjasama di bidang sistem dan keamanan jaringan;
d. menyusun laporan pelaksanaan tugas dan pertanggungjawaban kepada Wakil Ketua.

Bidang Sosialisasi dan Layanan Publik :

a. menyusun dan bekerjasama dengan pihak lain untuk menyelenggarakan sosialisasi publik;
b. menyusun desain dan melaksanakan IP *base contact/call center*;
c. mendokumentasikan dan mengklasifikasikan laporan kejadian/insiden, gangguan/serangan;
d. mengirimkan e-mail dan pesan peringatan kemungkinan terjadinya gangguan/serangan;
e. mengelola dan mengoperasionalkan aplikasi manajemen proyek Teknologi Informasi;
f. melakukan koordinasi dengan bidang Operasi dan Keamanan untuk menindaklanjuti laporan gangguan/serangan;
g. melakukan koordinasi dengan bidang Data Center, Aplikasi dan Database untuk penyimpanan data laporan insiden/gangguan;

6

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

h. melakukan koordinasi dengan bidang Riset dan Pengembangan untuk merencanakan pengembangan jaringan;
i. melakukan sosialisasi pada masyarakat tentang konsep dasar dan layanan ID-SIRTII;
j. menyusun laporan pelaksanaan tugas dan pertanggungjawaban kepada Wakil Ketua.

BAB II

PENGAWAS

Pasal 6

(1) Dalam hal dipandang perlu Direktur Jenderal dapat mengangkat Pengawas dari unsur Pemerintah.

(2) Pengawas bertugas membantu Direktur Jenderal untuk melakukan pengawasan terhadap pelaksanaan tugas dan fungsi ID-SIRTII.

(3) Pengawasan terhadap pelaksanaan tugas dan fungsi ID-SIRTII sebagaimana dimaksud pada ayat (2) adalah sebagai berikut :

a. kepatuhan terhadap standar operasi dan prosedur dalam pengelolaan ID-SIRTII;
b. prosedur kerja antara ID-SIRTII dengan penyelenggara telekomunikasi dan aparat penegak hukum;
c. prosedur kerahasiaan dokumen dan atau data yang disimpan oleh ID-SIRTII.

Pasal 7

(1) Berdasarkan pengawasan terhadap pelaksanaan tugas dan fungsi ID-SIRTII sebagaimana dimaksud dalam Pasal 6 ayat (3), Pengawas dapat mengusulkan Ketua dan atau Wakil Ketua untuk diberhentikan apabila terbukti tidak melaksanakan tugas dan fungsi ID-SIRTII dan atau tidak memenuhi Standar Kinerja yang ditetapkan oleh Direktur Jenderal tersendiri.

(2) Standar Kinerja sebagaimana dimaksud pada ayat (1) ditetapkan lebih lanjut dengan Keputusan Direktur Jenderal tersendiri.

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

Pasal 8

Susunan Keanggotaan dan Standar Operasi dan Prosedur Pengawas ID-SIRTII sebagaimana dimaksud dalam Pasal 6 ditetapkan oleh Direktur Jenderal dengan keputusan tersendiri.

BAB III

STANDAR OPERASI DAN PROSEDUR

Pasal 9

Pelaksana ID-SIRTII dalam melaksanakan tugas wajib mengikuti Standar Operasi dan Prosedur.

Pasal 10

Standar Operasi dan Prosedur terdiri dari:

a. proses penerimaan dan penyimpanan *log file*;
b. proses ekstraksi data;
c. proses penyerahan data.

Pasal 11

Proses penerimaan dan penyimpanan Log File sebagaimana dimaksud dalam Pasal 10 huruf a menggunakan metode sebagai berikut :

a. metode *on-line; dan*
b. metode *off-line.*

Pasal 12

(1) Dalam hal menggunakan metode *On-line* sebagaimana dimaksud dalam Pasal 11 huruf a, proses penerimaan dan penyimpanan *log file* dilaksanakan dengan cara :

   a. Bidang Operasional dan Keamanan melakukan:

      1. otentikasi, otorisasi dan validasi proses pengiriman;
      2. pengecekan kode cheksum setelah data diterima;
      3. penyerahan *log file* kepada Bidang Data Center Aplikasi dan Database setelah diverifikasi.

   b. Bidang Data Center, Aplikasi dan Database melakukan:

8

1. dekripsi data yang diterima;
2. menambahkan ke dalam database sesuai urutan;
3. enkripsi database yang baru ditambahkan;
4. mencatat data sequence record yang terdiri atas:
   a). *ticket number;*
   b). *operator ID;*
   c). *log file type;*
   d). *sender ID.*
5. *data sequence record* disimpan oleh ID-SIRTII;
6. data *sequence record* dikirimkan ke penanggung jawab ISP/NAP sebagai bukti penerimaan dan untuk disimpan sebagai arsip.

(2) Dalam hal menggunakan metode *Off-line* sebagaimana dimaksud dalam Pasal 11 huruf b, proses penerimaan dan penyimpanan *log file* dilaksanakan dengan cara:

a. Bidang Operasional dan Keamanan melakukan:

1. otentikasi, otorisasi dan validasi proses pengiriman;
2. pengecekan kode cheksum setelah data diterima.
3. penyerahan *log file* kepada Bidang Data Center Aplikasi dan Database setelah diverifikasi.

b. Bidang Data Center, Aplikasi dan Database melakukan:

1. dekripsi data yang diterima;
2. menambahkan ke dalam database sesuai urutan;
3. enkripsi database yang baru di tambahkan;
4. mencatat *data sequence record* yang terdiri atas:
   a). *ticket number;*
   b). *operator ID;*
   c). *log file type;*
   d). *sender ID;*
5. *data sequence record* disimpan oleh ID-SIRTII;
6. *data sequence record* dikirimkan ke penanggung jawab ISP/NAP sebagai bukti penerimaan dan untuk disimpan sebagai arsip.

(3) Bidang Operasional dan Keamanan sebagaimana di maksud dalam Pasal 12 ayat (1) huruf a dan ayat (2) huruf a bertugas menyimpan CD/DVD yang sudah diproses ke dalam tempat yang aman dan sudah ditentukan.

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

Pasal 13

Proses ekstraksi data sebagaimana dimaksud dalam Pasal 10 huruf b digunakan untuk keperluan sebagai berikut :

a. keperluan internal Ditjen Postel;dan
b. keperluan proses penyelidikan, penyidikan, penuntutan dan peradilan.

Pasal 14

(1) Proses Ekstraksi Data untuk keperluan Internal Ditjen Postel sebagaimana dimaksud dalam Pasal 13 huruf a dilakukan dengan ketentuan sebagai berikut :

a. harus berdasarkan surat perintah dari Direktur Jenderal Pos dan Telekomunikasi;
b. database hanya bisa dibuka menggunakan kode kunci yang hanya diketahui oleh Direktur Jenderal Pos dan Telekomunikasi dan dapat didelegasikan kepada Ketua ID-SIRTII;
c. *ekstraksi* data langsung dilakukan dari database yang tersimpan;
d. proses *ekstraksi* hanya boleh dilakukan oleh Manager Bidang Data Center, Aplikasi dan Database dan harus dilakukan pencatatan terhadap proses tersebut;
e. data yang harus dicatat adalah *Ticket number, Operator ID, Log file type* dan aplikasi tujuannya (pemanfaatan data hanya boleh dilakukan untuk aplikasi yang sudah ditentukan);
f. penyajian data hasil *ekstraksi* dan analisa harus dalam bentuk *template* tertentu yang sudah ditentukan;
g. setelah proses *ekstraksi* dan analisa selesai harus dibuatkan Berita Acara antara Manager Bidang Data Center, Aplikasi dan Database dengan Wakil Ketua ID-SIRTII serta diketahui oleh Ketua ID-SIRTII;
h. hasil *ekstraksi* dan analisa disampaikan kepada Instansi Pemohon oleh Ketua ID-SIRTII dengan tembusan kepada Direktur Jenderal Pos dan Telekomunikasi.

(2) Proses ekstraksi data untuk keperluan proses penyelidikan, penyidikan, penuntutan dan peradilan sebagaimana dimaksud dalam Pasal 13 huruf b dilakukan dengan ketentuan sebagai berikut :

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

a. harus ada permohonan resmi dari instansi penegak hukum yang berwenang berdasarkan Undang-Undang kepada Direktur Jenderal Pos dan Telekomunikasi dengan tembusan kepada Ketua ID-SIRTII;
b. Ketua ID-SIRTII dapat langsung memproses permohonan sebagaimana dimaksud pada huruf a;
c. database hanya bisa dibuka menggunakan kode kunci yang hanya diketahui oleh Direktur Jenderal Pos dan Telekomunikasi dan dapat didelegasikan kepada Ketua ID-SIRTII;
d. *ekstraksi* data langsung dilakukan dari database yang tersimpan;
e. proses *ekstraksi* hanya boleh dilakukan oleh Manager Bidang Data Center, Aplikasi dan Database dan harus dilakukan pencatatan terhadap proses tersebut;
f. data yang harus dicatat adalah *Ticket number, Operator ID, Log file type* dan aplikasi tujuannya (pemanfaatan data hanya boleh dilakukan untuk aplikasi yang sudah ditentukan);
g. penyajian data hasil *ekstraksi* dan analisa harus dalam bentuk *template* tertentu yang sudah ditentukan;
h. setelah proses *ekstraksi* dan analisa selesai harus dibuatkan Berita Acara antara Manager Bidang Data Center, Aplikasi dan Database dengan Wakil Ketua ID-SIRTII serta diketahui oleh Ketua ID-SIRTII;
i. hasil *ekstraksi* dan analisa disampaikan kepada Instansi Pemohon oleh Ketua ID-SIRTII dengan tembusan kepada Direktur Jenderal Pos dan Telekomunikasi.

Pasal 15

Proses penyerahan data sebagaimana dimaksud dalam Pasal 10 huruf c dilakukan dengan cara sebagai berikut :

a. petugas pengambil data hasil *ekstraksi* dan analisa harus dilengkapi surat tugas resmi dari instansinya;
b. petugas ID-SIRTII mencatat identitas petugas pengambil hasil *ekstraksi* dan analisa;
c. hasil *ekstraksi* dan analisa dibuatkan *ticket number;*
d. *ticket number* dikirimkan secara langsung ke instansi pemohon terpisah dari petugas pengambil dan digunakan sebagai konfirmasi atau bukti penyerahan data hasil *ekstraksi* dan analisa;

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

e. proses penyerahan data hasil *ekstraksi* dan analisa ini dilengkapi surat pengantar yang ditandatangani oleh Ketua ID-SIRTII;

Pasal 16

Peraturan ini mulai berlaku sejak tanggal ditetapkan.

Ditetapkan di : JAKARTA
PadaTanggal :12 Nopember 2007

DIREKTUR JENDERAL POS DAN TELEKOMUNIKASI,

Direktorat Jenderal Pos dan Telekomunikasi

BASUKI YUSUF ISKANDAR

SALINAN Peraturan ini disampaikan kepada :

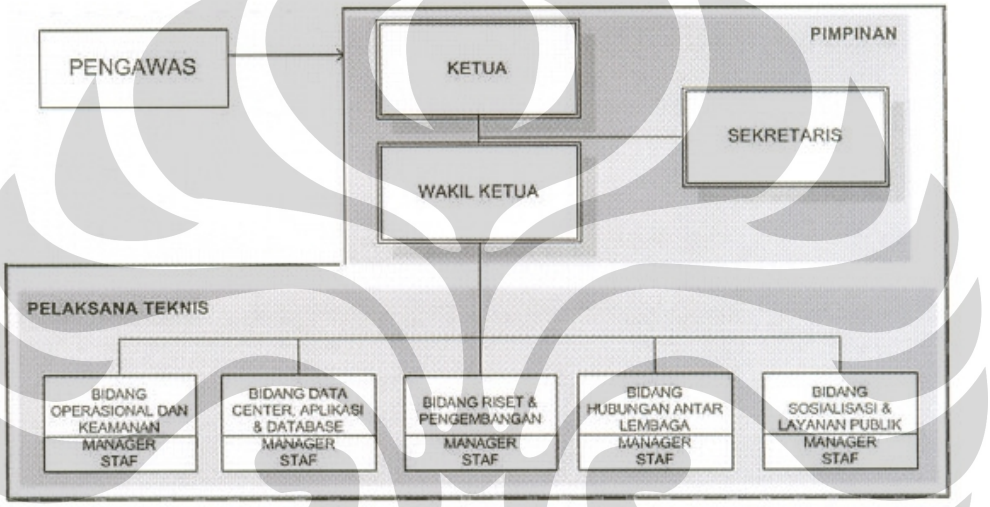
1. Menteri Komunikasi dan Informatika;
2. Sekditjen Postel;
3. Para Direktur di Lingkungan Ditjen Postel;

12

Lampiran 4: Peraturan Direktur Jendral Pos dan Telekomunikasi
Nomor 226/DIRJEN/2007
(lanjutan)

LAMPIRAN	:	PERATURAN DIREKTUR JENDERAL POS DAN TELEKOMUNIKASI
NOMOR	:	226 /DIRJEN/2007
TANGGAL	:	12 Nopember 2007

SUSUNAN ORGANISASI PENGAWAS DAN PELAKSANA *INDONESIA – SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE* (ID-SIRTII)



12