PENERAPAN MANAJEMEN KEAMANAN INFORMASI PADA *TRAFFIC MANAGEMENT CENTER* DIREKTORAT LALU LINTAS POLDA METRO JAYA DENGAN PENGENDALIAN ISO 27001:2005

T E S I S

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Sains Kajian Ilmu Kepolisian

PUNGKY BHUANA SANTOSO
0806447406

UNIVERSITAS INDONESIA
PROGRAM STUDI KAJIAN ILMU KEPOLISIAN
KEKHUSUSAN MANAJEMEN SEKURITI
JAKARTA
JUNI, 2010

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	**:**	**PUNGKY BHUANA SANTOSO**
NPM	**:**	**0806447406**
Tanda Tangan	**:**	
Tanggal	**:**	**9 Juni 2010**

HALAMAN PENGESAHAN

Tesis ini diajukan oleh:

Nama	:	PUNGKY BHUANA SANTOSO
NPM	:	0806447406
Program Studi	:	Universitas Indonesia Pasca Sarjana Kajian Ilmu Kepolisian Kekhususan Manajemen Sekuriti.
Judul Tesis	:	**Penerapan Manajemen Keamanan Informasi pada *Traffic Management Center* Direktorat Lalu Lintas Polda Metro Jaya dengan Pengendalian ISO 27001:2005**

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Sains pada Program Pasca Sarjana Kajian Ilmu Kepolisian, Universitas Indonesia.

DEWAN PENGUJI

1. **Drs.Suryadi MT.** (Pembimbing) — 1. .....
2. **Prof. Dr. Sarlito W. Sarwono, Psi.** (Penguji I) — 2. .....
3. **Prof. Drs. Koesparmono Irsan, SH, MM, MBA.** (Penguji II) — 3. .....
4. **Dr. dr. H. Hadiman, SH, M.Sc.** (Penguji III) — 4. .....

Ditetapkan di : Jakarta

Tanggal : 9 Juni 2010

KATA PENGANTAR

Alhamdulillah. Segala puji dan syukur penulis panjatkan kepada Allah SWT yang telah memberikan petunjuk dan kemudahan-Nya kepada penulis dalam menjalani kehidupan, proses belajar, penelitian dan penyelesaian penulisan tesis ini. Penulisan tesis ini merupakan salah satu syarat dalam rangka mencapai gelar Magister Sains pada Program Pascasarjana Universitas Indonesia.

Tesis ini membahas tentang manajemen keamanan sistem informasi yang dilakukan pada *Traffic Management Center* oleh Direktorat Lalu Lintas Polda Metro Jaya. Dengan latar belakang kemajuan teknologi yang berkolaborasi dengan perkembangan ilmu pengetahuan di bidang informasi yang sangat pesat telah menghasilkan terjadinya kejahatan jaringan informasi yang dikenal dengan *cyber crime.* Kondisi ini memberikan pemahaman bagi Direktorat Lalu Lintas Polda Metro Jaya melakukan kebijakan keamanan informasi untuk melindungi aset-aset informasi yang dimilikinya.

Fokus masalah pada upaya terciptanya keamanan informasi dalam operasional *Traffic Management Center* Polda Metro Jaya dengan mengimplementasikan ISO 27001:2005 sebagai standar internasional desain keamanan informasi. Penelitian ini menggunakan metode kualitatif dan pendekatan yuridis manajerial untuk memahami pengelolaan organisasi dan model keamanan informasi pada *Traffic Management Center* Polda Metro Jaya yang dituangkan ke dalam narasi dengan menggunakan metode penulisan deskriptif analitis.

Sebagai hipotesis yang dikembangkan pada tesis ini menyatakan bahwa penerapan kebijakan keamanan informasi yang dilakukan oleh Direktorat Lalu Lintas Polda Metro Jaya belum optimal untuk mengamankan aset-aset informasi yang ada pada *Traffic Management Center* Polda Metro Jaya sehingga perlu menerapkan manajemen keamanan informasi dengan mengimplementasikan pengendalian ISO 27001:2005 untuk meminimalisir ancaman dan gangguan yang terjadi.

Hasil penelitian telah diseminarkan dan disajikan ke dalam bentuk tulisan tesis secara utuh yang berisi gambaran tentang fakta-fakta atau gejala-gejala

empiris terhadap pelaksanaan kebijakan keamanan informasi yang dilakukan oleh Direktorat Lalu Lintas pada *Traffic Management Center* Polda Metro Jaya, yang telah dianalisis dengan menggunakan konsep-konsep dan teori-teori yang relevan.

Dengan selesainya penulisan tesis ini, diharapkan dapat menjadi sumbangan pemikiran atau masukan untuk menentukan kebijakan keamanan informasi Direktorat Lalu Lintas Polda Metro Jaya terhadap keamanan informasi *Traffic Management Center* Polda Metro Jaya serta masukan bagi pengembangan organisasi *Traffic Management Center* pada polda-polda lainnya di Indonesia.

Penelitian dan penulisan tesis ini dapat diselesaikan berkat bantuan, bimbingan dan motivasi dari pembimbing saya, yaitu Bapak Drs. Suryadi M.T, MT. Penulis mengucapkan rasa terima kasih yang setinggi-tingginya kepada pembimbing, dimana di tengah-tengah kesibukannya beliau masih menyempatkan diri untuk memberikan bimbingan dan petunjuk selama penelitian dan penulisan tesis ini. Ucapan terima kasih juga penulis sampaikan kepada Prof. Dr. Sarlito Wirawan Sarwono, Psi selaku Ketua Program Studi Kajian Ilmu Kepolisian Program Pascasarjana Universitas Indonesia dan seluruh dosen pengajar yang telah membimbing dan memberikan ilmu serta wawasan pengetahuan kepada penulis selama melaksanakan studi. Penulis juga menyampaikan rasa terima kasih kepada senior alumni angkatan XII, rekan-rekan angkatan XIII, mahasiswa angkatan XIV, serta seluruh staf sekretariat KIK yang telah memberikan dukungan kepada penulis selama menjadi mahasiswa sampai dengan selesainya penulisan tesis ini.

Rasa terima kasih dan penghargaan juga penulis sampaikan kepada Direktur Lalu Lintas Polda Metro Jaya Kombes. Pol. Drs. Condro Kirono, MM beserta seluruh staf Direktorat Lalu Lintas Polda Metro Jaya, Kompol. Adhie Santika, S.Ik, serta teman-teman yang tergabung dalam Tim IT TMC PMJ yang telah membantu proses pengumpulan data dan informasi selama melakukan penelitian di lapangan.

Penulis juga menyampaikan rasa terima kasih yang tulus kepada Ayahanda tercinta Kombes Pol. Drs. H. Himawan Santoso, M.Si (Alm.) dan Ibunda Hj. Isdiyanti Himawan serta kedua mertua Ayahanda R. Daryatmo Soeyudono dan Ibunda R.A. Endang Wahyu Tri Retno Hartaningsih (Almh.); dr. Kukuh Wibowo

Kustarto, SpOG sekeluarga; Rizky Bagaskara Santoso; Ibu Hj. Emy Sundari Mega sekeluarga; Hj. M. Mega Sjoukat, S.Pd; Bayu Isnawan sekeluarga, serta semua pihak yang tidak dapat penulis sebutkan satu-persatu, yang telah memberikan dorongan dan bantuan moral maupun material dalam menyusun tesis ini.

Tak lupa dengan penuh ikhlas dan bangga penulis menyampaikan rasa haru, terima kasih dan apresiasi yang sedalam-dalamnya kepada istri penulis tercinta Rr. ROSIANTI WAHYU SOVIARINI, SE serta kedua anak penulis GHAZLINA CETTAKIRANA BHUANA CHEDA dan GRIZELDA HELGAQILLA BHUANA AISYA, dimana dengan ketabahan, kesabaran, kasih sayang dan pengertiannya mereka telah memberikan doa restu, motivasi serta semangat baru kepada penulis meskipun selama proses perkuliahan mereka harus rela tinggal berjauhan dengan suami/bapak yang dicintainya.

Akhirnya saya berharap semoga Allah SWT membalas segala kebaikan bapak/ibu/saudara/saudari semua, serta senantiasa memberikan Rahmat dan Hidayah-Nya kepada kita semua. Amien..

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PEBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama	:	PUNGKY BHUANA SANTOSO
NPM	:	0806447406
Program Studi	:	Pascasarjana Kajian Ilmu Kepolisian
Jenis Karya	:	Tesis

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

Penerapan Manajemen Keamanan Informasi pada *Traffic Management Center* Direktorat Lalu Lintas Polda Metro Jaya dengan Pengendalian ISO 27001:2005

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 tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Dibuat di : Jakarta
Pada tanggal : 5 Juni 2010
Yang menyatakan,

(PUNGKY BHUANA SANTOSO)

ABSTRAK

Nama : Pungky Bhuana Santoso
Program Studi : Pascasarjana Kajian Ilmu Kepolisian
Judul Tesis : **Penerapan Manajemen Keamanan Informasi pada *Traffic Management Center* Direktorat Lalu Lintas Polda Metro Jaya dengan Pengendalian ISO27001:2005**

Tesis ini membahas tentang manajemen keamanan sistem informasi yang diterapkan oleh Direktorat Lalu Lintas Polda Metro Jaya dalam melakukan pengamanan terhadap informasi pada *Traffic Management Center*. Adanya latar belakang kemajuan teknologi yang berkolaborasi dengan perkembangan ilmu pengetahuan di bidang informasi yang sangat pesat telah malahirkan kejahatan jaringan informasi yang dikenal dengan *cyber crime*. Kondisi ini memberikan pemahaman bagi Direktorat Lalu Lintas Polda Metro Jaya melakukan kebijakan keamanan informasi untuk melindungi aset-aset informasi yang dimilikinya.

Penelitian berfokus pada upaya terciptanya keamanan informasi dalam operasional *Traffic Management Center* Polda Metro Jaya dengan mengimplementasikan ISO 27001:2005 sebagai standar internasional desain keamanan informasi. Penelitian ini menggunakan metode kualitatif dan pendekatan yuridis manajerial untuk memahami pengelolaan organisasi dan model keamanan informasi pada *Traffic Management Center* Polda Metro Jaya yang dituangkan ke dalam narasi dengan cara penulisan deskriptif analitis.

Hipotesis yang dikembangkan pada tesis ini menyatakan bahwa penerapan kebijakan keamanan informasi yang dilakukan oleh Direktorat Lalu Lintas Polda Metro Jaya belum optimal untuk mengamankan aset-aset informasi yang ada pada *Traffic Management Center* Polda Metro Jaya sehingga perlu menerapkan manajemen keamanan informasi dengan mengimplementasikan pengendalian ISO 27001:2005 untuk meminimalisir ancaman dan gangguan yang terjadi.

Berdasarkan penelitian yang telah dilakukan menjelaskan bahwa tindakan kebijakan keamanan yang dilaksanakan oleh Direktorat Lalu Lintas Polda Metro Jaya terhadap personel, fisik bangunan dan informasi pada *Traffic Management Center* Polda Metro Jaya masih tidak optimal dan sering mengalami gangguan. Belum adanya struktur organisasi yang permanen karena pengaruh faktor pengembangan organisasi dan belum ada dokumentasi standar operasional prosedur pengamanan informasi atas layanan-layanan aplikasi yang ada merupakan penyebab terjadinya gangguan keamanan terhadap aset-aset informasi tersebut. Untuk menanggulangi hal tersebut maka perlu dilakukan penerapan manajemen keamanan informasi dengan mengimplementasikan pengendalian ISO 27001:2005 agar dapat menciptakan keamanan informasi pada *Traffic Management Center* Polda Metro Jaya secara optimal.

Tesis ini menghasilkan beberapa rekomendasi berupa penentuan kebijakan keamanan, standar operasional prosedur, serta tindakan manajemen keberlangsungan bisnis terhadap *Traffic Management Center* Polda Metro Jaya agar mampu menciptakan sistem keamanan informasi secara efektif dan efisien.

Kata kunci:
Keamanan informasi, *Traffic Management Center*, ISO 27001:2005

ABSTRACT

Name : *Pungky Bhuana Santoso*
Study Program : *Pascasarjana Kajian Ilmu Kepolisian*
Thesis Title : ***Information Security Management Implementation at the Traffic Management Center, Directorate of Traffic Polda Metro Jaya with ISO 27001:2005***

This thesis discusses about the security management information system which has been implemented by the Directorate of Traffic Polda Metro Jaya in securing the information on the Traffic Management Center. With a background of technological progress in collaborating with the knowledge development in the highly developed field of information has resulted in the occurrence of crime information network known as cyber crime. These conditions provide an understanding for Directorate of Traffic Polda Metro Jaya to conduct information security policies in order to protect the information assets they have.

The research focuses on efforts to create safety information in the Traffic Management Center Polda Metro Jaya operations by implementing the ISO 27001:2005 as international standards of information security design. This study uses qualitative methods and managerial juridical approach with the intention of understanding the organization and management of information security model at the Traffic Management Center Polda Metro Jaya poured into narrative by using analytical descriptive writing method.

As a hypothesis developed in this thesis states that the application of information security policies made by Directorate of Traffic Polda Metro Jaya is not yet optimal for securing the existing information assets at the Traffic Management Center Polda Metro Jaya, therefore information security management need to be applied by implementing ISO 27001:2005 control due to minimize the threat and disruption that has been occurred.

Based on research that has been done, it is explained that the actions of the security policy implemented by Directorate of Traffic Polda Metro Jaya to personnel, physical buildings and information at Traffic Management Center Polda Metro Jaya still not optimal and often disrupted. The absence of a permanent organizational structure caused by the influence of organizational development factors and also there has been no operational standards documentation of information security procedures for the services of existing applications cause to a security disruptions to information assets within it. To solve the problem it is necessary to perform the security management application control information by implementing ISO 27001:2005 in order to create the security information on the Traffic Management Center Polda Metro Jaya optimally.

This thesis resulted in several recommendations in the form of determining the security policy, standard operating procedures and business continuity management actions against Traffic Management Center Polda Metro Jaya with the aim of being able to create information security systems effectively and efficiently.

Key word:
Security Information, Traffic Management Center, ISO 27001:2005

DAFTAR ISI

HALAMAN JUDUL i
LEMBAR PERNYATAAN ORISINALITAS ii
LEMBAR PENGESAHAN iii
KATA PENGANTAR iv
LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH vii
ABSTRAK viii
DAFTAR ISI x
DAFTAR GAMBAR xiii
DAFTAR TABEL xiv
DAFTAR LAMPIRAN xv
1. PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Masalah Penelitian 8
1.2.1. Ruang Lingkup Masalah 9
1.2.2. Fokus Penelitian 10
1.3. Hipotesis 11
1.4. Tujuan dan Manfaat Penelitian 11
1.4.1. Tujuan Penelitian 11
1.4.2. Manfaat Penelitian 12
1.5. Kajian Kepustakaan 13
1.6. Metode Penelitian 14
1.7. Tata Urut Penulisan (Sistematika Penulisan) 17

2. TINJAUAN LITERATUR 19
2.1. Literatur Teori 19
2.1.1. Teori Manajemen Keamanan Informasi 19
2.1.1.1. Strategi Keamanan Informasi 19
2.1.1.2. Manajemen Keberlangsungan Bisnis (*Business Continuity Management*-BCM) 21
2.1.2. Penerapan ISO 27001:2005 22
2.2. Literatur Konseptual 25
2.2.1. Organisasi dan Manajemen 25
2.2.2. Konsep Pengembangan Organisasi 27
2.2.3. Jaringan Komputer 29
2.2.4. *Cyber Crime* 33
2.2.5. Manajemen Sistem Informasi 36
2.2.6. Manajemen Keamanan Informasi 41
2.2.7. Strategi Keamanan Informasi 43
2.2.8. Manajemen Keberlangsungan Bisnis (*Business Continuity Management*-BCM) 51
2.2.9. ISO 27001:2005 53
2.2.10. *Traffic Management Center* (TMC) 56
2.2.11. Konsep Perpolisian Masyarakat (*Community Policing*) 58
2.2.12. Kepolisian Negara Republik Indonesia 61
2.3. Kerangka Pemikiran 66

3. GAMBARAN UMUM TMC PMJ 70
3.1. Kepolisian Daerah Metro Jaya 70
3.1.1. Visi dan Misi Polda Metro Jaya 71
3.1.2. Struktur Organisasi Polda Metro Jaya 73
3.2. Direktorat Lalu Lintas Polda Metro Jaya 75
3.3. *Traffic Management Center* Polda Metro Jaya 80

4. HASIL PENELITIAN 86
4.1. Karakteristik *Traffic Management Center* Polda Metro Jaya 87
4.1.1. Sejarah Berdirinya TMC PMJ 87
4.1.2. Penerapan Layanan Informasi pada TMC PMJ 90
4.2. Kebijakan Keamanan Informasi yang dilakukan oleh Direktorat Lalu Lintas saat ini 92
4.2.1. Kebijakan Keamanan terhadap Personel TMC PMJ 93
4.2.2. Kebijakan Keamanan terhadap Fisik Bangunan TMC PMJ 101
4.2.3. Kebijakan Keamanan terhadap Informasi TMC PMJ 110
4.3. Gangguan yang Masih Terjadi 120

5. PEMBAHASAN 124
5.1. Penerapan Manajemen Keamanan Informasi pada TMC PMJ saat ini 124
5.1.1. Karakteristik TMC PMJ 124
5.1.1.1. Bentuk Organisasi TMC PMJ 125
5.1.1.2. Aplikasi Layanan Informasi yang Diterapkan pada TMC PMJ 127
5.1.2. Kebijakan Keamanan Informasi yang telah Dilakukan 133
5.1.2.1. Kebijakan Keamanan terhadap Personel TMC PMJ 134
5.1.2.2. Kebijakan Keamanan terhadap Fisik Bangunan TMC PMJ 135
5.1.2.3. Kebijakan Keamanan terhadap Informasi TMC PMJ 136
5.2. Gangguan yang Masih Terjadi dan Penyebabnya 138
5.3. Penerapan Manajemen Keamanan Informasi pada TMC PMJ dengan Implementasi Pengendalian ISO 27001:2005 140
5.3.1. Identifikasi Ancaman yang Terjadi 141
5.3.2. Pendefinisian Resiko 144
5.3.2.1. Identifikasi Aset 145
5.3.2.2. Analisis Resiko 150
5.3.2.3. Menentukan Tindak Lanjut 154
5.3.3. Penentuan Kebijakan Keamanan 163
5.3.4. Implementasi Pengendalian ISO 27001:2005 175
5.3.5. Penerapan Manajemen Keberlangsungan Bisnis pada TMC PMJ 198

6. PENUTUP 200

6.1. Kesimpulan 200
6.2. Saran 201

Daftar Pustaka 203

Lampiran 209

DAFTAR GAMBAR

Gambar 2.1. Model Sistem secara Sederhana 37

Gambar 2.2. Sistem Komputer Beserta Interface 37

Gambar 2.3. Transformasi Data Menjadi Informasi 39

Gambar 2.4. Hubungan Antara Resiko, Ancaman,Kerentanan dan Aset Organisasi 48

Gambar 2.5. Keterkaitan Unsur Strategi Keamanan Informasi 51

Gambar 2.6. Skema Diagram Proses ISMS dengan Menerapkan PDCA 56

Gambar 2.7. Kerangka Pemikiran Penerapan Manajemen Keamanan Informasi pada TMC PMJ dengan Pengendalian ISO 27001:2005 69

Gambar 3.1. Struktur Organisasi Ditlantas Polda Metro Jaya 77

Gambar 4.1 Konsep Pengembangan Organisasi Ditlantas Polda Metro Jaya 94

Gambar 4.2. *Barrier* Pintu Masuk Utama TMC PMJ 102

Gambar 4.3. Ruangan Dalam TMC PMJ 104

Gambar 4.4. Denah Ruangan TMC PMJ 105

Gambar 4.5. Fire Extinguisher dan CCTV di ruangan utama TMC PMJ..... 107

Gambar 4.6. Ruangan Penyimpanan Server TMC PMJ 108

Gambar 4.7. Ruangan Analisis Jaringan TMC PMJ 110

Gambar 4.8. Aplikasi Jaringan Komputer pada TMC PMJ 113

Gambar 5.1. Skema Arus Informasi dalam Fungsi Komando pada TMC PMJ 128

Gambar 5.2. Skema Arus Informasi dalam Fungsi Komunikasi pada TMC PMJ 130

Gambar 5.3. Skema Arus Informasi dalam Fungsi Koordinasi pada TMC PMJ 132

DAFTAR TABEL

Tabel 2.1. Jaringan Komputer Berdasarkan Area 31

Tabel 2.2. Klasifikasi Nilai Ancaman 45

Tabel 2.3. Mitigasi Terhadap Resiko Saat Ini 49

Tabel 2.4. Nilai Likelihood 49

Tabel 2.5. Penjelasan Proses ISMS dengan Menerapkan PDCA 56

Tabel 3.1. Daftar Kekuatan Polri Ditlantas Polda Metro Jaya Bulan Februari 2010 79

Tabel 4.1. Daftar Perangkat Keras Jaringan TMC PMJ 110

Tabel 4.2. Daftar Perangkat Lunak jaringan TMC PMJ 112

Tabel 5.1. Kebijakan Keamanan Personel pada TMC PM 135

Tabel 5.2. Kebijakan Keamanan Fisik Bangunan pada TMC PMJ 136

Tabel 5.3. Kebijakan Keamanan Informasi pada TMC PMJ 136

Tabel 5.4. Klasifikasi Nilai Ancaman pada TMC PMJ 143

Tabel 5.5. Identifikasi Aset Informasi pada TMC PMJ 146

Tabel 5.6. Penilaian Kerentanan terhadap Aset TMC PMJ 148

Tabel 5.7. Nilai Dampak (*Impact Value*) terhadap Aset TMC PMJ 150

Tabel 5.8. Tabel Penentuan *Risk Level* berdasarkan *Impact Value* 155

Tabel 5.9. Penentuan *Inherent Risk* Terhadap *Impact Value* Aset TMC PMJ 155

Tabel 5.10. *Inherent Risk* terhadap Kebijakan Keamanan yang Telah Dilakukan 159

Tabel 5.11. Hasil Inherent Risk dengan Implementasi ISO 27001:2005 162

DAFTAR LAMPIRAN

Lampiran 1	Surat Perintah Penelitian di Ditlantas Polda Metro Jaya	209
Lampiran 2	Dokumentasi selama Penelitian	210
Lampiran 3	Struktur Organisasi Ditlantas Polda Metro Jaya berdasarkan Keputusan Kapolri No.Pol.: Kep/07/I/2005 tanggal 31 Januari 2005	213
Lampiran 4	Daftar Kekuatan Polri Ditlantas Polda Metro Jaya Bulan Februari 2010	214
Lampiran 5	Ajuan Pengembangan Struktur Organisasi Ditlantas Polda Metro Jaya	215
Lampiran 6	Surat Perintah Dirlantas Polda Metro Jaya Nomor:Sprin/ 39/I/2010/Ditlantas tentang Penunjukan Operator Operasional TMC PMJ	216
Lampiran 7	Absensi Regu Jaga Personel TMC PMJ	220
Lampiran 8	Rekapitulasi Laporan Masyarakat ke TMC PMJ 1x24 Jam	222
Lampiran 9	Laporan Harian TMC PMJ tentang Situasi Kamseltibcar Lantas	223
Lampiran 10	Kendala dan Saran dari Masing-Masing Operator TMC PMJ	230

BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam beberapa dasawarsa belakangan ini penggunaan teknologi informasi dan telekomunikasi telah menyentuh segi kehidupan dan penghidupan baik pada tingkat individual, kelompok, maupun semua jenis organisasi pada tingkat negara maupun dalam hubungan antarorganisasi antarnegara. Ini menunjukkan bahwa teknologi di bidang informasi dan telekomunikasi telah berkembang dengan sangat pesat dalam masyarakat modern.

Fenomena tersebut berawal ketika para ahli pada tahun 70-an menemukan komputer mini yang mempunyai ukuran lebih kecil dibandingkan dengan *mainframes* yang besar. Hasil temuan ini merupakan suatu proses evolusi perangkat keras komputer yang menjadi titik awal perubahan dramatis pada perkembangan sistem informasi dan komunikasi di dunia. Dengan temuan tersebut maka peranan komputer *mainframe* yang populer bagi kalangan pengguna ilmiah dan perusahaan serta organisasi besar, seperti yang digunakan pada Biro Sensus AS (*U.S. Census Bureau*) pada tahun 1951 dan pada perusahaan *General Electric* tahun 1954, tergantikan dengan komputer mini yang ditujukan kepada perusahaan kecil maupun komputer mikro untuk para pengguna individual yang dikenal sebagai *Personal Computer* atau PC (Mc.Leod & P.Schell, 2008). Proses evolusi ini sering disebut oleh para ahli sebagai era awal perkembangan komputer dalam masyarakat modern.

Seiring dengan perkembangan peradaban masyarakat modern maka mulai muncul kolaborasi antara perkembangan komputer dengan kemajuan teknologi di bidang informasi dan komunikasi. Kolaborasi ini akhirnya mempu menciptakan teknologi baru berupa sistem komunikasi antarkomputer digital yang sangat cepat secara *virtual* (internet). Dengan melakukan akses data informasi tanpa harus berhubungan secara langsung (*virtual*) tentunya akan memberikan *benefit* dan mendukung perkembangan organisasi berkaitan dengan efektifitas dan efisiensi operasionalnya.

Selain berdampak positif terhadap perkembangan organisasi, teknologi baru tersebut juga menghasilkan kontribusi yang sangat signifikan dalam kehidupan sehari-hari masyarakat modern. Aplikasinya dalam masyarakat pun menjadi beragam. Dunia perbankan, bursa saham, kontrol lalu lintas udara, telepon, tenaga listrik, lembaga kesehatan, keamanan, serta pendidikan merupakan beberapa contoh organisasi kemasyarakatan yang sebagian bergantung pada teknologi informasi dan telekomunikasi untuk mendukung kegiatan operasionalnya.

Di sisi lain, teknologi tesebut juga menyumbangkan dampak negatif yang dimanfaatkan oleh para pelaku kejahatan jaringan informasi untuk melakukan aksi kejahatannya. Dengan memanfaatkan internet sebagai media pendukung untuk melakukan akses data secara ilegal, maka para pelaku kejahatan jaringan informasi dan komunikasi menyempurnakan kejahatan konvensional yang sebelumnya telah ada. Tidak jarang merekan melakukan akses data informasi secara ilegal terhadap sasaran yang diinginkan untuk mendapatkan keuntungan material maupun immaterial. Aksi kejahatan ini disebut sebagai *cyber crime* (Mustofa, 2007). Sebagai contoh berikut ini dijelaskan tiga peristiwa aktual yang berkaitan dengan aksi *cyber crime*, sebagai berikut:

Estonia, negara kecil di Eropa yang pernah bergabung dengan Uni Soviet, pada bulan April-Mei 2007 dibuat lumpuh oleh ulah jutaan *zombie cyber* ciptaan robot *network* atau botnet. Kelumpuhan itu meliputi operasional pemerintahan, perbankan, hingga aktivitas warga. Perang *cyber* di Estonia tersebut disulut oleh keputusan pemerintah untuk memindahkan sebuah patung perunggu peringatan perang Soviet di ibu kota Estonia, Tallinn. Pemindahan itu menuai protes Rusia dan menimbulkan kerusuhan di antara etnis Rusia di Estonia. ("Forum-Pembaca-Kompas", 2009).

Peristiwa aktual lainnya yang terjadi berkaitan dengan isu keamanan jaringan informasi adalah tentang kasus ***hacker*** mencuri data 130 juta kartu kredit dan debit di Amerika yang merupakan kasus pencurian terbesar di dalam sejarah Amerika. Tindak kejahatan ini dilakukan oleh 3 (tiga) orang pelaku dengan cara melakukan konspirasi untuk mendapatkan akses ilegal ke komputer-komputer, melakukan penipuan dengan menggunakan koneksi komputer, serta perusakan

sistem komputer. Para pelaku kejahatan menggunakan teknik peretasan SQL *Injection* untuk menjebol *firewall* jaringan-jaringan perusahaan selanjutnya mereka mencuri data-data yang berisi tentang rahasia perusahaan antara 2006 hingga 2008. Mereka menargetkan perusahaan-perusahaan besar yang termasuk dalam daftar 500 perusahaan besar versi majalah Fortune untuk dijelajahi secara ilegal terhadap laman-laman perusahaan tersebut sebelum menerobos masuk dan mencuri informasi-informasi penting dari perusahaan tersebut yang berkaitan dengan penggunaan dan pembelanjaan ilegal terhadap kartu debit atau kredit tersebut. Akhirnya informasi tersebut mereka jual dengan cara mengirim kepada para pembeli yang menginginkannya melalui *server* ("Vivanews", 2009).

Aksi *cyber crime* yang dilakukan oleh pelaku kejahatan jaringan informasi dan komunikasi juga terjadi di Indonesia. Beberapa waktu yang lalu situs TNP Komisi Pemilihan Umum (KPU) juga dibobol oleh pelaku *cyber crime*. Pelaku melakukan aksinya dengan melakukan penyerangan ke *server* tnp.kpu.go.id dengan cara SQL (*Structure Query Language*) *Injection* dan berhasil menembus kunci pengaman *Internet Protocol* (IP) tnp.kpu.go.id. Setelah berhasil menembus kunci pengaman IP, selanjutnya pelaku menganalisis kembali variable-variabel yang ada di situs http://tnp.kpu.go.id dan melakukan penambahan kode SQL secara ilegal sehingga berhasil melakukan perubahan tampilan nama partai di situs resmi TNP KPU. Perubahan ini menyebabkan nama partai yang tampil pada situs yang diakses oleh publik setelah Pemilu Legislatif berubah menjadi nama-nama lucu, seperti Partai Jambu, Partai Kelereng, Partai Cucak Rowo, Partai Si Yoyo, Partai Mbah Jambon, Partai Kolor Ijo, dan sebagainya (*Seni Internet*, 2008).

Ketiga contoh kasus kejahatan yang telah terjadi di atas merupakan bukti bahwa *cyber crime* telah terjadi secara global yang tidak hanya terjadi di negara lain saja tetapi juga telah menimpa negara Indonesia. Suryadi (2009) menemukan bahwa kasus *cyber crime* di Indonesia dalam periode Januari hingga Agustus 2004 diduga telah menimbulkan kerugian materi bagi korbannya senilai lebih dari US$.4,3 juta. Jumlah kerugian ini mengalami peningkatan dibandingkan dengan tahun 2003 dengan nilai kerugian US$.1,2 juta. Data ini mengindikasikan bahwa telah terjadi peningkatan kerugian materi dari korban kejahatan yang dilakukan

oleh pelaku kejahatan jaringan informasi dan komunikasi di Indonesia dengan motif *cyber crime*.

Beberapa "kemudahan" yang didapati oleh para pelaku *cyber crime* untuk melakukan aksi kejahatannya tersebut mengakibatkan jumlah kejadian *cyber crime* meningkat dengan pesat secara global. Felson dan Cohen (1963) melalui *routine activities theory* memberikan pandangannya tentang terjadinya *cyber crime*, dimana kejahatan akan terjadi bila dalam suatu tempat dan waktu hadir secara bersamaan 3 (tiga) elemen yang mendukung pelaku melakukan kejahatan. Elemen tersebut adalah: (a) *A motivated offender* (penjahat yang termotivasi); (b) *a suitable target* (target atau sasaran kejahatan yang menarik dan mudah); serta (c) *the absence of capable guardian* (kondisi yang aman untuk melakukan kejahatan) (Saile et al., 2008, p. 57).

Dalam kasus *cyber crime*, pelaku kejahatan digerakkan untuk melakukan aksinya oleh motivasi yang tinggi untuk mencapai tujuannya. Menurut Suryadi (2009), unsur motivasi utama yang melatarbelakangi terjadinya *cyber crime* adalah adanya ketamakan, nafsu, kekuasaan, pembalasan, petualangan, dan keinginan untuk mencicipi "buah terlarang". Latar belakang ini akan menghasilkan suatu kepuasan tesendiri bagi para pelaku *cyber crime*, disamping keuntungan berupa materi secara ilegal, apabila kemampuan yang dimiliki oleh pelaku kejahatan ini mengakibatkan suatu dampak pada sistem-sistem besar sehingga mengakibatkan kerusakan maupun kerugian terhadap organisasi maupun individu.

Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi juga mengakibatkan hubungan dunia menjadi tanpa batas *(borderless)* sehingga terjadi perubahan secara cepat dan signifikan dalam bidang sosial, ekonomi dan budaya. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Pemanfaatan internet sebagai sarana untuk mendukung aksi kejahatan, para pelaku kejahatan jaringan informasi dan komunikasi menjadikan *cybercrime*

sebagai *borderless crime*. Mereka tidak mengenal batas wilayah dan waktu kejadian ketika sedang menjalankan aksinya terhadap korban yang tidak jarang berada di negara yang berbeda dengan pelaku kejahatan. Kondisi ini mengakibatkan para pelaku kejahatan ini merasa selalu dalam situasi yang aman dalam melakukan kejahatannya. Semua ini dilakukan hanya di depan komputer yang memiliki akses internet tanpa takut diketahui oleh orang lain sebagai saksi mata.

Uraian tentang kejahatan *cyber crime* tersebut menunjukkan bahwa saat ini kejahatan dengan menggunakan internet sebagai sarana pendukung utama para pelaku kejahatan dalam melakukan aksinya telah semakin berkembang. Pertumbuhan eksponensial dalam konektifitas komputansi dan komunikasi telah menciptakan kesempatan-kesempatan yang paralel untuk calon pelaku kejahatan serta diiringi dengan resiko-resiko paralel untuk calon korbannya. Walaupun produk hukum serta tindakan represif yang dilakukan oleh petugas kepolisian telah dilaksanakan, namun kejahatan ini masih tetap terjadi. Beberapa contoh kasus di atas telah memberi pelajaran bagi masyarakat modern, bahwa *cyber crime* dengan cara melakukan akses informasi secara ilegal merupakan ancaman serius dan bisa mengakibatkan kerugian yang sangat luar biasa terhadap negara, organisasi maupun individu. Implikasinya, isu keamanan terhadap jaringan informasi dan komunikasi menjadi perhatian serius bagi para pemerhati keamanan.

Saat ini masyarakat modern yang dikenal sebagai masyarakat informasional mengetahui arti pentingnya peranan teknologi informasi dalam kehidupan di era informasi. Masyarakat modern juga mulai memahami untuk menjaga seluruh sumberdaya mereka, baik secara fisik, personel, maupun yang bersifat *virtual,* agar aman dari segala ancaman baik dari dalam maupun dari luar. Dengan adanya kontribusi akan perkembangan kemajuan teknologi informasi yang sangat substansial tersebut telah menimbulkan kesadaran pada berbagai pihak akan pentingnya informasi sebagai salah satu sumber daya organisasi yang utama (Siagian, 2001)

Sebagai salah satu sumber daya organisasi *virtual* yang utama, informasi menjadi aset penting dari suatu organisasi yang juga harus diamankan. Upaya

bidang keamanan ini dilakukan untuk meminimalisasi terjadinya ancaman maupun gangguan terhadap sistem pengamanan perusahaan (*industrial security*), terutama terhadap gangguan kejahatan (*crime prevention*) maupun juga pencegahan kerugian (*loss prevention*) terhadap keamanan jaringan informasi.

Djamin (2008) menyatakan bahwa pada sektor modern, sistem pengamanan perusahaan (*industrial security*) adalah merupakan tanggung jawab dari pengelola perusahaan yang dilaksanakan secara swakarsa baik terhadap kawasan/lokasi, bangunan/instalasi, personel, maupun akses informasi yang ada di dalamnya. Lebih lanjut dikatakan oleh Djamin bahwa ruang lingkup dari *industrial security* ini salah satu diantaranya adalah *information security*.

Pemanfaatan teknologi informasi sebagai salah satu sumberdaya organisasi adalah untuk mendukung pelaksanaan tugas pokok juga dilakukan oleh Polri dalam rangka peningkatan pelayanan publik. Upaya tersebut merupakan penjabaran fungsi dan peranan Polri sebagai aparatur negara pengemban fungsi keamanan di negara Indonesia dengan mengedepankan upaya pre-emptif dan preventif daripada represif. Dilaksanakannya pelayanan samsat dan pelayanan BPKB secara *online* untuk area Jakarta Raya yang terletak di Kompleks Polda Metro Jaya merupakan bukti bahwa penggunaan teknologi informasi telah diterapkan dalam institusi Polri ("Layanan BPKB", 2009).

Selain pelayanan samsat BPKB yang dilakukan secara *online* di atas, maka saat ini Polri sedang mengembangkan sistem pelayanan publik dengan berbasis informasi secara *online*. Model pengembangan sistem pelayanan publik dengan memanfaatkan kemajuan teknologi dan informasi yang saat ini menjadi isu utama di wilayah Jakarta adalah operasionalisasi *Traffic Management Center* Polda Metro Jaya (TMC PMJ).

Pada hakekatnya TMC PMJ merupakan implementasi atas penyelenggaaraan UU No. 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan sebagai Pusat Kendali Sistem Informasi Lalu Lintas dan Angkutan Jalan di Jakarta Raya. Berkaitan dengan tugas-tugas kepolisian di bidang lalu lintas maka polisi lalu lintas juga mempunyai fungsi dan peran sebagai penyelenggaran Pusat K3I (Komunikasi, Koordinasi, dan Kendali Informasi) di Indonesia. Fungsi dan peranan ini merupakan perluasan fungsi dan peranan Polri di bidang lalu lintas

dan angkutan jalan terhadap perudang-undangan lalu lintas yang berlaku sebelumnya. Apabila mendasari dari perluasan fungsi dan peranan tersebut maka secara strategis berarti kemungkinan akan dibangun TMC lainnya di lingkungan Mabes Polri maupun polda-polda lainnya di Indonesia.

TMC PMJ dibangun dengan menggunakan teknologi komputer yang terintegrasi secara *online* sehingga merupakan sarana penunjang pelaksanaan tugas petugas Polri di jajaran Polda Metro Jaya. Sarana ini dapat digunakan untuk mengirimkan dan menerima informasi secara *real time* sehingga membantu kecepatan informasi yang disampaikan kepada seluruh pihak yang berkepentingan (*stake holder*), baik secara internal untuk petugas Polantas maupun secara eksternal kepada masyarakat umum.

Secara internal bagi petugas Polantas, TMC PMJ bermanfaat untuk mengetahui perkembangan situasi lalu lintas di seluruh wilayah Jakarta secara *real time* selama 24 jam sehari dan 7 hari seminggu sehingga petugas Polantas dapat mengetahui situasi lalu lintas terkini di seluruh wilayah Jakarta dan akan segera mendeteksi apabila terjadi gangguan atau permasalahan lalu lintas yang saat itu terjadi serta memberikan tindakan kepolisian secara cepat, efektif dan efisien untuk mengantisipasinya. Selain itu TMC PMJ bagi masyarakat umum berfungsi untuk memberikan informasi akurat dan *real time* kepada masyarakat secara *online* berkaitan dengan permasalahan lalu lintas.

Dalam pelaksanaan operasionalnya sebagai sarana penunjang pelaksanaan tugas petugas Polri di jajaran Polda Metro Jaya serta pemberian informasi secara akurat dan *real time* kepada masyarakat secara *online* berkaitan dengan permasalahan lalu lintas, ternyata TMC PMJ juga tidak terlepas dari gangguan kejahatan *cyber crime* yang merusak website TMC PMJ beberapa waktu yang lalu. Pada salah satu berita online menyebutkan bahwa pada tanggal 9 September 2008 website TMC PMJ dirusak oleh *cracker* sehingga tampilan website berubah dan mengakibatkan semua kegiatan operasional TMC PMJ menjadi lumpuh hingga beberapa hari. *Website* TMC PMJ yang biasanya menginformasikan kondisi lalu lintas menjadi berubah tampilan menjadi putih dan dipenuhi oleh berbagai kalimat hinaan terhadap korps kepolisian berbahasa Inggris. ("Detikinet.com, 2008).

Sebagai pengelola Pusat Kendali Sistem Informasi Lalu Lintas di wilayah Jakarta Raya maka Direktorat Lalu Lintas Polda Metro Jaya tentu saja harus mampu menciptakan sistem pengamanan terhadap informasi/data elektronik yang dikelolanya sehingga secara efektif dan efisien bisa mencegah terjadinya ancaman dan gangguan kejahatan baik secara eksternal maupun internal. Untuk itu diperlukan langkah-langkah antisipatif dalam melakukan pengamanan TMC PMJ khususnya berkaitan dengan keamanan informasi yang berada di dalamnya. Salah satu cara yang dilakukan dalam menghadapi dampak negatif akan perkembangan teknologi informasi dan telekomunikasi adalah dengan menyusun suatu *blue print* rumusan strategis mengenai kebijakan keamanan informasi terhadap pengelolaan TMC PMJ dengan berdasarkan pengendalian ISO 27001:2005 sebagai standar internasional terhadap keamanan informasi.

Penerapan standar internasional atas keamanan informasi pada TMC PMJ ini perlu dilakukan guna meminimalkan terjadinya ancaman dan gangguan yang diprakirakan terjadi. Disamping mempunyai *database* yang berisi tentang data dan informasi penting tentang registrasi dan identifikasi semua kendaraan bermotor di Jakarta yang disimpan di dalam *server*, TMC PMJ juga berfungsi untuk memberikan pelayanan informasi dengan mengutamakan prinsip kerahasiaan, ketersediaan, dan integritas terhadap keamanan informasi yang diberikan kepada masyarakat sebagai konsekuensi logis atas penyelenggaraan pusat K3I di wilayah Jakarta Raya.

Penelitian yang saya lakukan mengenai Penerapan Manajemen Keamanan Informasi dengan pengendalian ISO 27001:2005 pada *Traffic Management Center* di Polda Metro Jaya ini dapat digunakan sebagai masukan bagi Polri, khususnya Direktorat Lalu Lintas Polda Metro Jaya, sebagai masukan dalam rangka menyempurnakan suatu standar operasional prosedur keamanan terhadap informasi yang telah ada pada TMC PMJ.

1.2. Masalah Penelitian

Berangkat dari penjelasan teoritis maupun konsep-konsep yang digunakan serta latar belakang yang telah disampaikan sebelumnya, maka masalah dalam

penelitian ini adalah bagaimana penerapan manajemen keamanan informasi secara efektif dan efisien pada *Traffic Management Center* Polda Metro Jaya yang dilakukan oleh Direktorat Lalu Lintas Polda Metro Jaya dengan mengimplementasikan pengendalian ISO 27001:2005 sebagai standar internasional desain keamanan informasi sehingga mampu menciptakan desain keamanan informasi secara optimal.

1.2.1. Ruang Lingkup Masalah

Ruang lingkup masalah penelitian ini dibatasi pada penerapan manajemen keamanan informasi pada TMC PMJ yang dilakukan oleh Direktorat Lalu Lintas Polda Metro Jaya selaku pelaksana operasional. Melalui penerapan manajemen keamanan informasi ini diharapkan TMC PMJ dapat mewujudkan tiga tujuan utama dari keamanan informasi, yaitu kerahasiaan dan keutuhan serta mempunyai ketersediaan terhadap data sehingga informasi di dalamnya akurat, handal, dan dapat mencegah modifikasi data oleh pihak lain yang tidak berwenang.

Batasan masalah yang pertama adalah mengetahui penerapan manajemen keamanan informasi dalam bentuk tindakan keamanan informasi yang telah dilakukan oleh Ditlantas Polda Metro Jaya untuk melakukan kegiatan keamanan terhadap aset-aset informasi yang terdapat di dalam TMC PMJ, serta gangguan apa saja yang terjadi pada TMC PMJ.

Kemudian batasan selanjutnya adalah mengenai penyebab terjadinya gangguan tersebut walaupun manajemen keamanan informasi telah diterapkan oleh Ditlantas Polda Metro Jaya terhadap informasi sensitif yang terdapat pada TMC PMJ.

Batasan yang ketiga adalah mencari penerapan manajemen keamanan informasi yang ideal dengan mengimplementasikan pengendalian ISO 27001:2005 sebagai standar internasional desain keamanan informasi agar menghasilkan keamanan informasi yang optimal terhadap pelayanan operasional TMC PMJ dalam bidang lalu lintas di wiayah Jakarta Raya secara *online* baik secara internal Polantas maupun secara eksternal kepada masyarakat. Pada batasan ini diharapkan akan menghasilkan standar operasional prosedur yang berguna sebagai sarana pengendalian dan akuntabilitas atas aktifitas operasional

TMC PMJ sehingga dapat mencapai tujuan yang telah ditetapkan sebelumnya. Selain itu juga diharapkan akan menghasilkan penerapan manajemen keberlangsungan bisnis (*Business Continuity Management*-BCM) pada TMC PMJ. BCM merupakan suatu kegiatan aktifitas yang akan dilakukan TMC PMJ apabila terjadi gangguan sistem informasi sehingga gangguan yang terjadi itu tidak terlalu berpengaruh pada kegiatan operasionalnya dan tetap dapat melaksanakannya secara aman.

1.2.2. Fokus Penelitian

Beranjak dari konsepsi di atas, maka fokus penelitian ini adalah mengenai penerapan manajemen keamanan terhadap informasi pada *Traffic Manajement Center* (TMC) oleh Direktorat Lalu Lintas Polda Metro Jaya untuk menciptakan arsitektur keamanan atas data informasi yang terdapat di dalamnya. Agar dapat menciptakan suatu standar operasional prosedur tentang keamanan informasi yang diterapkan dalam operasional TMC PMJ maka perlu mengimplementasikan ISO 27001:2005 sebagai standar internasional desain keamanan informasi.

Untuk dapat menjawab masalah penelitian ini maka penulis menjabarkan menjadi beberapa pertanyaan penelitian, yaitu:

a. Apakah model manajemen keamanan terhadap informasi yang telah diterapkan oleh Direktorat Lalu Lintas Polda Metro Jaya saat ini telah optimal dalam mengamankan aset informasi yang berada di dalam TMC PMJ?
b. Gangguan apa sajakah yang masih terjadi setelah dilakukan manajemen keamanan informasi pada TMC PMJ oleh Direktorat Lalu Lintas Polda Metro Jayadan apa penyebabnya?
c. Bagaimanakah model manajemen keamanan terhadap informasi yang ideal pada TMC PMJ dengan mengimplementasikan pengendalian ISO 27001:2005 sebagai standar internasional desain keamanan informasi sehingga tercipta keamanan yang optimal terhadap informasi yang berada di dalamnya?

1.3. Hipotesis

Bertolak dari fokus penelitian di atas, maka hipotesis yang dikembangkan dalam penelitian ini adalah saat ini Ditlantas Polda Metro Jaya telah menerapkan manajemen keamanan informasi terhadap informasi yang dimiliki oleh TMC PMJ, namun penerapan tersebut dirasakan belum optimal yang ditunjukkan dengan masih adanya gangguan yang terjadi pada TMC PMJ. Apabila Direktorat Lalu Lintas Polda Metro Jaya selaku pengelola TMC telah menerapkan manajemen keamanan informasi dengan menggunakan implementasi pengendalian ISO 27001:2005 sebagai standard internasional desain keamanan informasi, maka upaya ini akan meminimalkan terjadinya ancaman dan gangguan terhadap keamanan sistem *database* informasi pada TMC PMJ baik terhadap gangguan kejahatan (*crime prevention*) maupun juga pencegahan kerugian (*loss prevention*).

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Secara umum penelitian ini bertujuan untuk mendalami proses dan memahami deskripsi perlunya melakukan manajemen keamanan terhadap sistem informasi TMC PMJ yang dikelola oleh Ditlantas Polda Metro Jaya dengan mengimplementasikan pengendalian ISO 279001:2005 sehingga dapat mencegah dan mengurangi resiko terjadinya ancaman dan gangguan pada informasi yang terdapat padaTMC PMJ.

Secara khusus untuk menunjukkan penerapan manajemen keamanan informasi dan implementasinya terhadap pelaksanaan operasional *Traffic Manajement Center* (TMC) yang dikelola oleh Ditlantas Polda Metro Jaya. Oleh karena itu secara lebih rinci dijelaskan bahwa penelitian ini berupaya untuk mendeskripsikan mengenai:

a. Model manajemen keamanan terhadap informasi pada TMC PMJ yang saat ini telah diterapkan oleh Direktorat Lalu Lintas Polda Metro Jaya.

b. Gangguan yang masih terjadi setelah dilakukan manajemen keamanan informasi pada TMC PMJ oleh Direktorat Lalu Lintas Polda Metro Jayadan penyebabnya.
c. Model manajemen keamanan terhadap informasi pada TMC PMJ dengan mengimplementasikan pengendalian ISO 27001:2005 sebagai standar internasional desain keamanan informasi sehingga tercipta keamanan yang optimal terhadap informasi yang berada di dalamnya.

1.4.2. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat yang berarti baik dari segi teoritis maupun praktis. Secara teoritis, hasil penelitian ini diharapkan dapat memberikan pemahaman akan semakin pentingnya pengamanan sistem informasi yang saat ini dipandang telah menjadi salah satu sumber daya bagi organisasi. Juga diharapkan menjadi *blue print* atas model arsitektur keamanan informasi dan implementasinya dalam rangka pengembangan pelayanan *Traffic Manajement Center* (TMC) pada masa yang akan datang. Serta memperkaya dan memperkuat khasanah teori pengamanan sistem informasi yang telah ada, khususnya pada pengamanan database sistem informasi di TMC PMJ.

Signifikansi penelitian ini secara praktis diharapkan dapat memberi kontribusi, yang meliputi:

a. Mengetahui bagaimana model manajemen keamanan terhadap informasi pada TMC PMJ yang saat ini telah diterapkan oleh Direktorat Lalu Lintas Polda Metro Jaya.
b. Mengetahui bentuk gangguan yang masih terjadi setelah dilakukan manajemen keamanan informasi pada TMC PMJ oleh Direktorat Lalu Lintas Polda Metro Jayadan penyebabnya.
c. Mengetahui bagaimana model manajemen keamanan terhadap informasi pada TMC PMJ dengan mengimplementasikan pengendalian ISO 27001:2005 sebagai standar internasional desain keamanan informasi sehingga tercipta keamanan yang optimal terhadap informasi yang berada di dalamnya.

1.5. Kajian Kepustakaan

Dalam pustaka yang terdahulu terdapat penelitian yang berkaitan dengan tema yang akan saya teliti, yaitu *Traffic Manajemen Center*. Bakharuddin (2009) dalam desertasinya tentang Manajemen Polantas Polda Metro Jakarta Raya, melakukan penelitian terhadap pola manajerial polisi lalu lintas (polantas) di Polda Metro Jaya. Lebih lanjut dikatakannya bahwa dalam pelaksanaan tugasnya terdapat hubungan yang saling mempengaruhi secara timbal balik antara Polantas dangan lingkungan masyarakat sebagai bagian dari *stake holder* bidang lalu lintas yang saling mendukung. Saling pengaruh tersebut, menurut Bakharuddin, muncul karena didorong kekuatan polisi untuk melakukan pemolisian dan adanya kebutuhan maupun dorongan dari masyarakat untuk mendapatkan rasa aman di wilayah Polda Metro Jaya.

Fokus dari desertasi ini adalah TMC PMJ sebagai implementasi Polmas atau *Community Policing* dalam tataran operasional polantas sebagai bagian dari upaya pelayanan prima terhadap masyarakat dalam lingkup kesatuan Polda Metro Jaya. Walaupun demikian, penelitian yang dilakukan oleh Bakharuddin tersebut belum mencakup aspek pengamanan terhadap sistem informasi yang terdapat di dalam *Traffic Manajemen Center*, penelitian tersebut masih berkaitan dengan pokok bahasan tentang pola manajemen yang dilakukan oleh Polantas Polda Metro Jakarta Raya.

Selain penelitian yang dilakukan oleh Bakharuddin, juga terdapat penelitian yang berkaitan dengan sistem keamanan informasi. Kurnia (2006) dalam tesisnya tentang Perencanaan Kebijakan Keamanan Informasi Berdasarkan *Information Security Management System* (ISMS) ISO 27001 Studi Kasus Bank XYZ, melakukan penelitian tentang perencanaan kebijakan keamanan informasi terhadap Bank XYZ untuk mendapatkan suatu tata kelola keamanan informasi. Tata kelola keamanan informasi itu bertujuan untuk melakukan pencegahan terjadinya pelanggaran keamanan maupun penyalahgunan sumber daya informasi berbasis ISO 27001:2005.

Sebagai langkah awal untuk mendapatkan bentuk keamanan informasi terhadap Bank XYZ maka Kurnia melakukan perencanaan kebijakan keamanan informasi sesuai dengan prinsip atau standar internasional. Kemudian langkah

selanjutnya melakukan manajemen resiko untuk mengidentifikasi, mengukur, memantau dan mengendalikan resiko yang diperkirakan terjadi. Sebagai tindak lanjut dari analisis resiko maka Kurnia melakukan tindakan kontrol untuk mengelola dan menangani resiko tersebut sehingga obyektif kontrol dapat digunakan sebagai petunjuk perencanaan kebijakan keamanan di Bank XYZ.

1.6. Metode Penelitian

Nasir (2003) menyatakan bahwa metode penelitian merupakan bagaimana secara berurut suatu penelitian dilakukan. Lebih lanjut dikatakannya bahwa metode penelitian berhubungan erat dengan desain penelitian, prosedur serta alat yang digunakan untuk melakukan penelitian.

Desain penelitian dimulai dengan melakukan pemilihan paradigma penelitian. Creswell (2002) menyatakan bahwa paradigma penelitian kualitatif merupakan sebuah proses penyelidikan untuk memahami masalah sosial atau masalah manusia, berdasarkan penciptaan gambaran holistik lengkap yang dibentuk dengan kata-kata, melaporkan pandangan informan secara terperinci, dan disusun dalam sebuah latar alamiah.

Pandangan tersebut dikuatkan oleh Parsudi (1994) yang mendefinisikan bahwa paradigma penelitian kualitatif merupakan pendekatan penelitian untuk memperoleh data mengenai pola-pola yang ada, sesuai dengan sasaran atau masalah penelitian, diperlukan informasi yang selengkap dan sedalam mungkin mengenai gejala-gejala yang ada dalam obyek yang diteliti. Gejala tersebut dapat dilihat sebagai suatu satuan-satuan yang masing-masing berdiri sendiri tetapi saling berkaitan sebagai suatu kesatuan yang bulat dan menyeluruh.

Paradigma penelitian yang digunakan dalam tesis ini adalah paradigma penelitian kualitatif dengan pendekatan yuridis manajerial. Paradigma ini digunakan untuk menemukan, mengangkat, memahami serta mendeskripsikan segala hal yang berkaitan dengan aturan-aturan pengelolaan pada organisasi dan model keamanan informasi pada TMC PMJ secara komprehensif dan holistik dengan cara mengumpulkan data dan informasi secara lengkap dan mendalam atas gejala-gejala yang ada pada TMC PMJ kemudian dituangkan ke dalam penulisan

dalam bentuk narasi kualitatif dengan menggunakan metode penulisan deskriptif analisis.

Paradigma penelitian kualitatif ini dipilih berdasarkan asumsi metodologis bahwa dengan menggunakan logika induktif dalam pelaksanaan penelitian akan lebih akurat untuk menentukan hasil penelitian ini. Informasi yang didapatkan dari informan kepada saya serta temuan-temuan hasil pengumpulan data di lapangan akan memberikan informasi yang akurat untuk bisa memberikan solusi atas persoalan-persoalan penelitian yang telah disampaikan, sehingga hasil penelitian ini sangat akurat untuk menjawab permasalahan.

Lebih lanjut Cresswell (2002) menjelaskan bahwa langkah pertama dalam prosedur penelitian kualitatif adalah dengan mengajukan asumsi desain paradigma kualitatif. Menurut Cresswell, asumsi desain paradigma kualitatif ini menjadi latar belakang dilakukan pemilihan paradigma penelitian kualitatif. pengajuan asumsi desain penelitian ini penting dilakukan karena akan memberikan arah selanjutnya untuk melakukan rancangan seluruh tahap penelitian serta peranan penulis dalam menuangkan hasil penelitian ke dalam penulisan.

Langkah kedua adalah melakukan prosedur pengumpulan data. Langkah ini melibatkan penetapan batas-batas penelitian, mengumpulkan informasi melalui pengamatan, wawancara, dokumen dan bahan-bahan audio-visual dan menetapkan aturan untuk mencatat informasi yang didapatkan.

Langkah ketiga menurut Cresswell adalah melakukan prosedur pencatatan data. Langkah ini mencakup tentang perencanaan kegiatan penelitian yang akan dilakukan. Terdapat dua hal penting berkaitan dengan langkah ketiga ini, yaitu apa yang akan dicatat dan bagaimana data tersebut akan dicatat.

Langkah selanjutnya adalah mengidentifikasi prosedur analisis data. Strauss dan Corbin (1980) dalam Cresswell (2002) menyatakan bahwa dalam langkah ini peneliti berusaha untuk membuat kategori dengan cara membandingkan secara konstan antara kejadian satu dengan yang lain sehingga muncul kategori dan dengan pengambilan sampel teoritis yang akan membawa ke munculnya kategori.

Menentukan langkah-langkah pembuktian adalah langkah kelima dalam prosedur penelitian kualitatif. Upaya ini akan menentukan keakuratan laporan

dengan cara membahas kemungkinan generalisasi dari laporan tersebut dan kemudian mengajukan kemungkinan sebuah penelitian yang telah dilaksanakan lalu dianggap sebagai bukti ilmiah dari penelitian ilmiah.

Selanjutnya langkah terakhir dalam prosedur penelitian kualitatif menurut Cresswell adalah menuangkan hasil penelitian ke dalam bentuk tulisan secara naratif kualitatif.

Langkah-langkah prosedur pengumpulan data pada tesis ini adalah menentukan batas-batas penelitian; mengumpulkan informasi melalui pengamatan, pengamatan terlibat, wawancara, penelitian dokumen serta bahan-bahan audio visual.

Identifikasi terhadap informan yang diteliti adalah petugas operator TMC PMJ, tim IT TMC PMJ dan para pejabat teras di lingkungan Ditlantas Polda Metro Jaya. Prosedur pengumpulan data ini dilakukan dengan cara berinteraksi secara langsung terhadap obyek yang diteliti serta mengumpulkan informasi yang berkaitan dengan obyek tersebut.

Prosedur pengumpulan dan pencatatan data yang dilakukan pertama kali dengan cara melakukan pengamatan dengan cara partisipan. Pengamatan terlibat (*participant observation*) bermakna bahwa selama penelitian berlangsung penulis berperan sebagai instrumen penelitian, artinya penulis tidak hanya mencatat apa yang diamati tetapi juga mendengar sebagai hasil bertanya maupun tidak dan merasakan setiap gejala-gejala yang berkaitan dengan fokus penelitian untuk memahami dan menemukan tindakan pengamanan informasi yang telah dilakukan oleh obyek yang diteliti.

Pengamatan yang penulis lakukan adalah dengan cara mengamati gambaran umum wilayah penelitian yang meliputi pelaksanaan operasional *Traffic Management Center* Ditlantas Polda Metro Jaya dalam menjalankan fungsinya, dan bentuk aplikasi layanan informasi yang dilakukan. Selanjutnya pengamatan terlibat yang penulis lakukan adalah dengan mengikuti kegiatan pelayanan informasi yang dilakukan oleh operator TMC PMJ dalam melakukan proses transmisi informasi berkaitan dengan fungsi yang telah ditetapkan serta prosedur keamanan informasi yang dilakukan oleh tim IT terhadap informasi di dalamnya.

Kemudian bertatap muka secara pribadi dan melakukan wawancara langsung dan mendalam kepada informan untuk mendapatkan hasil penelitian yang diharapkan. Wawancara yang penulis lakukan kepada informan kunci, informan penting dan informan biasa yang terdiri dari pejabat teras di lingkungan Ditlantas Polda Metro Jaya, tim IT dan petugas operator TMC PMJ.

Penelitian dokumen penulis lakukan juga terhadap dokumen-dokumen yang berkaitan dengan obyek penelitian. Kemudian melakukan pengumpulan data dengan menggunakan materi audio-visual berupa perangkat lunak komputer dan skema jaringan komputer pada TMC PMJ.

Setelah itu, prosedur analisis data penelitian ini dilakukan bersama-sama dengan pengumpulan data dan melakukan interpretasi data. Hasil informasi yang telah didapatkan kemudian dipilah dan melakukan format informasi ke dalam suatu narasi. Kemudian hasil identifikasi atas data yang didapat yang berkaitan dengan sistem pengamanan informasi dilakukan dengan menerapkan delapan langkah prosedur analisis data.

Langkah selanjutnya dalam prosedur penelitian kualitatif ini dilakukan dengan cara menentukan keakuratan laporan yang didapatkan serta membahas kemungkinan generalisasi laporan yang didapat untuk kemudian dituangkan ke dalam tesis secara naratif kualitatif dengan menggunakan metode deskriptif analitis. Tatacara penulisan tesis ini dilakukan berdasarkan pedoman teknis penulisan tesis yang diterbitkan oleh Universitas Indonesia tahun 2008 dengan menggunakan format *American Psychologycal Association* (APA).

1.7. Tata Urut Penulisan (Sistematika Penulisan)

Tata urutan penulisan (sistematika penulisan) hasil penelitian yang telah dilakukan diawali dengan pendahuluan yang berisi tentang latar belakang dari tema penelitian untuk menentukan masalah penelitian, fokus penelitian yang tertuang dalam pertanyaan penelitian, lalu menentukan satu hipotesis penelitian. Kemudian pernyataan signifikansi penelitian yang tertuang dalam tujuan dan kegunaan penelitian, dan menentukan metode penelitian yang diterapkan dalam melaksanaka penelitian.

Penulisan selanjutnya adalah tentang tinjauan literatur yang diawali dengan penulisan literatur teori tentang manajemen keamanan informasi dan penerapan ISO 27001:2005 kemudian melakukan penulisan literatur konsep sebagai operasionalisasi teori yang telah dibahas sebelumnya.

Tata urutan yang berikutnya adalah melakukan penulisan tentang gambaran umum *Traffic Management Center* Direktorat Lalu Lintas Polda Metro Jaya. Maksud dari penulisan ini adalah supaya bisa memberikan gambaran yang lengkap tentang definisi, latar belakang berdirinya, organisasi, teknologi dan infrastuktur dan operasional serta jaringan yang digunakan pada TMC PMJ.

Kemudian tata urutan yang keempat adalah menuangkan hasil penelitian yang telah dilaksanakan ke dalam bentuk narasi. Bagian ini berisi tentang karakteristik *Traffic Management Center* Polda Metro Jaya yang berupa sejarah berdirinya TMC PMJ dan penerapan layanan informasi pada TMC PMJ, kebijakan keamanan informasi yang telah dilakukan terhadap personel, fisik bangunan dan terhadap informasi pada TMC PMJ, serta gangguan yang terjadi pada TMC PMJ.

Tata urutan yang kelima adalah melakukan pembahasan terhadap permasalahan yang telah ditentukan, yaitu penerapan manajemen keamanan informasi yang dilaksanakan oleh Ditlantas Polda Metro Jaya terhadap TMC PMJ, gangguan yang masih terjadi dan penyebabnya, serta penerapan manajemen keamanan informasi pada TMC PMJ dengan implementasi pengendalian ISO 27001:2005 untuk menciptakan keamanan informasi yang optimal.

Bagian akhir dari tata urutan penulisan ini adalah kesimpulan dan saran yang berisi tentang kesimpulan dari hasil penelitian serta saran-saran mengenai penerapan kebijakan keamanan informasi pada TMC PMJ.

BAB II
TINJAUAN LITERATUR

2.1 Literatur Teori

2.1.1 Teori Manajemen Keamanan Informasi

Untuk menciptakan dan melaksanakan manajemen keamanan informasi yang komprehensif, konsisten, efektif dan efisien, maka manajemen TMC PMJ selain melakukan upaya untuk mengamankan aset sumber daya informasi yang berada di dalamnya agar senantiasa aman saja, juga diharapkan menjaga perusahaan tersebut tetap berfungsi setelah terjadi suatu bencana atau rusaknya sistem keamanan. McLeod dan P.Schell (2008, p. 271) mengemukakan pandangan tentang teori manajemen keamanan informasi, dimana ada dua hal utama dalam pelaksanaan manajemen keamanan informasi, yaitu:

a. Strategi keamanan informasi.

   Merupakan aktifitas untuk menjaga agar sumber daya informasi tetap aman.

b. Manajemen keberlangsungan bisnis.

   Merupakan aktifitas untuk menjaga agar perusahaan dan sumber daya informasinya tetap berfungsi setelah terjadinya bencana maupun gangguan yang lain.

2.1.1.1 Strategi Keamanan Informasi

Pengamanan terhadap sistem informasi bukan hanya sekedar mengamanankan data komputer semata, tetapi juga merupakan suatu proses perlindungan terhadap kekayaan intelektual dari suatu organisasi. Pengamanan terhadap sistem informasi terhadap sumber daya TMC PMJ harus dilaksanakan secara komprehensif, konsisten, secara efektif dan efisien baik dalam merumuskan strategi pengamanan maupun implementasinya. Selain itu dukungan penuh dari seluruh komponen TMC PMJ, termasuk di dalamnya *top level management*, mutlak diperlukan untuk menciptakan strategi keamanan informasi pada TMC PMJ.

Untuk melakukan perumusan strategi pengamanan terhadap informasi, McLeod & P.Schell (2008, p. 271) berpendapat bahwa dalam bentuk paling dasar manajemen keamanan informasi terdiri dari 4 (empat) tahapan yang harus dilakukan oleh manajemen perusahaan. Pentahapan tersebut adalah:

1. Mengidentifikasi Ancaman.

   Bentuk-bentuk ancaman apa saja yang dapat menyerang sumber daya informasi suatu perusahaan atau organisasi.

2. Mendefinisikan Resiko.

   Bentuk-bentuk resiko apa saja yang dapat disebabkan oleh ancaman-ancaman tersebut. Bentuk resiko ini didefinisikan dengan melakukan langkah-langkah pengelolaan resiko (manajemen resiko) dan diakhiri dengan menyusun analisis resiko.

3. Menentukan Kebijakan Keamanan Informasi.

   Suatu kebijakan keamanan informasi harus diterapkan untuk mengarahkan keseluruhan program yang telah ditentukan pada TMC PMJ.

4. Mengimplementasikan Pengendalian.

   Merupakan mekanisme yang diterapkan baik untuk melindungi TMC PMJ dari resiko atau untuk meminimalkan dampak resiko tersebut apabila resiko tersebut terjadi.

Istilah manajemen resiko (*risk management*) digunakan oleh Mc.Leod dan P.Schell untuk menggambarkan pendekatan ini dimana tingkat keamanan informasi organisasi TMC PMJ akan dibandingkan dengan tingkat resiko yang dihadapinya.

Kemudian empat pentahapan tersebut oleh Mc.Leod dan P.Schell dijabarkan dalam langkah-langkah sebagai berikut:

1. Identifikasi ancaman:

   Sumber ancaman yang diprakirakan terjadi (Hadiman, 2009):

   a. Unsur manusia.
   b. Unsur alam.
   c. Unsur teknologi.

Bentuk ancaman yang diprakirakan terjadi (McLeod & P.Schell, 2008, p.275):

a. Pengungkapan informasi yang tidak terotorisasi dan pencurian.
b. Penggunaan yang tidak terotorisasi.
c. Penghancuran yang tidak terotorisasi dan penolakan layanan.
d. Modifikasi yang tidak terotorisasi.

2. Pendefinisian resiko:

Pendefinisian resiko ini berkaitan erat dengan manajemen resiko yang merupakan bagian terpenting dalam pengelolaan keamanan sistem informasi. Untuk mendapatkan hasil analisis manajemen resiko secara komprehensif maka digunakan metodologi manajemen resiko, sebagai berikut:

a. Identifikasi aset.
b. Analisis resiko.
c. Tindak lanjut.

3. Penentuan kebijakan keamanan informasi:

Dalam menentukan kebijakan keamanan terhadap TMC PMJ akan disesuaikan dengan implementasi ISO 27001:2005 yang dilakukan dengan berdasarkan aspek pendefinisian resiko di atas, dengan tujuan dapat menjamin keberhasilan sasaran dan tujuan TMC PMJ.

4. Implementasi pengendalian:

Implementasi pengendalian dalam pelaksanaan kegiatan TMC PMJ juga menggunakan implementasi ISO 27001:2005 sebagai standar sistem keamanan informasi internasional.

2.1.1.2 Manajemen Keberlangsungan Bisnis (*Business Continuity Manage ment*-BCM)

Merupakan suatu aktifitas yang dilakukan oleh organisasi dalam menentukan operasional setelah terjadi gangguan sistem informasi sehingga menjaga agar perusahaan dan sumber daya informasinya tetap dapat melakukan operasional secara aman. McLeod dan P.Schell (2008, p.288) menerangkan bahwa Manajemen Keberlangsungan Bisnis memiliki 3 (tiga) subrencana yang

umum, mencakup: (a). Rencana darurat; (b). rencana cadangan; dan (c). rencana catatan penting.

2.1.2 Penerapan ISO 27001:2005

ISO 27001:2005 berisi tentang pengendalian dan pengawasan dalam bentuk standar operasional prosedur yang berguna untuk memberikan saran dan petunjuk pelaksanaan pada praktek terbaik dalam mendukung pengendalian. Isi dari ISO 27001:2005 terdiri dari 11 golongan (*sections*), 39 tujuan pengendalian (*control objectives*) dan 134 pengendalian (*controls*), sebagai berikut (Snare & Kuper, 2005):

A. 11 golongan (*sections*), yaitu:
   1. Kebijakan Keamanan (*Security Policy*).
   2. Organisasi Keamanan Informasi (*Organization of Information Security*).
   3. Manajemen Aset (*Asset Management*).
   4. Keamanan Sumber Daya Manusia (*Human Resources Security*).
   5. Keamanan Fisik dan Lingkungan (*Physical and Environmental Security*).
   6. Komunikasi dan Manajemen Informasi (*Communication And Operations Management*).
   7. Kendali Akses (*Access Control*).
   8. Akuisisi Sistem Informasi, Pengembangan dan Pemeliharaan (*Information System Acquisition, Development and Maintenance*).
   9. Manajemen Insiden Keamanan Informasi (*Information Security Incident Management*).
   10. Manajemen Kesinambungan Bisnis (*Business Continuity Management*).
   11. Pemenuhan (*Compliance*).

B. 39 *control objectives* (Tujuan Kendali), yaitu:
   1. Kebijakan keamanan informasi (*Information security policy*).
   2. Organisasi internal (*Internal organization*).
   3. Pihak-pihak eksternal (*External parties*).

4. Pertanggungjawaban aset (*Responsibility of assets*).
5. Pengklasifikasian informasi (*Information classification*).
6. Sebelum bekerja (*Prior to employment*).
7. Selama bekerja (*During employment*).
8. Pemutusan atau mengubah pekerjaan (*Termination or change of employment*).
9. Daerah aman (*Secure area*).
10. Peralatan keamanan (*Equipment security*).
11. Operasional prosedur dan pertanggungjawaban (*Operational procedure and responsibility*).
12. Manajemen pelayanan pihak ketiga (*Third party service delivery management*).
13. Sistem perencanaan dan penerimaan (*System planning and acceptance*).
14. Perlindungan terhadap kode berbahaya dan bergerak (*Protection against malicious and mobile code*).
15. Back up (*Back up*).
16. Manajemen keamanan jaringan (*Network security management*).
17. Media penanganan (*Media handling*).
18. Pertukaran informasi (*Exchanges of information*).
19. Layanan komersial elektronik (*Electronic commerse services*).
20. Pemantauan (*Monitoring*).
21. Kebutuhan bisnis untuk pengendalian akses (*Business requirement for access control*).
22. Manajemen akses penggunaan (*Use access management*).
23. Pertanggungjawaban pengguna (*User responsibilities*).
24. Pengendalian akses jaringan (*Network access control*).
25. Pengendalian akses terhadap sistem operasi (*Operating system access control*).
26. Pengendalian akses terhadap aplikasi dan informasi (*Application and information access control*).

27. Komputasi bergerak dan teleworking (*Mobile computing and teleworking*).
28. Kebutuhan keamanan terhadap sistem informasi (*Security requirement of information system*).
29. Aplikasi proses perbaikan (*Correct processing application*).
30. Pengendalian kriptografi (*Cryptographic control*).
31. Keamanaan sistem file (*Security of system files*).
32. Pengembangan keamanan dan proses pendukung (*Security in development and support process*).
33. Manajemen kerentanan teknis (*Technical vulnerabilities management*).
34. Pelaporan peristiwa keamanan informasi dan kelemahan (*Reporting information security events and weakness*).
35. Manajemen insiden keamanan informasi dan perbaikan (*Management of information security incidents and improvements*).
36. Aspek keamanan informasi terhadap manajemen keberlangsungan bisnis (*Information security aspects of business continuity management*).
37. Pemenuhan atas persyaratan hukum (*Compliance with legal requirements*).
38. Pemenuhan atas kebijakan keamanaan, standard an kepatuhan teknis (*Compliance with security policies, standards and technical compliance*).
39. Pertimbangan audit sistem informasi (*Information system audit consideration*).

Dalam implementasinya terhadap keamanan informasi suatu organisasi, ISO 27001:2005 tidak mutlak harus diterapkan secara keseluruhan tetapi menyesuaikan dengan aset organisasi yang ada.

2.2 Literatur Konseptual

2.2.1. Organisasi dan Manajemen

Secara harfiah, kata organisasi berasal dari bahasa Yunani "*organon*" yang berarti organ, alat atau instrumen. Mc.Crie (2001) mendefinisikan tentang organisasi sebagai berikut:

> "*Organizations are composed of groups of people bounded by a purpose a systematic scheme to achieve mutually agreed-upon objectives... Organization are created, therefore, in order to achieve objective deemed desirable by leader and planners of the organization, by those who carry out tasks, or in some cases from both.* "

Memperkuat dari pendapat di atas, Siagian (2001) menyatakan bahwa organisasi sebagai sekelompok orang yang terikat secara formal dan hierarkis serta bekerja sama untuk mencapai tujuan tertentu yang telah ditetapkan sebelumnya. Bakharuddin (2009) menyadur pendapat Stephen Robbins memberikan definisi yang lebih komprehensif tentang organisasi, dimana merupakan unit sosial yang sengaja didirikan untuk jangka waktu yang relatif lama, beranggotakan dua orang atau lebih yang bekerja bersama-sama dan terkoordinasi, mempunyai pola kerja tertentu yang terstruktur, dan didirikan untuk mencapai tujuan bersama atau seperangkat tujuan yang telah ditentukan sebelumnya.

Kemudian Thibault, M.Lynch dan Mc.Bride (2001) memperluas definisi organisasi menjadi dua aspek organisasi yang menjadi bagian dari definisi dasar di atas, yaitu pendekatan mekanis/struktural dan pendekatan humanis. Dalam pendekatan mekanis/struktural disebutkan bahwa organisasi merupakan seluruh susunan dan sub divisi kegiatan untuk menjamin ekonomi upaya melalui spesialisasi dan koordinasi kerja sehingga menuju ke kesatuan aksi (definisi ini menekankan aspek mekanis atau fisik dari organisasi). Selanjutnya dalam pendekatan humanis diikhtisarkan sebagai bentuk pendivisian dan pengelompokan kerja menjadi satuan pekerjaan dan mendefinisikan hubungan standar di antara individu yang mengisi tugas-tugas ini (definisi ini menekankan

bahwa manusia yang mendirikan organisasi dan melalui kegiatan manusia seluruh pekerjaan yang dijalankan).

Organisasi dan manajemen merupakan dua hal yang saling berkaitan antara satu dengan yang lain. Ibarat tubuh manusia maka organisasi merupakan raganya, sedangkan manajemen adalah ruh dari raga tersebut. Zamani (1998, p.7-9) mengutip pandangan dari Terry (1986) memberikan pengertian dari manajemen, dimana merupakan suatu pencapaian tujuan yang ditetapkan terlebih dahulu dengan menggunakan orang lain. Lebih lanjut dikatakan oleh Terry bahwa manajemen merupakan sebuah proses yang khas, yang terdiri dari tindakan-tindakan perencanaan, mengorganisasikan, menggerakkan dan pengawasan yang dilakukan untuk menentukan serta mencapai sasaran-sasaran yang telah ditetapkan melalui pemanfaatan sumber daya manusia serta sumber-sumber lainnya.

Djamin, Umar dan Siswanto (1995) memberikan definisi tentang manajemen yang merupakan ilmu dan kemahiran untuk pengelolaan orang-orang maupun aktifitasnya dalam organisasi tersebut. Lebih lanjut dikatakan mereka bahwa manajemen merupakan seni dan ilmu dalam pelaksanaan fungsi-fungsinya untuk mencapai tujuan. Manajemen sebagai seni dalam pengertian yang luas dan umum yaitu merupakan keahlian, kemahiran, kemampuan serta keterampilan dalam menerapkan prinsip-prinsip, metode dan teknik dalam menggunakan sumber daya manusia dan sumber daya alam secara efektif dan efisien untuk mencapai tujuan. Sedangkan manajemen sebagai ilmu merupakan akumulasi pengetahuan yang disistematiskan, atau pengetahuan yang terorganisir.

Sebagai intisari dari beberapa konsepsi di atas maka secara sederhana organisasi dapat dirumuskan sebagai kumpulan sekelompok orang yang mengadakan aktifitas bersama untuk mencapai tujuan bersama yang telah disepakati sebelumnya. Untuk mencapai tujuan bersama tersebut maka dalam pengelolaannya digunakan ilmu dan kemahiran tertentu. Ilmu dan kemahiran untuk pengelolaan orang-orang maupun aktifitasnya dalam organisasi tersebut dinamakan manajemen.

Untuk dapat menerapkan manajemen yang tepat terhadap suatu organisasi maka harus didukung dengan mengoptimalkan segala sumber daya yang ada pada

organisasi tersebut agar dapat mencapai tujuan yang diharapkan secara efektif dan efisien. Pada era informasi dan komunikasi yang semakin pesat seperti sekarang ini, sumber daya yang terdapat pada suatu organisasi tidak hanya bersifat fisik dalam bentuk manusia, pendanaan, material dan metode saja tetapi juga yang bersifat *virtual* dalam bentuk informasi.

Efektifitas yang harus diterapkan dalam proses manajemen berarti kemampuan untuk memilih sasaran yang tepat sehingga diperlukan profesionalisme seseorang dalam melaksanakan tugasnya. Sedangkan efisiensi bermakna bahwa seseorang harus mempunyai kemampuan untuk melaksanakan pekerjaannya dengan benar agar dapat meminimalkan beaya sumber daya yang digunakan untuk mencapai tujuan yang telah ditetapkan.

2.2.2. Konsep Pengembangan Organisasi

Menghadapi tuntutan lingkungan yang semakin berkembang dan senantiasa mengalami perubahan maka dibutuhkan kecepatan dan ketanggapan oleh para manajer dalam mengelola organisasi agar dapat menyesuaikan diri dengan perkembangan dan perubahan yang ada. Pihak manajemen masa kini dan masa depan akan selalu dituntut untuk tidak sekedar bersikap luwes dan beradaptasi dengan lingkungan yang bergerak sangat dinamis, akan tetapi juga mampu mengantisipasi berbagai bentuk perubahan yang diperlukan dan secara proaktif menyusun perbagai program yang diperlukan.

Tuntutan dari para pemangku kepentingan (*stakeholder*) tersebut pada gilirannya mengharuskan pihak manajemen untuk selalu terlibat dalam perubahan. Untuk itu diperlukan instrument ilmiah untuk mewujudkan perubahan tersebut dalam bentuk pengembangan organisasi (*organizational development*). Menurut Siagian (2000), pengembangan organisasi merupakan pendekatan yang terprogram dan sistematik dalam mewujudkan perubahan. Dengan adanya pengembangan organisasi akan memungkinkan organisasi untuk mampu beradaptasi dengan kondisi dan tuntutan lingkungan yang senantiasa berubah sehingga dapat meningkatkan efektifitas dan kesehatan organisasi itu.

Selanjutnya Siagian menyatakan bahwa pengembangan organisasi merupakan salah satu pembenaran yang paling kuat dalam mewujudkan suatu perubahan demi keberhasilan mencapai tujuan organisasi. Adanya pengembangan pada suatu organisasi secara konseptual terlihat dengan ditandai oleh empat hal, yaitu: *pertama*, ada proses konsultasi, dimana konsultan yang jasanya digunakan memegang teguh prinsip efisiensi dan semangat kerja yang tinggi dalam melakukan kegiatannya; *kedua*, pengenalan dan penggunaan strategi pengembangan organisasi, bahwa kegiatan pengembangan organisasi harus didasarkan pada pendekatan yang *taylor-made*; *ketiga*, melakukan suatu bentuk intervensi tertentu; serta *keempat*, adanya keadaan yang didambakan.

Selain pengembangan secara konseptual, juga terdapat beberapa indikator yang harus dimiliki agar pengembangan organisasi dapat berjalan dengan efektif dan efisien. Indikator yang pertama adalah memiliki suatu strategi yang terencana dalam mewujudkan perubahan organisasional. Strategi terencana tersebut pada hakekatnya terletak pada unsur manajemen untuk melakukan pengelolaan suatu organisasi dalam mencapai keberhasilan suatu tujuan dengan memanfaatkan segala sumber daya secara efektif dan efisien yang berada pada organisasi.

Indikator selanjutnya adalah pentingnya kolaborasi antara berbagai pihak yang akan terkena dampak perubahan yang akan terjadi. Indikator ini mengandung makna bahwa keterlibatan dan partisipasi dari keseluruhan *stakeholder* memegang peranan kunci dalam menentukan keberhasilan tujuan operasional organisasi.

Indikator ketiga untuk menentukan efektifitas dari pengembangan organisasi menurut Siagian adalah menekankan pada cara-cara baru sebagai program pengembangan organisasi yang diperlukan guna meningkatkan kinerja seluruh anggota organisasi dan semua satuan kerja dalam organisasi. cara-cara baru yang dilakukan pada TMC PMJ terlihat pada bentuk aplikasi layanan yang dioperasionalkan.

Menurut Santoso (1998) di dalam perkembangan organisasi maka pertama kali muncul aliran sistem yang memandang organisasi sebagai tatanan yang kompleks dan dinamis dari unsur-unsur yang saling terkait. Unsur-unsur tersebut adalah input, proses, output dan saluran *feedback* dan lingkungan tempat unsur-

unsur tersebut beroperasi. Adanya perubahan pada salah satu unsur tersebut akan mengakibatkan berubahnya unsur-unsur yang lain sehingga dapat dikatakan bahwa keterkaitan antarunsur tersebut menjadi kompleks dan dinamis.

2.2.3. Jaringan Komputer

Komputer diambil dari bahasa latin "*computare*" yang berarti menghitung (*to compute* atau *to reckon*). Arief (2009) menyatakan definisi komputer sebagai suatu alat elektronik yang mampu melakukan beberapa tugas seperti menerima input, memproses input sesuai dengan programnya, menyimpan perintah-perintah dan hasil pengolahan serta menyediakan output dalam bentuk informasi.

Pada dasarnya peralatan komputer terdiri dari dua bagian, yaitu peralatan keras (*hardware*) dan peralatan lunak (*software*). *Hardware* merupakan peralatan fisik komputer yang dapat dilihat, dipegang, maupun dipindahkan. Sedangkan *software* berfungsi sebagai prosedur atau program yang terdapat pada komputer tersebut untuk melakukan pemrosesan data sesuai dengan yang dikehendaki.

Hardware terdiri dari peralatan *input* (misalnya:keyboard), Unit Pemroses Sentral (Central Processing Unit/CPU) dan peralatan output (misalnya:layar monitor). Cara kerja dari peralatan hardware ini diawali dari proses input dari suatu data ke dalam proses pengolahan data melalui alat input (*input device*) kemudian dilakukan proses pengolahan data dengan alat pemroses (*processing device*) berupa proses menghitung, membandingkan, mengklasifikasikan, mengurutkan, mengendalikan atau mencari di ruang penyimpanan data (*storage*). Kemudian hasil proses data tersebut menghasilkan output dan dapat ditampilkan dalam bentuk informasi dengan menggunakan alat output (*output device*).

Agar dapat melakukan proses pengolahan data pada komputer maka digunakan *software* sebagai prosedur pengolahan data. *Software* tersebut ditulis menggunakan bahasa khusus yang dimengerti oleh komputer (bahasa pemrograman). Menurut Yuhefizar (2009), *software* terdiri dari lima jenis, yaitu: (a). Sistem operasi; (b). program *utility*; (c). program aplikasi; (d). program paket; dan (e). bahasa pemrograman.

Sistem operasi adalah *software* yang berfungsi untuk mengaktifkan seluruh perangkat yang terpasang pada komputer sehingga masing-masing perangkat tersebut dapat saling berkomunikasi. Tanpa ada sistem operasi maka komputer tak dapat difungsikan sama sekali. Program *utility* berfungsi untuk membantu atau mengisi kekurangan/kelemahan dari sistem operasi yang dijalankan pada komputer. Program aplikasi merupakan program khusus yang digunakan untuk melakukan suatu pekerjaan tertentu. Sedangkan program paket ialah program yang disusun sedemikian rupa sehingga dapat digunakan oeh pengguna dengan berbagai kepentingan. Untuk merancang keempat peranti lunak ini digunakan bahasa pemrograman. Bahasa pemrograman merupakan *software* yang khusus digunakan untuk membuat keempat program pada komputer, baik sistem operasi, program *utility*, program aplikasi maupun program paket,

Selain perangkat keras dan perangkat lunak yang berperan dalam operasional komputer, juga diperlukan unsur manusia sebagai pengoperasian komputer. Personel yang terlibat langsung dalam pemakaian komputer dinamakan *brainware*. *Brainware* biasa disebut dengan *user*, terdiri dari sistem analis, *programmer*, operator, *user*, dan sebagainya.

Beberapa unsur komputer di atas secara bersama-sama melakukan penerimaan data (input), mengolah data (proses) dan memberikan informasi (output) serta terkoordinasi di bawah kontrol program yang tersimpan di dalam memori komputer. Ketika unsur komputer tersebut dipergunakan secara bersama-sama maka hasilnya akan dapat digunakan untuk mendukung pengambilan keputusan. Secara rinci McLeod dan P.Schell menggambarkan arsitektur komputer sebagai berikut:

> "... inti dari sebuah komputer adalah prosesornya. Prosesor pada komputer dikendalikan oleh sebuah sistem operasi (seperti Windows) untuk mengelola alat input dan output, alat penyimpanan data, dan operasi atas data. Unit pemroses sentral (CPU) mengendalikan seluruh kompunen lainnya. Memory Akses Acak (*Random Access Memory*/RAM) bertindak sebagai tempat kerja sementara bagi CPU. Selanjutnya untuk melakukan penyimpanan data yang ada dilakukan pada alat penyimpanan data secara permanen pada komputer dengan menggunakan CD-ROM, USB *flash*

drive dan *hard disk*. Kesemuanya sarana ini saling terhubung dengan menggunakan papan sirkuit (*motherboard*)."

Jaringan komputer atau yang biasa dikenal dengan *computer network* adalah dua komputer atau lebih yang saling berhubungan dengan menggunakan media fisik dan software sebagai sarana untuk memfasilitasi terjadinya komunikasi antara komputer-komputer tersebut. Sofana (2010) menyatakan bahwa jaringan komputer dibagi menjadi tiga kriteria, yaitu: (a). berdasarkan luas areanya; (b). berdasarkan media penghantarnya; dan (c). berdasarkan pola pengoperasiannya.

Berdasarkan luas areanya maka jaringan komputer dapat dibedakan menjadi empat, yaitu PAN (*Personal Area Network*), LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), dan WAN (*Wide Area Network*). Sofana memberikan batasan luas area antara keempat area tersebut sebagai berikut:

Tabel 2.1: Jaringan Komputer Berdasarkan Area

JARAK (meter)	NETWORK	CONTOH AREA
1 s/d 10	PAN	Ruangan
10 s/d 1000	LAN	Gedung
10.000 s/d 100.000	MAN	Kota
Tak terbatas	WAN/Internet	Antar negara

Berdasarkan media penghantar yang digunakan, jaringan komputer dibagi menjadi dua kelompok, yaitu:

1. *Wire network* atau *wireline network* (jaringan kabel).

   Adalah jaringan komputer yang menggunakan kabel sebagai media penghantarnya. Bahan dasar kabel tersebut biasanya menggunakan tembaga, namun ada juga jenis kabel lain yang menggunakan bahan *fiber optic* atau serat optik. Untuk LAN biasanya menggunakan jenis kabel tembaga, sedangkan untuk MAN atau WAN menggunakan gabungan tembaga dan serat optik.
2. *Wireless network* (jaringan nirkabel).

Adalah jaringan komputer yang menggunakan media penghantar berupa gelombang radio (*bluetooth* dan *wifi*) atau cahaya (*infra red* atau laser). Frekuensi radio yang digunakan jaringan ini antara 2.4 GHz sampai 5,8 GHz, sedangkan penggunaan *infra red* dan laser umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan dua buah titik saja (*point to point*).

Berdasarkan pola pengoperasiannya maka jaringan komputer dibagi menjadi tiga pola, yaitu (Sofana, 2010):

1. *Peer to peer.*
   Merupakan pola jaringan komputer dimana setiap komputer bisa menjadi server sekaligus client, dimana setiap komputer dapat menerima dan memberikan access dari atau ke komputer lainnya. Pola pengoperasian jaringan ini sering digunakan pada jaringan komputer LAN.
2. *Client-server* (*server based*).
   Adalah pola jaringan komputer yang salah satu atau beberapa komputernya berfungsi sebagai *server* untuk melayani komputer yang lain (*client*). Dalam pola jaringan ini, server merupakan kunci utama jaringan dan akses kontrolnya bersifat *centralized*. Pola ini sering digunakan pada layanan internet maupun intranet.
3. *Hybrid.*
   Merupakan kombinasi dari pola jaringan peer to peer dan client-server, dimana pengguna dapat membagi *resources* yang dimiliki ke pengguna lain seperti pada jaringan *server-based.*

Agar dapat menghubungkan antara peralatan komputer dengan jaringan internet dibutuhkan beberapa perangkat keras. Dian (2004) memberikan deskripsi bahwa perangkat keras yang digunakan untuk membangun sebuah jaringan komputer adalah: *file server*, *workstation*, *network interface card*, *concentrators/hub*, *repeaters*, *bridges* dan *router*.

File server merupakan peralatan vital pada jaringan komputer yang bertugas untuk mengontrol komunikasi dan informasi diantara komponen suatu

jaringan. Di dalam server ini tersimpan sistem operasi jaringan dan beberapa aplikasi serta data yang diperlukan untuk jaringan maupun data penting lainnya.

Keseluruhan komputer yang terhubung ke file server dalam jaringan dinamakan *workstation*. Untuk menghubungkan masing-masing komputer yang terdapat pada *workstation* menggunakan media yang dinamakan kartu jaringan (*Network Interface Cards*/NIC). Komputer dari tiap-tiap *workstation*, server ataupun perangkat lainnnya yang telah memiliki kartu jaringan dihubungkan dengan kabel-kabel dan disatukan ke dalam sebuah *concentrators/hub*.

Repeater mempunyai peranan sebagai alat penguat sinyal dari kabel-kabel yang terkoneksi pada masing-masing komputer sehingga komputer terhubung masih mendapatkan sinyal kuat meskipun berada pada lokasi yang jauh. *Bridges* berfungsi untuk membagi satu buah jaringan ke dalam dua buah jaringan untuk mendapatkan jaringan komputer yang efisien. Dengan memanfaatkan brigde maka dapat diketahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan komputer lain di sebelahnya.

Apabila suatu organisasi mempunyai jaringan komputer dalam bentuk LAN dan menginginkan terkoneksi ke internet maka harus melengkapinya dengan peralatan *router*. *Router* berfungsi untuk menerjemahkan informasi antara LAN dengan internet, selain itu juga untuk mencarikan alternatif jalur yang telah diatur sebelumnya untuk mengirimkan dan menerima data melewati internet.

2.2.4. *Cyber Space* dan *Cyber Crime*

Perkembangan teknologi jaringan komputer global atau internet telah menciptakan dunia baru yang dinamakan *cyberspace*, sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru, yaitu realitas virtual. Walaupun dilakukan secara virtual namun dapat dirasakan seolah-olah hal tersebut dilakukan secara nyata, misalnya dalam hal bertransaksi jual beli, berdiskusi, dan lain-lain.

Secara etimologis, istilah *cyberspace* dalam *Cambridge Advanced Learner's Dictionary* didefinisikan sebagai "*the Internet considered as an imaginary area without limits where you can meet people and discover*

information about any subject." *The American Heritage Dictionary of English Language Fourth Edition* mendefinisikan cyberspace sebagai "*the electronic medium of computer networks, in which online communication takes place.*"

Gibson (1984) memunculkan istilah *cyberspace* pertama kali dalam tulisannya. Menurut Gibson, *cyberspace* merupakan:

> "*A consensual hallucination experienced daily billions of legitimate operators, in every nation... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receeding*".

Kemudian pengertian ini diperluas oleh Sterling (1990) yang menyatakan bahwa *cyberspace* tidak hanya terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet saja. Sterling memberikan asumsi bahwa *cyberspace* juga sebagai "*the 'place' where a telephone conversation appears to occur*".

Kehadiran teknologi internet sebagai bentuk sistem komunikasi antarkomputer digital ini mempunyai dampak positif bagi peningkatan efektifitas dan efisiensi operasional bagi suatu organisasi disamping juga menghasilkan kontribusi signifikan dalam kehidupan masyarakat modern. Selain itu internet juga menghasilkan dampak negatif yang dimanfaatkan para pelaku kejahatan jaringan informasi untuk melakukan aksi kejahatannya untuk mendapatkan keuntungan material maupun immaterial. Menurut Mustofa, aksi kejahatan ini disebut sebagai *cyber crime*.

Mengutip tulisan Golose (2006), berdasarkan dokumen kongres PBB tentang *The Prevention of Crime and The Treatment of Offenderes* di Havana pada tahun 1999 dan di Wina pada tahun 2000, terdapat dua istilah yang membagi definisi *cyber crime* ke dalam pengertian sempit dan luas:

a. *Cyber crime in a narrow sense* (*computer crime*): *any illegal behaviour directed by means of electronic operation that target the security of computer system and the data processed by them.*
b. *Cyber crime in a broader sense* (*computer related crime*): *any illegal behaviour committed by means on relation to, a computer system offering*

or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.

Istilah *cyber crime* untuk menjelaskan kejahatan yang berhubungan dengan komputer dan jaringannya dipergunakan oleh Shinder (2002), yang menyatakan bahwa dalam *cyber crime* terdapat berbagai hubungan tindak kejahatan dengan komputer atau jaringan komputer, diantaranya:

a. Komputer atau jaringan komputer dapat menjadi alat kejahatan dalam arti digunakan untuk melakukan kejahatan.
b. Komputer atau jaringan komputer dapat menjadi sasaran kejahatan atau korban.
c. Komputer atau jaringan komputer dapat digunakan untuk maksud-maksud insidental yang berkaitan dengan kejahatan, umpamanya mencatat semua penjualan obat-obatan illegal (*illegal drug trafficking*).

Keragaman kegiatan *cyber crime* yang dapat dilakukan dengan atau terhadap target yang diinginkan luar biasa beragam. Beberapa diantaranya bukanlah bentuk kejahatan yang baru dalam hal substansial namun hanya mediumnya saja yang baru, tetapi terdapat bentuk kejahatan lain yang merupakan bentuk ilegalitas baru. Suryadi memberikan contoh mengenai bentuk-bentuk generik ilegalitas yang melibatkan sistem informasi sebagai instrumen dan/atau target kejahatan adalah sebagai berikut:

a. Pencurian jasa informasi.
b. Komunikasi dalam pendorongan konspirasi criminal.
c. Pembajakan telekomunikasi.
d. Penyebaran bahan yang menyerang (ofensif).
e. Penyucian uang elektronik dan pengelakan pajak.
f. Vandalisme elektronik dan terorisme.
g. Kecurangan penjualan dan investasi.
h. Pencegatan illegal telekomunikasi.
i. Kecurangan transfer dana elektronik.

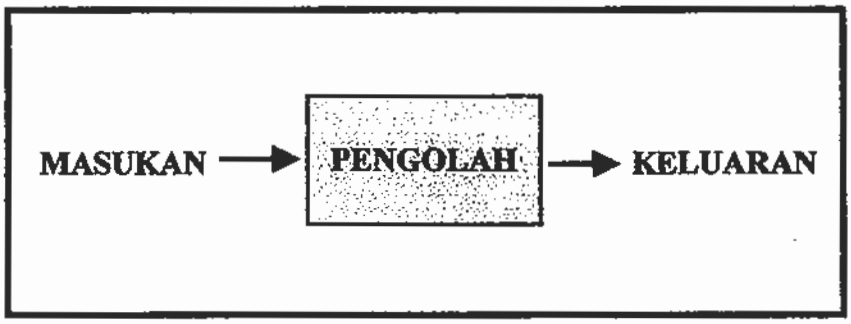
Kemudian keseluruhan keragaman kegiatan *cyber crime* tersebut menurut Mc.leod dan P.Schell dipandang mewakili tindakan yang tidak terotorisasi yang diklasifikasikan menjadi beberapa jenis di dalam resiko keamanan informasi, yaitu (a). pengungkapan informasi yang tidak terotorisasi dan pencurian, (b). penggunaan yang tidak terotorisasi, (c). penghancuran yang tidak terotorisasi dan penolakan layanan, dan (d). modifikasi yang tidak terotorisasi.

2.2.5. Manajemen Sistem Informasi

Sebuah manajemen sistem informasi merupakan suatu sistem informasi yang selain melakukan semua pengolahan transaksi yang perlu untuk organisasi, juga memberikan dukungan informasi dan pengolahan untuk fungsi manajemen dan pengambilan keputusannya. Gagasan sebuah sistem informasi telah ada sebelum munculnya komputer, namun komputer membuat gagasan tersebut menjadi lebih nyata.

Saat ini istilah sistem banyak dipakai dalam kehidupan bermasyarakat, diantaranya adalah sistem pendidikan, sistem tata surya, sistem perangkat lunak, dan sebagainya. Sistem berasal dari bahasa latin "*systema*" dan bahasa Yunani "*sustema*" artinya suatu kesatuan yang terdiri dari komponen atau elemen yang saling berhubungan. Organisasi selalu membutuhkan sistem-sistem untuk mengumpulkan, mengolah, menyimpan, melihat kembali, dan menyalurkan informasi.

Menurut Suryadi (2009), sistem adalah sekelompok elemen yang bekerja sama (terintegrasi) untuk mencapai suatu tujuan atau sasaran tertentu. Secara umum dan sederhana Davis (1995) memberikan definisi sistem dimana terdiri dari masukan, pengolah, dan keluaran. Kemudian Davis menjelaskan bahwa sistem juga mempunyai karakteristik tersendiri, dimana sebuah sistem merupakan seperangkat unsur (sub sistem) yang tersusun dan dapat dikenal sebagai saling melengkapi karena mempunyai satu maksud dan tujuan atau sasaran. Dalam gambar berikut ini dideskripsikan model dari sistem secara sederhana:



Gambar 2.1: Model Sistem secara Sederhana

Seperti yang telah dijelaskan di atas bahwa setiap sistem terdiri dari beberapa sub sistem, dan tidak menutup kemungkinan bahwa tiap sub sistem tersebut terdiri dari beberapa sub sub-sistem. Masing-masing sub sistem dibatasi oleh sempedannya (*boundary*) dan saling kaitan dan interaksi antar sub sistem yang disebut *interface* atau jalinan. Dalam gambar berikut ini memperlihatkan contoh sistem komputer beserta interface dalam sempedan, sebagai berikut:

SISTEM	SUB SISTEM	INTERFACE
Komputer	Unit pengolah pusat Unit masukan Unit keluaran Penyimpan tambahan	Saluran
Unit Pengolah Pusat	Unit penghitung Unit pengendali Unit penyimpan	Kawat penghubung
Pengolahan Batch dengan Kerja Terpisah (separate run)	Kerja edit Kerja sortir Kerja meremajakan (update) Kerja keluaran	Alih data kerja satu dengan lainnya, misalnya pita data.

Gambar 2.2: Sistem Komputer Beserta Interface

Lebih lanjut dikemukakan Davis bahwa sistem terdiri dari 2 (dua) jenis, yaitu sistem tertutup dan sistem terbuka. Sebuah sistem tertutup didefinisikan olehnya sebagai sistem yang mandiri (*self contained*). Sistem ini tidak bertukar materi, informasi atau energi dengan lingkungannya. Sedangkan sistem terbuka mengadakan pertukaran informasi, materi dan energy dengan lingkungannya.

Klasifikasi dari jenis sistem yang dikemukakan di atas, dikembangkan oleh Mc.Leod dan P.Schell pada aplikasi organisasi. Mc.Leod dan P.Schell berpendapat bahwa sistem tertutup (*closed system*) pada organisasi merupakan sistem yang tidak berkomunikasi dengan lingkungannya. Sistem yang benar-benar tertutup tidak akan berinteraksi dengan konsumen, manajer atau siapapun, dan tidak akan menjadi perhatian dari pengembang dan pengguna sistem informasi. Berbeda halnya dengan sistem terbuka (*open system*) yang selalu berinteraksi dengan lingkungannya melalui aliran sumber daya fisik. Salah satu contoh yang diberikannya sebagai sistem terbuka adalah sistem informasi.

Telah dijelaskan pada bab sebelumnya bahwa informasi merupakan salah satu sumber daya utama secara konseptual pada suatu organisasi. Hal ini ditegaskan kembali oleh McLeod dan P.Schell bahwa informasi merupakan suatu sumber daya yang berharga yang merupakan salah satu *critical success factor* (CSF) pada organisasi. Informasi yang dimiliki akan memperkaya penyajian atas sesuatu kepentingan yang diinginkan serta akan mengurangi suatu ketidakpastian sehingga mempunyai manfaat yang besar dalam proses pengambilan keputusan.

Davis (1995) memberikan definisi pokok berkaitan dengan informasi, yaitu merupakan data yang telah diolah menjadi sebuah bentuk yang berarti bagi penerimanya dan bermanfaat dalam mengambil keputusan saat ini atau mendatang. Selanjutnya Suryadi mendeskripsikan korelasi antara data dengan informasi, dimana antara data dan informasi merupakan suatu sumberdaya utama organisasi secara konseptual yang mempunyai perbedaan yang signifikan.

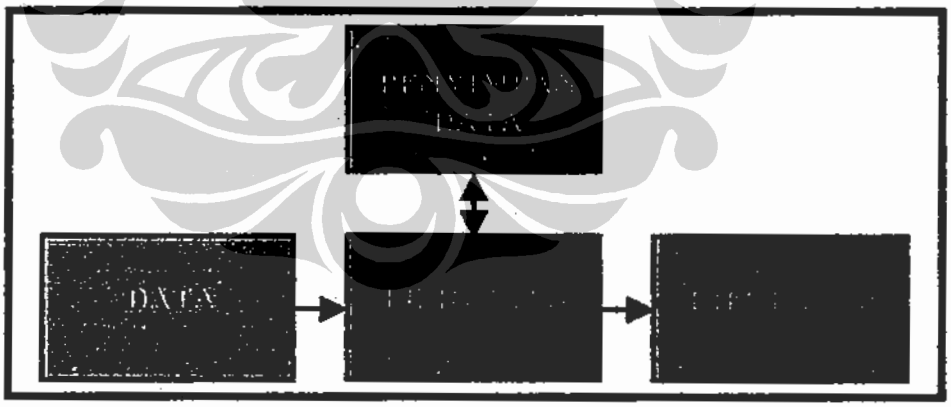
Seperti yang tertulis dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 1 ayat (1), menjelaskan bahwa Informasi Elektronik merupakan satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail)*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Sehubungan dengan hal tersebut di atas maka data merupakan bahan baku informasi yang terdiri dari fakta dan angka dari berbagai sumber dalam dunia

nyata menyangkut entitas manusia, obyek, kejadian dll yang bisa bersifat kualitatif atau kuantitatif serta bersifat internal maupun eksternal. (*data = the plural of datum*) yang relatif tidak mempunyai arti bagi pemakai. Sedangkan yang dimaksud dengan informasi adalah data yang telah diolah dengan menggunakan sistem pengolahan informasi sehingga mempunyai arti bagi pemakai. Davis menjelaskan bahwa sistem pengolahan informasi mempunyai andil dalam melakukan pengolahan data dari bentuk yang belum berguna menjadi berguna (informasi) bagi penggunanya.

Sejalan dengan penertian-pengertian di atas maka dapat diketahui bahwa informasi mempunyai bermacam-macam model yang berlainan. Dengan mempunyai bermacam-macam model tersebut maka informasi dapat dicetak atau ditulis di atas kertas, disimpan secara elektronik, dapat dikirimkan melalui pos atau dengan menggunakan sarana elektronik baik dalam format audio, video maupun kombinasi antara audio dan video.

Di bawah ini adalah skema transformasi data menjadi informasi yang dibutuhkan bagi organisasi, sebagai berikut:



Gambar 2.3: Transformasi Data Menjadi Informasi

Dalam organisasi yang ada saat ini, informasi yang dimiliki akan berbeda-beda tergantung pada bentuk dan tujuan organisasi tersebut didirikan. Beragam jenis informasi ini dijelaskan oleh Pipkins (2000) dimana informasi merupakan aset yang unik yang dimiliki oleh sebuah organisasi. Aset yang unik mengandung maksud bahwa tidak organisasi yang mempunyai kesamaan informasi dengan organisasi yang lainnya walaupun mempunyai kemiripan dalam bidang

operasional. Keunikan ini terjadi karena adanya perbedaan karakteristik dari masing-masing organisasi yang ada sehingga juga akan membedakan informasi dari masing-masing organisasi tersebut.

Dalam penjelasan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tertulis bahwa sistem informasi merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Secara teknis dan manajemen maka sistem informasi merupakan perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi lain secara teknis dan fungsional, sistem informasi merupakan keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input*, *process*, *output*, *storage,* dan *communication.*

Seperti yang telah dikemukaan pada sub bab di atas bahwa suatu sistem manajemen informasi merupakan sistem informasi yang selain melakukan semua pengolahan transaksi yang perlu untuk organisasi, juga memberikan dukungan informasi dan pengolahan untuk fungsi manajemen dan pengambilan keputusannya. Konsep manajemen terhadap sistem informasi merupakan perluasan secara mendasar dari perakunan manajerial dengan mengikutsertakan gagasan dan teknik-teknik ilmu manajemen dan teori keperilakuan tentang manajemen dan pengambilan keputusan (Davis, 1995). McLeod dan P.Schell mendefinisikannya sebagai suatu sistem berbasis komputer yang membuat informasi tersedia bagi para pengguna (*user*) yang mempunyai kebutuhan serupa.

Informasi yang diberikan oleh manajemen sistem informasi akan menjelaskan kepada organisasi tentang apa yang telah terjadi pada masa lalu, apa yang sedang terjadi, dan apa yang kemungkinan akan terjadi di masa depan. Selanjutnya output informasi yang dihasilkan akan digunakan oleh pihak-pihak yang akan memecahkan masalah (baik di lingkungan manajemen maupun

kalangan professional) dalam mengambil keputusan guna memecahkan masalah organisasinya itu.

2.2.6. Manajemen Keamanan Informasi

Informasi merupakan aset penting dalam suatu organisasi bisnis yang merupakan salah satu sumber daya utama dari organisasi terebut. Akibatnya, sumber daya informasi mempunyai potensi terjadinya gangguan terhadap berbagai ancaman dan kerentanan baik dari dalam maupun dari luar secara disengaja maupun tidak disengaja. Untuk mencegah terjadinya hal yang tidak diinginkan tersebut maka informasi harus selalu dilindungi secara efektif dan efisien dengan menggunakan upaya manajemen yang tepat.

Mc.Crie (2001) memberikan definisi keamanan sebagai upaya untuk melakukan proteksi terhadap aset-aset yang ada dari kerugian dan kehilangan. Fischer dan Green (1998) mengatakan: *"Security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury.*

Pengamanan terhadap sistem informasi bukan hanya sekedar mengamananankan data komputer semata, tetapi juga merupakan suatu proses perlindungan terhadap kekayaan intelektual dari suatu organisasi. Pengamanan terhadap sistem informasi terhadap sumber daya suatu organisasi harus dilaksanakan secara komprehensif, konsisten, serta dengan beaya yang efektif baik dalam merumuskan strategi pengamanan maupun implementasinya. Berkaitan dengan hal tersebut maka Fitzgerald (2006) dalam tulisannya menyatakan:

> *"...although each organization has diffferent values, principles, and strategies to move the business forward, it must have techniques for building management commitment through the implementation of a successful information security council."*

Memperkuat pendapat di atas, Pipkin (2000) dalam tulisannya mendefinisikan bahwa perlindungan terhadap sistem informasi sebagai pengurangan atas kerentanan dari organisasi dengan menerapkan sistem

perlindungan pengamanan. Lebih lanjut dikatakannya bahwa keamanan sistem informasi membutuhkan keseimbangan antara beaya keamanan dengan kemungkinan kerugian akibat pencurian, kerusakan, penyingkapan atau penolakan akses ke sumber daya yang dilindungi.

Kemudian Fitzgerald (2006) dalam pandangannya terhadap keamanan atas informasi dalam suatu organisasi juga menyatakan bahwa komitmen pihak manajemen yang dilakukan secara berkesinambungan atas sistem keamanan informasi harus mencakup tiga aspek tradisional tujuan keamanan dari informasi tersebut. Ketiga aspek tradisional tersebut adalah: (1). *Protect Confidentiality*; (2) *Ensure Data Integrity*; dan (3) *Ensure Data Availability*.

Melengkapi beberapa definisi di atas maka Price (2006) memberikan pandangannya tentang klasifikasi keamanan informasi. Menurut Price:

> "*Information security is a composition of people, processes, and products. People are system users, administrators, and managers. Processes represent the operational aspects of the system which are manual or automated. Products are the physical and intangible attributes such as facilities and the hardware and software components that make up a system.*"

Keamanan terhadap informasi mutlak dilaksanakan dalam setiap kegiatan operasional dari organisasi. Hal paling pokok yang perlu dicapai oleh organisasi dalam hal keamanan informasi, selain untuk mencapai misi atau sasarannya, adalah mendapatkan tingkat kepercayaan dari masyarakat akan keabsahan informasi tersebut. Rockley dan Hill (1981) menyatakan:

> "*...these penalties have several form. financial loss - whether of cash, goods or information - is the most common. Both the latter frequently have a market value, though the market value of goods is, however, not always realised. The penalties may take another and more insidious form. Costumers and clients who hear of security breaches which they - rightly or wrongly - attribute of laxity, may decide that the company is not trustworthy.*"

Mengacu dari cakupan teoritis di atas maka dapat dijelaskan bahwa keamanan informasi meliputi kebijakan, prosedur dan aktifitas untuk melindungi aset informasi, baik manusia, fisik bangunan maupun informasi itu sendiri, terhadap berbagai jenis ancaman yang dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan operasional suatu organisasi untuk menjamin organisasi tersebut mencapai misi atau sasaran yang ingin dicapainya serta mendapatkan kepercayaan dari masyarakat dengan mengimplementasikan sistem keamanan informasi.

Seperti halnya cakupan keamanan yang telah meluas, maka pandangan tentang tanggung jawab manajemen juga secara otomatis meluas. Manajemen diharapkan tidak hanya menjaga agar sumber daya informasi tetap aman, namun juga diharapkan untuk menjaga perusahaan tersebut tetap berfungsi setelah terjadinya suatu bencana atau gangguan pada sistem keamanan tersebut.

Kemudian Mc.Leod dan P.Schell (2008, p.271) melakukan pembagian aktifitas keamanan terhadap informasi, yaitu strategi keamanan informasi (*information security strategic*) yang merupakan aktifitas untuk menjaga agar sumber daya informasi tetap aman dan manajemen keberlangsungan bisnis (*business continuity management*) sebagai suatu aktifitas untuk menjaga agar perusahaan dan sumber daya informasinya tetap berfungsi setelah terjadinya bencana maupun gangguan yang lain.

2.2.7. Strategi Keamanan Informasi

Kata strategi merupakan turunan dari bahasa Yunani "*strategos*" yang memiliki makna komandan militer pada masa demokasi Athena. Pada awalnya strategi hanya dipergunakan untuk kepentingan militer saja, namun saat ini strategi juga digunakan oleh organisasi sebagai cara untuk mencapai tujuannya. Dalam upaya untuk mencapai keseluruhan tujuan dan berbagai sasaran organisasi memerlukan strategi yang mantap dan jelas. Siagian (2001) memberikan gambaran bahwa dalam lingkungan dunia bisnis, strategi pada umumnya didefinisikan sebagai pernyataan sadar oleh manajemen tentang bidang bisnis apa

yang ditekuni oleh organisasi sekarang dan dalam kegiatan bisnis apa organisasi akan bergerak di masa yang akan datang.

Strategi keamanan informasi merupakan implementasi dari proses pelaksanaan keamanan terhadap informasi dari suatu organisasi dengan menerapkan manajemen keamanan sistem informasi (*Information Security Management System*-ISMS). Sejalan dengan adanya keunikan dari suatu organisasi yang mencakup karakteristik organisasi, lokasi, aset, dan teknologi yang dimiliki dan digunakan maka tentunya terdapat perbedaan penerapan strategi keamanan informasi antara organisasi satu dengan organisasi lainnya. Keunikan yang menjadi ciri khas dari tiap-tiap organisasi tersebut akan mempengaruhi terhadap penentuan parameter dari masing-masing indikator yang akan diteliti (Suryadi, 2010).

Tahap pertama dari penerapan strategi keamanan informasi adalah melakukan identifikasi ancaman. Hadiman (2009) menyatakan bahwa ancaman atau bahaya merupakan suatu keadaan atau kejadian yang bila dibiarkan pasti akan membawa kerugian bagi organisasi. Untuk mendapatkan identifikasi ancaman dilakukan dengan melakukan analisis terhadap sumber ancaman yang diprakirakan terjadi serta dikolaborasikan dengan bentuk ancaman yang akan terjadi pada organisasi.

Sumber ancaman yang diprakirakan akan terjadi terbagi menjadi tiga hal, yaitu manusia, alam, dan teknologi. Hadiman menjelaskan bahwa ancaman yang bersumber dari manusia diklasifikasikan menjadi tiga kelompok, yaitu: (a). Group; (b). *Crowd*/khalayak; dan (c). Massa. Kemudian ancaman yang bersumber dari alam dapat berupa ancaman dari flora/fauna dan terjadinya bencana alam. Ancaman yang bersumber dari teknologi sebagai akibat dari proses dan akibat dari produk.

McLeod dan P.Schell menyatakan bahwa bentuk ancaman pada keamanan informasi pada dasarnya mewakili tindakan yang tidak terotorisasi. Bentuk ancaman ini dibagi menjadi empat jenis, yaitu: (a). Pengungkapan informasi yang tidak terotorisasi dan pencurian; (b). penggunaan yang tidak terotorisasi; (c). penghancuran yang tidak terotorisasi dan penolakan layanan; dan (d). modifikasi yang tidak terotorisasi.

Pengungkapan informasi yang tidak terotorisasi dan pencurian adalah ketika suatu basis data dan perpustakaan peranti lunak tersedia bagi orang-orang yang tidak berhak memiliki akses, hasilnya adalah hilangnya informasi yang dibutuhkan pada organisasi. Penggunaan yang tidak terotorisasi terjadi ketika orang-orang yang tidak berhak menggunakan sumber daya perusahaan mampu melakukan hal tersebut. Kemudian penghancuran yang tidak terotorisasi dan penolakan layanan maksudnya sesuatu yang dapat merusak aset informasi sehingga menyebabkan operasional organisasi menjadi tidak berfungsi. Sedangkan modifikasi yang tidak terotorisasi adalah perubahan yang dilakukan pada data, informasi, dan peranti lunak organisasi dimana perubahan tersebut berlangsung tanpa disadari sehingga menyebabkan para pengguna output informasi menjadi salah dalam mengambil keputusan.

Kemudian Hadiman (2009) mengklasifikasikan nilai ancaman menjadi enam kategori, yaitu: ancaman bencana, ancaman sangat tinggi, ancaman tinggi, ancaman sedang, ancaman rendah, dan ancaman yang tidak diketahui. Tabel berikut ini menunjukkan nilai terhadap ancaman berdasarkan teori Hadiman yang telah dimodifikasi, sebagai berikut:

Tabel 2.2: Klasifikasi Nilai Ancaman

ANCAMAN	NILAI ANCAMAN	DAMPAK
[illegible]		
Sangat Tinggi	5	Sangat Serius
Tinggi	4	Serius
Sedang	3	Sedang
Rendah	2	Relatif tidak penting
Tidak Diketahui	1	[illegible]

Tahap kedua adalah mendefinisikan resiko dengan menggunakan metodologi manajemen resiko. Metodologi manajemen resiko terdiri dari tiga langkah yang harus dilaksanakan, yaitu (a). melakukan identifikasi aset (aset manusia, aset fisik bangunan dan aset informasi); (b). melakukan analisis resiko; dan (c). melakukan tidak lanjut atau respon terhadap resiko (melakukan penerimaan, pengurangan, pemindahan dan penghilangan resiko).

Untuk mendapatkan identifikasi terhadap aset-aset yang tercakup di dalam TMC PMJ dilaksanakan dengan cara mengamati dan melakukan wawancara terhadap personel operasional TMC PMJ serta berinteraksi secara langsung terhadap aplikasi layanan operasional yang ada. Upaya pengidentifikasian aset ini didasari pada tiga aspek dasar tujuan keamanan informasi dengan memperhatikan aspek kerahasiaan, integritas maupun ketersediaan dari aset-aset tersebut. Selanjutnya aset-aset tersebut diklasifikasi menjadi tiga kategori dan dilambangkan dalam bentuk *numerik*, yaitu:

- Rendah (1).
- Sedang (2).
- Tinggi (3).

Angka 3 menunjukkan bahwa nilai aset tersebut tinggi, demikian sebaliknya untuk nilai 1 menunjukkan bahwa nilai aset tersebut rendah.

Selain melakukan penilaian terhadap aset yang ada, juga perlu memperhitungkan kerentanan aset tersebut terhadap situasi dan kondisi pada TMC PMJ. Menurut ISO 27001:2005, kerentanan suatu aset (*vulnerability*) merupakan " *a weakness of an asset or group of assets that can be exploited by a threat*" (Snare & Kuper, 2005). Hadiman (2009) menyatakan untuk melakukan penilaian terhadap kerentanan suatu obyek vital secara keseluruhan mencakup empat komponen penting, yaitu:

1. Ketersediaan (*Availability*).
   Keberadaan aset dan kemungkinan dalam kaitannya dengan rencana dan serangan.
2. Pengaksesan (*Accessibility*).
   Keterjangkauan aset terhadap skenario serangan.
3. Pengamanan organik (*Organic security*).
   Ketersediaan dari sistem atau personel untuk mengamankan aset.
4. Ketangguhan fasilitas (*Facility hardness*).
   Kemampuan target itu sendiri untuk tidak mudah diserang, biasanya karena bahan, kerumitan, atau rancangan dari aset itu sendiri.

Selanjutnya kerentanan aset tersebut diklasifikasi menjadi tiga kategori dan dilambangkan dalam bentuk *numerik*, yaitu:

- Rendah (1).
- Sedang (2).
- Tinggi (3).

Setelah melakukan identifikasi aset dengan melakukan penilaian terhadap nilai aset dan kerentanan terhadap aset tersebut maka langkah selanjutnya yang harus dilakukan adalah melakukan analisis terhadap resiko. Resiko keamanan merupakan konsekuensi yang tidak bisa ditolak atau dihilangkan dari operasional organisasi, oleh karena itu yang bisa dilakukan oleh organisasi adalah mengurangi dampak resiko yang diprakirakan akan terjadi. Untuk mengurangi dampak terjadinya resiko terhadap organisasi maka perlu melakukan manajemen resiko. Dengan melakukan manajemen resiko maka manajemen perusahaan dapat mengetahui secara jelas aset yang harus dilindungi, ancaman yang akan terjadi, perlindungan apa yang harus diberikan dan gambaran berapa besar kerugian yang bisa dihindari.

Resiko adalah kombinasi dari ancaman yang berakibat pada munculnya kerentanan dalam organisasi sehingga dapat menyebabkan masalah atau gangguan dari suatu aset. Secara komprehensif definisi resiko dinyatakan oleh Shaurette bahwa resiko merupakan akumulasi dari ancaman yang diprakirakan terjadi, nilai dari suatu aset, dan kerentanan terhadap aset tersebut. Hal ini juga dikuatkan dengan pernyataan dari Albert dan Dorofee (2002, p.13) dimana, "*An information security breaks down into four major components: asset, threat, vulnerability, and impact. An information security risk evaluation must account for all of these components.*"

Shaurette (2006, p.237) menyatakan bahwa hasil penghitungan matematis atas resiko merupakan hubungan antara resiko, ancaman, kerentanan dan aset organisasi yang telah didapatkan disebut nilai impact (*impact value*). Rumusan berikut akan mendeskripsikan hasil penghitungan dari nilai impact menurut Shaurette yang telah dimodifikasi, yaitu:

RISK (R) = THREAT (T)² x ASSET VALUE (AV) x VULNERABILITY (V)

Keterangan:
Resiko = (R) Risk → Impact Value.
Ancaman = (T) Threat (1-6).
Nilai Aset = (AV) Asset Value (1-3).
Kerentanan = (V) Vulnerability (1-3).

Gambar 2.4: Hubungan Antara Resiko, Ancaman, Kerentanan dan Aset Organisasi

Analogi terhadap rumusan tersebut adalah sebagai berikut:

- Semakin tinggi ancaman yang akan terjadi maka nilainya akan maksimum (6). Sebaliknya, semakin rendah ancaman yang akan terjadi maka nilainya akan minimum (1).
- Unsur penilaian kerentanan terhadap aset berada pada rentang nilai (1) untuk nilai minimum dan nilai (3) untuk nilai maksimum.
- Unsur penilaian nilai aset berada pada rentang nilai (1) untuk aset yang bernilai rendah dan nilai (3) untuk aset yang bernilai tinggi.
- Sehingga dapat ditentukan bahwa nilai resiko yang akan didapati berada pada rentang nilai (324) untuk resiko maksimum dan rentang nilai (1) untuk resiko minimum.
- Hasil penilaian terhadap resiko (analisis resiko) ini disebut nilai impact (*impact value*) sebagai dampak resiko yang terjadi.

Langkah ketiga dalam pendefinisian resiko adalah melakukan tindak lanjut penanganan atas hasil *impact value*. Langkah tindak lanjut ini diawali dengan evaluasi bagi penanganan resiko untuk menentukan rentang penilaian atas tingkatan *inherent risk* dalam menentukan tingkatan *risk level*, dan pemilihan current control untuk menangani resiko tersebut (*risk control*) berdasarkan kebijakan keamanan informasi yang telah dilakukan oleh Ditlantas Polda Metro Jaya terhadap keamanan informasi TMC PMJ. Hasil tingkatan *risk level* ini akan menentukan tindak lanjut efektifitas dan efisiensi penanganan resiko, yaitu: diterima, dikurangi, dipindahkan, atau dihilangkan.

Penentuan atas tingkatan *risk level* dilaksanakan dengan melakukan penggabungan hasil penilaian *impact value* terhadap mitigasi resiko yang dilakukan saat ini (*risk control*) dan frekuensi kemungkinan terjadinya suatu kejadian yang mengandung resiko (*likelihood*). Suryadi memberikan klasifikasi penilaian atas risk control adalah sebagai berikut:

Tabel 2.3: Mitigasi Terhadap Resiko Saat Ini

SCORE		
Rata-rata	3	Medium
Lemah	2	Significant

Selanjutnya Dougherty (2006) memberikan klasifikasi penilaian atas likelihood atas hal ini ke dalam tabel sebagai berikut:

Tabel 2.4: Nilai Likelihood

DESCRIPTION	SCORE	LIKELIHOOD
Moderate	3	The event should occur at some time.
Unlikely	2	The event could occur at some time.

Kemudian setelah dilakukan penghitungan secara matematis maka apabila ternyata perlakuannya ternyata tidak diterima atau melebihi tingkatan *risk level* yang telah ditentukan maka apabila organisasi menginginkan aset tersebut tetap ada maka dilakukan penilaian tambahan berdasarkan obyektif control dan control

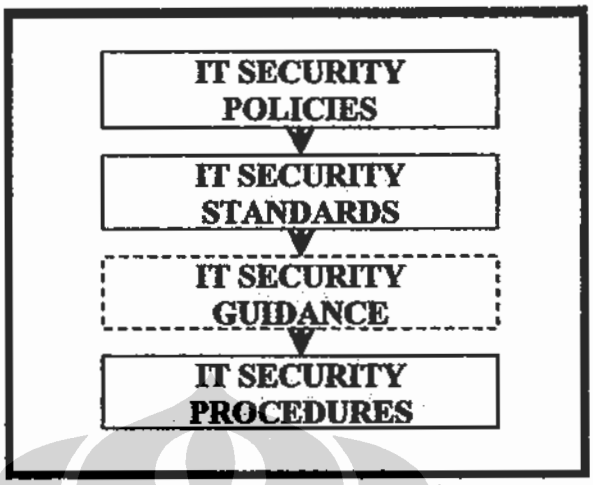
berdasarkan ISO 27001:2005, serta perlakuan atau tindakan terhadap *inherent risk* tersebut sehingga didapatkan kondisi diterima pada *risk level*.

Tahapan ketiga dan keempat dari strategi pengamanan terhadap informasi adalah menentukan kebijakan keamanan dan mengimplementasikan pengendalian yang akan diterapkan di dalam operasional organisasi. kedua tahapan ini merupakan hasil pendefinisian resiko atas organisasi yang telah dilakukan sebelumnya dengan mengimplementasikan ISO 27001:2005 sebagai standar sistem keamanan informasi internasional.

Kebijakan keamanan adalah rumusan tertulis yang berisi tentang tanggung jawab individu maupun manajemen dalam mengatur apa yang boleh dilakukan dan tidak untuk melindungi terhadap aset-aset informasi yang ada. Hal pokok yang harus dijadikan pedoman dalam melakukan penyusunan kebijakan keamanan pada organisasi adalah berkaitan dengan siapa yang melakukan akses informasi, informasi apa yang bisa diakses dan bagaimana pengamanannya yang diimplementasikan ke dalam bentuk prosedur pengendalian.

Kebijakan keamanan informasi mencakup semua aturan yang menjamin perlindungan terhadap aset informasi secara keseluruhan yang harus didukung oleh seluruh komponen organisasi agar dapat dilaksanakan dengan optimal. Untuk mendapatkan dukungan dari seluruh komponen perusahaan maka kebijakan keamanan informasi harus berisikan tentang empat hal, yaitu kebijakan keamanan, standar keamanan informasi, panduan keamanan informasi dan prosedur operasional keamanan informasi untuk melindungi informasi terhadap berbagai jenis ancaman yang dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan operasional suatu organisasi

. Keterkaitan antara kebijakan keamanan informasi, standar keamanan informasi, panduan keamanan informasi dan prosedur operasional keamanan informasi diilustrasikan ke dalam gambar sebagai berikut:



Gambar 2.5: Keterkaitan Unsur Strategi Keamanan Informasi

Kebijakan keamanan informasi merupakan pernyataan tertulis yang dibuat oleh manajemen senior dan menjadi elemen utama bagi penerapan standar keamanan informasi. Standar keamanan informasi ditetapkan dengan menggunakan metodologi yang telah ditetapkan dan bersifat wajib untuk dilaksanakan. Sedangkan panduan merupakan rekomendasi dari tindakan maupun operasional yang ditujukan kepada pengguna. Panduan ini tidak mutlak untuk dilaksanakan dalam menetapkan suatu prosedur operasional terhadap pengguna (digambarkan dengan garis putus-putus). Kemudian prosedur merupakan langkah-langkah detail yang perlu diikuti oleh setiap pengguna dalam melaksanakan tugas-tugasnya.

2.2.8. Manajemen Keberlangsungan Bisnis (Business Continuity Management-BCM)

Manajemen keberlangsungan bisnis merupakan suatu aktifitas yang ditujukan untuk menentukan operasional setelah terjadi gangguan terhadap sistem informasi. Awalnya aktifitas BCM ini disebut perencanaan bencana, namun istilah yang lebih positif perencanaan kontijensi (*contingency plan*) menjadi lebih populer dan akhirnya menjadi aktifitas manajemen keberlangsungan bisnis.

Aktifitas manajemen keberlangsungan bisnis merupakan dokumen tertulis formal yang menyebutkan detail tindakan-tindakan yang harus dilakukan jika

terjadi gangguan atau ancaman gangguan pada operasi komputasi suatu organisasi. Dalam implementasinya, aktifitas ini dibagi menjadi beberapa subrencana yang menjawab beberapa kontijensi yang spesifik (Plains, 1977). Berdasarkan hal tersebut maka McLeod dan P.Schell mengklasifkasikan aktifitas ini ke dalam tiga subrencana, yaitu:

1. Rencana Darurat.

   Berisi tentang cara-cara yang akan menjaga keamanan karyawan jika bencana terjadi. Rencana ini dilandasi pada antisipasi atas terjadinya ancaman bagi personel yang diprakirakan terjadi.

2. Rencana Cadangan.

   Rencana ini diperoleh melalui kombinasi dari redudansi, keberagaman, serta mobilitas yang bertujuan untuk membuat organisasi mampu melanjutkan operasinya (bahkan setelah hilangnya kemampuan komputer).

3. Rencana Catatan Penting.

   Catatan penting organisasi (*vital record*) organisasi adalah dokumen kertas, microfilm, serta media penyimpanan optis dan magnetis yang penting untuk meneruskan bisnis organisasi tersebut.

Dalam pembuatan rencana darurat meliputi standar operasional prosedur yang mencakup sistem alarm, prosedur evakuasi personel, dan sistem pemadaman api pada TMC PMJ jika bencana tersebut terjadi. Berkaitan dengan rencana cadangan maka manajemen TMC PMJ harus dapat mengatur agar fasilitas komputer cadangan tersedia seandainya fasilitas yang biasa digunakan hancur dan rusak sehingga tidak dapat digunakan.

Kegiatan untuk mendapatkan rencana cadangan dalam aktifitas manajemen keberlangsungan bisnis meliputi tiga aspek, yaitu:

1. Melakukan duplikasi peranti keras, peranti lunak, dan data yang ada pada TMC PMJ (redudansi) sehingga set cadangan dapat meneruskan proses operasional.
2. Sumber daya informasi tidak dipasang pada tempat yang sama dan terpisah untuk wilayah-wilayah operasi yang bebeda-beda (keragaman)

sehingga apabila terjadi bencana maka proses operasional dapat dilaksanakan di tempat lain dengan kualitas operasional yang sama.

3. Membuat perjanjian dengan para pengguna peralatan yang sama sehingga masing-masing organisasi dapat menyediakan cadangan kepada yang lain jika terjadi bencana besar.

Catatan penting (*vital record*) TMC PMJ meliputi dokumen kertas, microfilm dan media penyimpanan optis dan magnetis yang penting untuk meneruskan *core business* dari TMC PMJ. Dengan membuat rencana catatan penting akan menentukan cara tentang bagaimana catatan penting tersebut dilindungi. Selain menjaga catatan penting tersebut pada situs komputer, salinan cadangan juga diupayakan harus disimpan di lokasi yang terpencil. Dengan kata lain bahwa secara fisik semua jenis catatan penting tersebut dipindahkan ke lokasi terpencil tersebut, sedangkan catatan komputer dapat ditransmisikan secara elektronik.

2.2.9. ISO 27001:2005

ISO (*International Organization for Standardization*) merupakan organisasi internasional yang mempunyai tujuan memberikan informasi kepada para *stakeholder* yang berkaitan dengan penerapan standarisasi terhadap hal-hal yang berkaitan dengan kegiatan organisasinya ("Organization for Standardization", 2010). Dalam pengertian lain bahwa ISO berisikan tentang kerangka acuan atau bahasa teknologi umum yang berkaitan dengan spesifikasi atau kriteria tertentu untuk ditetapkan secara konsisten dalam klasifikasi materi, dalam bidang manufaktur dan pemasok produk, dalam pengujian dan analisis serta dalam bidang terminologi danpenyediaan layanan agar organisasi yang menerapkan standar internasional ini mempunyai pedoman dalam mencapai tujuannya.

ISO diambil dari bahasa Yunani "*iso*" yang berarti *equal* atau sebanding. Istilah ini diambil dengan maksud agar apabila digunakan dalam bahasa apapun dan negara manapun maka sebutan nama organisasinya akan tetap selalu berbunyi

"ISO". ISO mulai berdiri sejak tahun 1947 dan hingga sekarang telah menerbitkan lebih dari 18.000 standar internasional, mulai standar untuk kegiatan seperti pertanian dan konstruksi, hingga teknik permesinan, kemudian juga perangkat-perangkat medis, hingga perkembangan teknologi informasi yang terbaru.

ISO 27001:2005 adalah sebuah standar Sistem Manajemen Keamanan Informasi (Information Security Management System-ISMS) yang diterbitkan pada bulan Oktober 2005 oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC). ISO 27001:2005 merupakan pengembangan dari standar Sistem Manajemen Keamanan Informasi sebelumnya yang dikenal dengan nama ISO 27000

ISO 27001:2005 secara resmi menetapkan suatu sistem manajemen yang dimaksudkan untuk membawa keamanan informasi di bawah kendali manajemen secara eksplisit. Sebagian besar organisasi memiliki sejumlah kontrol keamanan informasi tanpa menerapkan ISMS. Kontrol keamanan ini mempunyai kelemahan dalam implementasinya karena cenderung tidak teratur dan terputus-putus (*unsustainable*). Dengan menerapkan ISO 27001:2005 akan mengharuskan manajemen untuk selalu melakukan pengendalian secara:

1. Sistematis memeriksa risiko keamanan informasi pada organisasi, dengan mempertimbangkan ancaman, kerentanan dan dampak yang akan terjadi;
2. perencanaan desain dan implementasi ruang yang koheren dan komprehensif berkaitan dengan kontrol keamanan informasi dan/atau bentuk lain terhadao perawatan risiko (seperti menghindari risiko atau transfer risiko) untuk mengatasi risiko-risiko yang dianggap dapat diterima; serta
3. mengadopsi proses manajemen menyeluruh untuk memastikan bahwa kontrol keamanan informasi tetap berjalan untuk memenuhi kebutuhan keamanan informasi suatu organisasi secara berkesinambungan.

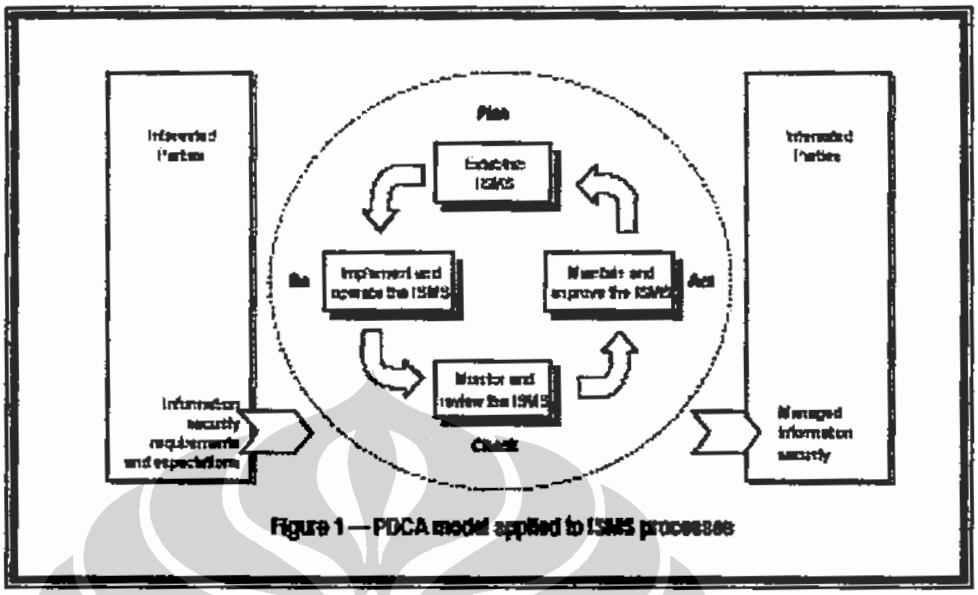
Strategi keamanan informasi suatu organisasi disusun berdasarkan Manajemen Keamanan Informasi, atau yang lebih dikenal sebagai *Information Security Management Information* (ISMS). Sebagai implementasi dalam penerapan Manajemen Keamanan Informasi pada TMC PMJ dilakukan

pendekatan sistemik berupa kontrol obyek dalam mengelola informasi yang bersifat sensitif dengan tujuan untuk mengamankan sumber daya informasi tersebut. Pendekatan yang dilakukan untuk mewujudkan hal tersebut adalah dengan menerapkan manajemen resiko berdasarkan pengendalian ISO 27001:2005 yang bertujuan untuk menilai sejauh mana dampak keamanan informasi yang mungkin dapat ditangani.

Dalam implementasi terhadap model arsitektur pengamanan tersebut, diperlukan pedoman umum yang harus dilaksanakan sebagai suatu standar operasional prosedur (SOP) agar segala aktifitas opersionalisasi TMC PMJ dapat berjalan dengan teratur dengan menerapkan model ISO 27001:2005 untuk membangun, melaksanakan, mengoperasikan,memantau, memeriksa, memelihara dan memperbaiki suatu Sistem Manajemen Keamanan Informasi (*Information Security Management System*-ISMS) yang berada di dalamnya. Semakin sederhana situasi lingkungan dari organisasi tersebut maka akan semakin sederhana pula ISMS yang dibangun.

Desain dan implementasi ISMS terhadap suatu organisasi dipengaruhi oleh kebutuhan dan tujuan, persyaratan keamanan, proses yang digunakan serta ukuran dan struktur organisasi tersebut. Disamping itu, desain dan implementasi atas sistem pendukung tersebut diharapkan selalu berubah disesuaikan dengan situasi dan kondisi terkini. Proses perubahan yang senantiasa terjadi tersebut membuat ISO 27001 menggunakan metode pendekatan proses dalam desain dan implementasi ISMS suatu organisasi.

ISO 27001 mengadopsi pendekatan proses: *Plan-Do-Check-Act* (PDCA) yang diaplikasikan di dalam proses model ISMS secara keseluruhan. Keempat hal tersebut dapat dituangkan ke dalam gambar diagram sebagai berikut (Snare & Kuper, 2005):



Gambar 2.6: Skema Diagram Proses ISMS dengan Menerapkan PDCA

Tabel 2.5: Penjelasan Proses ISMS dengan Menerapkan PDCA

Perencanaan (Membangun ISMS)	ISMS menetapkan kebijakan, tujuan, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi untuk memberikan hasil yang sesuai dengan organisasi secara keseluruhan kebijakan dan tujuan.
Tindakan (Implementasi dan Operasional ISMS)	Menerapkan dan mengoperasikan kebijakan ISMS, kontrol, proses dan prosedur.
Pemeriksaan (Memonitor & Meninjau ISMS)	Menilai dan jika memungkinkan, proses mengukur kinerja terhadap kebijakan ISMS, tujuan dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk diperiksa.
Pelaksanaan (Pemeliharaan & Peningkatan ISMS)	Mengambil tindakan korektif dan pencegahan, berdasarkan hasil audit internal ISMS dan pandangan pihak manajemen atau informasi lain yang relevan, untuk mencapai perbaikan ISMS yang berkelanjutan.

2.2.10. *Traffic Management Center* (TMC)

Traffic Management Center adalah sarana penunjang dengan menggunakan teknologi komputer yang *integrated* dan dapat membantu kecepatan informasi yang disampaikan kepada seluruh pihak yang berkepentingan, sehingga diharapkan mampu membantu pelaksanaan tugas Polisi

Lalu Lintas dalam menangani kemacetan, kecelakaan, dan pelanggaran lalu lintas secara cepat dan professional (Susilo, 2006).

TMC berfungsi untuk memberikan akses kepada masyarakat yang ingin mencari atrau memberikan informasi seputar informasi lalu lintas secara online. Lebih lanjut dikatakan Susilo, *Traffic Management Center* (TMC) didirikan dengan tujuan untuk:

a. Pelayanan Quick Response Time secara professional terhadap masyarakat.
b. Analisis pelanggaran dan kecelakaan lalu lintas.
c. Pusat informasi SIM, STNK, dan BPKB bagi Polri dan masyarakat.
d. Pusat kendali hilang-temu kendaraan bermotor.
e. Pusat kendali patroli kendaraan bermotor dalam mewujudkan kamseltibcar lantas.
f. Pusat informasi kualitas baku mutu udara.
g. Pusat pengendali lalu lintas.

Operasionalisasi TMC merupakan suatu penjabaran *action plan* dari Polda Metro Jaya, yang mengacu dari kebijakan Kapolri terhadap implementasi perpolisian masyarakat (*community policing*), dengan membentuk sistem manajemen penyelenggaraan keamanan di Jakarta oleh Polda Metropolitan Jakarta Raya untuk mewujudkan dan memelihara keamanan, keselamatan, ketertiban dan kelancaran lalu lintas. Fasilitas yang dimiliki oleh TMC adalah:

a. Terhubung dengan internet untuk melaksanakan pelayanan masyarakat secara online.
b. GIS (*Globai Information System*) untuk mempermudah kontrol kepada petugas di lapangan.
c. Call center 1717 untuk menerima input masukan laporan atau pengaduan dari masyarakat menggunakan SMS (*Short Message Service*),
d. Akses *database* SIM, STNK, dan BPKB secara *online*.
e. CCTV pada daerah rawan macet (144 CCTV yang terintegrasi dengan CCTV milik Pemprov DKI JAYA).
f. Pemantauan terhadap GPS yang dipasang pada tiap-tiap mobil patroli yang ada di Jakarta.

g. Faximile.

h. Peralatan komunikasi (telepon dan Handy Talkie).

2.2.11. Konsep Perpolisian Masyarakat (*Community Policing*)

Konsep perpolisian masyarakat (*Community Policing*) tertuang dalam Peraturan Kapolri Nomor 7 Tahun 2008 tentang Pedoman Dasar Strategi dan Implementasi Pemolisian Masyarakat dalam Penyelenggaraan Tugas Polri. Dalam ketentuan umum Peraturan Kapolri tersebut dijelaskan bahwa definisi perpolisian masyarakat (*Community Policing*) adalah sebagai berikut:

a. *Policing*, dapat diartikan sebagai:
   - Perpolisian, yaitu segala hal ihwal tentang penyelenggaraan fungsi kepolisian, tidak hanya menyangkut operasionalisasi (taktik/ teknik) fungsi kepolisian tetapi juga pengelolaan fungsi kepolisian secara menyeluruh mulai dari tataran manajemen puncak sampai dengan manajemen lapis bawah, termasuk pemikiran-pemikiran filsafati yang melatarbelakanginya.
   - Pemolisian, yaitu pemberdayaan segenap komponen dan segala sumber daya yang dapat dilibatkan dalam pelaksanaan tugas atau fungsi kepolisian guna mendukung penyelenggaraan fungsi kepolisian agar mendapatkan hasil yang lebih optimal.

b. *Community*, yang diterjemahkan komunitas, dapat diartikan sebagai:
   - Sekelompok warga (laki-laki dan perempuan) atau komunitas yang berada di dalam suatu wilayah kecil yang jelas batas-batasnya (*geographic-community*). Batas wilayah komunitas dapat berbentuk RT, RW, desa, kelurahan, ataupun berupa pasar/pusat belanja/mall, kawasan industri, pusat/ komplek olahraga, stasiun bus/kereta api, dan lain-lainnya.
   - Warga masyarakat yang membentuk suatu kelompok atau merasa menjadi bagian dari suatu kelompok berdasar kepentingan (*community of interest*), contohnya kelompok berdasar etnis/suku, agama, profesi, pekerjaan, keahlian, hobi, dan lain-lainnya.

- Polmas diterapkan dalam komunitas-komunitas atau kelompok masyarakat yang tinggal di dalam suatu lokasi tertentu ataupun lingkungan komunitas berkesamaan profesi (misalnya kesamaan kerja, keahlian, hobi, kepentingan dsb), sehingga warga masyarakatnya tidak harus tinggal di suatu tempat yang sama, tetapi dapat saja tempatnya berjauhan sepanjang komunikasi antara warga satu sama lain berlangsung secara intensif atau adanya kesamaan kepentingan. (misalnya: kelompok ojek, hobi burung perkutut, pembalap motor, hobi komputer dan sebagainya) yang semuanya bisa menjadi sarana penyelenggaraan Polmas.

Konsep ini berawal dari penelitian yang dilakukan Bayley (1996) pada kepolisian Amerika yang menemukan adanya korelasi negatif antara konsep peningkatan jumlah personel polisi, penambahan jumlah peralatan kepolisian serta peningkatan intensitas kegiatan kepolisian dibandingkan dengan situasi keamanan dan ketertiban yang diharapkan. Upaya-upaya konvensional yang telah dilaksanakan terbukti tidak mampu menekan gangguan kamtibmas yang terjadi dan bahkan berkembang semakin pesat di masyarakat Amerika.

Kemudian konsep ini dikembangkan oleh Friedmann (1998) dengan menyusun lima konsep hubungan antara polisi dengan masyarakat. Friedmann mengkaji adanya kemungkinan logis yang terjadi sebagai akibat dari hubungan tersebut, yaitu: (a). Polisi dan masyarakat yang keduanya eksklusif dan berdiri sendiri-sendiri; (b). polisi dan masyarakat yang keduanya berduplikasi penuh; (c). polisi merupakan bagian dari masyarakat; (d). masyarakat merupakan bagian dari polisi; serta (e). sebagian dari keduanya saling tumpang-tindih.

Pada akhir pengkajian dari lima konsep ini, Friedmann tegas menyatakan bahwa polisi bukanlah satu-satunya kekuatan dalam masyarakat yang bertindak sebagai penegak hukum dan ketertiban. Masyarakat pada dasarnya menyelenggarakan kepolisiannya sendiri dengan kekuatan lembaga kontrol sosial informal yang bersifat internal dan terbatas. Dalam banyak hal penjaga keamanan pribadi yang dilakukan secara internal oleh masyarakat menunjukkan bahwa mereka telah melakukan berbagai fungsi pemeliharaan ketertiban, dan dalam

kasus-kasus tertentu bahkan polisi pun tidak sanggup mempertahankan hukum dan ketertiban.

Lingkungan yang menyelenggarakan sistem kepolisiannya sendiri merupakan contoh yang baik bahwa dalam cakupan yang terbatas masyarakat dapat berjalan lestari tanpa kehadiran polisi yang berseragam. Namun ketika masalah tidak lagi tertangani oleh lingkungan masyarakat maka disini dibutuhkan peranan polisi untuk melakukan tindakan guna menyelesaikan masalah yang terjadi.

Berdasarkan beberapa hal tersebut maka Friedmann menarik kesimpulan bahwa mandat masyarakat luas kepada polisi mengamanatkan perluasan dan tindakan penegakan hukum yang terbatas dan reaktif seperti pada sistem kepolisian tradisional menjelma menjadi sistem kepolisian modern yang menekankan aspek layanan sosial yang lebih proaktif. Agar pelaksanaan tugas-tugas polisi menjadi lebih efektif dan efisien maka Friedmann merekomendasikan perubahan tindakan polisi tradisional reaktif, yang terbatas pada berpatroli, melayani pengaduan lewat telepon, melakukan penahanan tersangka yang melakukan kejahatan dan menjaga ketertiban, menjadi strategi polisi modern proaktif yang melibatkan masyarakatnya untuk turut melakukan upaya kepolisian terbatas dalam bentuk pemolisian masyarakat guna menciptakan serta mempertahankan keamanan dan ketertiban di lingkungan masyarakat tersebut.

Senada dengan kesimpulan di atas, Thibault, Linch & McBride memberikan rekomendasi positif berkaitan dengan penerapan strategi polisi modern proaktif untuk menciptakan keamanan dan ketertiban di dalam masyarakat. Mereka berasumsi bahwa pendekatan proaktif menjadi rahasia kesuksesan organisasi kepolisian modern. Pendekatan proaktif dianggap fleksibel dan bersifat utilitarian , tapi selaras dengan prinsip manajemen kepolisian modern sehingga model proaktif harus berisikan COP (*community-oriented policing*), POP (*problem-oriented policing*) dan TQM (*total quality management*) yang diterapkan pada operasi polisi modern saat ini.

Program pemolisian masyarakat merupakan Grand Strategi Polri dalam rangka melaksanakan tugas pokok Polri sebagai pemeliharan kamtibmas, penegakan hukum, pelindung, pengayom serta pelayan masyarakat. Grand

Strategi Polri dalam rangka pelaksanaan pemolisian masyarakat bertujuan untuk mewujudkan kemitraan Polri dengan warga masyarakat yang mampu mengidentifikasi akar permasalahan, menganalisis, menetapkan priorotas tindakan, mengevaluasi efektifitas tindakan dalam rangka memelihara keamanan, ketertiban dan ketentraman masyarakat serta peningkatan kualitas hidup masyarakat.

2.2.12. Kepolisian Negara Republik Indonesia

Istilah "polisi" mulanya berasal dari bahasa Yunani *Politeia* yang berarti seluruh pemerintahan negara kota. Ketika itu istilah polisi mempunyai pengertian yang sedemikian luasnya, bahkan meliputi seluruh pemeritahan kota (termasuk juga di dalamnya urusan-urusan keagamaan seperti penyembahan terhadap dewa-dewanya). Setelah munculnya agama Nasrani maka urusan keagamaan yang semula termasuk dalam urusan pemerintahan menjadi berdiri sendiri sehingga arti polisi mulai menyempit menjadi seluruh pemerintahan dikurangi urusan agama (Kelana, 1994). Pada masa sekarang definisi polisi dalam pengertian mendasar dan umum adalah bagian dari administrasi pemerintahan yang fungsinya memelihara keteraturan dan ketertiban di dalam masyarakat, menegakkan hukum serta mendeteksi dan mencegah terjadinya kejahatan.

Klockars (1985) menyatakan bahwa polisi adalah institusi atau individu yang diberikan otoritas atau kewenangan yang umum oleh negara untuk menggunakan paksaan maupun kekerasan dalam lingkup permasalahan domestik negara atau masalah dalam negeri suatu negara. Dalam upayanya memelihara keterturan dan ketertiban di dalam masyarakat maka pemerintahan pada suatu negara membentuk suatu institusi yang bertugas sebagai pengemban fungsi kepolisian.

Di Indonesia berdasarkan Undang-Undang RI Nomor 2 Tahun 2002 tentang Kepolisian dinyatakan secara tegas pada pasal 3 ayat (1) bahwa pengemban fungsi kepolisian adalah Kepolisian Negara Republik Indonesia yang dibantu oleh kepolisian khusus, penyidik pegawai negeri sipil serta bentuk-bentuk pengamanan swakarsa. Berdasarkan otoritas yang diberikan oleh undang-undang

tersebut maka Kepolisian Negara Republik Indonesia mengemban tugas dan fungsi pemerintahan negara dalam bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan pengayoman dan melaksanakan pelayanan kepada masyarakat agar dapat menciptakan keamanan dalam negeri dengan menjunjung tinggi hak asasi manusia.

Polisi Indonesia merupakan sebuah organisasi nasional yang tidak berada di bawah administrasi pemerintahan akan tetapi menjalankan fungsi-fungsi administratif pemerintahan dalam batas-batas tertentu. Oleh karena itu maka Djamin (1995) menegaskan bahwa fungsi polisi Indonesia lebih tepat berada di bawah negara,bukan di bawah administrasi pemerintahan karena polisi Indonesia juga menjalankan fungsi-fungsi yang mendukung terlaksananya fungsi yudikatif.

Dalam Keputusan Presiden RI Nomor 70 Tahun 2002 tentang Organisasi dan Tata Kerja Kepolisian Negara Republik Indonesia tertuang bahwa Kepolisian Negara Republik Indonesia (Polri) adalah Kepolisian Nasional yang berada di bawah Presiden. Organisasi Polri disusun secara berjenjang dan bersifat sentralistik dari tingkat pusat sampai ke kewilayahan yang dipimpin oleh Kapolri. Organisasi Polri dibagi menjadi dua yaitu organisasi Polri tingkat pusat yang biasa disebut Markas Besar Kepolisan Negara Republik Indonesia (MABES POLRI) dan organisasi Polri tingkat kewilayahan disebut Kepolisian Negara Republik Indonesia Daerah (POLDA).

Polda adalah satuan pelaksana utama kewilayahan yang berada di bawah Kapolri. Polda dipimpin oleh Kepala Kepolisian Negara Republik Indonesia Daerah (Kapolda) dengan dibantu Wakapolda yang bertugas menyelenggarakan tugas Polri pada tingkat kewilayahan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Kapolda dalam melaksanakan tugasnya pada tingkat kewilayahan bertanggung jawab langsung kepada Kapolri.

Untuk dapat mengoperasionalkan tugas-tugasnya sebagai pelindung, pengayom, dan pelayan masyarakat, serta melakukan penegakan hukum, maka Polri diberi kewenangan umum kepolisian. Kewenangan umum tersebut adalah kewenangan yang diberikan berdasarkan peraturan perundang-undangan sebagai produk hukum positif di Indonesia. Kewenangan umum kepolisian ini diatur

dalam pasal 15 ayat (1) Undang-Undang No. 2 Tahun 2002 tentang Polri, sebagai berikut:

a. Menerima laporan dan pengaduan warga masyarakat.
b. Membantu menyelesaikan perselisihan warga masyarakat yang dapat mengganggu ketertiban umum.
c. Mencegah dan menanggulangi penyakit masyarakat.
d. Mengeluarkan peraturan kepolisian dalam lingkup administrasi kepolisian.
e. Melaksanakan pemeriksaan khusus sebagai bagian dari tindakan kepolisian dalam rangka pencegahan.
f. Melakukan tindakan pertama di tempat kejadian.
g. Mengambil sidik jari dan identitas lainnya, serta memotret seseorang.
h. Mencari keterangan dan barang bukti.
i. Menyelenggarakan pusat informasi criminal nasional.
j. Mengeluarkan surat ijin dan atau surat keterangan yang diperlukan dalam rangka pelayanan masyarakat.
k. Memberikan bantuan pengamanan dalam sidang dan dalam pelaksanaan putusan pengadilan, kegiatan instansi lainnya, serta kegiatan masyarakat.

Disamping kewenangan umum kepolisian, Polri juga diberikan kewenangan lain yang dirumuskan dalam pasal 15 ayat (2), yaitu:

a. Memberikan ijin dan mengawasi kegiatan keramaian umum dan kegiatan masyarakat lainnya,
b. Menyelenggarakan registrasi dan identifikasi kendaraan bermotor.
c. Memberikan surat ijin mengemudi kendaraan bermotor.
d. Menerima pemberitahuan tentang kegiatan politik.

Berdasarkan tugas pokok dan kewenangan di atas maka ruang lingkup fungsi dan peranan Polri pada hakekatnya adalah menyelenggarakan fungsi-fungsi utama kepolisian, yakni fungsi pre-emptif, preventif, maupun represif. Djamin dalam hal ini berpendapat sesuai dengan fungsi utama kepolisian yang universal maka Polri lebih mengutamakan upaya pre-emptif dan preventif daripada represif. Ini sejalan dengan falsafah yang dianut dalam dunia kedokteran yang menegaskan

bahwa *prevention is better than cure*, sehingga diharapkan Polri mampu mewujudkan serta mempertahankan keamanan dan ketertiban di dalam masyarakat secara modern.

Upaya untuk mewujudkan keamanan dan ketertiban dalam lingkup berlalu lintas dan angkutan jalan merupakan salah satu bagian dari tugas pokok Kepolisian Negara Republik Indonesia sebagai institusi negara pengemban fungsi keamanan yang utama di Indonesia. Upaya ini sejalan dengan rumusan Pasal 13 Undang-Undang No. 2 Tahun 2002 tentang Polri bahwa tugas pokok Polri adalah memelihara keamanan dan ketertiban masyarakat; menegakkan hukum; dan memberikan perlidungan, pengayoman, dan pelayanan kepada masyarakat. Artinya bahwa Kepolisian Negara Republik Indonesia dituntut untuk mampu melaksanakan tugas pokok dan kewenangannya secara profesional dalam rangka mewujudkan dan mempertahankan keamanan dan ketertiban di dalam masyarakat secara menyeluruh, termasuk di dalamnya adalah bidang lalu lintas dan angkutan jalan.

Agar dapat melakukan akselerasi terhadap proses pembangunan khususnya di bidang lalu lintas dan angkutan jalan, maka Pemerintah Indonesia bersama-sama dengan semua pemangku kepentingan (*stakeholder*) serta didukung Dewan Perwakilan Rakyat Indonesia telah mengesahkan Undang-Undang Nomor 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan pada tanggal 22 Juni 2009. Undang-undang ini menggantikan UU No. 14 Tahun 1992 tentang Lalu Lintas dan Angkutan Jalan sebagai produk hukum lama yang dirasakan sudah tidak relevan dengan perkembangan situasi dan kondisi masyarakat Indonesia sekarang.

Berdasarkan UU No. 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan menyatakan bahwa polisi lalu lintas mempunyai peranan utama dalam melaksanakan tugas-tugas kepolisian di bidang lalu lintas dan angkutan jalan. Sebagai salah satu bagian dari fungsi operasional di dalam Manajemen Operasional Polri, polisi lalu lintas memiliki fungsi dan peranan dalam melaksanakan tugas-tugas kepolisian di bidang lalu lintas. Fungsi dan peran tersebut adalah:

a. Menyelenggarakan edukasi lalu lintas (*traffic education*).

b. Menyelenggarakan rekayasa lalu lintas (*traffic engineering*).
c. Menyelenggarakan penegakan hukum di jalan umum (*traffic law enforcement*).
d. Menyelenggarakan registrasi dan identifikasi terhadap kendaraan bermotor dan pengemudi (*traffic registration and identification*).
e. Menyelenggarakan Pusat K3I (Komunikasi, Koordinasi, dan Kendali Informasi).
f. Sebagai koordinator para pemangku kepentingan di bidang lalu lintas (*stake holder*).
g. Memberikan rekomendasi yang berkaitan dengan bidang lalu lintas.
h. Menyelenggarakan korwas PPNS.

Menyimak dari rumusan tugas pokok Polisi Lalu Lintas di atas maka tampak adanya perluasan fungsi dan peranan Polri dalam bidang lalu lintas dan angkutan jalan dari produk hukum sebelumnya berkaitan dengan penyelenggaraan Pusat K3I (Komunikasi, Koordinasi, dan Kendali Informasi). Pada Bab XVI Pasal 245-251 Undang-Undang Nomor 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan dijelaskan bahwa polisi lalu lintas juga mempunyai tugas mengelola Pusat Kendali Sistem Informasi Lalu Lintas dan Angkutan Jalan yang telah terintegrasi oleh subsistem-subsistem informasi (yang dikelola oleh para Pembina Lalu Lintas dan Angkutan Jalan lainnya sesuai dengan kewenangannya masing-masing). Pengintegrasian tersebut dilakukan subsistem-subsistem informasi Lalu Lintas dan Angkutan Jalan itu terpadu di dalam Pusat Kendali Sistem Informasi Lalu Lintas dan Angkutan Jalan untuk mewujudkan pelayanan Lalu Lintas dan Angkutan Jalan yang aman, tertib, lancar dan terpadu.

Menurut Suparlan (2009), fungsi polisi adalah fungsional dalam kehidupan manusia bermasyarakat dan bernegara. Lebih lanjut dikatakan bahwa fungsi polisi harus dilihat dalam perspektif bahwa individu, masyarakat, dan negara masing-masing yang merupakan sebuah sistem yang secara keseluruhan memproses masukan-masukan program pembangunan untuk menghasilkan keluaran berupa kemakmuran, keadilan dan kesejahteraan. Maksudnya bahwa fungsi polisi adalah untuk menjaga agar keluaran yang diharapkan sesuai dengan

tujuan yang ingin dicapai dan menjaga agar individu, masyarakat, dan Negara yang merupakan unsur utama sehingga tidak terganggu atau dirugikan.

Konsep fungsi selalu digunakan dalam kaitannya dengan konsep sistem, yaitu dalam kaitan dengan unsur-unsur dalam sebuah sistem yang berada dalam hubungan fungsional atau saling mendukung dan menghidupkan secara bersama-sama memproses masukan menjadu keluaran. Sedangkan peranan juga dinyatakan sebagai perilaku yang diharapkan dari seseorang yang mempunyai suatu status atau posisi tertentu dalam suatu kelompok atau posisi suatu kelompok dengan kelompok lainnya (Bakharuddin, 2009).

Sebagai penjabaran operasional terhadap fungsi dan peranan tersebut maka saat ini Polri sedang mengembangkan sistem pelayanan publik dengan memanfaatkan kemajuan teknologi informasi dan komunikasi secara *online*. Salah satu model pengembangannya adalah operasionalisasi *Traffic Management Center* (TMC) yang dikelola oleh Direktorat Lalu Lintas Polda Metro Jaya.

2.3 Kerangka Pemikiran

Kerangka pemikiran dalam penulisan tesis ini secara sederhana dapat diilustrasikan bahwa TMC PMJ merupakan penjabaran a*ction plan* Polda Metro Jaya terhadap implementasi perpolisian masyarakat (*community policing*). Sebagai sarana penunjang yang berada di bawah Direktorat Lalu Lintas Polda Metro Jaya, TMC PMJ berfungsi untuk memberikan akses informasi secara online kepada masyarakat umum seputar informasi lalu lintas dan membantu tugas-tugas polisi lalu lintas untuk mewujudkan dan memelihara keamanan, keselamatan, ketertiban dan kelancaran lalu lintas dengan memanfaatkan teknologi jaringan komputer yang terintegrasi. Untuk itu Ditlantas Polda Metro Jaya perlu menerapkan manajemen keamanan informasi untuk mengamankan aset-aset informasi sensitif dan kritis yang terdapat pada TMC PMJ.

Saat ini Ditlantas Polda Metro Jaya telah menerapkan manajemen keamanan informasi terhadap informasi sensitif dan kritis yang dimiliki oleh TMC PMJ, namun penerapan tersebut dirasakan belum optimal. Hal ini menimbulkan kerentanan terhadap aset informasi yang berada di dalamnya dari ancaman yang diprakirakan terjadi.

Dengan latar belakang tersebut maka Direktorat Polda Metro perlu mekakukan langkah-langkah pengamanan dengan menggunakan **Teori Keamanan Informasi (McLeod & Schell)** yang mencakup dua hal utama, yaitu **strategi keamanan informasi** dengan menerapkan manajemen keamanan sistem informasi (*Information Security Management System*-ISMS) sebagai aktifitas untuk menjaga sumber daya informasi agar tetap aman dan **manajemen keberlangsungan bisnis** (Business Continuity Management-BCM) sebagai aktifitas untuk menjaga sumber daya informasi tetap berfungsi seandainya terjadi bencana maupun gangguan yang lain.

Untuk dapat mengoperasionalkan strategi keamanan informasi pada TMC PMJ maka dilakukan empat pentahapan yang harus dilakukan. Tahapan pertama adalah mengidentifikasi ancaman berdasarkan sumber ancaman dan bentuk ancaman yang diprakirakan akan terjadi.

Tahapan selanjutnya adalah melakukan pendefinisian resiko dengan menerapkan tiga langkah yaitu identifikasi aset, analisis resiko dan melakukan tindak lanjut atas hasil penilaian terhadap resiko tersebut (*impact value*). Pada tahapan ini diawali dengan mengidentifikasi ketigaaset informasi yang ada di TMC (aset personel, aset fisik bangunan,serta aset informasi) dan melakukan penilaian aset dan kerentanan dari aset-aset terebut. Kombinasi antara identifikasi ancaman, nilai aset dan kerentanan terhadap aset akan menghasilkan impact value yang berfungsi untuk melakukan evaluasi penganan resiko.

Selanjutnya upaya evaluasi penanganan resiko dilakukan dengan cara menggabungan secara matematis atas hasil penilaian *impact value* terhadap mitigasi terhadap resiko saat ini (*risk control*) dan frekuensi kemungkinan terjadinya suatu kejadian yang mengandung resiko (*likelihood*). Tindakan penggabungan ini akan menghasilkan rentang penilaian atas resiko (*inherent risk*) yang berfungsi untuk menetapkan tingkatan resiko (*risk level*) tersebut.

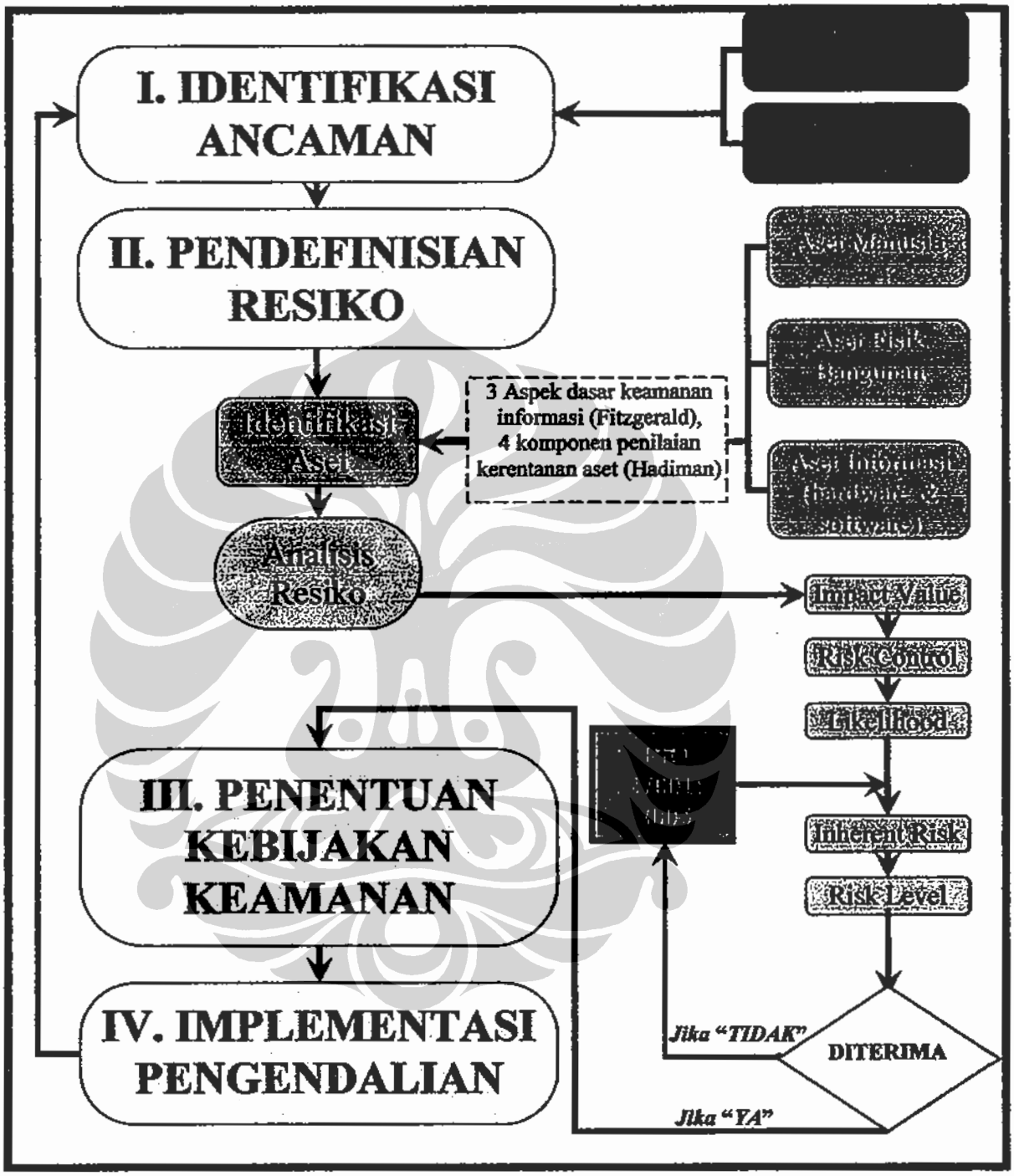
Hasil penggolongan risk level ini akan menentukan upaya tindak lanjut terhadap resiko, apakah resiko tersebut akan diterima, dikurangi, dipindahkan atau dihilangkan oleh manajemen TMC PMJ. Perlakuan tindak lanjut ini sebagai dasar untuk melakukan pemilihan *current control* berdasarkan pengendalian ISO 27001:2005 dalam rangka menangani resiko. Apabila perlakuan tersebut ternyata

tidak diterima (yang berarti melebihi batas tingkatan *risk level* yang telah ditetapkan), maka apabila organisasi menginginkan agar aset tersebut tetap ada maka dilakukan penilaian tambahan berdasarkan *obyektif control* dan *control* berdasarkan ISO 27001:2005 hingga didapatkan kondisi diterima pada *risk level*.

Tahapan ketiga dan keempat adalah menentukan kebijakan keamanan dan mengimplementasikan pengendalian yang akan diterapkan di dalam operasional organisasi. Penentuan kebijakan keamanan ini merupakan lanjutan dari perlakuan tindak lanjut pada tahap sebelumnya dengan mengimplementasikan ISO 27001:2005 yang dituangkan ke dalam dokumentasi dalam bentuk standar operasional prosedur penerapan keamanan informasi pada TMC PMJ.

Di dalam dokumentasi standar operasional prosedur penerapan keamanan informasi yang telah disusun berdasarkan implementasi ISO 27001:2005 tersebut nantinya akan berisikan tentang strategi keamanan informasi TMC PMJ sebagai aktifitas untuk menjaga sumber daya informasi pada TMC PMJ agar tetap aman dan manajemen keberlangsungan bisnis sebagai aktifitas untuk menjaga agar sumber daya informasi pada TMC PMJ tetap berfungsi seandainya terjadi bencana maupun gangguan yang lain.

Untuk memperjelas ilustrasi kerangka pemikiran ini maka penulis menuangkan dalam gambar diagram sebagai berikut:



Gambar 2.7: Kerangka Pemikiran Penerapan Manajemen Keamanan Informasi pada TMC PMJ dengan Pengendalian ISO 27001:2005.

BAB III
GAMBARAN UMUM TRAFFIC MANAGEMENT CENTER DIREKTORAT LALU LINTAS POLDA METRO JAYA

3.1 Kepolisian Daerah Metro Jaya

Polda Metro Jaya merupakan satuan pelaksana utama yang berada di bawah Kapolri yang bertanggung jawab pada kewilayahan yang mencakup seluruh wilayah di Propinsi DKI Jakarta, sebagian wilayah administratif di Propinsi Jawa Barat (Kabupaten Bekasi, Kota Bekasi dan Kota Depok), dan dua wilayah administratif Propinsi Banten (Kabupaten dan Kota Tangerang).

Polda Metro Jaya mempunyai motto "Pelayanan, Profesional, Proposional dan Humanis" dalam melaksanakan tugas-tugas kepolisian di wilayah Jakarta Raya. Berdasarkan Overview Polda Metro Jaya tahun 2009, situasi kamtibmas di bidang politik, ekonomi, sosial dan budaya selama tahun 2009 dinyatakan cukup kondusif. Dalam bidang politik, pelaksanaan Pemilu 2009 dapat dilaksanakan dengan mantap dan terkendali. Selain itu tuntutan penegakan Hak Asasi Manusia dan penyelesaian hukum dilaksanakan secara proporsional dan professional. Selain itu kegiatan pengamanan aksi unjuk rasa penyampaian aspirasi yang dilakukan oleh unsur-unsur masyarakat yang terjadi sepanjang tahun 2009 dapat dilaksanakan dengan tertib dan lancar ("Overview PMJ", 2009).

Di bidang ekonomi terbaca situasi perekonomian di wilayah Jakarta Raya berangsur-angsur mulai membaik. Walaupun dampak krisis ekonomi dunia masih mempengaruhi kehidupan masyarakat Jakarta namun tidak signifikan mengganggu situasi kamtibmas di Jakarta. Kemudian dalam bidang sosial budaya, aktifitas masyarakat yang menjurus kepada gangguan keamanan dan ketertiban, seperti penertiban bangunan dan pedagang kaki lima, perkelahian antarwarga, antarkelompok serta antaretnis yang menjurus kepada SARA mampu ditangani oleh Polda Metro Jaya secara profesional dan proporsional.

Di bidang ideologi diketahui bahwa globalisasi dan reformasi semakin mempengaruhi pola berfikir masyarakat Jakarta, yang ditandai dengan munculnya

berbagai asas kepentingan, masih dapat dikendalikan oleh Polda Metro Jaya sehingga tatanan Negara Kesatuan Republik Indonesia tetap terjaga.

3.1.1 Visi dan Misi Polda Metro Jaya

Polda Metro Jaya merupakan Polda yang terletak di ibu kota negara yang mempunyai penduduk yang beraneka ragam. Banyak penduduk lain selain penduduk asli Jakarta, namun hal itu justru menjadi tantangan petugas Polri untuk semakin meningkatkan pelayanannya kepada masyarakat. Untuk mewujudkan rasa aman dan nyaman, Polda Metro Jaya berpedoman pada Grand Strategi Polri 2005 – 2025 (2005) yang dirumuskan dalam tiga tahapan yang mencerminkan upaya Polri secara *gradual*, yaitu tahap I tahun 2005 – 2010 yakni tahap *trust building* (membangun kepercayaan), tahap II tahun 2011 – 2015 yakni *partnership building* (membangun kemitraan) dan tahap III tahun 2016 – 2025 yakni *strive for excellence* yaitu membangun kemampuan kemampuan pelayanan publik yang unggul dan dipercaya masyarakat.

Berdasarkan Grand Strategi Polri tersebut, Polda Metro Jaya mewujudkan kinerjanya dengan menetapkan visi, misi dan sasaran prioritas pada tahun 2010 sebagai berikut (*website* Bid Humas Polda Metro Jaya, 2010):

Visi:

Tergelarnya polisi yang dipercaya masyarakat disemua titik dan lini pelayanan masyarakat di sepanjang waktu dalam wujudkan keamanan di wilayah hukum Polda Metro Jaya dan tegaknya hukum sebagai sinergi pencapaian hasil pembangunan yang berwawasan keamanan.

Misi:

1. Perkuat dan tingkatkan kemampuan intelijen keamanan Polda Metro Jaya guna menjaring informasi untuk cegah gangguan keamanan dan pengungkapan kasus secara sistematis dan tuntas
2. Kembangkan pelayanan publik di setiap lini berbasis pelayanan prima

3. Menggelar polisi sebanyak-banyak di tengah masyarakat dalam memberikan perlindungan, pengayoman dan pelayanan masyarakat.
4. Kembangkan falsafah dan strategi perpolisian masyarakat (polmas) dalam bangun hub polisi dan masy yg lebih dekat dan interaktif dalam upaya wujudkan masyarakat patuh hukum.
5. Berdayakan seluruh kekuatan dan kemampuan organisasi pengemban fungsi lidik dan sidik dalam wujudkan Polri sebagai penegak hukum yang terdepan.
6. Tingkatkan kinerja Polda Metro Jaya secara profesional, transparan dan akuntabel guna dukung tupoksi Polri.

Sasaran prioritas:

1. Terwujudnya kondisi kamtibmas wilayah hukum Polda Metro Jaya yang kondusif pasca pelaksanaan Pemilu 2009.
2. Lanjutkan pembangunan sarana dan prasarana.
3. Tingkatkan kualitas kemampuan dan ketrampilan personel Polda Metro Jaya.
4. Melaksanakan pembinaan personil Polri
5. Tertanggulanginya penyalahgunaan narkoba melalui giat preventif dan represif.
6. Tertanggulanginya kejahatan transnasional (*trafficking in person* dan *people smugling*).
7. Terealisasinya program perpolisian masyarakat (polmas) untuk tingkatkan kemitraan dan kepatuhan hukum masyarakat.
8. Terpeliharanya kamtibmas perairan dan tertanganinya segala bentuk kejahatan di perairan yuridiksi Polda Metro Jaya.
9. Tertanganinya perkara-perkara korupsi.
10. Penanganan bencana banjir.
11. Meningkatkan pencapaian *quick wins*.
12. Terwujudnya kondisi lingkungan yang aman dan bebas dari premansme, kejahatan jalanan (street crime) dan perjudian.
13. Tingkatkan kualitas peserta pendidikan Polri (bintara).

3.1.2 Struktur Organisasi Polda Metro Jaya

Secara umum Polda Metro Jaya membawahi 13 Polres Metropolitan, 109 Polsek Metropolitan, 324 Polpos dan 55 Pospol. Jumlah personel yang bertugas di lingkup Polda Metro Jaya tahun 2009 terdiri dari 30.909 orang anggota Polri, 29.306 orang PNS dan 22 orang Capeg. Jumlah penduduk di wilayah hukum Polda Metro Jaya sebanyak 23.474.841, sehingga perbandingan Polri dengan masyarakat yang dilayani adalah 1 : 672 orang. (Overview PMJ, 2009 :15)

Mengingat luasnya wilayah yang menjadi kewenangan hukum yang diampu dan beragam etnis masyarakat yang mendiaminya, maka Polda Metro Jaya mempunyai karakteristik khusus berkaitan dengan struktur organisasi yang dimiliki. Kekhususan karakteristik ini menjadikan struktur organisasi Polda Metro Jaya berbeda dibandingkan dengan polda lainnya di Indonesia. Berdasarkan Keputusan Kapolri No. Pol.: Kep/7/I/2005 tanggal 3 Januari 2005 tentang Organisasi dan Tata Kerja Polda Metro Jaya masuk dalam kategori tipe A1-Khusus yang dipimpin oleh Kapolda yang berpangkat Inspektur Jenderal Polisi (Irjen Pol). Struktur organisasi Polda Metro Jaya berdasarkan kepada keputusan Kapolri, yaitu :

1. Organisasi Polda Metro Jaya disusun dalam dua tingkat, yaitu :
   a. Markas Kepolisian Negara Republik Indonesia Daerah Metro Jaya.
   b. Kepolisian Negara Republik Indonesia Resort.
2. Susunan organisasi Mapolda Metro Jaya, terdiri atas :
   a. Unsur pimpinan, yaitu :
      1) Kepala Polda Metro Jaya.
      2) Wakil Kepala Polda Metro Jaya.
   b. Unsur Pembantu Pimpinan, terdiri atas :
      1) Inspektorat Pengawasan Umum Daerah,
      2) Biro Perencanaan Umum dan Pengembangan,
      3) Biro Operasi,
      4) Biro Pembinaan Kemitraan,
      5) Biro Personel,
      6) Biro Logistik.

c. Unsur Pelaksana Staf Khusus atau Pendidikan dan Pelayanan, terdiri atas :
   1) Bidang Hubungan Masyarakat,
   2) Bidang Pembinaan Hukum,
   3) Bidang Profesi dan Pengamanan,
   4) Bidang Telekomunikasi dan Informatika,
   5) Bidang Kedokteran dan Kesehatan,
   6) Bidang Keuangan,
   7) Sekolah Polisi Negara,
   8) Sekretariat Umum,
   9) Detasemen Markas.

d. Unsur Pelaksana Utama, terdiri dari :
   1) Sentra Pelayanan Kepolisian,
   2) Direktorat Intelijen Keamanan,
   3) Direktorat Reserse Kriminal Umum,
   4) Direktorat Reserse Kriminal Khusus,
   5) Direktorat Reserse Narkotika,
   6) Direktorat Samapta,
   7) Direktorat Pengamanan obyek Vital,
   8) Direktorat Lalu Lintas,
   9) Direktorat Kepolisian perairan,
   10) Satuan Brigade Mobil,
   11) Densus 88 AT,
   12) Polrestro-Polrestro jajaran Polda Metro Jaya (13 polrestro).

Sesuai dengan konsep Metropolitan, terdapat Polres secara administratif pemerintah berada dalam wilayah propinsi lain diluar propinsi DKI Jakarta namun masuk dalam lingkup tugas di wilayah hukum Polda Metro Jaya. Polres Metro Bekasi dan Polres Bekasi, merupakan Polres yang berada dalam wilayah Propinsi Jawa Barat. Juga, Polres Kota Tangerang, Polres Kabupaten Tangerang dan Polres Metro Bandara Soekarno Hatta, merupakan Polres yang berada dalam wilayah Propinsi Banten.

Dalam kegiatan operasionalnya maka Polda Metro Jaya didukung oleh Polrestro-Polrestro di wilayah hukum Jakarta Raya, meliputi:

1. Polres Metro Jakarta Pusat.
2. Polres Metro Jakarta Barat.
3. Polres Metro Jakarta Timur.
4. Polres Metro Jakarta Selatan.
5. Polres Metro Jakarta Utara.
6. Polres Metro Kota Tangerang.
7. Polres Tangerang.
8. Polres Metro Bekasi.
9. Polres Bekasi.
10. Polres Metro Depok.
11. Polres Metro Bandara Soekarno Hatta.
12. Polres Metro KPPP Tanjung Priok.
13. Polres Kepulauan Seribu.

3.2 Direktorat Lalu Lintas Polda Metro Jaya

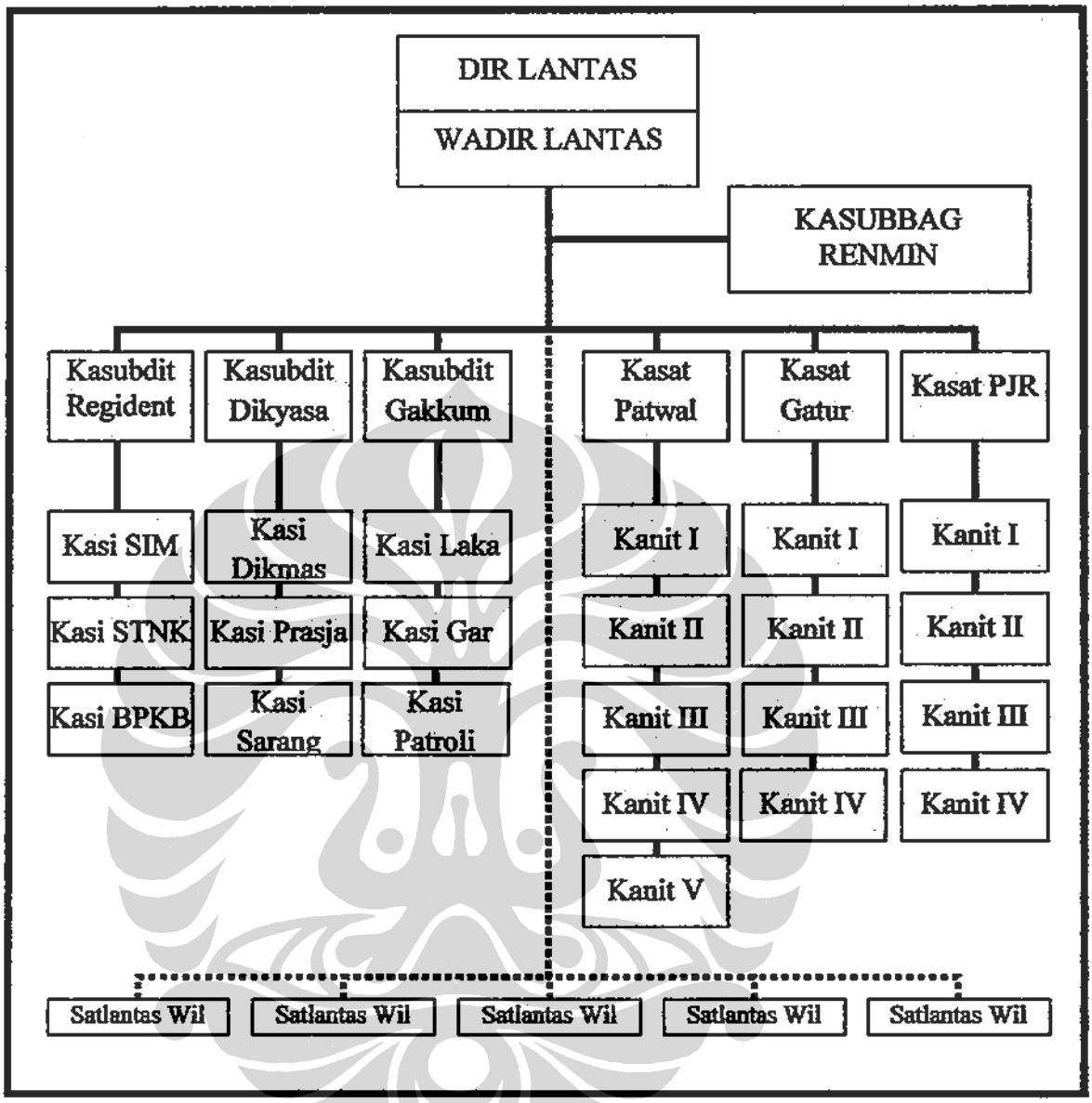
Ditlantas Polda Metro Jaya adalah pelaksana utama Polda Metro Jaya dan berada di bawah Kapolda Metro Jaya, yang bertugas menyelenggarakan dan membina fungsi lalu lintas kepolisian meliputi penjagaan, pengaturan, pengawalan dan patroli, pendidikan masyarakat, dan rekayasa lalu lintas, registrasi dan identifikasi pengemudi dan kendaraan bermotor, penyidikan kecelakaan lalu lintas dan penegakan hukum dalam bidang lalu lintas guna memelihara keamanan, ketertiban dan kelancaran lalu lintas di wilayah hukum Polda Metro Jaya (*Vademikum Lantas*, 2005).

Dalam melaksanakan tugasnya maka Ditlantas Polda Metro Jaya menyelenggarakan fungsi:

1. Pembinaan fungsi lalu lintas kepolisian dalam lingkungan Polda Metro Jaya.

2. Penyelenggaraan dan pembinaan partisipasi masyarakat melalui kerjasama lintas sektoral, pendidikan masyarakat dan pengkajian masalah di bidang lalu lintas.
3. Penyelenggaraan operasi kepolisian bidang lalu lintas dalam rangka penegakan hukum dan ketertiban lalu lintas.
4. Pembinaan dan penyelenggaraan registrasi dan identifikasi kendaraan bermotor dan pengemudi di seluruh wilayah Polda Metro Jaya termasuk melalui cabang-cabangnya di setiap polres-polres.
5. Penyelenggaraan patrol jalan raya dan penindakan pelanggaran serta penanganan kecelakaan lalu lintas serta menjamin kelancaran arus lalu lintas di jalan raya.

Struktur organisasi Ditlantas Polda Metro Jaya berdasarkan Keputusan Kapolri No. Pol.: Kep/07/I/2005 tentang Struktur Organisasi Ditlantas Polda Metro Jaya adalah sebagai berikut:



Gambar 3.1: Struktur Organisasi Ditlantas Polda Metro Jaya

Direktorat Lalu Lintas Polda Metro Jaya dipimpin oleh seorang Direktur Lalu Lintas yang bertanggungjawab kepada Kapolda Metro Jaya dan dalam pelaksanaannya sehari-hari berada di bawah kendali Wakapolda Metro Jaya. Dalam melakukan tugas pokoknya, Dirlantas dibantu oleh Wakil Dirlantas yang bertanggung jawab penuh kepada Dirlantas. Di dalam tubuh organisasi Ditlantas Polda Metro terdiri dari satu sub bagian, tiga sub direktorat dan tiga satuan yang masing-masing mempunyai tugas sebagai berikut:

1. Sub Bagian Perencanaan dan Administrasi (Subbag Renmin).
   Betugas merumuskan atau menyiapkan rencana atau program kerja dan anggaran, termasuk rencana administrasi dan operasional serta pelatihan dan menyelenggarakan pelayanan urusan administrasi, urusan dalam dan ketatausahaan, urusan pelayanan keuangan Ditlantas, termasuk pembinaan fungsi lalu lintas dalam lingkungan Polda Metro Jaya.
2. Sub Direktorat Registrasi dan Administrasi (Subdit Regident).
   Bertugas menyelenggarakan dan membina pelaksanaan administrasi registrasi dan identifikasi kendaraan bermotor dan pengemudi di seluruh wilayah Polda Metro Jaya termasuk melalui cabang-cabangnya di setiap Polres.
3. Sub Direktorat Pendidikan Masyarakat dan Rekayasa Lalu Lintas (Subdit Dikyasa).
   Bertugas menyelenggarakan dan membina pelaksanaan kerjasama lintas sektoral, pendidikan masyarakat, dan rekayasa bidang lalu lintas.
4. Sub Direktorat Pembinaan Penegakan Hukum (Subdit Gakkum).
   Bertugas membina pelaksanaan penegakan hukum termasuk tata tertib berlalu lintas oleh satuan pelaksana dalam lingkungan Polda Metro Jaya.
5. Satuan Patroli dan Pengawalan (Sat Patwal).
   Menyelenggarakan kegiatan patrol dan pengawalan di jalan raya.
6. Satuan Penjagaan dan Pengaturan (Sat Gatur).
   Bertugas menyelenggarakan dan melaksanakan patroli jalan raya dan tindakan pertama pada tempat kejadian perkara, termasuk kecelakaan lalu lintas serta tindakan pertolongan.
7. Satuan Patroli Jalan Raya (Sat PJR).
   Bertugas menyelenggarakan dan melaksanakan patroli jalan raya dan tindakan pertama pada tempat kejadian perkara, termasuk kecelakaan lalu lintas serta tindakan pertolongan.

Saat ini Ditlantas Polda Metro Jaya memiliki jumlah personel sebanyak 4444 orang yang terbagi dalam enam bagian, yaitu Mako Ditlantas, Polrestro Jakarta Pusat, Polrestro Jakarta Utara, Polrestro Jakarta Barat, Polrestro Jakarta

Selatan dan Polrestro Jakarta Timur. Berdasarkan daftar kekuatan Polri Ditlantas Polda Metro Jaya yang dikeluarkan oleh Kasubbag Renmin Ditlantas Kompol Jumarno pada bulan Februari 2010, maka perincian jumlah personel Ditlantas Polda Metro Jaya adalah sebagai berikut:

TABEL 3.1: Daftar Kekuatan Polri Ditlantas Polda Metro Jaya bulan Februari 2010

NO.	BAGIAN	DSP	PAMEN			PAMA			BINTARA						JML
			KOMBES	AKBP	KOMPOL	AKP	IPTU	IPDA	AIPTU	AIPDA	BRIPKA	BRIGADIR	BRIPTU	BRIPDA	
1.	Mako Ditlantas	1642	1	9	33	104	64	24	633	152	567	416	597	442	3042
2.	Res Jakpus	210	-	-	1	4	3	-	34	9	46	27	99	11	234
3.	Res Jakut	210	-	-	1	4	6	-	35	11	63	23	32	5	180
4.	Res Jakbar	210	-	-	1	4	9	1	49	8	70	37	52	7	238
5.	Res Jaksel	210	-	-	1	4	9	-	51	21	47	38	116	22	309
6.	Res Jaktim	210	-	-	1	4	11	-	115	29	142	50	80	8	440
JUMLAH		2692	1	9	38	124	102	25	917	230	935	591	976	495	4444

Agar dapat mewujudkan keamanan, keselamatan, ketertiban dan kelancaran lalu lintas di wilayah Polda Metro Jaya maka Ditlantas Polda Metro Jaya talah membuat strategi dan program untuk menangani masalah lalu lintas di kota Jakarta Raya dan sekitarnya. Ada tiga aspek yuridis yang menjadi acuan dari strategi dan program ini. Yaitu, pertama, UU No. 22 Tahun 2009 Pasal 5 ayat (3) huruf f yang menegaskan bahwa Polri berperan sebagai instansi pembina lalu lintas dan angkutan jalan yang meliputi urusan pemerintahan di bidang Registrasi dan Identifikasi Kendaraan Bermotor dan Pengemudi, Penegakan Hukum, Operasional Manajemen dan Rekayasa Lalu Lintas, serta pendidikan berlalu lintas. Kedua, Peraturan Presiden No. 7 Tahun 2005 tentang RPJMN 2005 dan ketiga, Surat Keputusan Kapolri No. Pol.: Skep/737/X/2005 tentang kebijakan dan strategi penerapan polmas dalam pelaksanaan tugas Polri.

Dalam strateginya ini Ditlantas Polda Metro Jaya menekankan agar segenap jajarannya melakukan tindakan pemolisian dengan segala usaha atau upaya untuk memelihara keamanan, pencegahan dan pengungkapan kejahatan melalui pengawasan, penjagaan, dan tindakan untuk memberikan sanksi hukum

berdasarkan hukum, petunjuk, aturan, dan kebijakan pimpinan. Sebagai implementasi dari strategi ini maka jajaran Ditlantas Polda Metro Jaya bertekad untuk menerapkan pemolisian modern dan meninggalkan pola-pola pemolisian konvensional. Prinsip utama model pemolisian modern yang diterapkan oleh jajaran Ditlantas Polda Metro Jaya adalah pemolisian proaktif yang bertujuan untuk menyelesaikan berbagai masalah sosial yang terjadi di masyarakat, khususnya yang berkaitan dengan masalah keamanan dan ketertiban lalu lintas.

Salah satu penerapan model pemolisian modern yang dilakukan oleh jajaran Ditlantas Polda Metro Jaya adalah melalui *Traffic Management Center* Polda Metro Jaya (TMC PMJ). Keberadaan TMC PMJ ini didukung penuh oleh aplikasi Sistem Informasi dan Aplikasi Polisi (SIAP) untuk memberikan tanggapan yang cepat oleh petugas jajaran Ditlantas Polda Metro Jaya sebagai respon terhadap laporan atau pengaduan masyarakat Jakarta.

3.3 Traffic Management Center Direktorat Lalu Lintas Polda Metro Jaya

Pemanfaatan teknologi informasi sebagai salah satu sumber daya organisasi untuk mendukung pelaksanaan tugas pokok dilakukan Polri dalam upayanya untuk meningkatkan pelayanan publik. Upaya yang telah dilakukan tersebut merupakan penjabaran fungsi dan peranan Polri sebagai aparatur Negara pengemban fungsi keamanan di Negara Indonesia. Salah satu implementasinya adalah membangun Traffic Management Center oleh Direktorat Lalu Lintas Polda Metro Jaya dengan menggunakan teknologi komputer yang terintegrasi.

TMC merupakan pusat manajemen lalu lintas di Polda Metro Jaya yang berfungsi sebagai K3I (Komando, Komunikasi, Koordinasi dan Informasi). Sarana ini merupakan implementasi yang dilakukan oleh Direktorat Lalu Lintas Polda Metro Jaya terhadap salah satu *action plan* Kapolda Metro Jaya tentang "SIAP" (Sistem Informasi Aplikasi Polisi) berdasarkan kebijakan dan strategi Kapolri pada tahun 2002-2004 untuk meningkatkan kinerja pelayanan Polri khususnya di bidang lalu lintas. Dengan adanya TMC diharapkan dapat membantu peningkatan kinerja kepolisian jajaran Polda Metro Jaya pada umumnya serta petugas Direktorat Lalu Lintas Polda Metro Jaya pada khususnya

dalam memberikan kecepatan informasi yang disampaikan kepada para *stake holder* yang berkepentingan sehingga diharapkan mampu membantu pelaksanaan tugas Polantas dalam menangani gangguan di bidang lalu lintas secara cepat dan profesional.

Fungsi komando mengandung pengertian bahwa TMC menjadi sarana untuk memmberikan suatu perintah sekaligus pengendalian bagi petugas-petugas yang ada di lapangan atau lokasi-lokasi yang terjadi permasalahan khususnya berkaitan dengan permasalahan lalu lintas. Dengan memanfaatkan TMC maka manajemen dapat memberikan perintah-perintah yang secara langsung disampaikan kepada petugas di lapangan untuk mengambil tindakan kepolisian (seperti pengalihan arus, penegakan hukum kejadian kecelakaan lalu lintas, dll) secara *real time* sehingga manajemen bisa memberikan arahan yang efektif dan efisien kepada para petugas di lapangan ketika masyarakat membutuhkan kehadiran polisi di lapangan untuk menangani keadaan *police hazard* secara cepat dan dengan tindakan yang tepat.

Komunikasi memiliki arti bahwa TMC merupakan wadah bagi petugas kepolisian, masyarakat umum maupun para *stake holder* untuk menyampaikan maupun mencari informasi yang berkaitan dengan informasi internal kepolisian maupun informasi kamtibmas di wilayah Jakarta Raya. Komunitas ini dikendalikan oleh para petugas operator TMC dan didukung oleh teknologi dan infra struktur komunikasi terkini untuk memberikan pelayanan maksimal kepada para *user*. Teknologi dan infra struktur yang telah *installed* pada TMC adalah GIS (*Geografican Information System*), GPS (*Global Positioning System*), internet, peralatan *faximile*, *call center*, SMS (*Short Message Service*), CCTV, kamera lapangan, HT, layar control, jaringan-jaringan online, dan beberapa *server* sebagai ruang penyimpanan data.

Fungsi koordinasi memiliki definisi sebagai tindakan Ditlantas Polda Metro Jaya yang dijembatani TMC untuk melakukan kemitraan dalam rangka *problem solving* terhadap para *stake holder* agar memperoleh berbagai masukan maupun kesepakatan-kesepakatan sehingga mendapatkan solusi yang terbaik dalam mengevaluasi berbagai masalah sosial di bidang lalu lintas. Koordinasi ini

bisa dilakukan secara internal maupun eksternal kepolisian baik dalam tataran manajemen maupun *level* operasional (petugas di lapangan).

Sedangkan fungsi informasi pada TMC mengandung makna bahwa TMC merupakan wadah berita/kejadian-kejadian/situasi/kebijakan-kebijakan/perintah-perintah/masukan/pengaduan yang diperoleh dari eksternal maupun internal dan dapat dijadikan acuan dalam mengambil tindakan-tindakan kepolisian baik dalam tingkat manajerial maupun operasional.

Ada delapan tujuan didirikannya TMC, yaitu:

1. Pelayanan *quick response time* secara professional terhadap masyarakat.
2. Analisis pelanggaran dan kecelakaan lalu lintas (*black spot*).
3. Pusat informasi kegiatan dan kemacetan lalu lintas.
4. Pusat informasi SIM, STNK, dan BPKB bagi Polri dan masyarakat.
5. Pusat informasi hilang temu kendaraan bermotor.
6. Pusat kendali patroli kendaraan bermotor dalam mewujudkan keselamatan dan kamtibcar lantas.
7. Pusat informasi kualitas baku mutu udara.
8. Pusat pengendalian lalu lintas.

Untuk menciptakan pelayanan *quick response time* terhadap masyarakat maka TMC diharapkan mampu merespon setiap laporan maupun pengaduan yang masuk dalam waktu kurang dari 15 menit. TMC memanfaatkan aplikasi teknologi GIS dan GPS serta jaringan internet digunakan untuk mendukung terciptanya pelayanan ini. Dengan dukungan teknologi tersebut maka diharapkan petugas patrol kepolisian dapat mendatangi lokasi sasaran dalam waktu kurang dari 15 menit untuk melakukan pengecekan informasi yang masuk dan melakukan tindakan kepolisian bila memang terjadi suatu gangguan kamtibmas di lokasi tersebut.

Aplikasi penjabaran *Action Plan* Kapolda Metro Jaya berkaitan dengan analisis pelanggaran dan kecelakaan lalu lintas (*black spot*) dilaksanakan dengan dukungan *programming system* TMC secara online. Dengan menggunakan teknologi informasi secara online ini maka dapat diketahui data pelanggaran seseorang di jalan raya. Sistem ini akan menghitung secara otomatis pelanggaran

seseorang di jalan raya. Apabila nilai pelanggar telah mencapai angka maksimum penalty 36 maka secara otomatis *programming system* TMC akan mengirimkan data kepada *database* Penerbitan SIM (yang telah terintegrasi dengan TMC) tentang nilai pelanggaran terhadap si pelanggar.Pada saat pelanggaran kembali terjadi maka petugas di lapangan akan melakukan pengecekan informasi pelanggaran ke *database* dan menerima informasi tentang angka penalty maksimum tersebut, kemudian memberikan tindakan tegas di lapangan dengan mencabut SIM si pelanggar untuk dilakukan uji ulang. Aplikasi ini juga diterapkan terhadap kejadian kecelakaan lalu lintas.

Berkaitan dengan aplikasi pusat informasi kegitan dan kemacetan lalu lintas yang dilakukan oleh TMC, digunakan untuk menerima dan mengirimkan informasi secara cepat, akurat dan professional kepada masyarakat. Program ini menggunakan teknologi internet secara online dan terintegrasi dengan data-data lain yang dimiliki oleh Polri berkaitan dengan informasi yang diinginkan oleh *user*. Layanan ini paling digemari oleh masyarakat luas untuk mengirimkan dan menerima informasi seputar kemacetan lalu lintas di wilayah Jakarta Raya. Dengan memanfaatkan jejaring sosial secara online, seperti *facebook* dan *twitter*, maka masyarakat luas dengan mudah dan murah dapat mengakses informasi ini sehingga mereka dapat mengirimkan maupun mendapatkan informasi yg aktual tentang situasi yang terjadi.

Pusat informasi SIM, STNK, dan BPKB berfungsi untuk memberikan pelayanan yang cepat, akurat dan professional dalam bidang registrasi dan identifikasi kendaraan bermotor. Dengan memanfaatkan teknologi informasi secara online maka anggota Polri dan masyarakat bisa mendapatkan informasi seputar registrasi dan identifikasi kendaraan bermotor secara cepat dan akurat. Permintaan informasi ini bisa dilakukan dengan memanfaatkan layanan SMS 1717 yang telah terintegrasi dengan sistem yang ada pada semua provider telepon seluler.

Salah satu program yang menarik adalah pusat informasi hilang temu kendaraan bermotor. Program ini juga menggunakan dukungan teknologi informasi secara online. Dengan mengakses alamat *website* TMC Polda Metro Jaya di internet maka petugas Polri maupun masyarakat umum dapat

mendapatkan informasi seputar kendaraan bermotor yang hilang ataupun yang telah ditemukan.

Dalam mewujudkan program keselamatan dan kamtibcar lantas maka program kendali patroli kendaraan bermotor dalam mewujudkan keselamatan dan kamtibcar lantas sangat berguna untuk melakukan pengendalian terhadap pelaksanaan patrol yang dilakukan oleh petugas Polantas dengan menggunakan kendaraan bermotor. Teknologi ini didukung aplikasi TMC dengan GPS sistem yang ditanamkan pada setiap kendaraan bermotor secara online sehingga operator TMC melalui layar monitor di ruangan TMC dapat melacak posisi masing-masing kendaraan patrol secara *real time* dan akurat sebagai kendali pelaksanaan kegiatan kepolisian rutin para petugas lalu lintas sesuai dengan beat patrol masing-masing.

Guna mencegah dan menanggulangi kemacetan lalu lintas yang sering terjadi di Jakarta Raya maka TMC juga mempunyai peranan yang sangat signifikan untuk mengatasinya. Program pusat pengendalian lalu lintas yang dimiliki oleh TMC ini dapat mengetahui dengan cepat simpul-simpul jalan yang terjadi kemacetan dengan memanfaatkan CCTV di lapangan dan informasi yang masuk secara online dan terintegrasi dengan sistem di dalam TMC sehingga dengan cepat operator TMC dapat memantau dan memberikan informasi yang akurat kepada petugas di lapangan mengenai akar penyebab kemacetan tersebut untuk dilakukan penguraian arus sehingga tidak terjadi kemacetan yang berkepanjangan.

Tujuan terakhir TMC adalah pusat pengendali kualitas baku mutu udara. Tujuan ini juga merupakan penjabaran dari *action plan* Kapolda Metro Jaya dalam rangka menjaga kelestarian alam dan lingkungan yang sehat dan berpolusi rendah. Program ini menggunakan dukungan aplikasi teknologi kualitas baku mutu lingkungan yang diletakkan di wilayah DKI Jakarta dan terintegrasi dengan sistem pada TMC secara online. Dengan aplikasi ini maka TMC dapat memberikan informasi baik buruknya kualitas udara di wilayah tersebut kepada para Polantas di lapangan maupun masyarakat umum.

Untuk mencapai tujuan tersebut maka TMC PMJ memanfaatkan jaringan komputer sebagai peralatan pendukung utama pelaksanaan tugasnya, baik dalam

bentuk jaringan aplikasi internet maupun intranet. Jaringan aplikasi komputer yang terdapat dalam TMC PMJ adalah:

1. Jaringan aplikasi internet, untuk sistem kecelakaan lalu lintas, pelanggaran SIM, dan layanan BPKB. Jaringan yang digunakan untuk mengintegrasikan antara server TMC PMJ dengan jaringan internet menggunakan *collocation* yang disewa dari PT. Telkom. Sedangkan jaringan yang digunakan oleh TMC untuk mengakses aplikasi tersebut secara internal menggunakan jaringan dengan teknologi ADSL (*Asymetric Digital Subscriber Line*).
2. Jaringan aplikasi intranet untuk SSB. Jaringan yang digunakan untuk mengintegrasikan antara server KPTI (Kantor Pengelola Teknologi Informasi) Pemprov DKI Jakarta dengan komputer TMC PMJ adalah jaringan milik PT. Telkom secara *leased line* (saluran khusus yang disewa terus-menerus) oleh KPTI Pemprov DKI.
3. Jaringan aplikasi GPS (*Global Positioning System*) dan GIS (*Geographycan Information System*). Jaringan yang digunakan dalam aplikasi ini adalah jaringan GPRS milik provider GSM PT. Telkomsel dengan kecepatan jaringan 14.400 kbps.
4. Jaringan aplikasi CCTV. Jaringan yang digunakan dalam aplikasi ini adalah jaringan frekuensi *radio trunking* milik Polda Metro Jaya.
5. Jaringan aplikasi SMS. Jaringan yang digunakan dalam aplikasi ini adalah jaringan internet milik *provider* SMS Service milik PT. VISITEL.
6. Jaringan aplikasi faximile. Jaringan yang digunakan dalam aplikasi ini adalah jaringan telepon milik PT. Telkom.
7. Jaringan aplikasi *Call Center*. Jaringan yang digunakan dalam aplikasi ini adalah jaringan telepon milik PT. Telkom.
8. Jaringan komunikasi radio. Jaringan yang digunakan dalam aplikasi ini adalah jaringan radio trunking dan radio standar milik Polda Metro Jaya.

BAB IV
HASIL PENELITIAN

Keamanan informasi yang diterapkan pada operasional TMC PMJ saat ini merupakan suatu kebijakan, prosedur dan aktifitas yang dilakukan untuk melindungi aset informasi suatu organisasi, baik terhadap manusia, fisik bangunan maupun informasi itu sendiri, terhadap berbagai jenis ancaman yang dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan operasional suatu organisasi untuk menjamin organisasi tersebut mencapai misi atau sasaran yang ingin dicapainya dengan mengimplementasikan sistem keamanan informasi. Dalam menentukan sistem keamanan informasi yang akan diterapkan tersebut akan dipengaruhi oleh keunikan karakteristik dari sistem informasi yang dimiliki oleh TMC PMJ baik secara teknis manajemen maupun secara teknis fungsional.

Secara teknis dan manajemen maka sistem informasi merupakan perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi lain secara teknis dan fungsional, sistem informasi merupakan keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input*, *process*, *output*, *storage*, dan *communication*.

Untuk dapat mengetahui keunikan karakteristik sistem informasi TMC PMJ maka upaya yang bisa dilakukan adalah dengan meneliti sejarah berdirinya TMC PMJ dan penerapan layanan aplikasi informasi pada TMC PMJ sehingga nantinya akan berguna untuk mengidentifikasi aset yang ada dalam rangka menentukan kebijakan keamanan informasi.

4.1 Karakteristik *Traffic Management Center* Polda Metro Jaya

Setiap organisasi mempunyai suatu sistem yang unik, khas dan berbeda dengan organisasi lainnya. Keunikan karakteristik ini berperan dalam menentukan struktur dan berbagai sistem operasional organisasi tersebut dalam rangka mengidentifikasi aset dalam menentukan kebijakan keamanan informasi pada TMC PMJ.

4.1.1. SEJARAH BERDIRINYA TMC PMJ

Rencana keamanan informasi berfungsi untuk menetapkan suatu kebijakan (tata kerja) terhadap pelaksanaan keamanan informasi. Pernyataan kebijakan yang dibuat dapat menentukan tujuan organisasi terhadap keamanan informasi TMC, pertanggungjawaban pada masing-masing keamanan informasi itu diletakkan serta komitmen organisasi terhadap keamanan informasi pada TMC.

Gagasan didirikan TMC berasal dari Direktur Lalu Lintas Ponda Metro Jaya pada tahun 2005 (Brigjen Pol. Drs. Joko Susilo-sekarang Dirlantas Mabes Polri). Gagasan ini terinspirasi mengingat kala itu Biro Operasional Polda Metro Jaya mempunyai program 911 yang bertujuan sebagai pusat layanan informasi kepada masyarakat namun program tersebut tidak berjalan lama dan akhirnya berhenti. Menurut hasil wawancara yang dilakukan kepada Okho, mengatakan sebagai berikut:

> "Awalnya ini kan dulu gara-gara program 911 di Biro Operasional yang ngga jalan trus akhirnya Pak Joko bikin ini pak. Waktu itu seingat saya Bapak Joko baru pulang dari Jepang pak, kemudian beliau memanggil kami (Okho dan Rahmat) untuk membahas tentang rencana beliau untuk membangun pusat manajemen lalu lintas di Jakarta secara *integrated, computerized* dan *online*. Mungkin beliau terinspirasi dengan sistem lalu lintas di Jepang yang telah teratur dan berhasrat untuk membangun sistem itu di Jakarta..."

Setelah pertemuan tersebut, maka Okho dan Rahmat mencoba melakukan eksperimen untuk membuat perencanan struktur jaringan pendukung TMC. Kemudian mereka mengajak dua orang lagi yang bernama Yudho dan Alfon,

untuk bersama-sama membangun infrastuktur jaringan dari TMC PMJ. Dengan mengandalkan kemampuan keilmuan yang mereka miliki dari keempat orang tersebut maka mereka berbagi tugas untuk mencoba membuat perencanaan terhadap arsitektur jaringan TMC PMJ.

Setelah mereka menyatakan mampu untuk membangun infrastruktur jaringan tersebut maka mereka kembali menghadap Dirlantas untuk menyampaikan hasil perkembangannya. Menurut wawancara yang dilakukan kepada Okho, mengatakan sebagai berikut:

> "... beberapa minggu setelahnya kami bertiga dipanggil lagi ama Beliau pak. Intinya beliau menanyakan kesanggupan kami, apakah kami mampu membangun infrastuktur jaringan buat bangun TMC. Waktu itu Beliau hanya menggambarkan 'pokoknya saya pengennya begini, begini, begini',gitu aja pak. Trus kami melakukan konsultasi kepada Beliau mengenai hasil rencana yang udah kami susun sebelumnya yang akhirnya disetujui oleh beliau."

Sebagai pelaksanaan dari rencana Dirlantas yang dilakukan secara lisan kepada ketiga orang terasebut akhirnya Dirlantas melakukan uji coba dengan membangun infrastruktur jaringan TMC secara sederhana pada Kantor Lantas Pancoran. Ketika itu TMC Lantas Pancoran hanya mampu melakukan beberapa layanan saja, yaitu GIS, CCTV, *call center*, dan operator HT yang dilakukan oleh 13 orang anggota Polantas secara bergiliran serta dukungan Rahmat, Okho, Yudho, dan Alfon sebagai *IT expert TMC*. Hal ini disampaikan oleh Perwira Siaga "C" TMC PMJ AKP. Sugeng Budiono dalam wawancara sebagai berikut:

> "...dulunya TMC tempatnya ngga disini pak, tapi di Kantor Lantas perempatan Pancoran. Waktu itu memang Pak Joko yang mengarahkan pembangunan di sana. Saya kurang 86 kenapa Beliau memilih perempatan Pancoran pak, mungkin beliau bermaksud untuk melakukan uji coba pelaksanaan TMC. ...ketika itu jumlah anggota yang mengawaki cuma 13 orang dan layanannya cuma ada 4 buah aja, operator HT 4 ada orang, operator call center ada 4 orang, CCTV ada 3 orang dan GIS ada 2 orang."

Pengorganisasian operasional TMC Pancoran ketika itu masih sangat sederhana den belum terstruktur. Ketika itu petugas operator TMC belum mempunyai *job desciption* yang jelas. Bahkan penunjukan pelaksanaan terhadap petugas operator pun tidak dibekali surat perintah tugas sebagaimana biasanya petugas Polantas dalam melakukan tugas, namun hanya bersifat penunjukan dari atasannya saja dimana petugas yang pada saat itu melaksanakan tugas di Perempatan Pancoran secara otomatis menjadi operator TMC dan Perwira Piket Ditlantas pada saat itu bertanggung jawab sekaligus melakukan pengendalian atas pelaksanaan kegiatan operasional TMC Pancoran. Hal ini disampaikan oleh Sugeng Budiono dalam wawancara sebagai berikut:

> "... dulu penempatan anggota operator TMC ngga tersprint pak, pokoknya arahan dari Dir (dirlantas) dulu kalo anggota jaga di perempatan Pancoran berari otomatis juga piket operator di TMC Pancoran. Trus yang ngawasi ya Perwira Piket Ditlantas pak, nanti tiap turun apel piket laporan tentang anev kejadian kepada pak Dir."

Senada dengan yang disampaikan dengan Sugeng Budiono di atas, Jumarno juga menyatakan hal yang sama dalam wawancara sebagai berikut:

> "Waktu saya masih berpangkat AKP dulu saya juga pernah piket di TMC Pancoran mas. Sebelum turun Perwira Piket Ditlantas, pagi harinya saya menghadap ke Direktur atau ke Wakil Direktur kalo pak Dir ngga ada untuk laporan situasi di TMC. Pokoknya kalo kita para AKP ini naik piket di Ditlantas, kita juga harus ngawasi pelaksanaan TMC di Pancoran..."

Beberapa waktu kemudian setelah melakukan uji coba pelaksanaan TMC di kantor Ditlantas Pancoran maka akhirnya Ditlantas Polda Metro Jaya membangun TMC dalam areal Polda Metro Jaya di samping kantor Ditlantas Polda Metro Jaya. Proses pembangunan TMC PMJ yang dilakukan secara swadaya oleh Direktur Lalu Lintas kala itu tidak berlangsung lancar karena pembangunan tersebut tidak didukung oleh anggaran dinas Polri. Hal ini disampaikan oleh Okho dalam wawancara sebagai berikut:

"Dulu itu (pembangunan TMC) sempet berhenti & *stuck* karena pak Joko bilang kehabisan uang buat bangun ini pak. Ini sempat terjadi beberapa bulan sebelum dilanjutin lagi..."

Dengan segala keterbatasan yang ada dan upaya maksimal yang dilakukan oleh berbagai pihak di dalamnya maka pembangunan infrastuktur TMC PMJ akhirnya selesai dilaksanakan. Pada bulan Juli tahun 2007, TMC PMJ telah resmi beroperasi dalam rangka memberikan pelayanan informasi kepada masyarakat Jakarta Raya dengan basis jaringan komputer secara online hingga sekarang.

4.1.2. Penerapan Layanan Informasi pada TMC PMJ

Pada dasarnya layanan informasi pada TMC PMJ diklasifikasikan menjadi tiga apikasi layanan, yaitu aplikasi layanan internal Polantas, aplikasi layanan eksternal masyarakat umum serta aplikasi layanan lintas sektoral. Aplikasi layanan internal berfungsi untuk menyediakan informasi yang dibutuhkan oleh petugas Polantas untuk mendukung pelaksanaan tugasnya. Aplikasi layanan eksternal digunakan untuk menyediakan akses informasi bagi masyarakat umum yang membutuhkan informasi berkaitan dengan situasi dan kondisi bidang lalu lintas secara *real time*. Sedangkan aplikasi layanan lintas sektoral berfungsi untuk melakukan koordinasi dengan direktorat atau biro lain pada lingkungan Polda Metro Jaya dan dengan instansi lain diluar Polda Metro Jaya untuk melakukan kemitraan atau upaya pemecahan masalah.

Penerapan layanan informasi yang dilakukan pada TMC PMJ yang saat ini telah dilaksanakan adalah aplikasi internet (*website*), aplikasi intranet untuk SSB, aplikasi GPS (*Global Positioning System*) dan GIS (*Geographycan Information System*), aplikasi CCTV, aplikasi SMS, aplikasi faximile, aplikasi *call center* serta komunikasi radio. Secara keseluruhan aplikasi yang ditanam pada TMC PMJ tersebut digunakan untuk melaksanakan fungsi Komando, Komunikasi, Koordinasi dan Informasi (K3I).

Aplikasi Layanan Internet (*website*) merupakan sarana untuk mengetahui informasi secara global dan juga untuk membangun *image* dan *trust building*

masyarakat dengan melalui website. E-mail dan juga dikembangkan untuk mendukung data online dengan sistem internet. Alamat website yang digunakan oleh Ditlantas Polda Metro Jaya adalah http://lantas.polri.go.id.

Aplikasi Layanan Intranet (*Internal Networking*) digunakan untuk menghubungkan perangkat-perangkat komputer secara internal pada TMC PMJ. Disamping itu juga digunakan untuk menghubungkan antara TMC PMJ dengan perangkat komputer instansi samping (database KPTI, samsat wilayah, satlantas wilayah), dan Sub Direktorat Lalu Lintas.

Aplikasi Layanan GPS (*Global Positioning System*) merupakan alat yg digunakan untuk mengontrol dan memantau keberadaan petugas dilapangan, apabila dibutuhkan untuk kecepatan pengamanan dapat di komando/dikendalikan dari TMC. Sedangkan GIS (*Geographycan Information System*) merupakan program pendukung pengawalan dan pemantauan wilayah untuk mengetahui situasi dan kondisi aktual di lapangan yang dapat di pantau melalui peta di layar kontrol.

Aplikasi Layanan CCTV ini berbentuk kamera kontrol yang dipasang di titik-titik potensi terjadinya masalah-masalah sosial dibidang lalu lintas yang dapat di monitor dari layar kontrol TMC untuk mengetahui situasi aktual dilapangan. Saat ini seluruhnya telah ada 50 CCTV yang tersebar di seluruh pelosok Jakarta.

Aplikasi Layanan SMS (*Short Message Service*) adalah layanan singkat dan praktis dalam rangka pemberian informasi dan menerima berbagai masukkan, informasi, aduan dan sebagainya dari masyarakat yang dibuat dalam jaringan 1717. Dari layanan program ini juga masyarakat dapat memperoleh data-data tentang kendaraan bermotor. Selain layanan SMS 1717, TMC PMJ juga menyediakan layanan SMS *gateway* yang digunakan secara internal Direktorat Lalu Lintas.

Selain aplikasi layanan yang memanfaatkan teknologi online, TMC PMJ juga mempunyai layanan yang menggunakan saluran telepon dan komunikasi radio. Layanan Faximile adalah salah satu layanan yang memanfaatkan saluran telepon untuk mengirimkan dan menerima berita, bukti-bukti maupun data-data secara visual. Selain itu juga terdapat layanan *Call Center* yang berperan sebagai

alat komunikasi dari masayarakat atau media cetak/elektronik kepada TMC demikian juga sebaliknya. TMC PMJ juga memanfaatkan layanan komunikasi radio dengan menggunakan HT untuk melakukan komunikasi kendali terhadap para petugas Polantas di lapangan.

Beberapa waktu yang lalu, tepatnya tanggal 23 Mei 2010, TMC PMJ telah menorehkan prestasi nasional dengan mendapat penghargaan dari Museum Rekor Indonesia (MURI) atas penyediaan layanan informasi masyarakat di bidang lalu lintas dengan memanfaatkan jejaring sosial (*tweeter*) yang mempunyai *follower* terbanyak di Indonesia. Selama tiga bulan dioperasionalkan layanan informasi di bidang lalu lintas dengan memanfaatkan jejearing sosial *tweeter*, TMC PMJ mendapatkan apresiasi dari *follower* sebanyak 16.500 orang. Hal ini disampaikan oleh Adhie dalam wawancara sebagai berikut:

> "...kita memanfaatkan jejaring sosial secara online dalam bentuk *tweeter* mas. Alhamdulillah saat ini udah banyak yang ikut ke kita untuk mendapatkan dan memberikan informasi seputar lalu lintas di Jakarta. Beberapa waktu lalu kita dapat penghargaan dari MURI atas layanan kita ini mas, MURI mencatat ada 16 ribu-an orang yang jadi *follower* kita di TMC PMJ."

Senada dengan hal tersebut maka Okho juga menyampaikan hal yang sama dalam wawancara sebagai berikut:

> "Alhamdulillah pak jumlah *follower* kita di *tweeter* TMC PMJ terus bertambah. Beberapa waktu yang lalu ketka dapat penghargaan, *follower* kita mencapai 16.500 orang. Sekarang (bulan Juni) di catatan kita jumlah follower TMC PMJ jumlahnya udah mencapai 40 ribuan orang. Mungkin ini masih akan nambah lagi pak..."

4.2. Kebijakan Keamanan Informasi yang Dilakukan oleh Ditlantas Polda Metro Jaya Saat Ini

Seperti yang telah disampaikan sebelumnya, bahwa keamanan informasi meliputi kebijakan, prosedur dan aktifitas untuk melindungi aset informasi baik

manusia, fisik bangunan maupun informasi itu sendiri terhadap berbagai jenis ancaman yang dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan operasional suatu organisasi. Sebagai penjabarannya maka penulis mengklasifikasikan kebijakan keamanan pada TMC PMJ saat ini menjadi tiga sub bab, yaitu kebijakan keamanan terhadap personel, kebijakan keamanan terhadap fisik bangunan, dan kebijakan keamanan terhadap informasi.

4.2.1 Kebijakan Keamanan Terhadap Personel TMC PMJ

Unsur manusia menjadi salah satu bahan yang penting dalam pengembangan dan penggunaan sistem informasi. Personel dalam keamanan sistem informasi adalah sumber daya informasi yang dapat memberikan suatu kontribusi nyata dalam mencapai sasaran strategis dan meraih keunggulan kompetitif dalam upaya mewujudkan keamanan sistem organisasi sehinga bermuara pada tercapainya tujuan organisasi serta meminimalkan resikonya.

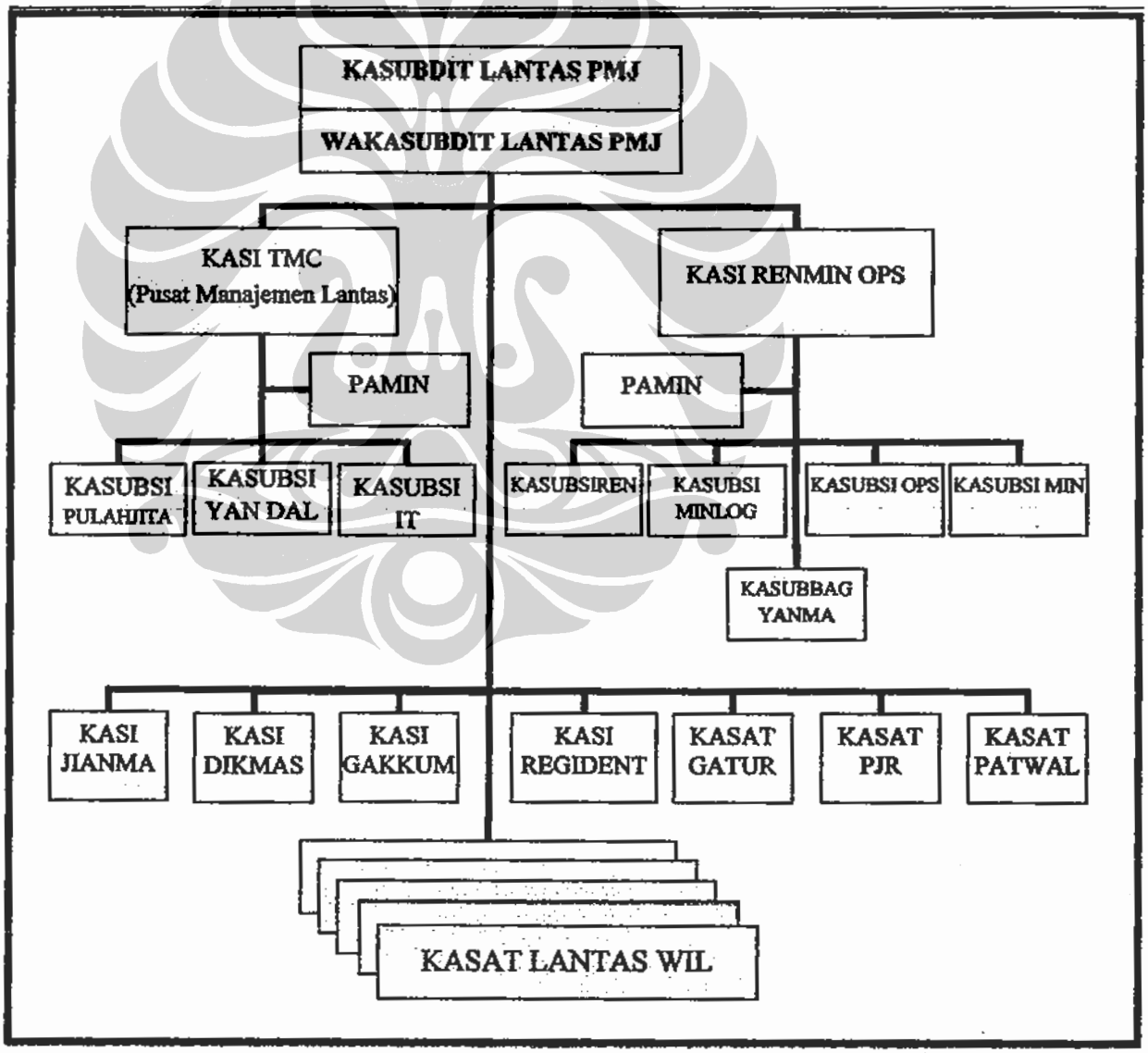
Dalam menuangkan hasil penelitian tentang kebijakan keamanan terhadap personel TMC PMJ maka peneliti berpijak kepada pernyataan Djamin (1995, p.11) yang menegaskan bahwa fungsi pokok manajemen personel meliputi perencanaan, pengorganisasian, pengarahan, pemotivasian dan pengendalian.

Secara umum personel yang mengawaki TMC PMJ diklasifikasikan menjadi empat kelompok berdasarkan tugasnya, yaitu: (a). Kelompok penanggungjawab, yang terdiri dari Dirlantas, Wadir Lantas, Kasubditmin Regident, Kasubbag Renmin dan Kasubdit Dikyasa; (b). Kelompok petugas operasional TMC; (c). Kelompok IT (*information technology*); dan (d). Kelompok teknisi.

Dalam buku operasional TMC dijelaskan bahwa organisasi TMC PMJ berada di bawah Ditlantas Polda Metro Jaya dengan Direktur Lalu Lintas sebagai penanggung jawab secara keseluruhan. Di dalam struktur organisasi Direktorat Lalu Lintas Polda Metro Jaya seperti yang telah disampaikan sebelumnya dapat dilihat bahwa organisasi TMC PMJ belum tercantum di dalamnya. Untuk perkembangan ke depan maka Ditlantas Polda Metro Jaya telah mengajukan konsep pengembangan organisasi yang bertujuan untuk memasukkan TMC PMJ

ke dalam struktur Ditlantas yang baru. Hal ini disampaikan oleh Jumarno dalam wawancara sebagai berikut:

"... TMC sekarang betul-betul berperan penting dalam pelaksanaan tugas kita mas. Saat ini memang TMC PMJ belum mempunyai kejelasan struktur di dalam lingkungan Ditlantas, namun kami sudah melakukan konsep pengembangan organisasi Ditlantas kepada beliau yang diajukan untuk tahun anggaran 2011 nanti disesuaikan dengan kebutuhan struktural kita dan jumlah personel yang memadai."



Gambar 4.1: Konsep Pengembangan Organisasi Ditlantas PMJ

Dalam mengelola TMC PMJ, Dirlantas dibantu oleh Wadir Lantas sebagai penanggung jawab harian, Kasubditmin Regident sebagai penanggung jawab pemeliharaan, Kasubdit Dikyasa sebagai penanggung jawab komunikasi dan informasi, dan Kasubbag Renmin sebagai penanggung jawab kontrol dan kendali. Hal ini juga disampaikan oleh Jumarno dalam wawancara sebagai berikut:

> "TMC itu berada langsung di bawah Dirlantas mas, jadi Beliau bertanggung jawab penuh atas semua kegiatan di dalammya. Trus pak Wadir jadi penanggung jawab harian. Lalu ada lagi Kasubditmin Regident, Kasubdit Dikyasa, dan saya termasuk di dalamnya. Masing-masing kasubdit ini punya peran di dalam TMC, kalo Kasubditmin Regident itu bertanggung jawab utk pemeliharaan, trus Dikyasa tanggung jawabnya di bidang informasi dan komunikasinya. Nah saya kebagian control dan pengendalian mas..."

Hal senada juga disampaikan oleh Adi dalam wawancara sebagai berikut:

> "... TMC ini dikelola langsung oleh pak Dir mas. Selain itu Beliau nunjuk para Kasubdit dan Renmin bertanggung jawab di bidangnya masing-masing yang berkaitan dengan TMC ini."

Sebagai penjabaran operasionalisasi TMC PMJ maka Dirlantas menunjuk personel organik dari Ditlantas Polda Metro Jaya untuk menjadi petugas operasional TMC PMJ. Penunjukan tersebut tertuang dalam surat perintah Dirlantas Polda Metro Jaya Nomor: Sprin/39/I/2010/Ditlantas tanggal 31 Januari 2010. Isi dari surat perintah tersebut adalah penunjukan jabatan bagian TMC PMJ yang dilaksanakan oleh personel organik Ditlantas Polda Metro Jaya. Hal ini bermakna bahwa selain juga melaksanakan tugas dan jabatan struktural sehari-hari dalam lingkungan Ditlantas Polda Metro Jaya, mereka juga mendapatkan tugas sebagai operator operasional TMC PMJ.

Menurut Jumarno, saat ini personel yang mengawaki TMC PMJ berjumlah 67 orang dengan pangkat pamen, pama, dan bintara. Lebih lanjut dikatakannya bahwa mereka ditunjuk sebagai operator operasional TMC berdasarkan surat

perintah yang ditanda tangani oleh Dirlantas. Hal tersebut disampaikan oleh Jumarno dalam wawancara sebagai berikut:

> "... anggota TMC itu jumlahnya 67 mas, mereka kita ambil dari masing-masing struktural yang ada di kita kemudian mereka kita tunjuk untuk menjadi operator TMC. Penunjukan ini kita laksanakan atas perintah dari Dirlantas, kemudian kita buatkan sprin untuk mereka..."

Berdasarkan Surat Perintah Dirlantas Polda Metro Jaya Nomor: Sprin/39/I/2010/Ditlantas tanggal 31 Januari 2010, Koordinator TMC PMJ diemban oleh Kasat PJR Ditlantas Polda Metro Jaya, dan Kasi BPKB Ditlantas Polda Metro Jaya sebagai Wakil Koordinator TMC PMJ. Koordinator operasional TMC PMJ mempunyai tanggung jawab penuh atas pelaksanaan operasional TMC PMJ dalam rangka melakukan kegiatan K3I (Komando, Komunikasi, Koordinasi, dan Informasi). Dalam pelaksanaan operasional TMC PMJ, Koordinator operasional TMC PMJ dibantu oleh Wakil Koordinator TMC PMJ, team analis yang dipimpin oleh Ketua Tim Analis, staf TMC yang terdiri dari satu orang staf TMC PMJ dan lima orang operator STNK serta tiga regu petugas siaga sebagai petugas pelaksana operasionalisasi peralatan TMC PMJ (biasai disebut Regu Siaga A, B dan C) yang masing-masing regu dipimpin oleh seorang Perwira Siaga dengan pangkat AKP.

Masing-masing regu siaga TMC PMJ terdiri dari seorang perwira berpangkat AKP yang membawahi satu orang staf, petugas operator call center, petugas operator cakra (HT), petugas operator CCTV, petugas operator GIS, petugas operator internet, petugas operator SMS 1717, petugas operator report SMS 1717, dan satu orang teknisi. Ketiga regu petugas siaga tesebut melaksanakan tugasnya selama 24 jam secara bergiliran. Mereka dibagi menjadi dua *shift* dengan format pembagian waktu siaga selama 12 jam mulai pukul 08.00 hingga 20.00 dan mulai pukul 20.00 hingga 08.00, demikian seterusnya.

Khusus untuk petugas operator STNK, mereka tidak berada di bawah regu siaga TMC PMJ melainkan berada dalam unsur staf TMC. Dalam pelaksanaannya, petugas operator STNK tetap bergiliran mengikuti pola pembagian waktu yang dilaksanakan oleh regu jaga namun mereka bertanggung

jawab langsung kepada Ketua Team Analis (bukan kepada perwira siaga regu). Hal ini dilakukan sebagai upaya untuk menjaga keamanan informasi data STNK yang dimiliki oleh TMC PMJ untuk membatasi kendali akses. Hal ini diungkapkan oleh Adi dalam wawancara sebagai berikut:

> "... operator STNK itu melekat pada kita, mereka tidak berada di bawah pa siaga tetapi langsung dengan saya. Tapi kalo pelaksanaan tugasnya mereka mengikuti piket regu TMC mas. Ini dari pertama udah seperti itu, soalnya ini hal rawan mas. Maksudnya biar anggota yang lain segan mo tanya tentang informasi yang berkaitan dengan STNK, juga biar data STNK itu cuma mereka aja yang tau."

Proses penunjukan personel Ditlantas untuk menjadi operator TMC PMJ yang dilakukan oleh Dirlantas melalui surat perintah tersebut merupakan hasil saran masukan yang diberikan oleh Wadir Lantas dan Kasubbag Renmin. Kriteria yang paling signifikan dalam menentukan penunjukan tersebut dilandasi pada kemampuan seseorang dalam mengoperasionalkan komputer, sebagaimana yang disampaikan oleh Jumarno dalam wawancara sebagai berikut:

> "... penunjukan ini bukan didasari pada rasa sentimen mas, tapi kita ngeliat dari kemampuan komputer orang itu. Apa dia bisa komputer ato tidak. Soalnya TMC itu semuanya kan pake komputer to mas, lha kalo mereka ngga bisa pake komputer kan malah susah kita. Itu alasan utama penunjukan kita..."

Kemampuan komputer yang dimiliki oleh operator TMC PMJ sebagai persyaratan awal penunjukan personel Ditlantas menjadi operator TMC PMJ ini juga diungkapkan oleh Erwan dalam wawancaranya sebagai berikut:

> "... memang dari dulu saya hobi komputer pak. Dulu saya bertugas di Satpas, namun karena pimpinan melihat saya bisa main komputer kemudian saya dipanggil dan diarahkan untuk jadi operator disini."

Dalam surat perintah Dirlantas tersebut juga tercantum tiga orang teknisi yang melekat dalam masing-masing regu siaga. Ketiga orang ini berstatus pekerja harian lepas (PHL) dengan latar belakang pendidikan sarjana S1 komputer. Tugas

mereka adalah melakukan perbaikan dan perawatan terhadap peralatan komputer dan jaringannya yang berada di dalam ruangan TMC PMJ. Hal ini disampaikan oleh Adhi dalam wawancara sebagai berikut:

> "Kita punya tiga orang teknisi, mereka itu sehari-hari melekat ama regu siaga mas. Tugasnya kalo komputer atau jaringannya di dalam ada yang gangguan, mereka yang betulin."

Hal senada juga disampaikan oleh Hendrik dalam wawancara berikut:

> "... saya udah lama kerja disini pak. Saya lulusan S1 Universitas X. Tugasnya kalo ada yang rusak, komputer hang, trus kalo kena virus, atau *hard disc*nya tiba-tiba mati gara-gara udah waktunya ganti, itu saya yang betulin pak."

Selain petugas operator TMC PMJ dan teknisi yang ditunjuk berdasarkan surat perintah Dirlantas, masih ada lima personel lain yang termasuk di dalam tim IT dan berperan sebagai *system administrator* TMC PMJ. Kelima orang tersebut adalah Rahmat (sebagai koordinator tim IT), Okho (penanggungjawab jaringan, GIS dan sistem pendukung layanan), Alfon dan Bayu (penanggungjawab data SSB), serta Yudho (penanggungjawab hardware). Mereka bertanggung jawab penuh atas pelaksanaan keamanan, perawatan serta pengoperasian aplikasi jaringan komputer yang digunakan untuk mendukung operasional TMC PMJ.

Secara struktural mereka tidak memiliki posisi dalam organisasi Ditlantas maupun TMC PMJ. Proses perekrutan mereka dilakukan berdasarkan pada keyakinan Dirlantas ketika itu akan kemampuan mereka untuk membangun jaringan TMC PMJ seperti yang telah disampaikan sebelumnya. Walaupun demikian, secara lesan mereka berada di bawah kendali Dirlantas sebagai penanggung jawab umum TMC PMJ, seperti yang dituturkan oleh Rahmat dalam wawancara sebagai berikut:

> "Iya mas kita ngga terstruktur disini. Waktu itu pak Dir Cuma bilang begini, 'ya udah kalo gitu kamu di bawah saya aja.' Ya udah akhirnya kita ngikut beliau... sering kali Pak Dir manggil kita ke ruangan untuk *sharing* tentang tugas kita, ada kendala apa ngga. Trus biasanya tiap akhir bulan

sambil ngobrol Beliau kasih uang untuk kita, katanya sih buat makan minum kita disini..."

Untuk memotivasi para operator TMC PMJ sehingga tetap melaksanakan tugasnya dengan optimal maka ada kebijakan yang tidak tertulis dimana apabila para petugas operator telah melaksanakan tugas dengan sebaik-baiknya maka mereka diperbolehkan untuk mengajukan usul mutasi ke tempat yang diinginkan. Namun apabila mereka tidak melaksanakan tugas dengan baik maka mereka akan digantikan oleh petugas Ditlantas lain yang menginginkannya. Hal ini diungkapkan oleh Sugeng dalam wawancara sebagai berikut:

"...saya sudah bertugas disini selama hamper tiga tahun pak. Biasanya Beliau itu melihat kinerja kita. Kalo menurut penilaian Beliau bagus, nanti saya bisa mengajukan pindah ke tempat lain. Trus beliau pasti mendukung proses mutasi kita sesuai dengan apa yang kita mau. Tapi kalo kita disini elek-elekan, ngga lama pasti orang itu akan diganti oleh Beliau pak. Ini contohnya udah ada."

Adhi juga menyatakan hal yang sama dalam wawancara sebagai berikut:

" ...pokoknya disini kita harus tunjukkan kinerja yang terbaik mas. Soalnya Beliau menilai kita selama dinas di TMC. Turunannya kalo kita kerja bagus disini, nanti kita bisa milih mo kemana dan Beliau pasti dukung."

Agar pelaksanaan operasional TMC PMJ dapat berjalan sesuai dengan harapan maka dilakukan upaya pengendalian terhadap masing-masing personel yang mengawaki TMC PMJ. Upaya pengendalian ini terdiri dari pengendalian yang dilakukan oleh unsur pimpinan TMC PMJ kepada petugas operator (*top-down approach*) dalam bentuk pengawasan yang dilaksanakan secara berjenjang. Selain itu juga dilakukan pengendalian oleh masing-masing petugas operator kepada unsur pimpinan dalam bentuk pelaporan hasil kerja selama mereka melaksanakan tugas (*bottom-up approach*).

Di dalam gedung TMC PMJ terdapat dua buah CCTV yang dipasang pada sudut kanan depan dan sudut kiri belakang. CCTV ini terhubung dengan layar monitor di dalam ruangan Dirlantas yang berfungsi untuk memantau dan mengawasi kinerja masing-masing petugas operator dalam melaksanakan kegiatannya. Dengan menggunakan CCTV ini maka setiap saat Dirlantas dapat melakukan pengendalian atas personel yang sedang bertugas dan dapat memberikan tindakan kepada petugas operator apabila mereka tidak melakukan kegiatan yang semestinya. Seperti yang disampaikan oleh Sugeng dalam wawancara sebagai berikut:

> "... itu pak liat di ujung kanan atas kita sama di ujung belakang kiri kita. Itu ada CCTV yang nyambung ke ruangan Dir. Yang di depan itu bisa di *zoom* ke seluruh operator disini pak, jadi beliau pasti akan tau kalo kita kerja ngga bener."

Sebagai bukti atas pelaksanaan tugasnya, maka masing-masing petugas operator TMC PMJ membuat laporan hasil kegiatannya secara tertulis yang disampaikan secara berjenjang kepada Dirlantas dan Koordinator TMC PMJ. Bagi para operator layanan TMC PMJ, mereka membuat rekapitulasi laporan yang masuk ke TMC PMJ baik dari masyarakat maupun dari petugas Ditlantas di lapangan selama 1x24 jam. Rekapitulasi laporan tersebut berisi tentang jumlah dan isi laporan yang masuk melalui SMS 1717, telepon, internet, radio dan faximile serta HT.

Para Perwira Siaga TMC PMJ juga membuat laporan harian situasi kamseltibcar lantas selama 1x24 jam yang terjadi di wilayah hukum Polda Metro Jaya. Laporan harian tersebut berisi tentang data laka lantas yang terjadi, pelanggaran tilang, kemacetan lalu lintas, kejadian unjuk rasa, kegiatan pengawalan VIP/VVIP, gangguan *traffic light*, pohon tumbang, banjir dan genangan air, kebakaran, gangguan kendaraan roda dua atau empat, ancaman bom serta jalan berlubang dan galian.

Hal yang sama juga berlaku bagi Tim Analis TMC PMJ dalam hal pembuatan laporan. Kepala Tim Analis diharuskan untuk membuat laporan hasil analisis setiap seminggu sekali terhadap kendala yang terjadi di lingkungan

internal TMC PMJ dan melakukan evaluasi atas kendala tersebut dalam bentuk saran yang diajukan kepada Dirlantas dan Koordinator TMC PMJ.

4.2.2 Kebijakan Keamanan Terhadap Fisik Bangunan TMC PMJ

Seperti yang telah ditulis sebelumnya bahwa fisik bangunan merupakan salah satu dari aset informasi yang harus dilindungi terhadap berbagai jenis ancaman yang dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan operasional suatu organisasi.

Menurut Hadiman (2009), sasaran penelitian terhadap fisik adalah kegiatan fisik yang digelar dalam rangka pengamanan fisik dari suatu bangunan. Lebih lanjut dikatakannya bahwa dalam rangka melakukan penelitian terhadap fisik bangunan agar memfokuskan perhatiannya kepada kondisi dari berbagai *barriers* yang ada, keberadaan peralatan atau *barriers* tersebut, kelemahan dan gangguan yang terjadi dengan peralatan atau *barriers* tersebut serta upaya yang dilakukan oleh manajemen, dan pemanfaatannya oleh pihak-pihak yang berkepentingan dalam rangka pengamanan fisik tersebut.

Ruangan TMC PMJ terletak di lantai dua gedung utama Ditlantas Polda Metro Jaya dengan luas areal ±700 m². Akses untuk menuju ke dalam ruangan ini melalui pintu kaca sebelah kiri yang dijaga oleh satu orang petugas jaga Ditlantas. Kemudian menaiki tangga menuju ke lantai dua, disana juga dijaga oleh seorang petugas jaga Ditlantas. Setelah itu menyusuri koridor kaca, melingkar setengah bangunan dan menjumpai pintu besar TMC PMJ yang diapit oleh dua buah ruangan perwira pengawas Ditlantas di kiri dan kanan pintu masuk ruangan TMC PMJ.

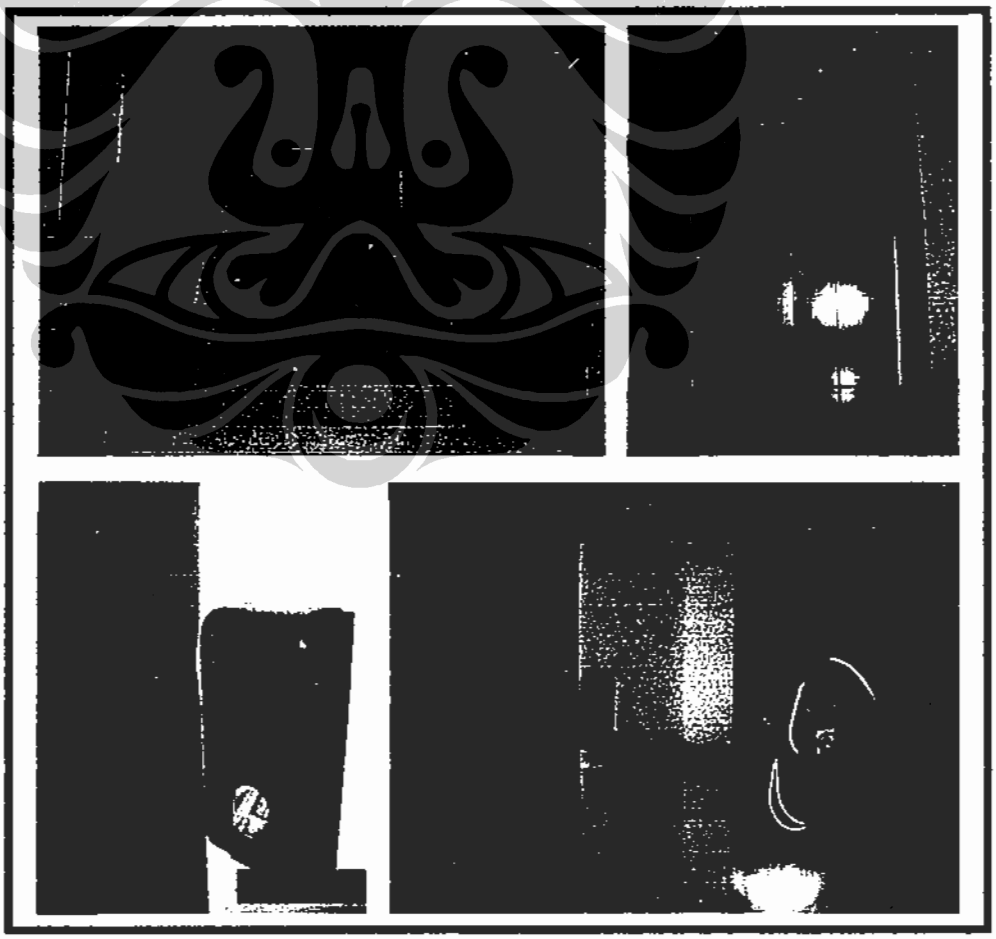
Pintu masuk utama ruangan TMC PMJ mempunyai *barrier* berupa peralatan *digital lock* yang dipasang pada dinding sebelah kanan pintu utama. Bahan material yang digunakan sebagai pintu utama adalah kayu papan hardplex dengan ketebalan 2 cm. *Digital lock* yang terpasang pada pintu utama ini menggunakan *finger print* sebagai sarana identifikasi bagi siapapun yang akan memasuki areal ruangan TMC PMJ. Yudho mengatakan bahwa *digital lock* dengan *finger print* tersebut sudah diprogram untuk orang-orang yang

berkepentingan saja yang bisa memasuki ruangan TMC. Hal ini disampaikan oleh Yudho dalam wawancara sebagai berikut:

> "...untuk bisa akses ke dalam ruangan ngga semuanya bisa pak. Ini kitaset yang bisa masuk cuma untuk orang-orang tertentu aja, kaya pak Dir, petugas operator, itu aja pak. Kalo yang lainnya mereka ngga bisa akses ke dalam, kecuali mereka di *direct* ama orang yang udah kita kasih ijin."

Hal senada juga disampaikan oleh Adhi dalam wawancara sebagai berikut:

> "...duhh mas saya aja ngga bisa masuk karena ada *finger print* itu. Ini saya baru mo minta Yudho buat nge*set finger print* saya biar bisa masuk ke dalam. Saya kan kepala analis disini jadi saya bisa dapat kode aksesnya mas."



Gambar 4.2: *Barrier* Pintu Masuk Utama TMC PMJ

Selain akses masuk ke dalam ruangan TMC PMJ melalui pintu utama, juga ada akses masuk melalui pintu samping. Bahan material yang digunakan sebagai pintu utama adalah kayu papan hardplex dengan ketebalan 2 cm. Pintu ini hanya digunakan sebagai pintu cadangan apabila terjadi keadaan darurat untuk proses evakuasi bagi para operator TMC PMJ. Selain itu, pintu ini juga hanya digunakan untuk memasukkan peralatan-peralatan yang dibutuhkan bagi kepentingan operasional TMC PMJ. Hal ini disampaikan dalam wawancara sebagai berikut:

> "Pintu samping itu gunanya untuk evakuasi dan memasukkan barang dan peralatan aja pak. Biar gampang masuknya pak. Kalo lewat pintu utama itu susah, lagian tempatnya tinggi jadi agak ribet."

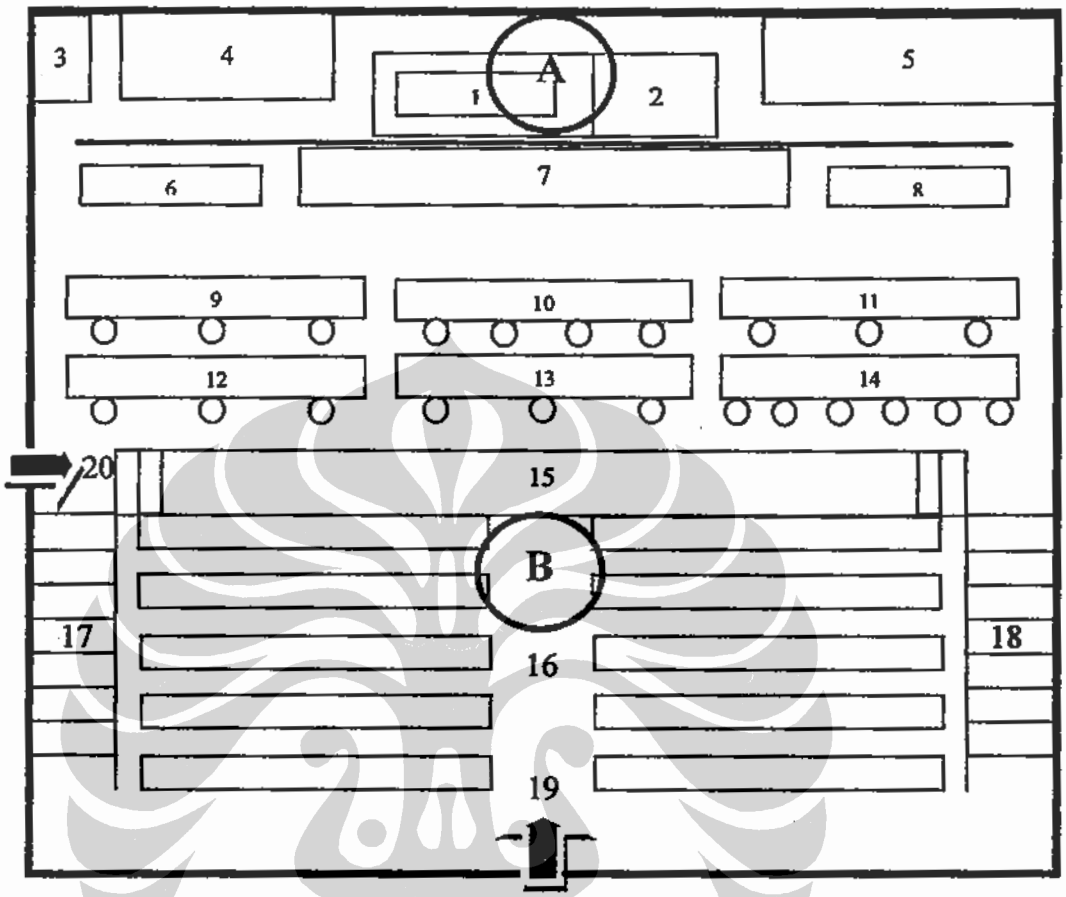
Pintu samping ini tidak mempunyai alat *digital lock* dengan *finger print*, sebagai pengaman maka digunakan kunci pintu manual. Ini berfungsi apabila terjadi kerusakan pada alat *digital lock* pada pintu utama maka petugas operator masih dapat keluar masuk melalui pintu samping. Dalam pengamatan yang peneliti lakukan, sehari-harinya pintu ini selalu dalam keadaan terkunci rapat dan tidak pernah digunakan untuk akses masuk bagi petugas operator TMCC PMJ. Menurut penuturan dari Adhi, kunci pintu itu ada dua buah dipegang oleh Dirlantas dan Koordinator TMC PMJ. Hal ini disampaikan dalam wawancaar sebagai berikut:

> "...pintu itu ngga pernah dibuka kecuali untuk barang aja mas. Tiap harinya selalu dikunci dan kunci dipegang ama Dirlantas dan Koordinator TMC PMJ. Jadi kalo kita mau masuk ke dalam ruangan ya harus lewat pintu utama itu. Itu cuma buat evakuasi ama kalo semisal *digital lock*-nya pintu utama rusak, baru kita pake pintu samping."

Agar dapat melakukan pemantauan terhadap situasi yang terjadi di luar ruangan maka dipasang 2 buah CCTV pada masing-masing pintu utama dan pintu samping. Peralatan CCTV ini terhubung dengan layar monitor yang berada pada ruangan Dirlantas dan area *command control*, untuk selanjutnya dilakukan pengawasan selama 24 jam oleh Perwira Siaga TMC PMJ.

Ruangan di dalam TMC PMJ terbagi menjadi dua bagian, yaitu ruangan utama dan ruangan belakang. Ruangan utama merupakan tempat operasional TMC PMJ. Disini terdapat hampir keseluruhan peralatan *hardware* yang digunakan untuk mendukung pelaksanaan tugas-tugas para operator dalam melakukan kegiatannya. Sedangkan untuk ruangan belakang digunakan untuk tempat main server TMC PMJ. Selain itu juga terdapat musholla, kamar mandi, dan ruangan istirahat bagi para operator TMC PMJ. Kedua ruangan tersebut disekat dengan dinding tembok dan dihubungkan melalui akses pintu terbuka pada samping kiri dan kanan layar monitor besar.

Gambar 4.3: Ruangan Dalam TMC PMJ



GAMBAR 4.4: Denah Ruangan TMC PMJ

Keterangan:

A. Ruangan belakang:
   1. Server TMC PMJ.
   2. Ruangan server TMC PMJ.
   3. Kamar mandi.
   4. Ruangan musholla.
   5. Ruangan istirahat.

B. Ruangan utama:
   6. Layar monitor kecil kiri.
   7. Layar monitor besar.
   8. Layar monitor kecil kanan.
   9. Operator layanan GPS.
   10. Operator layanan CCTV.

11. Operator layanan SMS center 1717 dan SSB.
12. Operator layanan Website
13. Operator layanan GIS
14. Operator layanan Call Center.
15. Area command control.
16. Area kunjungan tamu.
17. Tangga kiri.
18. Tangga kanan.
19. Pintu masuk utama.
20. Pintu masuk samping.

Di dalam ruangan utama TMC PMJ terdapat 1 buah layar monitor besar, 12 buah layar monitor kecil, 25 unit komputer yang dipakai oleh para operator dan area *command control*, 3 unit komputer yang dipakai untuk *running text*, staf TMC PMJ dan Perwira Siaga, 2 buah *virtual projector*, 12 unit AC split, 4 unit AC atap, 4 unit AC standing, 2 set CCTV camera (night vision color dome dan outdoor long range) serta 4 set *fire extinguisher*.

Peralatan keamanan yang diletakkan pada ruangan ini berkaitan dengan sistem keamanan fisik dalam ruangan utama adalah 4 set *fire extinguisher* yang diletakkan pada tiap sudut ruangan utama dan 2 set CCTV yang tersambung pada layar monitor di ruangan Dirlantas. Menurut keterangan dari Sugeng, diketahui bahwa keempat set *fire extinguisher* tersebut sudah lama diletakkan di situ dan belum pernah sekalipun dicoba. Hal ini disampaikan oleh Sugeng dalam wawancara sebagai berikut:

> "Sejak pertama TMC PMJ berdiri kita sudah punya perlengkapan pemadam api pak. Tabungnya ditaruh di setiap ujung ruangan. Ini untuk antisipasi kita kalo misal ada kebakaran kecil, apakah itu konslet listrik, jadi kebakarannya ngga merembet dan membesar. Tapi alat itu memang belum pernah dicoba pak. Dari baru trus langsung ditaruh disitu..."

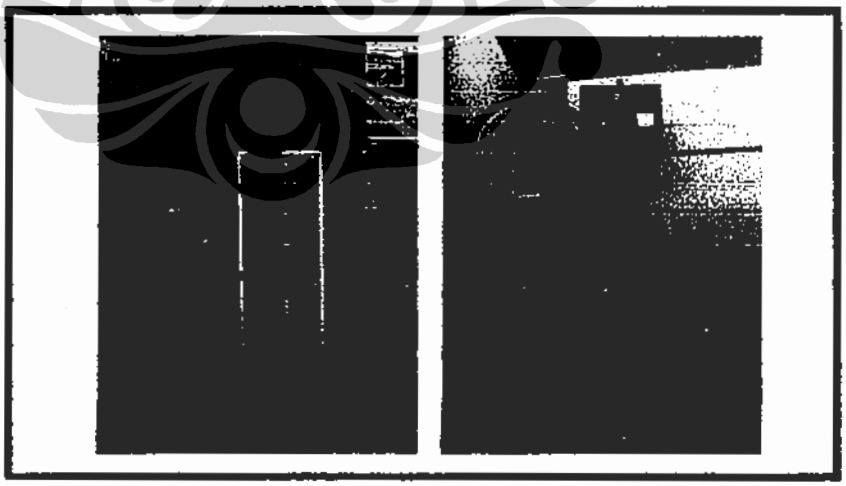
Kemudian untuk peralatan CCTV yang dipasang digunakan untuk mengawasi kinerja para petugas operator. Selain itu berdasarkan hasil wawancara

yang telah dilakukan oleh Sugeng dapat diketahui bahwa TMC PMJ belum mempunyai standar operasional prosedur dalam penanganan kebakaran ataupun ancaman bencana lainnya. Selain itu selama berdirinya TMC PMJ belum pernah dilakukan pelatihan terhadap penanggulangan bencana terhadap para operator TMC PMJ. Hal ini disampaikan oleh Sugeng dalam wawancara sebagai berikut:

> "... kita belum buat SOP tentang bencana pak. Alhamdulillah selama ini belum pernah terjadi, mudah-mudahan jangan terjadi ya pak. Petugas disini juga belum pernah dilatih tentang evakuasi. Tapi kalo pimpinan memberikan arahan tentang keselamatan berkaitan dengan evakuasi ya sering pak. Contohnya kita dikasih tau kalo terjadi bencana trus mau evakuasi harus lewat pintu samping. Takutnya kalo lewat pintu utama kunci digital nya rusak jadi kita ngga bisa keluar."

Hal senada juga disampaikan oleh Adhi dalam hasil wawancara sebagai berikut:

> "...sering mas kita APP anggota tentang masalah keselamatan kalo terjadi kebakaran ato yang lainnya. Saya juga pernah peragakan caranya pake alat pemadam api itu, tapi memang alat itu belum pernah dicoba mas."



Gambar 4.5: *Fire Extinguisher* dan CCTV di Ruangan Utama TMC PMJ

Pada ruangan belakang TMC PMJ terdapat 10 unit komputer yang digunakan untuk menjalankan server, 1 unit komputer untuk teknisi, 4 unit AC

split 2 unit AC atap, 2 set *fire extinguisher*, dan ruangan server yang berisi 10 unit server.

Ruang belakang TMC PMJ mempunyai peranan penting sistem keamanan informasi. Di dalam ruangan ini terdapat satu ruangan yang berdinding kaca dan mempunyai *barrier* pada pintu masuk berupa *digital lock* dengan menggunakan *finger print* yang jenis dan bentuknya sama seperti pada pintu masuk utama TMC PMJ di depan. Ruangan tersebut dipakai sebagai tempat penyimpanan beberapa server yang menjadi peralatan utama dari operasional sistem jaringan komputer secara online oleh TMC PMJ.

Gambar 4.6: Ruangan Penyimpanan Server TMC PMJ

Ruangan server ini terlihat sangat terlindungi. Pintu masuk yang dipasangi *digital lock* dengan menggunakan *finger print* tersebut hanya diprogram untuk beberapa orang saja yang bisa mengaksesnya, yaitu: Dirlantas, dan lima orang tim IT TMC PMJ saja. Apabila ada orang lain diluar keenam orang tersebut yang akan memasuki ruangan ini, maka Perwira Siaga akan menanyakan kepentinganny. Bila diijinkan oleh Perwira Siaga maka untuk memasuki ruangan tersebut harus didampingi oleh salah satu tim IT TMC PMJ. Disamping itu tembok yang berada dalam ruangan tersebut terbuat dari kaca tebal. Menurut Yodho, ini dimaksudkan agar kondisi di dalam ruangan tetap terpantau dari luar

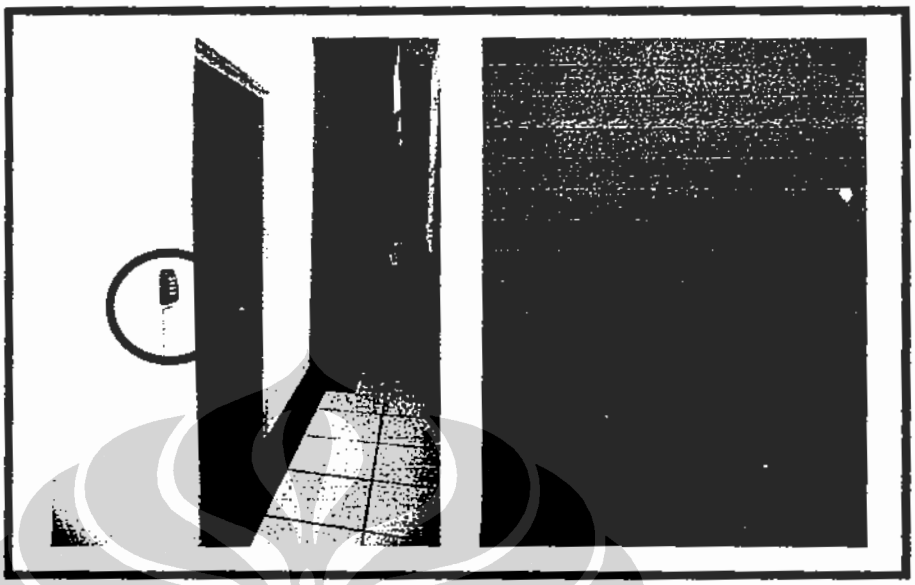
berkaitan dengan pengendalian akses. Di dekat pintu masuk server disiapkan satu buah alat *fire extinguisher*. Hal ini disampaikan oleh Dani dalam hasil wawancara sebagai berikut:

> "...ruangan ini bagi kami adalah intinya TMC PMJ pak. Itu sebabnya kami pasang *digital lock* dan yang bisa masuk cuma kami berlima dan Direktur aja. Yang lainnya ngga bisa. Trus kami pasang kaca di sekeliling ruangan sebagai pengganti tembok biar yang piket bisa memantau kondisi dalam ruangan server ini."

Selain ruangan TMC PMJ sebagai tempat operasional layanan aplikasi terhadap masyarakat, ada satu ruangan lagi yang menjadi tempat pengendalian aplikasi semua jaringan yang dimiliki TMC PMJ. Tempat itu disebut ruangan analisis jaringan TMC PMJ yang terletak di samping ruangan TMC PMJ sebelah luar. Di dalam ruangan ini tersimpan beberapa set peralatan komputer dan layar monitor yang berfungsi untuk memantau dan mengendalikan semua aplikasi layanan jaringan operasional TMC PMJ. Dari ruangan ini mereka bisa memantau dan mengendalikan aplikasi layanan yang sedang dioperasionalkan oleh petugas operator TMC PMJ. Ruangan ini juga bersifat tertutup dengan menggunakan *barrier digital lock*. Menurut Yudho, ruangan analisis jaringan ini hanya bisa dimasuki oleh Dirlantas dan personel tim IT saja.

Ruangan analisis jaringan ini tidak bisa dimasuki oleh petugas operator TMC PMJ selain atas perintah dari Dirlantas. Hal ini disampaikan oleh Sugeng dalam hasil wawancara sebagai berikut:

> "...Ruangan analisis itu sifatnya tertutup pak. Saya pun tidak bisa masuk ke ruangan itu. Seandainya terjadi gangguan pada layanan jaringan TMC PMJ maka saya cuma bisa mengetuk pintu dari luar saja dan tidak bisa diperkenankan masuk. Soalnya pintunya terkunci pake *digital lock* dan hanya tim IT aja yang punya kode akses masuknya."



Gambar 4.7: Ruangan Analisis Jaringan TMC PMJ

4.2.3 Kebijakan Keamanan Terhadap Informasi TMC PMJ

Keamanan informasi dilakukan untuk menjaga kerahasiaan, ketersediaan serta integritas pada semua aset informasi pada TMC PMJ. Jika ditinjau secara manajemen dan fungsional, maka sistem informasi merupakan wujud penerapan teknologi informasi sesuai dengan tujuan berdirinya TMC PMJ dengan memadukan antara unsur manusia dan mesin yang mencakup aset perangkat keras, perangkat lunak, dan fungsi informasi itu sendiri (*input, process, output, storage and communication*).

Berdasarkan data yang dihimpun dari tim IT TMC PMJ maka perangkat keras dan lunak yang digunakan untuk mendukung sistem jaringan pada TMC PMJ adalah sebagai berikut:

Tabel 4.1: Daftar Perangkat Keras Jaringan TMC PMJ

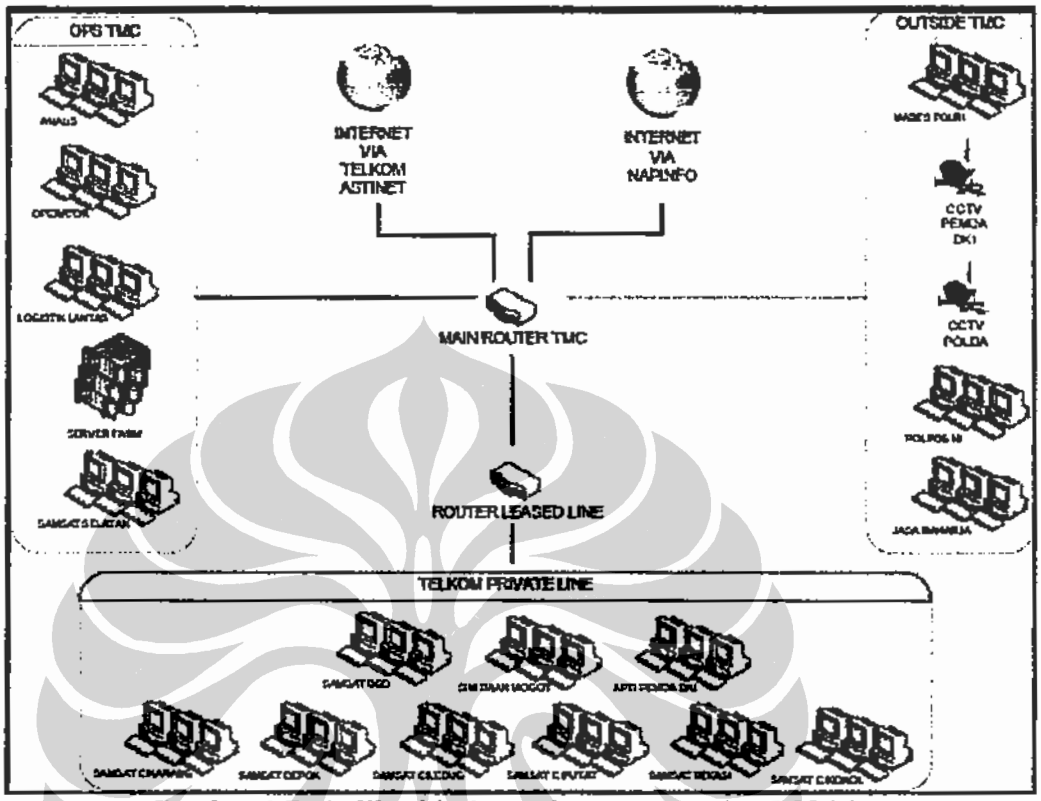
NO.	PERALATAN HARDWARE	MERK	KET
1.	Server:		
	a. Server GIS	Intel Xeon	
	b. Server SSB	IBM x 3650	
	c. Back up data SSB	IBM x 3650	

	d. Back up data TMC e. Server SSB KPTI f. Server SSB 01 g. Server website (internet) h. Server laka langgar i. Mail server j. Call center	Asus Dual Core (rakitan) Intel Xeon Gigabyte Core Two Duo IBM x 3650 Sun Xeon Asus Dual Core (rakitan) Asus Dual Core (rakitan)	
2.	Hub/switch: a. Switch Hub 1 24 port b. Switch Hub 2 16 port c. Switch Hub 3 24 port	 3 Com Allied Telesis D-link	
3.	UPS Server: a. UPS 1000 VA b. UPS 3000 VA	 APC APC	
4.	Komputer Operator (LCD + CPU): a. SMS 1717 b. STNK Online c. CCTV TMC d. CCTV Crisis Center e. GPS f. Internet g. Laka/langgar h. GIS i. Call Center + Speaker j. CCTV Room TMC k. Running Text l. SMS Gateway m. Pa siaga n. Staff TMC o. Ruang Teknisi	 Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV Lenovo Pentium IV	
10.	Virtual Projector (MGP 464)	Extron	
11.	Cross Point 3216	Extron	
12.	Printer Laser Black	Canon Laserjet	
13.	Wireless remote Projector	Cue Panasonic	
14.	Wireless Wifi (WLAN)	Corega	
15.	TV Plasma	Panasonic	
16.	Proyektor	Panasonic	

Tabel 4.2: Daftar perangkat lunak jaringan TMC PMJ

NO.	PERALATAN SOFTWARE	KET
1.	Oracle	System Database Server
2.	Linux Ubuntu	Operating system untuk server selain SSB
3.	Windows XP	Operating system untuk komputer operator TMC, teknisi dan tim IT.

Untuk mencapai tujuan yang diinginkan, TMC PMJ memanfaatkan jaringan komputer sebagai peralatan pendukung utama dalam melaksanakan tugasnya baik dalam bentuk jaringan aplikasi internet maupun intranet. Jaringan yang digunakan untuk mengintegrasikan antara server di TMC PMJ dengan internet menggunakan *collocation* dari Telkom Astinet. Sedangkan jaringan komputer yang digunakan secara internal pada TMC PMJ menggunakan saluran Napinfo dengan teknologi ADSL. Berikut ini adalah gambar aplikasi jaringan komputer pada TMC PMJ baik internet maupun intranet:



Gambar 4.7: Aplikasi jaringan komputer pada TMC PMJ

Pada gambar 4.1 terlihat bahwa semua peralatan yang ada pada TMC PMJ tersambung dengan jaringan internet dengan menggunakan jaringan internet Telkom Astinet maupun Napinfo melalui *main router* TMC PMJ.[1] *Main router* TMC PMJ ini terhubung dengan *router* BPKB yang secara *mirror* menghubungkan TMC PMJ dengan server samsat Cikarang, Depok, Ciledug, Ciputat, Bekasi, Cikokol, BSD, server satpas Daan Mogot dan server KPTI (Kantor Pengelola Teknologi Informasi) Pemprov DKI Jakarta. Server KPTI ini berisi tentang data identifikasi STNK yang dimiliki oleh Pemprov DKI Jakarta.[2]

---

[1] Router adalah suatu alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya melalui proses (routing) yang berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya.

[2] Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah *jaringan komputer. Server didukung dengan prosesor yang bersifat scalable dan RAM yang besar,* juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan atau network operating system. Dilihat dari fungsinya, server bisa di kategorikan dalam beberapa jenis, seperti: server aplikasi (application server), server data (data server) maupun server proxy (proxy server).

Selanjutnya *main router* TMC PMJ juga tersambung ke dua server CCTV untuk operasional sehari-hari, yaitu server CCTV DKI dan CCTV Pancoran dengan. Server ini berfungsi untuk melakukan penyimpanan atas data yang dihasilkan oleh penggunaan operasional CCTV dipasang menyebar di jalan-jalan utama di Jakarta.

Main router TMC PMJ juga tersambung ke server-server lokal yang terletak di TMC PMJ. Server-server lokal tersebut adalah:

a. *Server* GIS .
b. *Server* manajemen nopol-SSB.
c. *Server* back up data SSB.
d. Server SSB KPTI.
e. *Server* SSB 01.
f. *Server* website lantas.
g. Server laka dan langgar.
h. *Mail server.*
i. VPN *server.*
j. Tiga buah *storage server* pada *call center*, yaitu:
   - Storage A.
   - Storage B.
   - Storage C.

Untuk *server* GIS, GPS, laka dan langgar digunakan untuk melakukan pencatatan data terhadap aplikasi GIS, GPS, kecelakaan yang terjadi di Jakarta dan pelanggaran yang dilakukan oleh para pengguna kendaraan bermotor di jalan raya. Aplikasi ini hanya digunakan secara internal di TMC PMJ saja mengingat dalam aplikasi ini berisi tentang pelaksanaan operasional kepolisian yang dilakukan oleh Ditlantas Polda Metro Jaya. Hal ini disampaikan oleh Bayu dalam wawancara sebagai berikut:

> "Kita juga punya server laka untuk mencatat data kecelakaan yang terjadi, ada juga untuk server langgar buat catat data pelanggaran... Untuk GIS ini khusus untuk internal kita aja. Jadi disini ada informasi tentang pos polisi, data petugas lantas, kemacetan, kecelakaan. Untuk menyampaikan

informasi di dalam GIS ini kepada anggota di lapangan melalui HT maupun telepon."

Server SSB KPTI berfungsi untuk melakukan koneksi ke seluruh samsat di wilayah Jakarta Raya. Server ini mempunyai akses informasi yang berbeda dengan server SSB utama di luar TMC PMJ. Server ini digunakan sebagai akses layanan database SSB untuk *user* umum yang ingin mencari informasi seputar SSB secara online sehingga aplikasi layanannya hanya memunculkan tampilan informasi umum dari identifikasi kendaraan bermotor yang terdaftar di samsat. Hal ini disampaikan oleh Alfon dalam wawancara sebagai berikut:

"...ada server SSB KPTI yang juga digunakan untuk koneksi ke samsat-samsat juga, jadi database yang cuma boleh diakses oleh dunia luar (database STNK). Akses ini sebenarnya sama dengan akses yang dilakukan oleh internal TMC, bedanya ngga semua info yang ada di situ. Misalnya nama ngga keluar, alamat ngga keluar, no mesin dan rangka ngga keluar. Yang keluar cuma warna kendaraan, jenis kendaraan, pokoknya identifkasi yang kita keluarkan itu cuma yang bersifat umum aja pak."

Mail server berfungsi sebagai layanan akses email yang menggunakan alamat email TMC@lantasmetro.polri.go.id yang dibuat oleh tim IT sebagai admin TMC PMJ. Dengan layanan mail server maka semua arus email keluar dan masuk yang menggunakan alamat TMC PMJ akan tersimpan di dalam server ini. Hal ini disampaikan oleh Bayu dalam wawancara sebagai berikut:

"Kita juga punya mail server. Ini maksudnya kita kan punya alamat email: TMC@lantasmetro.polri.go.id nah itu masuknya ke mail server ini. Jadi masuknya semua email melalui server ini."

Sebagai back up atas semua data yang ada pada TMC PMJ diletakkan pada ruang penyimpanan tetap berupa back up server. Tim IT mengklasifikasikan semua data yang ada menjadi dua kelompok besar, yaitu data yang berkaitan dengan SSB dan data lalu lintas lainnya. Untuk data yang berkaitan dengan SSB disimpan pada empat server yang berbeda, yaitu *Server* manajemen nopol-SSB,

server back up data SSB, *Server* SSB KPTI dan *Server* SSB 01. Berkaitan dengan hal ini maka Bayu memberikan keterangan dalam wawancara sebagai berikut:

> "...Khusus untuk data SSB kita punya server back up untuk SSB, soalnya menurut saya datanya sedemikian penting. Kita mentreatment data ssb lebih dibandingkan lainnya, kita punya empat server untuk memback up SSB yaitu database utamanya itu, trus ada back up nya sendiri, trus ada database yang bisa diakses oleh orang luar itu trus ama *application* servernya. Kita taruh semua di ruangan server TMC."

Kemudian untuk data selain SSB, oleh tim IT disimpan pada tiga buah *storage* server pada server lokal TMC PMJ. *Storage* ini khusus digunakan untuk menyimpan data-data TMC PMJ selain data SSB yang tersimpan pada server back up SSB. Proses kerja storage server ini dijelaskan oleh Yudho dalam wawancara sebagai berikut:

> "...untuk *storage* kita punya tiga pak, ada di 100.7 di 100.20 dan di 100.200. *storage* ini fungsinya untuk nyimpen file aja. Jadi misalnya ada kegiatan lantas trus kita foto-foto, nah foto-foto ini disimpan disini pak. *Storage* ini khusus untuk nyimpen file selain SSB pak, jadi kalo kita mo install apa gitu masuknya di *storage* pak. Makanya *storage* ini yang kita gedein cuma *space* nya doang jadi spesifikasi servernya biasa aja cuma kapasitasnya yang besar."

Berkaitan dengan kondisi arus listrik yang sering padam maka tim IT mengantisipasi hal tersebut dengan menggunakan beberapa UPS dan memasang generator sebagai daya listrik cadangan. UPS tersebut dipasang pada server yang ada di TMC sehingga apabila listrik tiba-tiba padam maka server akan tetap menyala. Tindakan ini dilakukan untuk mengantisipasi terjadinya kerusakan maupun kehilangan data pada server akibat padamnya listrik secara tiba-tiba. Hal ini disampaikan oleh Yudho dalam wawancara sebagai berikut:

> "...disini kami punya dua UPS yang totalnya 4000 VA. Saya pasang di tempat server kita pak. Jadi kalo pas tiba-tiba mati lampu, server nya ngga rusak. Sambil berjalan kita nyalakan generator untuk nyalain lampu

semuanya. Kalo di komputer masing-masing operator kami ngga pasang UPS pak."

Untuk menciptakan sistem keamanan atas keseluruhan penggunaan aplikasi jaringan online antara *public user* dengan operator TMC PMJ maka tim IT TMC PMJ menggunakan aplikasi VPN server sebagai *security layer*. VPN (*Virtual Private Network*) merupakan model jaringan pribadi yang menggunakan media internet untuk menghubungkan antar *remote-site* secara aman. Agar dapat mengakses informasi yang berada di dalam TMC PMJ dengan melalui *VPN server* ini dibutuhkan *user id* dan *password* sehingga dengan menggunakan *VPN server* maka informasi penting yang berada di dalam TMC PMJ tidak dapat diakses oleh masyarakat umum untuk menjamin kerahasiaan, keutuhan dan ketersediaan atas informasi yang ada. Cara kerja VPN server ini dijelaskan oleh Bayu dalam wawancara sebagai berikut:

"Disini kita pake VPN. Karena kita ke samsat DKI itu ngga ada jalur khusus maka samsat DKI connect melalui VPN server di 100.68 jadi kita dial lewat internet masuk melalui modem astinet lalu masuk ke TMC *main router* terus diarahkan ke VPN server baru kita bisa mengakses di dalam sini semua. Jadi kalo saya mo nge-*remote* ke TMC lewat luar itu harus melalui VPN server. Jadi dari rumah kalo saya mo ngeliat TMC juga bisa lewat VPN dulu. Sebagai pengamanannya kita kasih *user password*, jadi ini untuk orang internal TMC yang berada di luar mo ngecek sini melalui VPN Server."

Peranan penting VPN server ini berkaitan dengan keamanan akses jaringan TMC PMJ juga disampaikan oleh Okho dalam wawancara sebagai berikut:

"...kalo kita mo akses TMC dari luar melalui address www.lantasmetro.polri.go.id, itu nanti oleh main router kita akan di routing ke web server lantas kita. Jadi dari internet dia masuk melalui astinet ini trus setelah itu nanti di*direct* ke web werver lantas. Cuma ini kan cuma baca doang, jadi mereka hanya bisa mengakses http-nya aja. Kalo melalui VPN kita bisa full akses, tapi ini harus pake *user-id* dan

password. Jadi VPN ini cuma untuk internal TMC aja pak, orang lain ga bisa masuk."

Disamping menerapkan kendali akses terhadap jaringan komputer, tim IT juga memberlakukan hal yang sama kepada para petugas operator TMC PMJ dalam mengoperasionalkan aplikasi layanannya masing-masing. Agar dapat membuka aplikasi layanan yang ada, para petugas operator harus memiliki *user id* dan *password* yang harus dimasukkan pada saat aplikasi tersebut akan dijalankan. Penerapan *login* ini bersifat rahasia dan hanya operator itu sendiri saja yang mengetahuinya.[3] Berkaitan dengan hal ini maka Okho menjelaskan pelaksanaan penggunaan *user id* dan *password* dalam wawancara sebagai berikut:

"... pertamanya, *user id* dan *password* itu kita yang tentukan pak. Kita gunakan NRP mereka sebagai *user-id* dan *password* awal lalu kita kasihkan ke operator. Kemudian *user-id* dan *password* ini di *update* lagi oleh mereka, jadi kita pun ngga tau apa *password* yang mereka pake sekarang pak. Untuk *user-id*, mereka bisa merubah tapi harus seijin kita dulu baru setelah itu kita masukkan ke dalam sistem biar mereka bisa mengakses aplikasi yang ada.."

Dalam menjalankan aplikasi pada TMC PMJ, masing-masing operator aplikasi hanya bisa membuka aplikasi yang telah ditentukan saja. Artinya, mereka tidak bisa membuka aplikasi lain yang bukan merupakan tanggung jawabnya. Pengendalian akses ini dibuat oleh tim IT untuk menerapkan batas lapis keamanan terhadap informasi yang ada dengan berdasarkan tingkatan kewenangan dan tanggung jawab seseorang yang akan mengakses informasi tersebut. Semakin tinggi kewenangan dan tanggung jawab petugas operasional maka semakin luas cakupan akses informasi yang bisa didapatkan, demikian sebaliknya. Proses

[3] *Login* adalah proses untuk mengakses komputer dengan memasukkan identitas dari akun pengguna dan kata sandi guna mendapatkan hak akses menggunakan sumber daya komputer tujuan. *Login* ini biasanya terdiri dari dua kriteria, yaitu rekening pengguna (*user-id*) yang digunakan sebagai identitas berupa runtutan karakter yang dimiliki oleh pengguna dan kata sandi (*password*) yang merupakan runtutan karakter berupa kunci yag dijaga kerahasiaannya terhadap orang lain. Kedua pasang runtutan karakter ini harus tepat dan tidak dapat dipisahkan.

keamanan informasi bertingkat ini dijelaskan oleh Bayu dalam hasil wawancaranya sebagai berikut:

> "...Ini semua *based* dari NRP mereka. Kita sebagai admin udah program NRP mereka sebagai *user-id* nya, *user-id* ini kita atur untuk *layer-layer* nya.Untuk petugas operator TMC PMJ kalo mo ngisi data ada *login* nya, masing-masing aplikasi layanan kalo mo bikin data harus ada *login* nya. Jadi memang kita buat *layer-layer login* secara bertingkat biar mereka ngga bisa sembarangan *login* ke aplikasi satu ke aplikasi yang lain. Misalnya untuk Dirlantas bisa buka aplikasi SSB semuanya, tapi untuk Kasubsi samsat cuma area dia yang punya kewenangan aja yang bisa dibuka, lainnya ga bisa. Misalnya Kasubsi Samsat Cikokol cuma bisa buka SSB Cikokol doang. Dia ngga bisa buka SSB di BSD. Kemudian kalo operator SSB cikokol ya cuma bisa liat dan entry data di Cikokol doang, ngga bisa yang lainnya."

Tim IT juga melakukan upaya pengamanan terhadap server-server lain yang terhubung pada jaringan TMC PMJ. Pengendalian akses keamanan informasi secara bertingkat terhadap jaringan ini dilakukan dengan menerapkan pengamanan *firewall*. *Firewall* merupakan sistem yang berfungsi untuk memberikan ijin atau tidak terhadap lalu lintas jaringan yang dianggap aman dalam rangka akses data di dalamnya. Dengan menggunakan firewall maka tim IT bisa memilah server mana yang diijinkan untuk mengakses data dan server mana yang tidak diijinkan untuk melakukan akses data. Upaya ini dijelaskan oleh Alfon dalam wawancara sebagai berikut:

> "Tentang *firewall*, dari ruang analis kita bisa *connect* ke semuanya. Tapi kalo dari samsat yang lain, mereka cuma bisa *connect* ke webserver SSB doang. Untuk server yang lainnya mereka ngga bisa. Kalo masyarakat hanya bisa akses webserver lantas doang. Utk KPPI cuma bisa ke SSB KPPI doang, mentok, tapi kita bisa akses data secara *full* ke KPPI soalnya kita dikasih *account user-id* dan *password* untuk bisa *login* ke mereka."

Untuk mengetahui siapa saja yang melakukan akses keluar dan masuk informasi baik secara internal (petugas operator TMC PMJ) maupun eksternal (masyarakat umum) dilakukan oleh tim IT dengan membuat aplikasi *log* yang dipasang pada semua server yang ada. Aplikasi *log* sebagai sistem deteksi gangguan ini mempunyai peranan penting untuk membaca siapa yang merusak atau mengganggu sistem jaringan komputer TMC PMJ. Okho menjelaskan hal ini dalam wawancara sebagai berikut:

> "...kalo misalnya kita *login* melalui akses manapun ke TMC maka akan masuk ke aplikasi *log* pak. Kita me-*log* semua arus informasi baik keluar ataupun masuk, semuanya di-*log* jadi kita tau siapa-siapa yang mengakses. Untuk operator TMC PMJ kita set di *log* akan keluar *user name*-nya apa, dia ngapain aja di aplikasi ini. Misalnya dia ngedit berita di aplikasi GIS maka yang keluar di *log* itu siapa *user name*-nya, kapan dia ngisi berita, ama aktifitas apa yang dia lakukan."

Menambahkan keterangan di atas, maka Bayu menjelaskan dalam wawancara sebagai berikut:

> "...untuk aplikasi log yang kita miliki untuk web site kita cuma bisa melihat *IP address user* ama waktu akses aja. Ini fungsinya untuk menghitung berapa user yang mengakses web site kita aja, biar kita tau berapa jumlah yang mengakses kita. Tapi untuk operator TMC kita set di *log* akan keluar user name nya apa, dia ngapain aja di aplikasi ini..."

4.3. Gangguan yang Masih Terjadi

Meskipun telah melaksanakan tindakan manajemen keamanan terhadap informasi yang ada pada TMC PMJ, namun masih ditemukan beberapa gangguan yang terjadi sehingga mengganggu pelaksanaan operasional TMC PMJ. Gangguan yang terjadi tersebut meliputi gangguan pada aspek keamanan personel serta pada aspek informasi itu sendiri.

Pada awal mula pelaksanaan operasioanalisasi TMC PMJ sering menemui kendala berkaitan dengan kekurangmampuan operator dalam menguasai aplikasi komputer yang telah dibangun oleh tim IT TMC PMJ. Kendala ini terjadi

mengingat petugas operasional belum dibekali dengan pendidikan dan pelatihan yang berkaitan dengan operasionalisasi aplikasi yang ada pada TMC PMJ. Tidak jarang mereka seringkali diberikan pelajaran singkat dan sederhana baik oleh teknisi maupun tim IT sehingga mampu mengoperasionalkan peralatan yang ada. Hal ini disampaikan oleh Alfons dalam wawancara sebagai berikut:

> "Dulu di operator TMC kan polisinya jarang pegang komputer to pak. Yang bisa pegang komputer itu Cuma bisa dihitung dengan jari. jadi ya udah sekalian aja sy ajarin caranya pake komputer. Nahh dulu kan lagi heboh tentang online kan pak. Biar mereka terbiasa ngetik, cara pertama saya ya kalo malem gitu saya suruh mereka *chatting*. Akhirnya dari situ mereka mulai tertarik ngetik, trus ada juga sebagian yang ngga familier dengan mouse. Caranya kami suruh mereka mainan games. Gitu pak, pelan-pelan akhinya mereka terrbiasa dan bisa ngoperasionalkan komputer."

Hal senada juga disampaikan oleh Hendrik dalam wawancara sebagai berikut:

> "... wahh dulu pertama kali mereka masuk ya agak kerepotan kita pak. Soalnya mereka itu kebanyakan dari lapangan, trus disuruh pegang komputer yaaa akhirnya saya ikut ngajari mereka pegang operator masing-masing. Kalo yang masih muda mungkin ga masalah pak, tapi kalo orang yang udah agak tua ini agak repot. Tapi sekarang mereka udah bisa pegang pak, *at least* untuk masing-masing peralatan operatornya ya mereka bisa lah pak."

Demikian halnya dengan apa yang disampaikan oleh Sugeng dalam wawancara berikut ini:

> "... saya terus terang waktu masuk kesini rasanya susah sekali untuk bisa jalankan peralatannya pak. Sama pak, anak buah saya juga begitu. Tapi waktu itu kita dikasih tau caranya oleh teknisi dan sekali-sekali oleh tim IT, khususnya untuk aplikasi masing-masing operator yang telah ditunjuk..."

Selain terjadi gangguan pada aspek personel, gangguan juga terjadi pada aspek keamanan informasi meskipun upaya pengamanan terhadap informasi telah dilakukan oleh tim IT TMC PMJ. Pada tahun 2008 *website* TMC PMJ pernah di-*hack* oleh hacker Akibatnya, seluruh tampilan website TMC PMJ yang muncul pada layar monitor pada saat diakses melalui internet berubah. Terjadinya gangguan ini diduga sebagai akibat dari kelemahan *login* yang dilakukan oleh petugas operator. Hal ini dijelaskan oleh Rahmat dalam wawancara sebagai berikut:

> "Iya dulu pada tahun 2008 website kita pernah di *hack*[4] dari luar pak. Sepertinya sih mereka melakukan *SQL injection* terhadap database kita. Tapi saya ngga yakin itu pak soalnya saya cek di *log, SQL injection*[5] nya ngga bisa masuk. Jadi kemungkinan orang itu masuk lewat aksen internal, dia pake user-id nya operator trus dia nebak-nebak password nya apa. Nahh kebetulan tebakannya tepat pak, akhirnya dia bisa jebol website kita."

Atas kejadian gangguan tersebut maka tim IT melakukan perbaikan terhadap manajemen database yang telah dibuat untuk mengantisipasi terjadinya hal yang sama. Kemudian sebagai upaya mencegah terjadinya kasus serupa maka mereka memasang VPN server untuk memastikan keamanan informasi berkaitan dengan pengendalian akses yang dilakukan oleh operator TMC PMJ dengan masyarakat umum secara berlapis. Selain memasang VPN server, mereka juga melakukan perbaikan aplikasi dengan cara *prepare query* agar aplikasi yang diterapkan pada TMC PMJ hanya memiliki celah seminimal mungkin sehingga sulit untuk diterobos oleh *hacker*. Hal ini disampaikan oleh Bayu dalam wawancara sebagai berikut:

---

[4] *Hack* adalah upaya menerobos keamanan sistem komputer tanpa ijin. Umumnya dilakukan dengan maksud untuk mengakses komputer-komputer yang terkoneksi ke jaringan tersebut.

[5] SQL (*Structured Query Language*) adalah bahasa pemrograman yang digunakan untuk mengakses dan melakukan manajemen data. Saat ini hamper semua server basis data yang ada mendukung bahasa ini untuk melakukan manajemen datanya. *SQL injection* adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Suatu database yang berhasil dimasuki *hacker* dengan menggunakan SQL injection ini biasanya akan mengalami perubahan manajemen data.

"...kejadian rubah *website* yang lalu itu jadi pembelajaran untuk kita bahwa untuk akses internal yang lebih aman menggunakan VPN menggunakan *user password.* Apabila ada *user* asing yang menginginkan untuk *hack* kita, kita udah punya langkah antisipatif untuk ini pak. Apabila mereka menggunakan *SQL Injection* maka kita antisipasi dengan menggunakan metode *prepare query*."

Jenis ancaman *malicious ware* secara internal juga sering terjadi dalam operasional jaringan pada TMC PMJ. Jenis ini lebih sering terjadi dibandingkan dengan ancaman yang berasal dari luar, seperti *hack* dengan cara *SQL injection* di atas. Sebagai langkah antisipatif terjadinya gangguan *malware* maka tim IT melakukan langkah langkah sebagai berikut: (a). Memasang aplikasi antivirus jenis *freeware* yang di-*download* dari internet secara gratis dan melakukan *update* untuk menghadapi malware yang senantiasa berkembang; (b). melakukan back up data di storage back up sesering mungkin untuk menghindari rusak atau hilangnya data yang ada; (c). memberlakukan pembagian segmen-segmen terhadap seluruh akses jaringan yang ada. Hal ini diungkapkan oleh Bayu dalam wawancara sebagai berikut:

"...Sebenernya ancaman yang paling sering terjadi itu sebetulnya bukan ada pada sistem pengamanan kaya kasus *hack* itu atau firewall nya pak, tapi lebih cenderung ke sosialnya (orang). Contohnya orang ini pake flash disk sembarangan trus satu jaringan kena virus dan jaringannya lambat semua. Ini sering pak. Yah rata2 dalam 3 bulan sekali pasti ada aja virus. Biasanya virus jaringan yang kena, namanya virus salipi. Ini bikin lambat jaringan banget. Trus recovery nya ya di install ulang. Untungnya kita udah bagi-bagi segmen, jadi kalo misalnya TMC kena virus maka yang kena ya cuma segment TMC doang (IP 97). Ini cara kita batasinya. Untuk langkah antisipasinya, kita harus biasain sering-sering back up di storage back up itu."

BAB V
PEMBAHASAN

Seperti yang telah disampaikan sebelumnya bahwa informasi adalah aset penting dari suatu organisasi yang menjadi salah satu sumberdaya utama dari organisasi tersebut. Dalam operasional TMC PMJ, kecepatan dan keakuratan suatu informasi memegang peranan penting terhadap dukungan keberhasilan pelaksanaan tugas Polantas di lapangan dan tingkat kepercayaan masyarakat dalam melakukan akses informasi tersebut untuk mengambil suatu keputusan. Untuk itu informasi tersebut harus selalu dilindungi secara efektif dan efisien dengan menggunakan upaya manajemen yang tepat sehingga ketiga aspek utama tujuan keamanan informasi (meliputi kerahasiaan, keutuhan dan ketersediaan informasi) dapat tercapai dengan memperhatikan ciri karakteristik pada TMC PMJ.

5.1. Penerapan Manajemen Keamanan Informasi pada TMC PMJ Saat Ini

Dalam menyelenggarakan segala operasional TMC PMJ, Ditlantas Polda Metro Jaya telah melakukan upaya kebijakan keamanan informasi terhadapnya. Penerapan kebijakan keamanan informasi tersebut dilakukan berdasarkan karakteristik TMC PMJ yang mencakup aspek bentuk pengembangan organisasi serta aplikasi layanan informasi yang diterapkan pada operasional TMC PMJ.

5.1.1. Karakteristik TMC PMJ

Masing-masing organisasi mempunyai keunikan karakteristik tersendiri sebagai akibat adanya bentuk dan tujuan organisasi tersebut berdiri. Berdasarkan asumsi tersebut maka penulis mengklasifikasikan keunikan karakteristik TMC PMJ menjadi dua hal utama, yaitu: *pertama*, berdasarkan bentuk organisasi dan *kedua*, aplikasi informasi yang diterapkan berdasarkan fungsi layanan yang ada untuk mencapai tujuan yang diharapkan.

5.1.1.1. Bentuk Organisasi TMC PMJ

Dari hasil penelitian yang telah disampaikan sebelumnya diketahui bahwa TMC PMJ merupakan implementasi atas penyelenggaraan UU No. 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan sebagai pusat kendali sistem infomasi lalu lintas dan angkutan jalan di Jakarta Raya yang berada di bawah Direktorat Lalu Lintas Polda Metro Jaya. Ini merupakan perluasan fungsi dan peranan Polri di bidang lalu lintas sebagai penyelenggara Komando, Komunikasi, Koordinasi dan Informasi (K3I) yang dilakukan oleh Ditlantas Polda Metro Jaya.

Sebagai perluasan dari fungsi dan peranan Polri di bidang lalu lintas dari fungsi dan peranan yang telah ada maka TMC PMJ merupakan jawaban atas tuntutan untuk mengikuti perubahan yang terjadi pada berbagai pihak yang berkepentingan dalam bidang lalu lintas yang setiap saat selalu berkembang. Tuntutan yang dilakukan oleh pada *stakeholder* tersebut pada gilirannya mengharuskan Direktorat Lalu Lintas Polda Merto Jaya untuk selalu terlibat dalam perubahan.

TMC PMJ merupakan model pengembangan organisasi yang dilakukan oleh Ditlantas Polda Metro Jaya dalam beradaptasi terhadap kondisi dan tuntutan lingkungan yang senantiasa berubah agar dapat meningkatkan efektifitas pelaksanaan tugas petugas Polantas untuk melaksanakan tugas pokoknya. Pembentukan pengembangan organisasi TMC PMJ diawali dengan adanya proses konsultasi yang dilakukan oleh Dirlantas waktu itu kepada Rahmat sebagai koordinator tim IT TMC PMJ untuk membangun pusat manajemen lalu lintas di Jakarta secara *integrated, computerized* dan *online*. Proses konsultasi ini berfungsi untuk menjembatani pemahaman konsultan akan permasalahan yang terjadi sehingga Rahmat bisa memberikan intervensi dalam bentuk aplikasi layanan yang ditanamkan pada operasional TMC PMJ sehingga dapat mendukung pelaksanaan tugas pokok Polantas.

Menyadari bahwa agar organisasi bersikap adaptif dan proaktif dalam menghadapi masa depannya maka tidak sedikit organisasi yang mengambil berbagai tindakan yang mengarah pada perubahan kemampuan sendiri secara internal guna mewujudkan perubahan. Siagian memandang hal ini sebagai upaya yang dilakukan untuk mewujudkan pengembangan organisasi. Pada

pengembangan organisasi TMC PMJ, tim IT TMC PMJ menjadi konsultan operasional layanan aplikasi yang berperan sebagai agen perubahan sehingga status konsultan dipandang sebagai seseorang yang menekuni profesi terhormat dengan cara menempatkannya langsung di bawah dan bertanggung jawab kepada Direktur Lalu Lintas Polda Metro Jaya.

Agar TMC PMJ dapat berjalan dengan efektif dan efisien, maka indikator pertama yang harus dimiliki adalah unsur manajemen dengan memanfaatkan segala sumber daya yang ada sebagai strategi terencana untuk mewujudkan perubahan organisasional. Hingga sekarang TMC PMJ belum mempunyai struktur organisasi yang jelas. Tidak adanya struktur organisasi ini berakibat pada ketidakjelasan tugas dan tanggung jawab yang diemban oleh para petugas operasional TMC PMJ dalam melaksanakan tugasnya.

Selain itu, karena belum ada struktur organisasi yang baku maka TMC PMJ belum bisa menggunakan anggaran dukungan operasional dari dinas. Sebagai salah satu sumber daya fisik pada suatu organisasi, unsur pendanaan merupakan hal yang penting untuk melakukan kegiatan operasionalnya. Tanpa dukungan anggaran dinas maka menyulitkan TMC PMJ untuk melakukan perawatan dan perbaikan terhadap aset-aset yang ada.

Indikator selanjutnya agar TMC PMJ dapat berjalan dengan efektif dan efisien adalah kolaborasi antara seluruh *stakeholder* dalam menentukan keberhasilan tujuan operasional TMC PMJ. Disini peranan pemolisian masyarakat yang dikolaborasikan dengan petugas operator serta dukungan dari satuan/sub direktorat/renmin di bawah struktur Ditlantas menjadi sangat signifikan dan penting dalam mewujudkan tujuan yang telah digariskan sebelumnya oleh Direktur Lalu Lintas.

Berdasarkan hasil penelitian yang dilakukan oleh Thibault, Linch & McBride (2001) menunjukkan bahwa 80% dari upaya kepolisian yang dilakukan oleh polisi dilakukan berdasarkan hasil pengaduan atau laporan masyarakat. Hasil penelitian ini menunjukkan bahwa hasil pengaduan dan laporan masyarakat memegang peranan penting dalam terciptanya keamanan dan ketertiban di lingkungan masyarakat. Apabila merujuk dari penghargaan Museum Rekor Indonesia kepada TMC PMJ beberapa waktu yang lalu, maka dapat dikatakan

bahwa strategi pemolisian masyarakat melalui TMC PMJ berhasil dilakukan oleh Direktorat Lalu Lintas melalui TMC PMJ.

Dukungan yang diberikan oleh masyarakat Jakarta Raya dalam memberikan informasi seputar situasi lalu lintas di wilayah Jakarta Raya kepada TMC PMJ ini tidak terlepas dari adanya perasaan homogen yang menjadi landasan penerapan pemolisian masyarakat. Rasa kebersamaan dari para pengguna jalan yang sehari-hari menghadapi kemacetan dan gangguan di sepanjang jalan Jakarta mengakibatkan mereka memiliki harapan dan keinginan untuk merasakan suasana lancar, aman dan tertib di jalan. Kebersamaan ini menggugah para pengguna jalan untuk memberikan informasi di sekitar lingkungannya apabila terjadi kemacetan atau gangguan di bidang lalu lintas lainnya kepada TMC PMJ agar informasi tersebut dapat ditransmisikan kepada seluruh pengguna jalan lainnya untuk mengantisipasi terjadinya gangguan tersebut.

Indikator keefektifan dan efisiensi dari TMC PMJ yang selanjutnya adalah melakukan terobosan baru sebagai program pengembangan organisasi yang diperlukan guna meningkatkan kinerja seluruh personel TMC PMJ dan semua satuan kerja dalam TMC PMJ dalam bentuk aplikasi layanan yang diterapkan pada TMC PMJ.

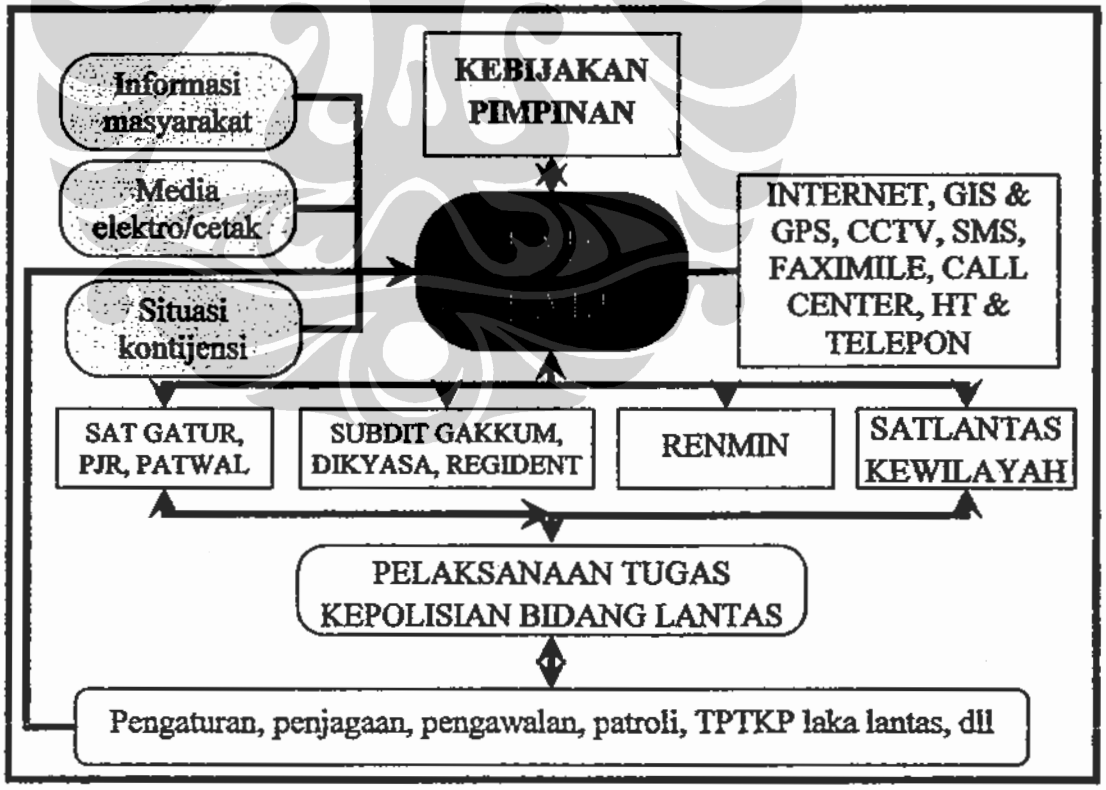
5.1.1.2. Aplikasi Layanan Informasi yang Diterapkan pada TMC PMJ

Aplikasi layanan yang diterapkan pada TMC PMJ merupakan salah satu karakteristik yang membedakan organisasi TMC PMJ dengan organisasi lainnya. Selain itu, aplikasi layanan juga merupakan terobosan baru dari Ditlantas Polda Metro Jaya sebagai salah satu indikasi efektifitas dan efisiensi dalam rangka program pengembangan organisasi TMC PMJ.

TMC PMJ merupakan pusat manajemen lalu lintas di Polda Metro Jaya yang berfungsi sebagai pusat Komando, Komunikasi, Koordinasi serta Informasi (K3I) dalam bidang lalu lintas. Berkaitan dengan fungsi tersebut maka penerapan semua aplikasi layanan informasi yang berada pada TMC PMJ dilandasi pada keempat nilai fungsi tersebut dalam rangka menciptakan delapan tujuan utama TMC PMJ.

A. Aplikasi Layanan Informasi pada Fungsi Komando

Sebagai pusat komando, TMC PMJ mempunyai tugas memberikan komando dan menyalurkan perintah pimpinan direktorat kepada beberapa satuan direktorat, sub direktorat dan renmin direktorat serta semua satuan lalu lintas kewilayahan untuk melaksanakan tugas-tugas kepolisian sesuai dengan bidang tugasnya masing-masing yang kemudian dijabarkan ke dalam bentuk pelaksanaan tugas kepada seluruh petugas polantas yang ada di lapangan. Komando dan perintah pimpinan direktorat tersebut dilandasi pada permasalahan lalu lintas yang terjadi sebagai hasil informasi yang didapatkan dari masyarakat, media cetak maupun elektronik, kebijakan pimpinan serta situasi kontijensi yang mengharuskan pimpinan direktorat mengambil tindakan kepolisian untuk menciptakan keamanan, keselamatan, ketertiban dan kelancaran lalu lintas diilayah Jakarta Raya.



Gambar 5.1: Skema arus informasi dalam fungsi komando pada TMC PMJ

Pada gambar 5.1. di atas tampak layanan aplikasi internet, GIS dan GPS, CCTV, SMS, faximile, call center, HT maupun telepon memegang peranan

penting dalam dukungan pelaksanaan operasional TMC PMJ pada fungsi komando. Ketujuh layanan aplikasi ini saling bersinergi untuk memberkan dukungan kepada TMC PMJ dalam menerima dan menyampaikan informasi kemudian ditransmisikan ke masing-masing satuan, sub direktorat, renmin dan satuan lalu lintas kewilayahan sehingga dapat menentukan pelaksanaan tugas kepolisian di bidang lalu lintas dalam bentuk pelaksanaan tugas lalu lintas yang dilakukan oleh petugas di lapangan.

Untuk memudahkan pemahaman mengenai proses transmisi arus informasi pada fungsi komando dan pengendalian ini maka penulis memberikan analogi contoh kasus sebagai berikut: Berita di koran dan televisi menyebutkan bahwa besok akan ada aksi unjuk rasa di Bundaran HI, kemudian dalam waktu yang bersamaan rombongan VVIP akan melintasi jalur jalan di Bundaran HI. Keesokan harinya ternyata aksi unjuk rasa tersebut mengalami peningkatan intensitas menjadi cenderung anarkis. TMC PMJ mendapatkan informasi unjuk rasa yang cenderung anarkis tersebut dari masyarakat melalui layanan internet yang kemudian dilakukan pengecekan oleh operator TMC PMJ kepada petugas di lapangan dengan menggunakan HT atau telepon kepada petugas lalu lintas yang ter*plotting* di lapangan sekitaran Bundaran HI dengan melihat GIS pada layar monitor.

Apabila informasi tersebut dinyatakan benar dan akurat oleh petugas di lapangan maka TMC PMJ memberikan informasi tersebut kepada Direktur Lalu Lintas. Kemudian berdasarkan pertimbangan penilaian yang dilakukan oleh Direktur Lalu Lintas kemudian memberikan komando melalui TMC PMJ kepada Kasat Gatur, Kasat Patwal dan Kasat Lantas Jakarta Pusat untuk melakukan tindakan kepolisian lalu lintas untuk mengamankan rombongan pengawalan VVIP tersebut. Melalui GPS dan CCTV yang terpasang di Bundaran HI maka operator TMC PMJ dapat memantau dan mengarahkan keberadaan mobil patrol yang sudah diberikan komando melakukan tindakan kepolisian untuk mengamankan jalur yang akan dilalui oleh rombongan pengawalan sehingga rombongan VVIP dapat melanjutkan perjalanannya dengan aman, selamat, tertib, dan lancar.

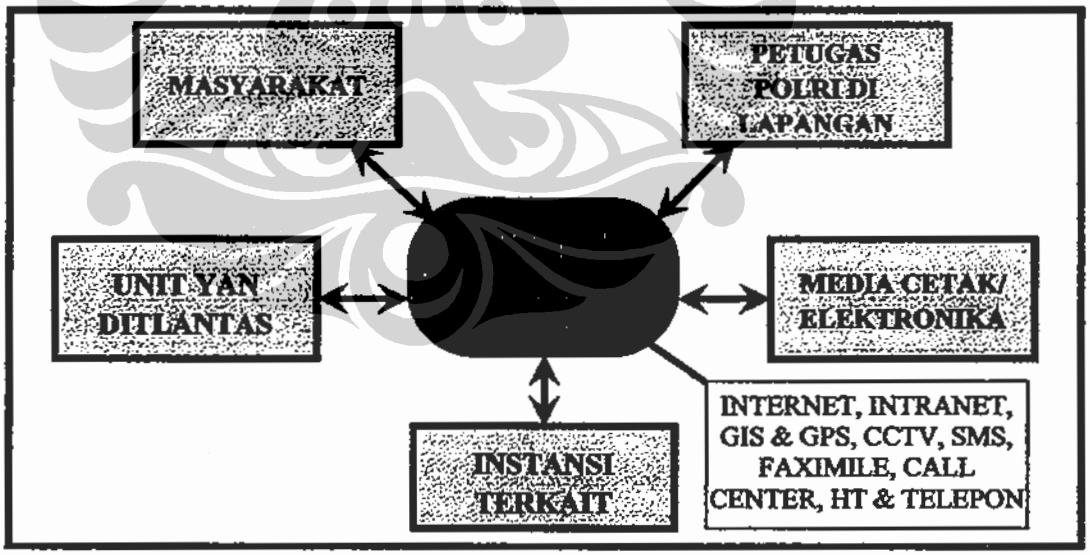
Kemudian setelah melakukan pengamanan tersebut, maka para petugas di lapangan melakukan pelaporan secara berjenjang sebagai wujud pengendalian.

Hasil pelaporan yang telah dilakukan akan dianalisis untuk upaya pelaksanaan tugas selanjutnya serta sebagai bahan masukan bagi pimpinan.

B. Aplikasi Layanan Informasi pada Fungsi Komunikasi

Fungsi kedua pada TMC PMJ adalah pusat komunikasi. Komunikasi memiliki makna bahwa TMC PMJ merupakan wadah bagi petugas kepolisian, masyarakat umum maupun para *stake holder* untuk menyampaikan maupun mencari informasi yang berkaitan dengan informasi internal kepolisian maupun informasi kamtibmas di wilayah Jakarta Raya.

Ada lima jalur komunikasi yang dilakukan oleh TMC PMJ kepada para *stakeholder*, yaitu: *pertama,* TMC PMJ kepada masyarakat dan sebaliknya; *kedua,* TMC PMJ kepada Petugas Polri di lapangan dan sebaliknya; *ketiga,* TMC PMJ kepada media elektronik/cetak dan sebaliknya; *keempat,* TMC PMJ ke instansi terkait dan sebaliknya; serta *kelima,* TMC PMJ ke unit-unit pelayanan Ditlantas (SIM, STNK dan BPKB) dan sebaliknya.



Gambar 5.2: Skema Arus Informasi dalam Fungsi Komunikasi

Pada gambar 5.2. menunjukkan informasi yang berada pada TMC PMJ dikomunikasikan secara dua arah. Dalam fungsi ini operator TMC PMJ memegang peranan penting karena proses komunikasi yang terjadi diatur dan

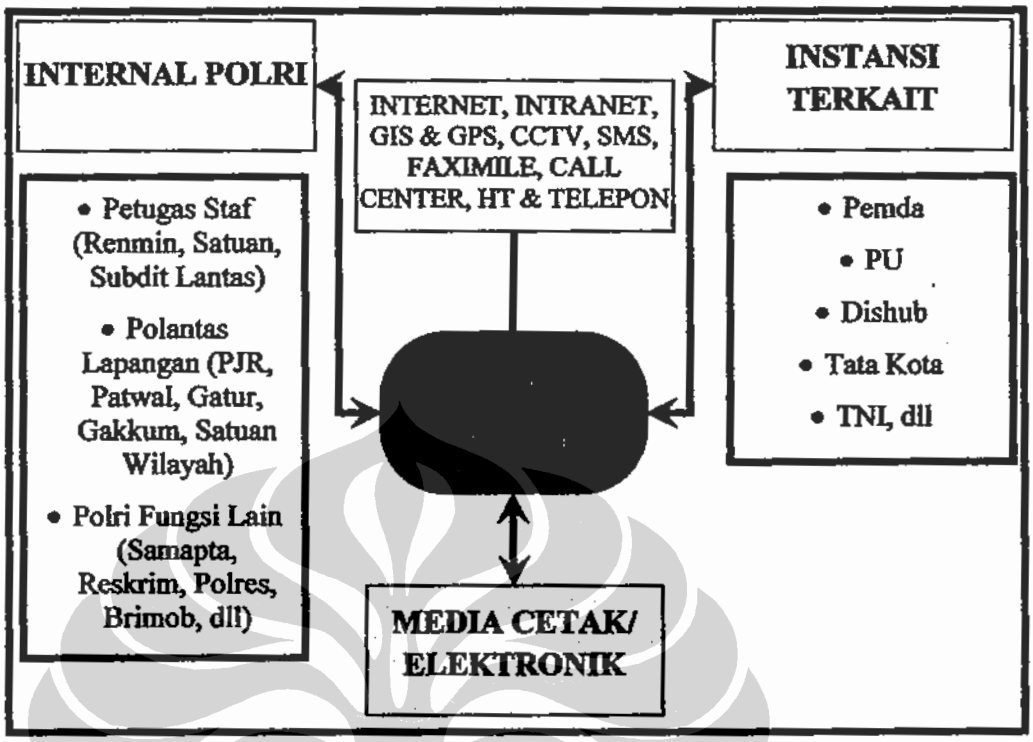
dikendalikan sepenuhnya oleh operator dengan dukungan seluruh aplikasi layanan informasi yang terdapat di dalam TMC PMJ.

Setelah menerima informasi dari kelima jalur komunikasi tersebut maka operator berkewajiban untuk meneruskan informasi yang ada sesuai dengan tingkatan kebutuhan dari informasi tersebut. Agar dapat mengkomunikasikan informasi yang ada maka petugas operator harus menguasai situasi dan kondisi wilayah di bidang lalu lintas melalui penggunaan aplikasi yang telah ditanamkan di dalam TMC PMJ. Tindakan petugas operator ini juga mendukung promosi, kampanye dan pembentukan opini serta citra positif bagi Polri dalam upaya melakukan pelayanan terhadap masyarakat.

Apabila dianalogikan dengan contoh kasus unjuk rasa yang mengarah anarkis di Bundaran HI serta rombongan pengawalan VVIP yang akan melintas, maka proses transmisi informasi berkaitan dengan fungsi komunikasi pada TMC PMJ adalah sebagai berikut: Setelah mendapatkan informasi dari masyarakat maka TMC PMJ berperan memberitahukan dan mengkomunikasikan akan perkembangan informasi yang ada kepada petugas Polantas di lapangan, unit pelayanan Ditlantas, instansi terkait dan memberitahukan penanganannya tersebut kepada media cetak/elektronik maupun kepada masyarakat agar masing-masing *stakeholder* mengetahui informasi perkembangan permasalahan yang terjadi.

C. Aplikasi Layanan Informasi pada Fungsi Koordinasi

Peranan TMC PMJ pada fungsi koordinasi terfokus pada aspek penyelesaian masalah seputar lalu lintas dengan berbagai pihak. Fungsi koordinasi dilakukan oleh TMC PMJ kepada para *stakeholder* baik secara internal petugas Polri, instansi terkait maupun media cetak/elektronik untuk mendapatkan berbagai masukan maupun kesepakatan-kesepakatan sehingga mendapatkan solusi yang terbaik dalam mengevaluasi berbagai masalah sosial di bidang lalu lintas.



Gambar 5.3: Skema Arus Informasi dalam Fungsi Koordinasi

Pada skema diatas menjelaskan proses koordinasi yang dilakukan oleh TMC PMJ terhadap adanya informasi yang didapatkan untuk menghasilkan solusi berkaitan dengan permasalahan di bidang lalu lintas. Merujuk pada contoh kasus tentang adanya aksi unjuk rasa yang mengarah kepada anarkis dan pengamanan rombongan VVIP, berdasarkan fungsi koordinasi maka proses transmisi informasi ini dapat dianalogikan bahwa TMC PMJ melakukan koordinasi secara efektif dan efisien dengan memanfaatkan seluruh aplikasi layanannya kepada petugas Samapta untuk melakukan upaya pengendalian aksi unjuk rasa, petugas Intelkam untuk melaksanakan fungsi intelijen, melakukan koordinasi kepada petugas Polantas di lapangan untuk melakukan tugas kepolisian di bidang lalu lintas, berkoordinasi dengan petugas Dishub untuk melaksanakan upaya pengalihan arus rombongan VVIP dengan menggunakan rambu-rambu yang ada di sekitar Bundaran HI, serta melakukan koordinasi kepada media cetak maupun elektronik untuk menyampaikan situasi dan kondisi kamseltibcar lalu lintas di seputar Bundaran HI.

D. Aplikasi Layanan Informasi pada Fungsi Informasi

Fungsi informasi pada TMC PMJ mempunyai peranan strategis dalam pengambilan keputusan atas informasi yang dihasilkan oleh TMC PMJ. Sebagai fungsi informasi pada TMC mengandung makna bahwa TMC merupakan wadah berita/kejadian-kejadian/situasi/kebijakan-kebijakan/perintah-perintah/masukan/ pengaduan yang diperoleh dari eksternal maupun internal dan dapat dijadikan acuan dalam mengambil tindakan-tindakan kepolisian baik dalam tingkat manajerial maupun operasional.

Sebagai pusat informasi maka TMC PMJ merupakan pusat pengumpulan, pengolahan dan penyajian data tentang segala informasi yang berkaitan dengan bidang lalu lintas, seperti: *database* pengemudi dan pemilik SIM, *database* identifikasi kendaraan bermotor, *database* lokasi penugasan personel Polantas di wilayah hukum Polda Metro Jaya beserta identitas petugas tersebut, *database* kecelakaan lalu lintas, *database* pelanggaran lalu lintas dan tilang, *database* program-program dan produk-produk upaya kepolisian di bidang lalu lintas yang dilakukan oleh Ditlantas Polda Metro Jaya, dll.

Untuk menunjang fungsi informasi ini maka TMC PMJ memanfaatkan seluruh layanan aplikasi yang ada sehingga dapat memberikan layanan optimal atas penyediaan informasi yang dibutuhkan oleh unsur pimpinan Ditlantas maupun seluruh *stakeholder* yang membutuhkannya dalam rangka pengambilan keputusan.

5.1.2. Kebijakan Keamanan Informasi yang telah Dilakukan.

Pada hakekatnya TMC PMJ didirikan oleh Ditlantas Polda Metro Jaya untuk membantu pelaksanaan tugas Polantas dalam menangani tugas-tugas kepolisian di bidang lalu lintas secara cepat dan profesional. Selain itu, secara eksternal TMC PMJ juga diharapkan agar masyarakat mendapatkan informasi yang berkaitan dengan situasi dan kondisi lalu lintas di Jakarta Raya secara akurat dan *real time*. Sebagai sarana untuk mewujudkan tujuan yang telah digariskan maka TMC PMJ menerapkan pola *community policing* dengan memanfaatkan fasilitas layanan-layanan *online* yang diaplikasikan di dalamnya.

Keberhasilan operasional TMC PMJ untuk mencapai tujuan yang telah digariskan merupakan prioritas utama yang harus diperhatikan. Agar mampu mewujudkan keberhasilan tersebut maka saat ini TMC PMJ telah menerapkan model kebijakan keamanan informasi terhadap layanan-layanan informasi yang terdapat di dalamnya untuk mengantisipasi terjadinya gangguan terhadap keamanan informasi dari berbagai ancaman dan kerentanan secara internal maupun ekstenal baik disengaja maupun yang tidak disengaja.

Berikut ini tertuang kebijakan keamanan terhadap aspek keamanan informasi yang telah dilakukan oleh Ditlantas Polda Metro Jaya terhadap TMC PMJ. Untuk memudahkan melakukan analisis terhadap kebijakan yang telah diterapkan dengan menggunakan pengendalian ISO 27001:2005 maka penulis melakukan penggolongan klasifikasi terhadap kebijakan keamanan tersebut ke dalam bentuk kode seperti pada pengendalian ISO 27001:2005. Bentuk kode yang digunakan adalah **OKKXXYZ. OKK** adalah kebijakan keamanan informasi, XX adalah klasifikasi golongan kebijakan keamanan informasi, Y adalah klasifikasi tujuan pengendalian, Z adalah klasifikasi pengendalian. Misalnya: OKK02A1, artinya adalah kebijakan keamanan informasi golongan organisasi keamanan informasi; tujuan pengendalian organisasi internal; pengendalian komitmen manajemen terhadap keamanan informasi. Demikian seterusnya.

5.1.2.1. Kebijakan Keamanan terhadap Personel TMC PMJ

Manusia merupakan salah satu unsur operasional komputer yang berfungsi untuk mengoperasionalkan komputer beserta jaringannya. Unsur manusia mempunyai peranan penting di dalam pelaksanaan operasional TMC PMJ, sehingga Ditlantas memandang perlu melakukan upaya pengamanan dalam bentuk kebijakan keamanan terhadap personel TMC PMJ. Upaya yang telah dilakukan oleh Ditlantas Polda Metro Jaya terhadap personel TMC PMJ dituangkan ke dalam tabel sebagai berikut:

Tabel 5.1. Kebijakan Keamanan Personel pada TMC PMJ

NO.	KEBIJAKAN KEAMANAN PERSONEL TMC PMJ	KODE
1.	Komitmen Dirlantas sebagai pimpinan manajemen Direktorat Lalu Lintas terhadap keamanan informasi.	OKK02A1
2.	Alokasi pertanggungjawaban keamanan informasi.	OKK02A3
3.	Menyusun peran dan tanggung jawab personel TMC PMJ.	OKK04A1
4.	Melakukan penyaringan personel TMC PMJ yang akan melaksanakan tugas sebagai personel TMC PMJ.	OKK04A2
5.	Membuat persyaratan dan kondisi kerja kepada petugas TMC PMJ.	OKK04A3
6.	Melaksanakan pertanggungjawaban tugas terhadap keamanan informasi.	OKK04B1
7.	Melaksanakan proses disipliner	OKK04B3
8.	Melaksanakan proses penghentian dari tanggung jawab terhadap personel yang diberhentikan (mutasi/alih tugas).	OKK04C1
9.	Melaksanakan pengembalian aset terhadap personel yang diberhentikan (mutasi/alih tugas).	OKK04C2
10.	Melakukan penghapusan hak akses terhadap informasi bagi personel yang diberhentikan (mutasi/alih tugas).	OKK04C3
11.	Melakukan pemisahan tugas dan kewenangan.	OKK06A3

5.1.2.2. Kebijakan Keamanan terhadap Fisik Bangunan TMC PMJ

Telah dijelaskan sebelumnya bahwa keamanan informasi meliputi kebijakan, prosedur dan aktifitas untuk melindungi aset informasi, salah satunya adalah keamanan terhadap fisik bangunan, terhadap berbagai jenis ancaman yang dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan operasional suatu organisasi untuk menjamin organisasi tersebut mencapai misi atau sasaran yang ingin dicapainya.

Upaya yang telah dilakukan oleh Ditlantas dalam melakukan keamanan terhadap fisik bangunan dituangkan ke dalam tabel sebagai berikut:

Tabel 5.2: Kebijakan Keamanan Fisik Bangunan TMC PMJ

NO.	KEBIJAKAN KEAMANAN FISIK BANGUNAN TMC PMJ	KODE
1.	Melakukan inventarisasi aset.	OKK03A1
2.	Melakukan penunjukan pertanggungjawaban aset.	OKK03A2
3.	Menerapkan perimeter keamanan fisik.	OKK05A1
4.	Menerapkan pengendalian akses masuk secara fisik.	OKK05A2
5.	Melakukan pengamanan kantor, ruangan dan fasilitas.	OKK05A3
6.	Melakukan perlindungan terhadap ancaman eksternal dan lingkungan.	OKK05A4
7.	Bekerja di area aman.	OKK05A5
8.	Melakukan penempatan peralatan dan perlindungan.	OKK05B1
9.	Menggunakan dukungan utilitas.	OKK05B2

5.1.2.3. Kebijakan Keamanan terhadap Informasi TMC PMJ.

Informasi merupakan salah satu sumber daya utama konseptual pada TMC PMJ, sehingga informasi yang dimiliki akan memperkaya penyajian atas sesuatu kepentingan yang diinginkan serta akan mengurangi suatu ketidakpastian sehingga mempunyai manfaat yang besar dalam proses pengambilan keputusan. Mengingat akan pentingnya informasi yang dimiliki maka Ditlantas Polda Metro Jaya melakukan penerapan kebijakan keamanan terhadap informasi secara lebih detail dan komprehensif apabila dibandingkan dengan kebijakan keamanan lainnya. Bentuk kebijakan tersebut adalah:

Tabel 5.3: Kebijakan Keamanan Informasi TMC PMJ

NO.	KEBIJAKAN KEAMANAN INFORMASI TMC PMJ	KODE
1.	Melakukan pedoman klasifikasi informasi.	OKK03B1
2.	Melakukan pelabelan informasi dan penanganannya.	OKK03B2
3.	Melakukan pengendalian terhadap kode berbahaya (*malicious ware*).	OKK06D1
4.	Melakukan back up data informasi.	OKK06E1
5.	Melakukan pengendalian jaringan.	OKK06F1
6.	Melakukan keamanan layanan jaringan.	OKK06F2

7.	Melakukan prosedur penanganan informasi.	OKK06G3
8.	Melakukan audit pencatatan informasi.	OKK06J1
9.	Melakukan pemantauan penggunaan sistem.	OKK06J2
10.	Melakukan kebijakan pengendalian akses.	OKK07A1
11.	Melakukan registrasi pengguna.	OKK07B1
12.	Menerapkan manajemen hak istimewa.	OKK07B2
13.	Menerapkan manajemen *password* pengguna.	OKK07B3
14.	Melakukan tinjauan hak akses pengguna.	OKK07B4
15.	Mempertanggungjawabkan penggunaan password oleh pengguna.	OKK07C1
16.	Mengendalikan kebijakan penggunaan layanan jaringan.	OKK07D1
17.	Mengendalikan otentikasi pengguna untuk sambungan eksternal.	OKK07D2
18.	Mengendalikan peralatan identifikasi dalam jaringan.	OKK07D3
19.	Mengendalikan dan melindungi *remote diagnostic* dan konfigurasi port.	OKK07D4
20.	Mengendalikan pemisahan dalam jaringan.	OKK07D5
21.	Mengendalikan pengendalian sambungan jaringan	OKK07D6
22.	Mengendalikan *routing* jaringan.	OKK07D7
23.	Menerapkan prosedur keamanan *log-on*.	OKK07E1
24.	Melakukan otentikasi dan identifikasi pengguna.	OKK07E2
25.	Menerapkan sistem manajemen *password*.	OKK07E3
26.	Menerapkan penggunaan utilitas sistem.	OKK07E4
27.	Pengendalian pembatasan akses informasi.	OKK07F1
28.	Mengisolasi sistem yang sensitif.	OKK07F2
29.	Mengendalikan komputansi bergerak dan komunikasi.	OKK07G1
30.	Melakukan validasi input data.	OKK08B1
31.	Melakukan validasi output data.	OKK08B4
32.	Mengendalikan keamanan software operasional.	OKK08D1
33.	Mengendalikan perlindungan terhadap sistem pengujian data.	OKK08D2
34.	Pengendalian akses kepada kode sumber program.	OKK08D3
35.	Melakukan pelaporan peristiwa keamanan.	OKK09A1
36.	Melakukan pelaporan kelemahan keamanan.	OKK09A2

5.2. Gangguan yang Masih Terjadi dan Penyebabnya.

Penerapan kebijakan keamanan telah dilaksanakan oleh Ditlantas Polda Metro Jaya demi mencegah maupun mengurangi gangguan dan ancaman yang diprakirakan terjadi. Namun demikian, gangguan masih saja tetap terjadi sehingga seringkali layanan operasional TMC PMJ mengalami gangguan.

Pada suatu organisasi terdapat dua aspek dasar yang menjadi bagian dari organisasi tersebut, yaitu aspek pendekatan mekanis/struktural dan aspek pendekatan humanis/fungsional. Apabila kedua aspek ini disandingkan pada organisasi TMC PMJ saat ini maka tampak bahwa kedua aspek tersebut tidak sempurna dimiliki oleh TMC PMJ. Secara mekanis, susunan personel yang melaksanakan tugas operasional pada TMC PMJ tidak terbentuk secara solid. Penunjukan personel TMC PMJ hanya mengacu pada surat perintah Dirlantas saja dan belum terorganisir secara baku melalui regulasi administratif dalam bentuk struktur organisasi TMC PMJ sebagai bagian dari Direktorat Lalu Lintas Polda Metro Jaya. Tanpa adanya struktur organisasi baku maka akan terjadi kesimpangsiuran persepsi mengenai analisis pekerjaan dari masing-masing personel yang ditunjuk yang tentu akan berimbas pada ketidakjelasan deskripsi pekerjaan mereka.

Dalam manajemen organisasi Polri diberlakukan konsep birokrasi, ini berarti segala sesuatu yang berkaitan dengan aktifitas organisasi (termasuk anggaran organisasi) diberlakukan secara baku sesuai dengan yurisdiksi baku melalui regulasi administratif. Berkaitan dengan hal ini maka belum adanya struktur organisasi yang baku pada TMC PMJ akhirnya membuahkan tidak adanya anggaran dinas yang digunakan untuk membiayai operasional TMC PMJ dalam melaksanakan kegiatannya.

Kajian aspek dasar organisasi yang kedua adalah pendekatan humanis/fungsional. Berdasarkan hasil penelitian dan pengamatan yang dilakukan maka dapat diketahui bahwa TMC PMJ belum mempunyai bentuk pendivisian dan pengelompokan kerja menjadi satuan pekerjaan dan mendefinisikan hubungan standar diantara individu-individu yang mengisi tugas-tugas tersebut secara tertulis. Walaupun telah disusun dan didokumentasikan terhadap penunjukan personel dalam melaksanakan tugas seperti yang tercantum dalam surat perintah

penunjukan Dirlantas dan buku pedoman TMC PMJ yang diterbitkan oleh Ditlantas namun belum mendefinisikan secara jelas tentang penjabaran bidang tugas/kewajiban, tanggung jawab dan pertanggungjawabannya. Salah satu akibatnya adalah penunjukan penugasan dan pertanggungjawaban yang dilakukan tidak dapat meng-*cover* semua aset penting yang ada dalam TMC PMJ.

Dengan ketidaksempurnaan kedua aspek dasar yang dimiliki oleh TMC PMJ tersebut berakibat sering terjadi gangguan terhadap TMC PMJ, khususnya yang berkaitan dengan aspek keamanan informasinya, baik keamanan personel, fisik maupun terhadap informasi itu sendiri. Kekurangpahaman personel operasional TMC PMJ akan pentingnya keamanan informasi dan belum terlaksananya program pendidikan dan pelatihan untuk meningkatkan profesionalisme para personel di lingkungan internal TMC PMJ (khususnya bagi petugas operator) mengakibatkan kerentanan yang tinggi atas keamanan informasi yang ada.

Pada aspek kemampuan operasional aplikasi layanan yang ada, para operator sering mengalami kendala teknis sebagai akibat kekurangpahaman mereka akan teknologi yang diterapkan. Hal ini sering terjadi pada petugas Polantas yang baru melaksanakan tugasnya sebagai operator TMC PMJ. Selain itu juga ditemukan minimnya motivasi terhadap personel TMC PMJ. Kejadian teknisi yang sering meninggalkan tugasnya ketika sedang melaksanakan piket, seperti yang disampaikan oleh kepala analis TMC PMJ, merupakan bukti terhadap aspek motivasi yang ada.

Minimnya anggaran ini juga berimbas pada pemeliharaan dan perawatan peralatan yang digunakan pada operasional TMC PMJ. Kerusakan yang terjadi pada peralatan fisik bangunan, perangkat hardware dan software jaringan komputer (seperti pada CCTV, proyektor, dll) akhirnya tidak bisa dilakukan penggantian secara cepat sehingga dapat mengganggu operasional sehari-hari. Ini berarti terjadi gangguan terhadap kinerja operasional TMC PMJ.

Selain itu tanpa dukungan anggaran yang mencukupi maka upaya pengembangan peranti *hardware* dan *software* pada aplikasi jaringan komputer juga tidak bisa dilaksanakan secara maksimal. Hal ini tampak pada penggunaan *software* antivirus pada seluruh peralatan komputer TMC PMJ menggunakan

freeware gratis yang di-*download* dari internet. Walaupun setiap saat dilakukan *update* untuk mengantisipasi terinfeksi virus terbaru yang bisa menyerang sistem komputer yang ada namun tentu saja tidak bisa memberikan *immune* maksimal bila dibandingkan dengan aplikasi antivirus berbayar yang disediakan oleh penyedia jasa pembuatan *software* antivirus.

Gangguan lainnya berkaitan dengan karakteristik layanan informasi pada TMC PMJ terletak pada fungsi pengendalian akses yang ada. Salah satu fungsi dari TMC PMJ adalah menyediakan akses informasi bidang lalu lintas secara online kepada masyarakat umum, ini berarti bahwa masyarakat bebas melakukan akses informasi tersebut tanpa bisa dihalangi. Akses informasi yang dilakukan oleh *user* baik secara internal maupun eksternal mengakibatkan website TMC PMJ di-*crack* oleh pihak yang tidak bertanggung jawab dengan memasukkan kode berbahaya dalam bentuk SQL *injection*. Selain itu konfigurasi data yang tidak terotorisasi dan masuknya virus baru yang merusak sistem operasional jaringan komputer serta aplikasi layanan yang ada juga merupakan akibat akses informasi yang terjadi.

Beberapa gangguan yang masih terjadi tersebut dapat mempengaruhi tingkat kepercayaan masyarakat yang akan melakukan akses informasi lalu lintas melalui TMC PMJ. Apabila tingkat kepercayaan masyarakat menjadi rendah sebagai akibat dari banyaknya kejadian gangguan informasi pada TMC PMJ maka ini akan menggagalkan terciptanya praktik *community policing* yang telah berhasil dilakukan TMC PMJ selama ini, sehingga Ditlantas perlu melakukan perubahan terhadap tindakan keamanan informasi yang telah dilakukannya dengan melakukan penerapan manajemen keamanan informasi yang mengimplementasikan pengendalian ISO 27001:2005.

5.3. Penerapan Manajemen Keamanan Informasi pada TMC PMJ dengan Implementasi Pengendalian ISO 27001:2005

Informasi pada TMC PMJ merupakan sumber daya utama yang harus dilakukan upaya keamanan oleh Ditlantas Polda Metro Jaya. Untuk itu harus dilindungi secara efektif dan efisien agar terhindar dari kerugian dan kehilangan

dengan menggunakan upaya manajemen yang tepat sehingga tujuan operasional TMC PMJ dapat tercapai.

Untuk dapat menciptakan manajemen keamanan terhadap informasi yang efektif dan efisien maka Ditlantas Polda Metro Jaya harus membuat suatu kebijakan, prosedur maupun aktifitas yang diperlukan untuk melindungi aset informasi, baik manusia, fisik bangunan maupun informasi itu sendiri dengan menerapkan strategi keamanan informasi dengan implementasi pengendalian ISO 27001:2005 pada TMC PMJ.

Strategi keamanan informasi merupakan implementasi dari proses pelaksanaan keamanan terhadap informasi dari suatu organisasi dengan memperhatikan aspek keunikan karakteristik dari TMC PMJ. Keunikan ini akan mempengaruhi penentuan parameter dari masing-masing indikator yang akan diteliti. Pentahapan dalam menentukan strategi keamanan informasi adalah melakukan identifikasi ancaman yang terjadi, mendefinisikan resiko, menentukan kebijakan keamanan dan melakukan implementasi pengendalian ISO 27001:2005.

5.3.1. Identifikasi Ancaman yang Terjadi

Ancaman merupakan suatu keadaan atau kejadian yang bila dibiarkan pasti akan membawa kerugian bagi TMC PMJ. Ada dua hal yang perlu diperhatikan dalam menyusun identifikasi ancaman, yaitu mempedomani gangguan yang telah terjadi dan melakukan analisis terhadap sumber ancaman dan bentuk ancaman lain yang diprakirakan akan terjadi.

Berdasarkan analisis terhadap sumber ancaman dan bentuk ancaman yang diprakirakan terjadi maka didapatkan bahwa terdapat sembilan identifikasi ancaman yang mungkin terjadi pada keamanan aset informasi TMC PMJ. Identifikasi ancaman tersebut adalah: (a). Personel yang melakukan akses secara online kepada jaringan komputer TMC PMJ; (b). personel yang melakukan akses bangunan fisik; (c). operator yang tidak profesional; (d). terjadi kerusakan pada database; (e). kerusakan terhadap bangunan fisik; (f). kerusakan pada perangkat *hardware* jaringan komputer; (g). kerusakan pada perangkat *software*/aplikasi layanan; (h). bencana alam; dan (i). konfigurasi transmisi data yang tidak terotorisasi.

Belakangan ini sering sekali terjadi bencana di Indonasia, baik yang bersifat alam maupun buatan. Hingga saat ini TMC PMJ masih belum terjadi bencana, namun perlu dilakukan langkah antisipatif berkaitan dengan bencana yang kemungkinan akan terjadi menimpa TMC PMJ.

Identifikasi ancaman keamanan informasi pada TMC PMJ dilandasi pada tiga sumber ancaman yang diprakirakan terjadi dan empat bentuk ancamannya, sebagai berikut:

a. Bentuk pengungkapan informasi yang tidak terotorisasi dan pencurian.
   Bentuk ancaman ini terjadi bersumber pada manusia dan teknologi. Identifikasi ancaman yang diprakirakan terjadi adalah:
   - Personel yang melakukan akses kepada jaringan.
   - Personel yang melakukan akses bangunan fisik.

b. Bentuk penggunaan yang tidak terotorisasi.
   Bentuk ancaman ini terjadi bersumber pada unsur manusia dan teknologi. Identifikasi ancaman yang diprakirakan terjadi adalah:
   - Personel yang melakukan akses kepada jaringan.
   - Personel yang melakukan akses bangunan fisik.
   - Operator TMC PMJ yang tidak profesional.

c. Bentuk penghancuran yang tidak terotorisasi dan penolakan layanan.
   Bentuk ancaman ini terjadi bersumber pada unsur manusia, alam dan teknologi. Identifikasi ancaman yang diprakirakan terjadi adalah:
   - Bencana alam
   - Personel yang melakukan akses kepada jaringan.
   - Personel yang melakukan akses bangunan fisik.
   - Operator TMC PMJ yang tidak profesional.
   - Kerusakan bangunan fisik.
   - Kerusakan *hardware*.
   - Kerusakan data.
   - Kerusakan *software*/aplikasi layanan.
   - Konfigurasi transmisi data yang tidak terotorisasi.

d. Bentuk modifikasi yang tidak terotorisasi.

Bentuk ancaman ini terjadi bersumber pada unsur manusia dan teknologi. Identifikasi ancaman yang diprakirakan terjadi adalah:

- Personel yang melakukan akses kepada jaringan.
- Personel yang melakukan akses bangunan fisik.
- Operator TMC PMJ yang tidak profesional.
- Konfigurasi transmisi data yang tidak terotorisasi.

Kemudian dilakukan penilaian ancaman terhadap identifikasi ancaman yang telah ditentukan, sebagai berikut:

Tabel 5.4: Klasifikasi Nilai Ancaman pada TMC PMJ

IDENTIFIKASI ANCAMAN	NILAI ANCAMAN	DAMPAK
Bencana alam	6	Fatal bagi organisasi
Personel yang melakukan akses kepada jaringan	4	Serius
Personel yang melakukan akses bangunan fisik	4	Serius
Operator TMC PMJ yang tidak profesional	2	Relatif tidak penting
Kerusakan bangunan fisik	2	Relatif tidak penting
Kerusakan *hardware*	2	Relatif tidak penting
Kerusakan database informasi	4	Serius
Kerusakan *software*/aplikasi layanan	3	Sedang
Konfigurasi transmisi data yang tidak terotorisasi	5	Sangat serius

Pada tabel di atas tampak bahwa bencana alam menjadi ancaman tertinggi yang akan mengakibatkan kerusakan fatal bagi TMC PMJ. Kemudian berturut-turut adalah konfigurasi transmisi data yang tidak terotorisasi akan mengakibatkan dampak yang sangat serius terhadap operasional TMC PMJ karena di dalam database tersimpan informasi penting berkaitan dengan identifikasi kendaraan bermotor. Apabila informasi identifikasi kendaraan bermotor ini tertransmisikan kepada pihak yang tidak terotosisasi maka penyalahgunaan berkaitan informasi ini

dapat digunakan untuk melegalkan kendaraan-kendaraan curian dengan cara memberikan surat-surat palsu berdasarkan informasi penting tersebut.

Nilai ancaman berikutnya adalah identifikasi ancaman terhadap personel yang melakukan akses kepada jaringan, personel yang melakukan akses bangunan fisik serta kerusakan database informasi. Personel yang melakukan akses tidak sah terhadap jaringan komputer maupun ke dalam bangunan TMC PMJ berdampak pada ancaman serius terhadap operasional TMC PMJ. Selain itu kerusakan pada database informasi akan berakibat pada hilangnya data-data penting, terutama berkaitan dengan data identifikasi kendaraan bermotor yang ada.

Identifikasi ancaman yang memiliki nilai sedang adalah kerusakan pada software/aplikasi layanan. Apabila software/aplikasi layanan tersebut rusak maka otomatis layanan operasional pada TMC PMJ tidak bisa dioperasionalkan. Butuh waktu yang cukup lama untuk membetulkan kerusakan ini sehingga TMC PMJ tidak dapat melaksanakan fungsi yang telah digariskan kepada *stakeholder* bidang lalu lintas.

Untuk identifikasi ancaman yang berkaitan dengan operator TMC PMJ yang tidak profesional, kerusakan bangunan fisik serta kerusakan hardware hanya menimbulkan dampak yang relatif tidak penting bagi organisasi TMC PMJ. Dampak yang muncul sebagai akibat dari identifikasi ancaman ini akan mengakibatkan gangguan yang bersifat sementara dan dapat diperbaiki dengan cepat.

5.3.2. Pendefinisian Resiko

Resiko adalah kombinasi dari ancaman yang berakibat pada munculnya kerentanan dalam organisasi sehingga dapat menyebabkan masalah atau gangguan dari suatu aset pada organisasi TMC PMJ. Dalam setiap organisasi yang ada, resiko keamanan merupakan konsekuensi yang tidak bisa ditolak atau dihilangkan oleh karena itu maka resiko yang akan terjadi harus dapat dinilai sehingga dapat menentukan prioritas tindakan keamanan dalam rangka menciptakan strategi keamanan informasi. Berdasarkan besar kecilnya hasil penilaian tersebut menunjukkan prioritas penanganan keamanan yang harus dilakukan. Semakin

besar nilai resiko maka akan semakin banyak perlakuan keamanan yang akan dilakukan.

Upaya yang dilakukan dalam melakukan penilaian resiko adalah melalui tahapan pendefinisian resiko dengan menerapkan metodologi manajemen resiko. Metodologi manajemen resiko terdiri dari tiga langkah yang harus dilaksanakan, yaitu (a). melakukan identifikasi aset; (b). melakukan analisis resiko; dan (c). melakukan tidak lanjut atau respon terhadap resiko.

5.3.2.1. Identifikasi Aset.

Aset informasi merupakan bagian dari sumber daya informasi yang bernilai tinggi sesuai dengan karakteristik pada TMC PMJ. Untuk mencegah dan mengurangi terjadinya kerugian-kerugian bagi kelangsungan operasional TMC PMJ maka perlu dilakukan upaya keamanan informasi yang meliputi kebijakan, prosedur dan aktifitas untuk melindungi aset informasi tersebut baik manusia, fisik bangunan maupun informasi sensitif tersebut.

Penentuan identifikasi atas aset yang tercakup di dalam TMC PMJ dilaksanakan dengan cara melakukan analisis terhadap hasil penelitian terhadap aset yang ada pada TMC PMJ. Upaya pengidentifikasian aset ini didasari pada tiga aspek dasar tujuan keamanan informasi dengan memperhatikan aspek kerahasiaan, integritas maupun ketersediaan aset tersebut. Apabila terjadi kemungkinan ancaman atau gangguan terhadap aset ini maka akan menyebabkan resiko yang besar bagi organisasi TMC PMJ.

Identifikasi aset pada TMC PMJ diklasifikasikan berdasarkan tingkat kepentingan dan keamanannya yang dibagi menjadi tiga kategori dalam bentuk *numerik*, yaitu:

- Rendah (1).
- Sedang (2).
- Tinggi (3).

Tabel 5.2. memperlihatkan mengenai penilaian kategori dari identifikasi aset pada TMC PMJ yang terdiri dari aset personel, aset fisik bangunan serta aset informasi itu sendiri.

Tabel 5.5: Identifikasi Aset Informasi pada TMC PMJ

NO.	IDENTIFIKASI ASET	KATEGORI
Aset Manusia/Personel TMC PMJ		
1.	Kelompok penanggungjawab	2
2.	Kelompok petugas operasional TMC PMJ	2
3.	Kelompok IT	3
4.	Kelompok teknisi	1
Aset Fisik Bangunan TMC PMJ		
5.	Bangunan utama TMC PMJ	2
6.	Ruangan server TMC PMJ	3
7.	Ruangan analisis jaringan operasional TMC PMJ	3
Aset Informasi TMC PMJ		
Perangkat hardware:		
8.	Server GIS	2
9.	Server GPS	2
10.	Server aplikasi SSB	3
11.	Server SSB 01	3
12.	Server SSB KPTI	3
13.	Server back up data SSB	3
14.	Server website	1
15.	Server laka/langgar	2
16.	Mail server	2
17.	Server jaringan TMC PMJ	2
18.	Komputer operator	1
19.	Virtual projector	1
20.	Peralatan CCTV	2
Perangkat software:		
21.	Sistem Operasi Microsoft Windows XP	1
22.	Linux Ubuntu server	2
23.	Sistem database (oracle, mysql, dll)	3

Pada aset personel, kategori identifikasi aset tertinggi terletak pada tim IT TMC PMJ yang mempunyai peran sangat strategis dalam operasional TMC PMJ. Tim IT harus dijaga dengan perlakuan yang tepat karena melalui tim IT semua aplikasi, database dan back up sistem informasi TMC PMJ disusun dan didokumentasikan.

Pada aset fisik bangunan, ruangan server dan ruangan analisis jaringan operasional TMC PMJ mendapatkan kategori identifikasi aset tinggi. Ruangan ini berfungsi sebagai tempat peyimpanan informasi sensitif dan tempat pengendalian aplikasi semua jaringan pada TMC PMJ sehingga perlu penanganan keamanan informasi yang lebih dibandingkan dengan ruangan-ruangan lainnya.

Selain itu server SSB dan sistem database pada aset informasi mendapatkan kategori tinggi dalam identifikasi aset. Data yang tersimpan di dalam server SSB berisi tentang identifikasi kendaraan bermotor seluruh Jakarta Raya sehingga bila terjadi ancaman dan dan gangguan pada server SSB dan sistem database ini maka akan berakibat fatal bagi organisasi TMC PMJ.

Beberapa aset di atas teridentifikasi mempunyai nilai yang sangat penting bagi kelangsungan operasional TMC PMJ. Apabila terjadi ancaman atau gangguan terhadap beberapa aset tersebut maka akan menyebabkan resiko yang besar bagi kelangsungan operasional TMC PMJ.

Dari faktor kerahasiaan (*confidentially*), terbukanya aset ini oleh pihak yang tidak terotorisasi akan mengakibatkan terbukanya informasi sensitif dan dapat mengakibatkan penyalahgunaan informasi yang ada. Dari faktor ketersediaan informasi (availability), apabila terjadi ancaman atau gangguan terhadap aset tersebut maka kehilangan atau tidak tersedianya informasi akan menghambat jalannya aktifitas operasional TMC PMJ. Selain itu modifikasi yang dilakukan secara tidak terotorisasi atas beberapa aset tersebut akan mengakibatkan terjadinya inkonsistensi atas isi informasi sehingga faktor keutuhan informasi (*integrity*) dapat terganggu dan informasi menjadi tidak valid.

Setelah mengetahui kategori penilaian terhadap identifikasi aset berdasarkan tingkat kepentingan dan keamanannya maka langkah selanjutnya adalah menentukan penilaian kerentanan atas identifikasi aset yang ada.

Kerentanan aset adalah kondisi lemah dari identifikasi aset yang dapat dieksploitasi oleh ancaman yang ada. Dalam menentukan penilaian kerentanan terhadap identifikasi aset pada TMC PMJ dilaksanakan dengan melakukan analisis terhadap ancaman dan gangguan yang masih terjadi pada TMC PMJ serta dengan memperhatikan keempat komponen penting kerentanan (ketersediaan, pengaksesan, pengamanan organik dan ketangguhan fasilitas) yang dibagi menjadi tiga penilaian kerentanan dalam bentuk numerik, yaitu:

- Rendah (1).
- Sedang (2).
- Tinggi (3).

Tabel 5.6. memperlihatkan mengenai kerentanan terhadap identifikasi aset pada TMC PMJ yang terdiri dari aset personel, aset fisik bangunan serta aset informasi itu sendiri.

Tabel 5.6.: Penilaian Kerentanan terhadap Aset TMC PMJ

NO.	IDENTIFIKASI ASET	KERENTANAN
Aset Manusia/Personel TMC PMJ		
1.	Kelompok penanggungjawab	1
2.	Kelompok petugas operasional TMC PMJ	1
3.	Kelompok IT	2
4.	Kelompok teknisi	1
Aset Fisik Bangunan TMC PMJ		
5.	Bangunan utama TMC PMJ	1
6.	Ruangan server TMC PMJ	1
7.	Ruangan analisis jaringan operasional TMC PMJ	1
Aset Informasi TMC PMJ		
Perangkat hardware:		
8.	Server GIS	1
9.	Server GPS	1
10.	Server aplikasi SSB	1
11.	Server SSB 01	1
12.	Server SSB KPTI	1

13.	Server back up data SSB	1
14.	Server website	3
15.	Server laka/langgar	1
16.	Mail server	1
17.	Server jaringan TMC PMJ	1
18.	Komputer operator	2
19.	Virtual projector	1
20.	Peralatan CTV	2
Perangkat software:		
21.	Sistem Operasi Microsoft Windows XP	2
22.	Linux Ubuntu server	1
23.	Sistem database (oracle, mysql, dll)	2

Pada tabel 5.6. dapat diketahui bahwa nilai kerentanan yang paling tinggi terdapat pada server website. Aset ini mendapatkan nilai tertinggi berdasarkan penggunaan akses (faktor pengaksesan) tidak terbatas yang bisa dilakukan oleh masyarakat umum secara online melalui internet sehingga diperlukan tindakan keamanan informasi untuk mengantisipasinya.

Selanjutnya kategori nilai sedang dalam nilai kerentanan berada pada kelompok IT TMC PMJ, komputer operator, peralatan CCTV, sistem operasi Microsoft Windows XP dan pada sistem database server. Pada kelompok IT penilaian sedang dilakukan berdasarkan dari upaya yang dilakukan oleh Ditlantas dalam melakukan faktor pengamanan organik secara terbatas. Sedangkan pada komputer operator, walaupun telah dilakukan pengamanan penggunaan peralatan berupa penerapan *user-id* namun dalam penggunaan sehari-hari masih dilaksanakan secara tumpang tindih oleh petugas operator (faktor pengaksesan). Kemudian aset pada sistem operasi Microsoft Windows XP dan sistem database server terjadi kerentanan dalam penilaian sedang karena berkaitan dengan penggunaan akses yang tidak terbatas pada server website yang dimanfaatkan oleh masyarakat umum secara online.

Untuk identifikasi aset yang lainnya, berdasarkan hasil analisis yang dilakukan, mempunyai nilai kerentanan yang rendah. Ini terjadi karena telah

dilakukan upaya oleh Ditlantas untuk melakukan pembatasan atau penghalangan secara terencana, terjaga dan telah menerapkan pelaksanaan komunikasi yang baik.

5.3.2.2. Analisis Resiko.

Langkah kedua dalam mendefinisikan resiko adalah melakukan analisis terhadap resiko yang ada. Resiko merupakan akumulasi dari ancaman yang diprakirakan terjadi terhadap aset yang ada, penilaian terhadap aset, dan kerentanan yang ada di dalam aset tersebut yang menghasilkan nilai dampak resiko (*impact value*) dari identifikasi aset yang ada. Pada analisis resiko di bawah ini tidak mengikutsertakan ancaman berupa bencana alam karena apabila hal tersebut terjadi maka sudah dapat dipastikan akan terjadi kerusakan berat baik dalam lingkup aset personel, fisik bangunan dan aset informasi pada TMC PMJ.

Tabel 5.7. menunjukkan hasil nilai dampak resiko yang dilakukan secara matematis dengan menggunakan rumus berdasarkan pada gambar 2.4. sebagai berikut:

Tabel 5.7.: Nilai Dampak (*Impact Value*) terhadap Aset TMC PMJ

NO.	IDENTIFIKASI ASET	IDENTIFIKASI ANCAMAN	RATA-RATA NILAI ANCAMAN	BENTUK ANCAMAN	NILAI ASET	NILAI RENTAN	NILAI DAMPAK
1	Kelompok *penanggungjawab*	☑ Personel yang *melakukan* akses kepada jaringan. ☑ Personel yang melakukan akses bangunan fisik.	4	☑ Penggunaan yang tidak *terotorisasi*. ☑ Penghancuran yang tidak terotorisasi.	3	1	48
2.	Kelompok petugas operasional TMC PMJ	☑ Personel yang melakukan akses kepada jaringan. ☑ Personel yang melakukan akses bangunan fisik. ☑ Operator TMC PMJ yang tidak profesional.	3,3	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi.	2	1	21,8
3.	Kelompok IT	☑ Personel yang melakukan akses kepada jaringan. ☑ Personel yang melakukan akses	4	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak	3	2	96

		bangunan fisik.		terotorisasi. ☑ Penghancuran yang tidak terotorisasi.			
4.	Kelompok teknisi	☑ Personel yang melakukan akses kepada jaringan. ☑ Personel yang melakukan akses bangunan fisik.	4	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	1	1	16
5.	Bangunan utama TMC PMJ	☑ Personel yang melakukan akses kepada jaringan. ☑ Personel yang melakukan akses bangunan fisik. ☑ Kerusakan bangunan fisik. ☑ Kerusakan hardware.	3	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi.	2	1	18
6.	Ruangan server TMC PMJ	☑ Personel yang melakukan akses bangunan fisik. ☑ Kerusakan bangunan fisik. ☑ Kerusakan hardware. ☑ Kerusakan database informasi. ☑ Kerusakan software aplikasi layanan.	3	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi.	3	1	27
7.	Ruangan analisis jaringan operasional TMC PMJ	☑ Personel yang melakukan akses kepada jaringan. ☑ Personel yang melakukan akses bangunan fisik. ☑ Kerusakan bangunan fisik. ☑ Kerusakan hardware.	3	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	3	1	27
8.	Server GIS	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan.	3,6	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	2	1	25,9
9.	Server GPS	☑ Personel yang	3,6	☑ Pengungkapan informasi	2	1	25,9

		melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan.		yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.			
10.	Server aplikasi SSB	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan. ☑ Konfigurasi transmisi data yang tidak terotorisasi.	4	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	3	1	48
11.	Server SSB 01	☑ Personel yang melakukan akses kepada jaringan ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan. ☑ Konfigurasi transmisi data yang tidak terotorisasi.	4	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	3	1	48
12.	Server SSB KPTI	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan. ☑ Konfigurasi transmisi data yang tidak terotorisasi.	4	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	3	1	48
13.	Server back up data SSB	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan. ☑ Konfigurasi	4	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	3	1	48

		transmisi data yang tidak terotorisasi.					
14.	Server website	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan.	3,6	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	1	3	38,9
15.	Server laka/langgar	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan.	3,6	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	2	1	25,9
16.	Mail server	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan.	3,6	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	2	1	25,9
17.	Server jaringan TMC PMJ	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan database informasi. ☑ Kerusakan *software*/aplikasi layanan.	3,6	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	2	1	25,9
18.	Komputer operator	☑ Personel yang melakukan akses kepada jaringan ☑ Kerusakan *hardware*. ☑ Kerusakan sofrware/aplikasi jaringan.	3	☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi.	1	2	18
19.	Virtual projector	☑ Kerusakan *hardware*.	2	☑ Penghancuran yang tidak terotorisasi.	1	1	4
20.	Perlengkapan CCTV	☑ Kerusakan hardware	2	☑ Penghancuran yang tidak terotorisasi.	2	2	16
21.	Sistem Operasi Microsoft	☑ Personel yang melakukan akses	3,5	☑ Penggunaan yang tidak terotorisasi.	1	2	24,5

	Windows XP	kepada jaringan. ☑ Kerusakan software/aplikasi layanan		☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.			
22.	Linux Ubuntu server	☑ Personel yang melakukan akses kepada jaringan. ☑ Kerusakan software/aplikasi layanan.	3,5	☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	2	1	24,5
23.	Sistem database (oracle, mysql, dll)	☑ Personel yang melakukan akses kepada jaringan ☑ Kerusakan database informasi. ☑ Kerusakan software/aplikasi layanan.	3,6	☑ Pengungkapan informasi yang tidak terotorisasi dan pencurian. ☑ Penggunaan yang tidak terotorisasi. ☑ Penghancuran yang tidak terotorisasi. ☑ Modifikasi yang tidak terotorisasi.	3	2	77,8

5.3.2.3. Menentukan Tindak Lanjut.

Langkah ketiga dalam pendefinisian resiko adalah melakukan tindak lanjut penanganan atas hasil *impact value* yang telah dihitung. Langkah ini merupakan evaluasi atas kebijakan keamanan yang telah diterapkan saat ini oleh Ditlantas Polda Metro Jaya terhadap keamanan informasi di TMC PMJ. Apabila diketahui tenyata kebijakan keamanan yang telah dilakukan tersebut melebihi tingkatan *risk level* yang telah ditetapkan maka akan dilakukan penilaian tambahan berdasarkan obyektif kontrol dan kontrol menggunakan ISO 27001:2005 sehingga didapatkan kondisi diterima pada *risk level*.

Agar memudahkan melakukan analisis terhadap kebijakan keamanan tarhadap aset informasi TMC PMJ yang telah dilakukan maka perlu menentukan *risk level* berdasarkan *impact value* terlebih dahulu untuk mengetahui sampai sejauh mana kondisi tersebut diterima, sebagai berikut:

Tabel 5.8: Tabel Penentuan *Risk Level* Berdasarkan *Impact Value*

IMPACT VALUE	INHERENT RISK	RISK LEVEL	ACTION PLAN
0 – 15	Low	Diterima	Standar Operasional Prosedur
15- 30	Low to Medium	Tidak diterima	Penilaian tambahan berdasarkan ISO 27001:2005
30-60	Medium	Tidak diterima	Penilaian tambahan berdasarkan ISO 27001:2005
60-120	Medium to High	Tidak diterima	Penilaian tambahan berdasarkan ISO 27001:2005

Nilai *impact value* pada tabel 5.8 tersebut merupakan tetapan asumsi dari penulis,dimana semakin kecil *range* dari nilai *impact value* maka tingkat keamanannya menjadi semakin tinggi, demikian sebaliknya. Tetapan asumsi ini disusun dengan alasan tingginya tingkat kerawanan di wilayah Polda Metro Jaya dan pandangan bahwa Polda Metro Jaya merupakan barometer keamanan seluruh polda di Indonesia sehingga penulis berasumsi bahwa kebijakan keamanan informasi yang diimplementasikan pada TMC PMJ harus mempunyai tingkat keamanan yang tinggi.

Berdasarkan klasifikasi *inherent risk* yang telah ditetapkan tersebut, maka dilakukan pengkategorisasian aset informasi TMC PMJ sesuai dengan *impact value* yang telah didapatkan, sebagai berikut:

Tabel 5.9.: Penentuan Inherent Risk Terhadap Impact Value Aset TMC PMJ

NO.	IDENTIFIKASI ASET	IMPACT VALUE	INHERENT RISK
1.	Kelompok penanggungjawab	48	Medium
2.	Kelompok petugas operasional TMC	21,8	Low to Medium

	PMJ		
3.	Kelompok IT	96	Medium to High
4.	Kelompok teknisi	16	Low to Medium
5.	Bangunan utama TMC PMJ	18	Low to Medium
6.	Ruangan server TMC PMJ	27	Low to Medium
7.	Ruangan analisis jaringan operasional TMC PMJ	27	Low to Medium
8.	Server GIS	25,9	Low to Medium
9.	Server GPS	25,9	Low to Medium
10.	Server aplikasi SSB	48	Low to Medium
11.	Server SSB 01	48	Low to Medium
12.	Server SSB KPTI	48	Low to Medium
13.	Server back up data SSB	48	Low to Medium
14.	Server website	38,9	Low to Medium
15.	Server laka/langgar	25,9	Low to Medium
16.	Mail server	25,9	Low to Medium
17.	Server jaringan TMC PMJ	25,9	Low to Medium
18.	Komputer operator	18	Low to Medium
19.	Virtual projector	4	Low
20.	Perlengkapan CCTV	16	Low to Medium
21.	Sistem Operasi Microsoft Windows XP	24,5	Low to Medium
22.	Linux Ubuntu server	24,5	Low to Medium
23.	Sistem database (oracle, mysql, dll)	77,8	Medium to High

Dalam tabel 5.9. menunjukkan bahwa hanya aset *virtual projector* saja yang berada dalam kondisi diterima, sedangkan aset lainnya berada pada level tidak diterima sehingga perlu melakukan analisis kebijakan keamanan informasi yang telah dilakukan oleh Ditlantas Polda Metro Jaya terhadap aset-aset tersebut dengan menggunakan *risk control*.

Risk control merupakan pemilihan kebijakan keamanan yang telah dilakukan oleh Ditlantas Polda Metro Jaya terhadap aset-aset informasi pada TMC PMJ. Upaya kebijakan keamanan yang telah dilakukan meliputi aspek keamanan

personel, keamanan fisik dan keamanan informasi itu sendiri. Setiap upaya kebijakan keamanan yang diterapkan kepada aset-aset yang ada akan menurunkan impact value dari masing-masing aset tersebut sehingga diharapkan dapat berada dalam level diterima pada *risk level*.

Penghitungan *inherent risk* terhadap upaya kebijakan keamanan yang telah dilakukan oleh Ditlantas Polda Metro Jaya pada tesis ini dilakukan secara matematis dengan berdasarkan pada pedoman implementasi ISO 27001:2005. Dalam ISO 27001:2005 dinyatakan bahwa implementasi kontrol diterapkan dengan menyempurnakan kebijakan keamanan yang telah ada sebelumnya guna mengurangi resiko yang akan terjadi.

Seperti yang telah disampaikan sebelumnya bahwa ISO 27001:2005 mengimplementasikan 134 kontrol dalam pengendalian kebijakan keamanan terhadap informasi. Masing-masing kontrol pada ISO 27001:2005 merupakan koefisien dari impact value maksimal suatu aset informasi dalam organisasi. Ini berarti bahwa diasumsikan apabila secara keseluruhan kontrol tersebut diimplementasikan pada aset informasi suatu organisasi maka akan berpengaruh pada perubahan nilai dari impact value maksimal dan akhirnya berada pada kondisi diterima dalam *inherent risk*.

Asumsi dasar yang penulis kemukakan adalah bahwa kebijakan keamanan informasi yang diimplementasikan pada TMC PMJ harus mempunyai tingkat keamanan yang tinggi. Pada penetapan impact value diketahui bahwa rentang nilai resiko tertinggi berada pada nilai 324 sedangkan kondisi *inherent risk* yang dapat diterima berada pada nilai 0-15. Demi memudahkan penghitungan maka penulis berasumsi bahwa kondisi ideal dari *inherent risk* yang dapat diterima tepat berada pada nilai 10. Bila keseluruhan kontrol pada ISO 27001:2005 diterapkan maka nilai resiko tertinggi akan berada pada nilai 10 (diterima).

Menindaklanjuti asumsi tersebut maka akan didapatkan nilai koefisien dari masing-masing kontrol pada ISO 27001:2005 yang disusun di dalam rumusan sebagai berikut:

$$\frac{324}{134 \times c} = 10 \Rightarrow c = \frac{324}{10} \times \frac{1}{134}$$

$$= 0{,}24$$

Keterangan:
c = koefisien kontrol
324 = nilai resiko tertinggi
134 = jumlah seluruh kontrol
10 = nilai *inherent risk* yang diterima

Setelah mengetahui nilai koefisien dari masing-masing kontrol maka dilakukan penghitungan kebijakan keamanan yang telah dilakukan oleh Ditlantas Polda Metro Jaya untuk mendapatkan *impact value* akhir dan *inherent risk*. Untuk mendapatkan *impact value* akhir dari identifikasi aset pada TMC PMJ maka dilakukan penghitungan berdasarkan tiga asumsi, yaitu:

- Jika jumlah tindakan keamanan yang diterapkan terhadap aset yang teridentifikasi berjumlah lebih dari atau sama dengan 5 ($T \geq 5$), maka:

  IV Awal : T = IV Akhir

- Jika jumlah tindakan keamanan yang diterapkan terhadap aset yang teridentifikasi berjumlah lebih dari atau sama dengan 1 dan kurang dari atau sama dengan 4 ($1 \leq T \leq 4$), maka:

  IV Awal x T = IV Akhir

- Jika aset yang teridentifikasi tersebut belum dilakukan tindakan keamanan ($T = 0$), maka:

  IV Awal = IV Akhir

Keterangan: IV Awal = Impact Value Awal
IV Akhir = Impact Value Akhir
T = Jumlah tindakan kebijakan keamanan yang diterapkan

Setelah menetapkan ketiga asumsi tersebut maka dilakukan penghitungan terhadap Impact Value Awal serta tindakan kebijakan keamanan informasi yang ditulis dengan menggunakan kode berdasarkan Tabel 5.3. untuk mendapatkan Impact Value Akhir dalam rangka menentukan Inherent Risk, yang dituangkan pada tabel 5.10.:

Tabel 5.10.: Inherent Risk terhadap Kebijakan Keamanan yang Telah Dilakukan

NO.	IDENTIFIKASI ASET	IMPACT VALUE AWAL	KEBIJAKAN KEAMANAN YANG TELAH DILAKUKAN	IMPACT VALUE AKHIR	INHERENT RISK
1.	Kelompok penanggungjawab	48	OKK02A1; OKK02A3; OKK04A1; OKK04A2; OKK04A3; OKK04B1; OKK04B3; OKK04C1; OKK04C2; OKK04C3; OKK06A3	18	Low to medium
2.	Kelompok petugas operasional TMC PMJ	21,8	OKK02A1; OKK02A3; OKK04A1; OKK04A2; OKK04A3; OKK04B3; OKK04C1; OKK04C2; OKK04C3; OKK08A1	9	Low
3.	Kelompok IT	96	OKK02A1; OKK02A3; OKK05A3; OKK04A4; OKK06A1; OKK06A3; OKK06D1; OKK06E1; OKK 06E2; OKK06F1; OKK06F2; OKK06G3; OKK07B1; OKK07B2; OKK07B3; OKK07D1; OKK07D4; OKK07D7; OKK07E2; OKK07E3; OKK07F1; OKK08D1; OKK08D3; OKK09A1; OKK09A2	16	Low to medium
4.	Kelompok teknisi	16	OKK04A1; OKK04A2;	7,68	Low
5.	Bangunan utama TMC PMJ	18	OKK03A1; OKK05A1; OKK05A2; OKK05A3; OKK05A5; OKK05B1	12,5	Low
6.	Ruangan server TMC PMJ	27	OKK03A2; OKK05A1; OKK05A2; OKK05A3; OKK05A4; OKK05A5; OKK05B2	16	Low to medium
7.	Ruangan analisis	27	OKK03A1; OKK03A2; OKK05A1;	14	Low

	jaringan operasional TMC PMJ		OKK05A2; OKK05A3; OKK05A4; OKK05A5; OKK05B2		
8.	Server GIS	25,9	OKK06D1; OKK06E1; OKK06J2; OKK07B1; OKK07B2; OKK07C1; OKK07D4; OKK07D5; OKK07E3	12	Low
9.	Server GPS	25,9	OKK06D1; OKK06E1; OKK06J2; OKK07B1; OKK07B2; OKK07C1; OKK07D4; OKK07D5; OKK07E3	12	Low
10.	Server aplikasi SSB	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1; OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	16,6	Low to medium
11.	Server SSB 01	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1; OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	16,6	Low to medium
12.	Server SSB KPTI	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1; OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	16,6	Low to medium
13.	Server back up data SSB	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1; OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	16,6	Low to medium
14.	Server website	38,9	OKK03B1; OKK06F1; OKK07B1; OKK07B3; OKK07D1; OKK07D2; OKK07D3; OKK07D6; OKK07D7; OKK07G1	16,2	Low to medium
15.	Server laka/langgar	25,9	OKK06D1; OKK06E1; OKK06J2; OKK07B1; OKK07B2; OKK07C1; OKK07D4; OKK07D5; OKK07E5	12	Low
16.	Mail server	25,9	OKK06D1; OKK06E1; OKK06J2; OKK07B1; OKK07B2; OKK07C1; OKK07D4; OKK07D5; OKK07E5	12	Low
17.	Server jaringan TMC PMJ	25,9	OKK06D1; OKK06E1; OKK06J2; OKK07B1; OKK07B2; OKK07C1; OKK07D4; OKK07D5; OKK07E5	12	Low
18.	Komputer operator	18	OKK06D1; OKK07B1; OKK07B3; OKK07D2; OKK07E3	15	Low
19.	Perlengkapan CCTV	16	-	16	Low to medium
20.	Sistem Operasi Microsoft Windows XP	24,5	OKK06D1; OKK06J1; OKK07B3; OKK07E1; OKK07E2; OKK07F1; OKK07G1; OKK08D3	12,7	Low
21.	*Linux Ubuntu server*	24,5	OKK06G3; OKK07D3; OKK07D4; OKK07E1; OKK07E2; OKK07E3; OKK08D1; OKK08D2; OKK09A1; OKK09A2	10,2	Low

22.	Sistem database (oracle, mysql, dll)	77,8	OKK03B1; OKK03B2; OKK06E1; OKK06F1; OKK06G3; OKK06J1; OKK07D3; OKK07D4; OKK07E1; OKK07E2; OKK07E3; OKK07E4; OKK07F2; OKK07G1; OKK08D1; OKK08D2; OKK08D3; OKK09A1; OKK09A2	17	Low to medium

Berdasarkan hasil penghitungan Tabel 5.10. maka dapat diketahui bahwa masih ada beberapa aset informasi yang telah diidentifikasi berada pada posisi "*Low to Medium*" dalam ***inherent risk***, ini berarti bahwa aset-aset tersebut masih berada pada posisi tidak diterima dalam risk level. Aset-aset yang berada dalam posisi tidak diterima dalam risk level adalah:

- Kelompok penanggungjawab
- Kelompok IT
- Ruangan server TMC PMJ
- Perlengkapan CCTV
- Server aplikasi SSB
- Server SSB 01
- Server SSB KPTI
- Server back up data SSB
- Server website
- Sistem database (oracle, mysql, dll)

Sebagai tindak lanjut atas kondisi tersebut maka dilakukan penilaian tambahan menggunakan implementasi pengendalian ISO 27001:2005 hingga mendapatkan hasil "diterima" dalam *risk level*.

ISO 27001:2005 berisi tentang kontrol dan pengawasan dalam bentuk parameter yang berguna untuk memberikan saran dan petunjuk pelaksanaan pada praktek terbaik dalam mendukung pengendalian. Isi dari ISO 27001:2005 terdiri dari 11 golongan, 39 tujuan pengendalian dan 134 pengendalian. Pengendalian ISO 27001:2005 yang diterapkan pada aset TMC PMJ terhadap identifikasi aset yang belum mendapatkan hasil "diterima" dalam *risk level* dilaksanakan dengan melakukan penyesuaian pada kondisi aset tersebut di TMC PMJ. Pengendalian

tambahan yang akan digunakan untuk mendapatkan hasil tersebut merupakan bagian dari tujuh tujuan pengendalian ISO 27001:2005, yaitu:

1. Pengendalian kebijakan keamanan informasi.
2. Pengendalian terhadap pihak-pihak eksternal pada organisasi keamanan informasi.
3. Pengendalian terhadap keamanan sumber daya manusia selama bekerja.
4. Pengendalian peralatan keamanan.
5. Pengendalian media penanganan informasi.
6. Pengendalian pertukaran informasi.
7. Pengendalian aspek keamanan informasi terhadap manajemen keberlangsungan bisnis.

Dalam tabel berikut ini merupakan hasil penghitungan dari inherent risk dengan menggunakan implementasi ISO 27001:2005, sebagai berikut:

Tabel 5.11.: Hasil Inherent Risk dengan implementasi ISO 27001:2005

NO.	IDENTIFIKASI ASET	IV AWAL	KEBIJAKAN KEAMANAN	KENDALI TAMBAHAN	IV AKHIR	RISK LEVEL
1.	Kelompok penanggung jawab	48	OKK02A1; OKK02A3; OKK04A1; OKK04A2; OKK04A3; OKK04B1; OKK04B3; OKK04C1; OKK04C2; OKK04C3; OKK06A3	OKK01A1; OKK01A2; OKK11C1	14,2	Diterima
2.	Kelompok IT	96	OKK02A1; OKK02A3; OKK05A3; OKK04A4; OKK06A1; OKK06A3; OKK06D1; OKK06E1; OKK 06E2; OKK06F1; OKK06F2; OKK06G3; OKK07B1; OKK07B2; OKK07B3; OKK07D1; OKK07D4; OKK07D7; OKK07E2; OKK07E3; OKK07F1; OKK08D1; OKK08D3; OKK09A1; OKK09A2	OKK10A1 OKK10A3	14,8	Diterima
3.	Ruangan server TMC PMJ	27	OKK03A2; OKK05A1; OKK05A2; OKK05A3; OKK05A4; OKK05A5; OKK05B2	OKK05B3; OKKO5B4	12,5	Diterima
4.	Perlengkapan CCTV	16	-	OKK05B3; OKKO5B4	7,68	Diterima
5.	Server aplikasi	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1;	OKK06G1; OKK06G4;	14	Diterima

	SSB		OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	OKK06H1; OKK10A1; OKK10A3		
6.	Server SSB 01	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1; OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	OKK06G1; OKK06G4; OKK06H1; OKK10A1; OKK10A3	11,8	Diterima
7.	Server SSB KPTI	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1; OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	OKK06G1; OKK06G4; OKK06H1; OKK10A1; OKK10A3	11,8	Diterima
8.	Server back up data SSB	48	OKK03B1; OKK06E1; OKK06F2; OKK07A1; OKK07B4; OKK07D1; OKK07E4; OKK07F2; OKK08B1; OKK08B4; OKK09A1; OKK09A2	OKK06G1; OKK06G4; OKK06H1; OKK10A1; OKK10A3	11,8	Diterima
9.	Server website	38,9	OKK03B1; OKK06F1; OKK07B1; OKK07B3; OKK07D1; OKK07D2; OKK07D3; OKK07D6; OKK07D7; OKK07G1	OKK06G1; OKK06G4; OKK06H1;	12,5	Diterima
10.	Sistem database (oracle, mysql, dll)	77,8	OKK03B1; OKK03B2; OKK06E1; OKK06F1; OKK06G3; OKK06J1; OKK07D3; OKK07D4; OKK07E1; OKK07E2; OKK07E3; OKK07E4; OKK07F2; OKK07G1; OKK08D1; OKK08D2; OKK08D3; OKK09A1; OKK09A2	OKK06G1; OKK06G4; OKK06H1; OKK09A1; OKK09A2; OKK09B1; OKK09B2; OKK10A1; OKK10A3	5,8	Diterima

Keterangan:

OKKXXYZ = Golongan Kebijakan Keamanan Informasi, XX = Tujuan Kebijakan Keamanan Informasi, YZ = Pengendalian pada ISO 27001:2005.

5.3.3. Penentuan Kebijakan Keamanan.

Kebijakan keamanan adalah rumusan tertulis yang berisi tentang tanggung jawab individu maupun manajemen dalam mengatur apa yang boleh dilakukan dan tidak, untuk melindungi terhadap aset-aset informasi yang ada. Penyusunan kebijakan keamanan dilakukan pada saat akan dibentuknya organisasi, secara

insidentil ketika kebijakan keamanan lama dirasakan sudah tidak efektif melakukan upaya keamanan terhadap aset yang ada, dan secara periodik guna pembaharuan kebijakan keamanan dalam menyikapi perkembangan lingkungannya.

Penentuan kebijakan keamanan terhadap informasi harus menerapkan enam persoalan, yaitu (a). kebijakan atau tata kerja yang mengindikasikan tujuan-tjuan dari upaya keamanan informasi dan keinginan berusaha untuk mencapai tujuan tersebut; (b). keadaan yang berlaku, yang menjelaskan status keamanan informasi pada saat diterapkan kebijakan keamanan; (c). rekomendasi persyaratan, yang mengarah kepada tujuan-tujuan kebijakan keamanan; (d). tanggung jawab, yang menguraikan siapa yang bertanggung jawab pada setiap aktifitas keamanan informasi; (e). jadwal waktu, guna mengidentifikasi ketika fungsi-fungsi keamanan informasi yang berbeda agar segera dilakukan; serta (f). perhatian yang berkelanjutan, guna menetapkan stuktur untuk memutakhirkan dan memeperbaharui rencana keamanan informasi secara berkala.

Penentuan kebijakan keamanan berkaitan erat dengan penunjukan tugas atau kewajiban, tanggung jawab dan pertanggungjawaban yang diemban oleh komponen personel pada TMC PMJ yang dituangkan dalam struktur organisasi TMC PMJ. Karena TMC PMJ belum mempunyai struktur organisasi secara tetap maka penulis mengklasifikasikan komponen personel dengan mengacu pada penunjukan operator operasional berdasarkan Surat Perintah Dirlantas Polda Metro Jaya Nomor: Sprin/39/I/2010/Ditlantas tentang Penunjukan Operator Operasional TMC PMJ.

Dalam melakukan penyusunan penentuan kebijakan keamanan ini dilakukan berdasarkan visi, misi dan sasaran prioritas Polda Metro Jaya yang diambil dari website Bidang Humas Polda Metro Jaya (http://humas-poldametrojaya.com/) dan penjabaran visi dan misi Direktorat Lalu Lintas Polda Metro Jaya yang diambil dari website Ditlantas Polda Metro Jaya (http://202.59.168.243/profil/index.php?id=0). Gambaran penentuan kebijakan keamanan TMC PMJ yang disusun berdasarkan hasil analisis strategi keamanan informasi adalah sebagai berikut:

A. Visi Polda Metro Jaya:

Tergelarnya polisi yang dipercaya masyarakat disemua titik dan lini pelayanan masyarakat di sepanjang waktu dalam wujudkan keamanan di wilayah hukum Polda Metro Jaya dan tegaknya hukum sebagai sinergi pencapaian hasil pembangunan yang berwawasan keamanan.

B. Misi Polda Metro Jaya:

1. Perkuat dan tingkatkan kemampuan intelijen keamanan Polda Metro Jaya guna menjaring informasi untuk cegah gangguan keamanan dan pengungkapan kasus secara sistematis dan tuntas
2. Kembangkan pelayanan publik di setiap lini berbasis pelayanan prima
3. Menggelar polisi sebanyak-banyak di tengah masyarakat dalam memberikan perlindungan, pengayoman dan pelayanan masyarakat.
4. Kembangkan falsafah dan strategi perpolisian masyarakat (polmas) dalam bangun hub polisi dan masy yg lebih dekat dan interaktif dalam upaya wujudkan masyarakat patuh hukum.
5. Berdayakan seluruh kekuatan dan kemampuan organisasi pengemban fungsi lidik dan sidik dalam wujudkan Polri sebagai penegak hukum yang terdepan.
6. Tingkatkan kinerja Polda Metro Jaya secara profesional, transparan dan akuntabel guna dukung tupoksi Polri.

C. Sasaran Prioritas Polda Metro Jaya:

1. Terwujudnya kondisi kamtibmas wilayah hukum Polda Metro Jaya yang kondusif pasca pelaksanaan Pemilu 2009.
2. Lanjutkan pembangunan sarana dan prasarana.
3. Tingkatkan kualitas kemampuan dan ketrampilan personel Polda Metro Jaya.
4. Melaksanakan pembinaan personil Polri
5. Tertanggulanginya penyalahgunaan narkoba melalui giat preventif dan represif.
6. Tertanggulanginya kejahatan transnasional (*trafficking in person* dan *people smugling*).

7. Terealisasinya program perpolisian masyarakat (polmas) untuk tingkatkan kemitraan dan kepatuhan hukum masyarakat.
8. Terpeliharanya kamtibmas perairan dan tertanganinya segala bentuk kejahatan di perairan yuridiksi Polda Metro Jaya.
9. Tertanganinya perkara-perkara korupsi.
10. Penanganan bencana banjir.
11. Meningkatkan pencapaian *quick wins*.
12. Terwujudnya kondisi lingkungan yang aman dan bebas dari premansme, kejahatan jalanan (street crime) dan perjudian.
13. Tingkatkan kualitas peserta pendidikan Polri (bintara).

D. Visi Direktorat Lalu Lintas Polda Metro Jaya:

Polantas yang mampu menjadi pelindung, pengayom, pelayanan masyarakat yang selalu dekat dan bersama-sama dengan masyarakat serta sebagai aparat penegak hukum yang profesional dan proporsional yang selalu menjunjung tinggi supremasi hukum dan hak azasi manusia, memelihara keamanan, ketertiban dan kelancaran lalu lintas.

E. Misi Direktorat Lalu Lintas Polda Metro Jaya:

1. Memberikan perlindungan, pengayoman dan pelayanan para pemakai jalan sehingga para pemakai jalan aman selama dalam perjalanan dan selamat sampai tujuan.
2. Memberikan bimbingan kepada masyarakat lalu lintas melalui upaya preventif yang dapat meningkatkan kesadaran dan ketaatan serta kepatuhan kepada ketentuan peraturan lalu lintas.
3. Menegakkan peraturan lalu lintas secara profesional dan proporsional dengan menjunjung tinggi supremasi hukum dan HAM.
4. Memelihara keamanan, ketertipan dan kelancaran lalu lintas dengan memperhatikan norma-norma dan nilai hukum yang berlaku.
5. Meningkatkan upaya konsolidasi ke dalam sebagai upaya menyamakan misi polantas.

F. Fungsi *Traffic Management Center* (TMC PMJ):

Traffic Management Center Polda Metro Jaya (TMC PMJ) merupakan pusat manajemen lalu lintas di Polda Metro Jaya yang berfungsi sebagai Pusat Komando, Komunikasi, Koordinasi dan Informasi (K3I) sebagai bentuk perpolisian masyarakat terhadap segenap *stakeholder* bidang lalu lintas dengan memanfaatkan aplikasi-aplikasi layanan jaringan komputer yang ada secara online demi terciptanya keamanan, keselamatan, ketertiban, dan kelancaran berlalu lintas di wilayah Jakarta Raya.

G. Tujuan *Traffic Management Center* (TMC PMJ):
   1. Pelayanan *quick response time* secara professional terhadap masyarakat.
   2. Analisis pelanggaran dan kecelakaan lalu lintas (*black spot*).
   3. Pusat informasi kegiatan dan kemacetan lalu lintas.
   4. Pusat informasi SIM, STNK, dan BPKB bagi Polri dan masyarakat.
   5. Pusat informasi hilang temu kendaraan bermotor.
   6. Pusat kendali patroli kendaraan bermotor dalam mewujudkan keselamatan dan kamtibcar lantas.
   7. Pusat informasi kualitas baku mutu udara.
   8. Pusat pengendalian lalu lintas.

H. Tugas, tanggung jawab dan pertanggungjawaban unsur pelaksana TMC PMJ:
   1. Manajemen Ditlantas Polda Metro Jaya/kelompok penanggungjawab:
      a. <u>Tugas:</u>
         - Menyelenggarakan operasional TMC PMJ.
         - Menyelenggarakan kebijakan keamanan informasi pada TMC PMJ
         - Menyelenggarakan keamanan sumber daya manusia sebelum bekerja maupun pada saat pemutusan atau mengubah pekerjaan para petugas operasional TMC PMJ.
         - Menyelenggarakan manajemen kesinambungan bisnis terhadap aspek keamanan informasi dan perbaikan pada TMC PMJ

- Menyelenggarakan pemenuhan atas pertimbangan audit sistem informasi pada TMC PMJ secara berkala.

b. Tanggung jawab:

- Melakukan dokumentasi terhadap kebijakan keamanan informasi.
- Melakukan tinjauan secara berkala terhadap kebijakan keamanan informasi.
- Mengdefinisikan peranan dan pertanggungjawaban para petugas operasional TMC PMJ.
- Melakukan penyaringan/rekrutmen para petugas operasional TMC PMJ.
- Menentukan persyaratan dan kondisi kerja para petugas operasional TMC PMJ.
- Melakukan penghentian dari tanggung jawab para petugas operasional TMC PMJ.
- Memasukkan keamanan informasi ke dalam proses keberlangsungan operasional TMC PMJ.
- Mengembangkan dan menerapkan rencana kesinambungan keamanan informasi.
- Melakukan pengendalian audit sistem informasi pada TMC PMJ.

c. Pertanggungjawaban:

Bertanggung jawab kepada Direktur Lalu Lintas Polda Metro Jaya.

2. Koordinator TMC PMJ:

a. Tugas:

- Mengelola pengorganisasian keamanan informasi pada TMC PMJ.
- Mengelola manajemen aset pada TMC PMJ.
- Mengelola keamanan sumber daya manusia pada TMC PMJ.
- Mengelola keamanan fisik dan lingkungan pada TMC PMJ.

- Mengelola komunikasi dan manajemen informasi pada TMC PMJ.
- Mengelola pengendalian akses.
- Mengelola akuisisi sistem informasi, pengembangan dan pemeliharaan informasi.
- Mengelola manajemen insiden keamanan informasi.

b. Tanggung jawab:

- Mengendalikan organisasi keamanan informasi secara internal.
- Mengendalikan organisasi keamanan informasi terhadap pihak-pihak eksternal.
- Mengendalikan manajemen aset dengan melakukan pertanggungjawaban terhadap aset yang ada.
- Mengendalikan manajemen aset dengan melakukan klasifikasi terhadap informasi yang ada.
- Mengendalikan keamanan sumber daya manusia yang ada selama bekerja pada TMC PMJ dan pada saat dilakukan penutusan atau pengubahan pekerjaan terhadap para petugas operasional TMC PMJ.
- Mengendalikan keamanan fisik dan lingkungan pada TMC PMJ dengan melakukan klasifikasi terhadap daerah aman dan peralatan keamanan.
- Mengendalikan komunikasi dan manajemen informasi terhadap operasional prosedur dan pertanggungjawaban komunikasi dan informasi, perlindungan pada kode berbahaya dan mobile, back up data, manajemen keamanan jaringan, media penanganan, pertukaran informasi serta pemantauan terhadap transmisi komunikasi dan informasi.
- Melakukan pengendalian akses terhadap kebutuhan layanan operasional TMC PMJ, manajemen akses pengguna, pertanggungjawaban para petugas operasional, pengendalian akses terhadap jaringan, pengendalian akses terhadap sistem

operasi, pengendalian akses terhadap aplikasi dan informasi, serta komputasi bergerak dan teleworking.

- Mengendalikan akuisisi sistem informasi, pengembangan dan pemeliharaan informasi berupa kebutuhan keamanan terhadap sistem informasi, pelaksanaan proses yang benar pada aplikasi dan keamanan sistem file.
- Mengendalikan manajemen insiden keamanan informasi berupa pelaporan peristiwa keamanan informasi dan kelemahannya dan melakukan manajemen insiden keamanan informasi dan perbaikan.

c. Pertanggungjawaban:

Bertanggung jawab kepada Direktur Lalu Lintas Polda Metro Jaya.

3. Kepala Team Analis:

a. Tugas:

- Melaksanakan pengorganisasian keamanan informasi secara internal dalam lingkup kerjanya.
- Melaksanakan keamanan sumber daya manusia selama bekerja pada TMC PMJ.
- Melaksanakan komunikasi dan manajemen informasi terhadap operasional prosedur dan pertanggungjawaban komunikasi dan informasi.
- Melaksanakan akuisisi sistem informasi, pengembangan dan pemeliharaan informasi.
- Melaksanakan manajemen insiden keamanan informasi berupa pelaporan peristiwa keamanan informasi dan kelemahannya serta melakukan manajemen insiden keamanan informasi dan perbaikan.
- Melaksanakan pemenuhan atas pertimbangan audit sistem informasi.

b. Tanggung jawab:

- Melaksanakan komitmen manajemen terhadap keamanan informasi.
- Mengalokasikan pertanggungjawaban keamanan informasi.
- Melaksanakan kesadaran terhadap keamanan informasi, mengikuti pendidikan dan pelatihan.
- Mendokumentasikan operasional prosedur berkaitan dengan lingkup kerjanya.
- Melaksanakan analisis dan spesifikasi peralatan keamanan.
- Melaporkan peristiwa keamanan informasi kepada atasan.
- Melaporkan kelemahan keamanan informasi kepada atasan.
- Menganalisis prosedur dan pertanggungjawaban.
- Melaksanakan pembelajaran dari insiden keamanan informasi yang terjadi.
- Melakukan analisis terhadap pengendalian audit sistem informasi.

c. Pertanggungjawaban:

Bertanggung jawab langsung kepada Koordinator TMC PMJ

4. Perwira Siaga:

a. Tugas:

- Melaksanakan pengorganisasian keamanan informasi secara internal dalam lingkup kerjanya.
- Melaksanakan pertanggungjawaban aset yang telah ditentukan berkaitan dalam bidang tugasnya.
- Melaksanakan keamanan sumber daya manusia selama bekerja pada TMC PMJ.
- Melaksanakan ketentuan keamanan fisik dan lingkungan yang telah ditetapkan terhadap daerah aman dan peralatan keamanan.
- Melaksanakan komunikasi dan manajemen informasi terhadap operasional prosedur dan pertanggungjawaban komunikasi dan informasi.

- Melaksanakan manajemen insiden keamanan informasi berupa pelaporan peristiwa keamanan informasi dan kelemahannya serta melakukan manajemen insiden keamanan informasi dan perbaikan.

b. Tanggung jawab:

- Melaksanakan komitmen manajemen terhadap keamanan informasi.
- Melaksanakan alokasi pertanggungjawaban keamanan informasi.
- Melakukan inventarisasi aset fisik bangunan pada TMC PMJ.
- Melaksanakan penunjukan pertanggungjawaban aset fisik bangunan pada TMC PMJ.
- Melaksanakan kesadaran terhadap keamanan informasi, mengikuti pendidikan dan pelatihan.
- Mengamankan perimeter keamanan fisik pada TMC PMJ.
- Mengamankan pengendalian akses masuk fisik pada TMC PMJ.
- Mengamankan bangunan fisik TMC PMJ, ruangan serta fasilitas-fasilitasnya.
- Melaksanakan perlindungan terhadap ancaman eksternal dan lingkungan.
- Mengamankan area aman untuk bekerja.
- Menjaga tempat peralatan keamanan dan perlindungan.
- Menggunakan dukungan utilitas peralatan keamanan.
- Melaksanakan pemeliharaan peralatan fisik bangunan.
- Mendokumentasikan operasional prosedur berkaitan dengan lingkup kerjanya.
- Melaporkan peristiwa keamanan informasi kepada atasan.
- Melaporkan kelemahan keamanan informasi kepada atasan.
- Melakukan prosedur dan pertanggungjawaban.

- Melaksanakan pembelajaran dari insiden keamanan informasi yang terjadi.

c. Pertanggungjawaban:

Perwira Siaga bertanggung jawab kepada Koordinator TMC PMJ.

5. Tim IT TMC PMJ:

a. Tugas:

- Melaksanakan pengorganisasian keamanan informasi secara internal dalam lingkup kerjanya serta berkaitan dengan pihak eksternal.
- Melaksanakan pertanggungjawaban aset serta mengklasifikasi informasi yang telah ditentukan berkaitan dalam bidang tugasnya.
- Melaksanakan keamanan sumber daya manusia selama bekerja pada TMC PMJ.
- Melaksanakan ketentuan keamanan fisik dan lingkungan yang telah ditetapkan terhadap daerah aman dan peralatan keamanan.
- Melaksanakan komunikasi dan manajemen informasi terhadap operasional prosedur dan pertanggungjawaban komunikasi dan informasi, perlindungan pada kode berbahaya dan mobile, back up data, manajemen keamanan jaringan, media penanganan, pertukaran informasi serta pemantauan terhadap transmisi komunikasi dan informasi.
- melakukan pengendalian akses terhadap kebutuhan layanan operasional TMC PMJ, manajemen akses pengguna, pertanggungjawaban para petugas operasional, pengendalian akses terhadap jaringan, pengendalian akses terhadap sistem operasi, pengendalian akses terhadap aplikasi dan informasi, serta komputasi bergerak dan teleworking.
- Melaksanakan akuisisi sistem informasi, pengembangan dan pemeliharaan informasi berupa kebutuhan keamanan terhadap

sistem informasi, pelaksanaan proses yang benar pada aplikasi dan keamanan sistem file.

- Melaksanakan manajemen insiden keamanan informasi berupa pelaporan peristiwa keamanan informasi dan kelemahannya dan melakukan manajemen insiden keamanan informasi dan perbaikan.

b. Tanggung jawab:

- Melaksanakan komitmen manajemen terhadap keamanan informasi.
- Melaksanakan alokasi pertanggungjawaban keamanan informasi.
- Membuat dan melaksanakan perjanjian pihak ketiga.
- Menginventarisir aset informasi yang ada berkaitan dengan bidang tugasnya.
- Melaksanakan penunjukan pertanggungjawaban aset informasi.
- Melaksanakan pedoman klasifikasi informasi.
- Melakukan pelabelan informasi dan penanganannya.
- Melaksanakan kesadaran terhadap keamanan informasi, mengikuti pendidikan dan pelatihan.
- Mengamankan pengendalian akses masuk fisik yang berkaitan dengan lingkup kerjanya.
- Mengamankan bangunan fisik TMC PMJ, ruangan serta fasilitas-fasilitas yang berkaitan dengan lingkup kerjanya.
- Melaksanakan perlindungan terhadap ancaman eksternal dan lingkungan.
- Mengamankan area aman yang berkaitan dengan lingkup kerjanya.
- Melaksanakan keamanan sistem kabel.
- Melaksanakan pemeliharaan peralatan yang berkaitan dengan lingkup kerjanya.
- Melakukan dokumentasi operasional prosedur terhadap semua kegiatan operasional Tim IT TMC PMJ.

- Melakukan pemisahan tugas terhadap para petugas operasional TMC PMJ.
- Melakukan pengendalian terhadap kode berbahaya.
- Melakukan pengendalian terhadap kode mobile.
- Melakukan back up data.
- Melakukan pengendalian jaringan.
- Melakukan keamanan layanan jaringan.
- Melakukan manajemen *removable media.*
- Melakukan prosedur penanganan informasi.
- Melakukan keamanan sistem dokumentasi.
- Melakukan prosedur dan kebijakan pertukaran informasi.
- Melakukan audit pencatatan informasi.
- Melakukan pemantauan penggunaan sistem.
- Melakukan kebijakan pengendalian akses.
- Melakukan registrasi pengguna pada para petugas operasional TMC PMJ.
- Melakukan manajemen hak istimewa.
- Melakukan pelaksanaan password pengguna pada para petugas operasional TMC PMJ.
- Melakukan tinjauan hak akses pengguna pada para petugas operasional TMC PMJ.
- Melakukan pengendalian penggunaan password.
- Melakukan kebijakan penggunaan layanan jaringan
- Melakukan otentikasi pengguna untuk sambungan eksternal
- Melakukan identifikasi peralatan dalam jaringan
- Melakukan perlindungan remote diagnostic dan konfigurasi port
- Melakukan pemisahan dalam jaringan
- Melakukan pengendalian sambungan jaringan
- Melakukan pengendalian routing (arah) jaringan
- Melakukan prosedur keamanan log-on

- Melakukan otentikasi dan identifikasi pengguna
- Melakukan sistem manajemen password
- Melakukan penggunaan utilitas sistem
- Melakukan pembatasan akses informasi
- Mengisolasi sistem yang sensitif
- Melakukan komputasi mobile dan komunikasi
- Melakukan analisis dan spesifikasi peralatan keamanan
- Melakukan validasi input data
- Melakukan validasi output data
- Melakukan pengendalian software operasional
- Melakukan perlindungan terhadap sistem pengujian data
- Melakukan pengendalian akses ke kode sumber program
- Melaporkan peristiwa keamanan informasi kepada atasan.
- Melaporkan kelemahan keamanan informasi kepada atasan.
- Melakukan prosedur dan pertanggungjawaban.
- Melaksanakan pembelajaran dari insiden keamanan informasi yang terjadi.

c. Pertanggungjawaban:

Tim IT TMC PMJ bertanggung jawab kepada Koordinator TMC PMJ.

6. Petugas Operator TMC PMJ:

a. Tugas:

- Melaksanakan pengorganisasian keamanan informasi secara internal dalam lingkup kerjanya.
- Melaksanakan pertanggungjawaban aset serta menglkasifikasi informasi yang telah ditentukan berkaitan dalam bidang tugasnya.
- Melaksanakan keamanan sumber daya manusia selama bekerja pada TMC PMJ.

- Melaksanakan ketentuan keamanan fisik dan lingkungan yang telah ditetapkan terhadap daerah aman dan peralatan keamanan.
- Melaksanakan komunikasi dan manajemen informasi terhadap operasional prosedur dan pertanggungjawaban komunikasi dan informasi serta media penanganan.
- Melakukan pengendalian akses terhadap manajemen akses pengguna dan pertanggungjawaban para petugas operasional.
- Melaksanakan akuisisi sistem informasi, pengembangan dan pemeliharaan informasi berupa pelaksanaan proses yang benar pada aplikasi.
- Melaksanakan manajemen insiden keamanan informasi berupa pelaporan peristiwa keamanan informasi dan kelemahannya serta melakukan manajemen insiden keamanan informasi dan perbaikan.

b. Tanggung jawab:

- Melaksanakan komitmen manajemen terhadap keamanan informasi.
- Melaksanakan alokasi pertanggungjawaban keamanan informasi.
- Menginventarisir aset informasi yang ada berkaitan dengan bidang tugasnya.
- Melaksanakan penunjukan pertanggungjawaban aset informasi.
- Melaksanakan kesadaran terhadap keamanan informasi, mengikuti pendidikan dan pelatihan.
- Mengamankan bangunan fisik TMC PMJ, ruangan serta fasilitas-fasilitas yang berkaitan dengan lingkup kerjanya.
- Melaksanakan perlindungan terhadap ancaman eksternal dan lingkungan.
- Mengamankan area aman yang berkaitan dengan lingkup kerjanya.
- Melaksanakan pemeliharaan peralatan yang berkaitan dengan lingkup kerjanya.

- Melakukan dokumentasi operasional prosedur terhadap semua kegiatan operasional Tim IT TMC PMJ.
- Melakukan pemisahan tugas terhadap para petugas operasional TMC PMJ.
- Melakukan manajemen *removable media.*
- Melakukan registrasi pengguna pada para petugas operasional TMC PMJ.
- Melakukan pelaksanaan password pengguna pada para petugas operasional TMC PMJ.
- Melakukan pengendalian penggunaan password.
- Melakukan otentikasi pengguna untuk sambungan eksternal.
- Melakukan validasi input data.
- Melakukan validasi output data.
- Melaporkan peristiwa keamanan informasi kepada atasan.
- Melaporkan kelemahan keamanan informasi kepada atasan.
- Melakukan prosedur dan pertanggungjawaban.
- Melaksanakan pembelajaran dari insiden keamanan informasi yang terjadi.

c. Pertanggungjawaban:

Petugas Operator bertanggung jawab kepada Perwira Siaga TMC PMJ.

7. Teknisi:

a. Tugas:

- Melaksanakan pengorganisasian keamanan informasi secara internal dalam lingkup kerjanya.
- Melaksanakan pertanggungjawaban aset serta menglkasifikasi informasi yang telah ditentukan berkaitan dalam bidang tugasnya.
- Melaksanakan keamanan sumber daya manusia selama bekerja pada TMC PMJ.

- Melaksanakan manajemen insiden keamanan informasi berupa pelaporan peristiwa keamanan informasi dan kelemahannya serta melakukan manajemen insiden keamanan informasi dan perbaikan.

b. Tanggung jawab:
   - Melaksanakan komitmen manajemen terhadap keamanan informasi.
   - Melaksanakan alokasi pertanggungjawaban keamanan informasi.
   - Melaksanakan kesadaran terhadap keamanan informasi, mengikuti pendidikan dan pelatihan.
   - Melaporkan peristiwa keamanan informasi kepada atasan.
   - Melaporkan kelemahan keamanan informasi kepada atasan.
   - Melakukan prosedur dan pertanggungjawaban.
   - Melaksanakan pembelajaran dari insiden keamanan informasi yang terjadi.

c. Pertanggungjawaban:

   Teknisi bertanggung jawab kepada Perwira Siaga TMC PMJ.

Menentukan kebijakan keamanan merupakan konsekuensi manajemen Ditlantas Polda Metro Jaya berkaitan dengan rekomendasi yang didapatkan dari hasil identifikasi ancaman dan pendefinisian resiko yang telah dilakukan sebelumnya agar menghasilkan kebijakan keamanan baru yang efektif untuk dilaksanakan bagi para petugas operator TMC PMJ. Kebijakan keamanan pada TMC PMJ merupakan pernyataan tertulis yang dibuat oleh Dirlantas dan menjadi elemen utama bagi penerapan standar keamanan informasi yang diberlakukan untuk menciptakan keamanan informasi sensitif yang terdapat pada TMC PMJ.

Agar kebijakan keamanan informasi ini dapat diterima oleh seluruh komponen personel dan manajemen TMC PMJ maka perlu dilakukan upaya penyamaan persepsi keamanan informasi TMC PMJ dalam bentuk sosialisasi dan pengenalan kebijakan keamanan informasi kepada seluruh komponen personel dan manajemen TMC PMJ. Sosialisasi dan pengenalan ini dapat dilakukan

melalui program pelatihan dan edukasi berkaitan dengan kebijakan baru yang ditetapkan.

Untuk mendapatkan penentuan kebijakan keamanan yang holistik dan komprehensif maka hasil kebijakan ini dituangkan ke dalam surat perintah yang dikeluarkan oleh Direktur Lalu Lintas yang berisi tentang petujuk teknis operasional TMC PMJ beserta Standar Operasional Prosedur pelaksanaan layanan aplikasi yang hendak diterapkan.

5.3.4. Implementasi Pengendalian ISO 27001:2005.

Sebagai tindak lanjut dari penentuan kebijakan keamanan, maka perlu disusun suatu standar operasional prosedur terhadap pelaksanaan operasional TMC PMJ berdasarkan ISO 27001:2005. ISO 27001:2005 merupakan sebuah standar internasional sistem manajemen keamanan informasi yang menetapkan suatu sistem manajemen untuk membawa keamanan informasi di bawah kendali manajemen secara eksplisit.

Seperti yang telah diuraikan pada bab sebelumnya, penyusunan standar operasional prosedur ini dilakukan dengan cara menyempurnakan pelaksanaan kebijakan keamanan informasi yang telah ada dengan mengimplementasikan pengendalian ISO 27001:2005. Artinya bahwa pemilihan golongan pengendalian, tujuan pengendalian serta pengendalian yang hendak diterapkan mengacu pada penyesuaian pada kondisi di TMC PMJ berkaitan dengan identifikasi ancaman yang terjadi dan pendefinisian resiko yang telah ditetapkan sebelumnya, yaitu:

1. Golongan kebijakan keamanan (OKK01):
   a. Tujuan pengendalian kebijakan keamanan informasi (A).
2. Golongan organisasi keamanan informasi (OKK02):
   a. Tujuan pengendalian organisasi internal (A).
   b. Tujuan pengendalian pihak-pihak eksternal (B).
3. Golongan manajemen aset (OKK03):
   a. Tujuan pengendalian pertanggungjawaban aset (A).
   b. Tujuan pengendalian pengklasifikasian informasi (B).
4. Golongan keamanan sumber daya manusia (OKK04):

a. Tujuan pengendalian sebelum bekerja (A).
b. Tujuan pengendalian selama bekerja (B).
c. Tujuan pengendalian pemutusan atau mengubah pekerjaan (C).

5. Golongan keamanan fisik dan lingkungan (OKK05):
   a. Tujuan pengendalian daerah aman (A).
   b. Tujuan pengendalian peralatan keamanan (B).
6. Golongan komunikasi dan manajemen informasi (OKK06):
   a. Tujuan pengendalian operasional prosedur dan pertanggungjawaban (A).
   b. Tujuan pengendalian perlindungan terhadap kode berbahaya dan bergerak (D).
   c. Tujuan pengendalian *back up* (E).
   d. Tujuan pengendalian manajemen keamanan jaringan (F).
   e. Tujuan pengendalian media penanganan (G).
   f. Tujuan pengendalian pertukaran informasi (H).
   g. Tujuan pengendalian pemantauan (J).
7. Golongan kendali akses (OKK07):
   a. Tujuan pengendalian kebutuhan bisnis untuk pengendalian akses (A).
   b. Tujuan pengendalian manajemen akses pengguna (B).
   c. Tujuan pengendalian pertanggungjawaban pengguna (C).
   d. Tujuan pengendalian akses jaringan (D).
   e. Tujuan pengendalian akses terhadap sistem operasi (E).
   f. Tujuan pengendalian akses terhadap aplikasi dan informasi (F).
   g. Tujuan pengendalian komputansi bergerak dan *teleworking* (G).
8. Golongan akuisisi sistem informasi, pengembangan dan pemeliharaan (OKK08).
   a. Tujuan pengendalian proses yang benar pada aplikasi (B).
   b. Tujuan pengendalian keamanan sistem file (D).
9. Golongan manajemen insiden keamanan informasi (OKK09).
   a. Tujuan pengendalian pelaporan peristiwa keamanan informasi dan kelemahan (A).

b. Tujuan pengendalian manajemen insiden keamanan informasi dan perbaikan (B).

10. Golongan manajemen kesinambungan bisnis (OKK10).
    a. Tujuan pengendalian aspek keamanan informasi terhadap manajemen keberlangsungan bisnis (A).
11. Golongan pemenuhan (OKK11).
    a. Tujuan pengendalian pertimbangan sistem audit informasi (C)

Pengelolaan aset tersebut harus dilakukan dengan tepat untuk mengurangi atau memperkecil besarnya resiko karena apabila terjadi kegagalan menangani resiko maka akan mengakibatkan kerugian bagi TMC PMJ. Selanjutnya tujuan pengendalian tersebut di*breakdown* menjadi pengendalian yang telah ditentukan dengan penyesuaian pada kondiri TMC PMJ dan dapat digunakan sebagai standar operasional prosedur pelaksanaan operasional TMC PMJ dalam melaksanakan kebijakan keamanan informasi yang telah dirumuskan. Dengan adanya penerapan golongan pengendalian, tujuan pengendalian dan pengendalian ini diharapkan resiko ancaman maupun gangguan terhadap aset informasi dapat dicegah dan dikurangi.

Berikut ini adalah standar operasional prosedur dengan implementasi pengendalian berdasarkan ISO 27001:2005 yang telah dimodifikasi disesuaikan dengan kondisi keamanan informasi pada TMC PMJ:

Kebijakan Keamanan	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK01	

Tujuan:

Untuk memberikan arahan dan dukungan penuh terhadap keamanan informasi sesuai dengan fungsi komando, koordinasi, komunikasi dan informasi yang dimiliki oleh TMC PMJ terhadap semua aplikasi layanan di dalamnya dalam rangka menciptakan kamseltibcar lantas di wilayah Jakarta Raya.

A. Tujuan Pengendalian Kebijakan Keamanan Informasi:

1. Melakukan dokumentasi kebijakan keamanan informasi.
2. Melakukan tinjauan terhadap kebijakan keamanan informasi.

Petunjuk implementasi:

- Sebuah dokumen kebijakan keamanan informasi harus disetujui oleh Dirlantas selaku manajemen tertinggi di Direktorat Lalu Lintas Polda Metro Jaya, diterbitkan dan dikomunikasikan kepada semua personel komponen TMC PMJ serta pihak-pihak eksternal yang relevan.
- Kebijakan keamanan informasi harus ditinjau ulang sedikitnya tiap setahun sekali atau jika terjadi perubahan signifikan yang terjadi terus-menerus untuk memastikan kesesuaian, kecukupan dan efektifitasnya.

Organisasi Keamanan Informasi	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK02	

Tujuan:

Untuk mengelola keamanan informasi di dalam organisasi TMC PMJ.

A. Tujuan Pengendalian Organisasi Internal:

1. Adanya komitmen manajemen Ditlantas terhadap keamanan informasi.
2. Adanya alokasi pertanggungjawaban keamanan informasi.

B. Tujuan Pengendalian Pihak-Pihak Eksternal:

1. Perjanjian keamanan terhadap pihak ketiga.

Petunjuk implementasi:

- Manajemen Ditlantas harus secara aktif mendukung keamanan informasi dalam organisasi TMC PMJ melalui arahan yang jelas, komitmen yang jelas, penugasan yang jelas serta pertanggungjawaban terhadap keamanan informasi TMC PMJ.
- Semua pertanggungjawaban terhadap keamanan informasi harus ditetapkan secara jelas.
- Perjanjian dengan melibatkan pihak ketiga dalam melakukan akses, pengolahan, berkomunikasi atau mengelola informasi atau fasilitas pengolahan informasi pada TMC PMJ, atau menambahkan aplikasi layanan informasi untuk fasilitas pengolahan informasi harus mencakup semua aspek persyaratan keamanan yang relevan.

Manajemen Aset	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK03	

Tujuan:

A. Tujuan Pengendalian Pertanggungjawaban Aset:

1. Inventarisasi aset.
2. Penunjukan pertanggungjawaban aset.

B. Tujuan Pengendalian Pengklasifikasian Informasi:

1. Pedoman klasifikasi.
2. Pelabelan informasi dan penanganannya.

Petunjuk implementasi:

- Semua aset harus secara jelas diidentifikasi, disusun dan dipertahankan untuk inventarisasi aset penting pada TMC PMJ.
- Semua informasi dan aset penting berkaitan dengan fasilitas aplikasi layanan informasi pada TMC PMJ harus dikuasakan oleh seseorang yang telah ditunjuk dari manajemen.
- Informasi harus diklasifikasikan dalam hal nilai, persyaratan hukum, kepekaan, dan yang kritis bagi TMC PMJ.
- Suatu prosedur aturan yang tepat untuk pelabelan informasi dan penanganannya harus dikembangkan dan dilaksanakan sesuai dengan skema klasifikasi yang telah diadopsi oleh manajemen TMC PMJ

Keamanan Sumber Daya Manusia	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK04	

Tujuan:

Untuk memastikan bahwa para petugas operator operasional dan pihak ketiga pada TMC PMJ memahami tanggung jawab mereka, juga mempertimbangkan kesesuaian peran bagi masing-masing untuk mengurangi resiko pencurian, penipuan atau penyalahgunaan fasilitas layanan aplikasi pada TMC PMJ.

A. Tujuan Pengendalian Sebelum Bekerja:

1. Proses penyaringan.
2. Persyaratan dan kondisi kerja.

B. Tujuan Pengendalian Selama Bekerja:

1. Pertanggungjawaban manajemen.
2. kesadaran terhadap keamanan informasi, pendidikan dan pelatihan.
3. Proses disipliner.

C. Tujuan Pengendalian Pemutusan atau Berubahnya Pekerjaan:

1. Penghentian dari tangguna jawab.
2. Pengembalian aset informasi.
3. Penghapusan hak akses informasi.

Petunjuk implementasi:

- Latar belakang verifikasi pemeriksaan pada semua calon petugas operator operasional dan pihak ketiga pada TMC PMJ harus dilakukan sesuai dengan prosedur yang relevan berdasarkan aturan dan etika, serta sebanding dengan kebutuhan layanan aplikasi dan klasifikasi informasi yang akan diakses.

- Sebagai bagian dari kewajiban yang harus dilakukan, para petugas operator operasional dan pihak ketiga pada TMC PMJ harus setuju dan menandatangani syarat dan kondisi kerja mereka, yang menyatakan bahwa mereka mempunyai tanggung jawab terhadap keamanan informasi pada TMC PMJ.
- Ditlantas harus memerlukan petugas operator operasional dan pihak ketiga pada TMC PMJ untuk menerapkan keamanan informasi yang ditetapkan sesuai dengan kebijakan dan prosedur yang ada.
- Semua petugas operator operasional dan (bila memungkinkan) pihak ketiga pada TMC PMJ harus menerima pendidikan dan pelatihan yang sesuai dengan fungsi pekerjaan mereka.
- Harus ada proses disiplin formal bagi petugas operator operasional yang telah melakukan pelanggaran terhadap keamanan informasi pada TMC PMJ.
- Tanggung jawab untuk melakukan pemberhentian kerja atau perubahan pekerjaan harus didefinisikan secara jelas dan terdokumentasikan.
- Semua petugas operator operasional dan pihak ketiga pada TMC PMJ harus mengembalikan semua aset TMC PMJ yang mereka miliki ketka mereka berhenti dari pekerjaannya.
- Hak akses semua petugas operator operasional dan pihak ketiga pada TMC PMJ terhadapaplikasi layanan dan informasi harus dihapuskan ketika terjadi penghentian kerja.

Keamanan Fisik dan Lingkungan	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK05	

Tujuan:

Untuk mencegah akses fisik yang tidak sah, terjadinya kerusakan dan gangguan kepada fisik bangunan TMC PMJ dan informasinya.

A. Tujuan Pengendalian Area yang Aman:

1. Perimeter keamanan fisik.
2. Pengendalian akses masuk ke dalam gedung TMC PMJ.
3. Pengamanan gedung, ruangan dan fasilitas fisik TMC PMJ.
4. Perlindungan terhadap ancaman eksternal dan lingkungan.
5. Bekerja di area yang aman.

B. Tujuan Pengendalian Peralatan Keamanan:

1. Penempatan dan perlindungan terhadap peralatan.
2. Dukungan utilitas.
3. Keamanan sistem kabel.
4. pemeliharaan peralatan.

Petunjuk implementasi:

- Perimeter keamanan di sekeliling bagunan fisik TMC PMJ harus digunakan untuk melindungi area-area yang berisikan informasi dan aplikasi layanan pengolahan informasi.
- Area yang aman harus dilindungi oleh pengendalian akses masuk yang tepat untuk memastikan bahwa hanya petugas yang berwenang saja yang diperbolehkan melakukan akses masuk gedung.
- Melakukan rancangan terhadap keamanan fisik untuk kantor, ruangan dan fasilitas fisik yang ada pada TMC PMJ.
- Melakukan rancangan dan menerapkan terhadap antisipasi terjadinya kerusakan fisik dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan

sipil dan bentuk lain dari ancaman alam atau bencana buatan manusia.

- Melakukan rancangan terhadap perlindungan fisik dan pedoman untuk bekerja di area aman.
- Peralatan harus diletakkan atau dilindungi untuk mengurangi resiko dan ancaman terhadap lingkungan, serta kesempatan akses yang tidak terotorisasi.
- Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam sarana penunjang.
- Daya dan kabel telekomunikasi pembawa data atau informasi pendukung layanan aplikasi harus dilindungi dari kerusakan maupun pencurian.
- Peralatan yang ada harus dipelihara untuk selalu menjamin ketersediaan dan integritas.

Komunikasi dan Manajemen Informasi	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK06	

Tujuan:

Untuk memastikan kebenaran dan keamanan terhadap fasilitas-fasilitas pengolahan dan pengoperasian informasi dalam rangka kerahasiaan, keutuhan dan ketersediaan informasi.

A. Tujuan Pengendalian Operasional Prosedur dan Pertanggungjawaban:
   1. Pemisahan tugas.

B. Tujuan Pengendalian Perlindungan terhadap Kode Berbahaya dan Bergerak:
   1. Pengendalian terhadap kode berbahaya.

C. Tujuan Pengendalian Back Up:
   1. Back up informasi.

D. Tujuan Pengendalian Manajemen Keamanan Jaringan:
   1. Pengendalian jaringan.
   2. Keamanan layanan Jaringan.

E. Tujuan Pengendalian Media Penanganan:
   1. Manajemen *removable media.*
   2. Prosedur penanganan informasi.
   3. Dokumentasi keamanan sistem.

F. Tujuan Pengendalian Pertukaran Informasi:
   1. Prosedur dan kebijakan pertukaran informasi.

G. Tujuan Pengendalian Pemantauan:
   1. Audit pencatatan informasi.
   2. Penggunaan pemantauan sistem.

Petunjuk implementasi:

- Bidang tugas dan tanggung jawab harus dipisahkan untuk mengurangi peluang modifikasi informasi yang tidak sah, atau penyalahgunaan terhadap aset informasi pada TMC PMJ.
- Melaksanakan prosedur deteksi pencegahan dan pemulihan kontrol untuk melikdungi kode berbahaya maupun terhadap pengguna informasi.
- Salinan cadangan informasi dan perangkat lunak harus disimpan dan diuji secara teratur sesuai dengan kebijakan keamanan yang telah disetujui.
- Jaringan harus dikelola dan dikendalikan secara memadai sebagai perlindungan terhadap ancaman dan untuk menjaga keamanan sistem dan aplikasi layanan yang menggunakan jaringan.
- Fitur keamanan, tingkat layanan danpersyaratan manajemen dari semua layanan informasi harus diidentifikasi, termasuk didalamnya adalah perjanjian layanan aplikasi (apakah tersedia secara inhouse atau outsorcing).
- Harus ada prosedur yang berlaku untuk pengelolaan *removable media.*
- prosedur penanganan dan penyimpanan informasi harus ditetapkan untuk melindungai informasi dari pengungkapan yang tidak terotorisasi atau penyalahgunaan.
- Dokumentasi terhadap sistem harus dilindungi terhadap akses yang tidak sah.
- Kebijakan, prosedur dan pengendalian formal diperlukan untuk melindungi pertukaran informasi melalui penggunaan semua jenis fasilitas komunikasi.
- Log audit berfungsi untuk merekam kegiatan seluruh pengguna tanpa terkecuali, serta disimpan dalam jangka waktu lama untuk emmbantu penyelidikan dan pemantauan kendali akses.
- Prosedur untuk memantau penggunaan fasilitas pengolahan informasi harus dibentuk dan dipantau serta ditinjau ulang secara berkala.

Pengendalian Akses	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK07	

Tujuan:

Untuk melakukan pengendalian akses terhadap informasi.

A. Tujuan Pengendalian Kebutuhan Layanan Aplikasi Informasi untuk Pengendalian Akses:
   1. Kebijakan pengendalian akses.

B. Tujuan Pengendalian Manajemen Pengguna Akses:
   1. Registrasi pengguna.
   2. Manajemen hak istimewa.
   3. Manajemen password pengguna.
   4. Tinjauan hak akses pengguna.

C. Tujuan Pengendalian Pertanggungjawaban Pengguna:
   1. Penggunaan password.

D. Tujuan Pengendalian Akses Jaringan:
   1. Kebijakan pengguna layanan jaringan.
   2. Otentikasi pengguna untuk sambungan eksternal.
   3. Identifikasi peralatan dalam jaringan.
   4. Perlindungan *remote diagnostic* dan konfigurasi port.
   5. Pemisahan dalam jaringan.
   6. Pengendalian sambungan jaringan.
   7. Pengendalian *routing* jaringan.

E. Tujuan Pengendalian Akses terhadap Sistem Operasi:
   1. Prosedur keamanan *log-on*.
   2. Otentikasi dan identifikasi pengguna.

3. Sistem manajemen *password*.
4. Penggunaan utilitas sistem.

F. Tujuan Pengendalian Akses terhadap Aplikasi Layanan dan Informasi:

1. Pembatasan akses informasi.
2. Mengisolasi sistem informasi yang sensitif.

G Tujuan Pengendalian Komputansi Bergerak dan Teleworking.

3. Komputansi mobile dan komunikasi.

Petunjuk implementasi:

- Kebijakan pengendalian akses harus ditetapkan, didokumentasikan, dan ditinjau berdasarkan layanan informasi yang ada serta persyaratan akses keamanan.
- Harus ada pendaftaran pengguna resmi dan prosedur pendaftaran di tempat untuk memberikan atau mencabut akses ke semua sistem dan layanan informasi yang ada.
- Alokasi dan penggunaan hak-hak istimewa harus dibatasi dan dikendalikan.
- Alokasi *password* harus dikontrol melalui proses manajemen formal.
- Manajemen Ditlantas harus meninjau pengguna hak akses secara berkala dengan menggunakan prosedur formal.
- Pengguna harus diminta untuk mengikuti praktik keamanan yang baik dalam pemilihan dan penggunaan *password*.
- Pengguna hanya boleh diberikan akses ke layanan yang telah ditentukan oleh manajemen Ditlantas.
- Metode otentikasi yang telah ditetapkan harus digunakan untuk mengendalikan akses oleh *remote-user*.
- Identifikasi peralatan otomatis harus dianggap sebagai alat untuk proses otentikasi koneksi dari spesifikasi tempat dan peralatan.

- Akses fisik dan virtual terhadap diagnostik dan konfigurasi port harus dilakukan pengendalian.
- Kelompok operator layanan aplikasi, pengguna, dan sistem informasi harus dipisahkan pada jaringan.
- Dalam rangka *sharing* jaringan, khususnya terhadap jaringan internet pada TMC PMJ, kemampuan pengguna untuk terhubung kepada jaringan harus dibatasi sejalan dengan pengendalian akses dan persyaratan aplikasi layanan TMC PMJ.
- Pengendalian *routing* pada jaringan komputer harus dilakukan untuk memastikan bahwa koneksi dan arus informasi tidak melanggar kebijakan pengendalian akses aplikasi layanan informasi pada TMC PMJ.
- Akses terhadap sistem operasi harus dikendalikan oleh perosedur keamanan *log-on*.
- Semua pengguna harus memiliki pengenal unik dalam bentuk *user-id* yang sesuai dengan teknik otentikasi yang telah dipilih untuk penggunaa pribadi dalam rangka memperkuat identifikasi pengguna.
- Sistem yang digunakan untuk mengelola *password* harus bersifat interaktif dan harus memasukkan kualitas *password*.
- Penggunaan program utilitas yang mungkin mampu meng-*override* aplikasi sistem dan pengendalian yang ada, harus dibatasi dan dikendalikan secara ketat.
- Akses terhadap informasi dan fungsi sistem aplikasi oleh pengguna dan komponen TMC PMJ harus dibatasi sesuai dengan kebijakan pengendalian yang telah didefinisikan.
- Sistem uang sensitif harus didedikasi untuk terisolasi dari lingkungan komputasi.
- Langkah-langkah keamanan yang sesuai dengan kebijakan formal harus diterapkan untuk melindungi informasi terhadap resiko komputasi mobile maupun fasilitas komunikasi lainnya.

Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK08	

Tujuan:

Untuk memastikan bahwa keamanan merupakan bagian integral dari sistem informasi pada TMC PM.

A. Tujuan Pengendalian Proses Pengolahan yang benar pada Aplikasi:

1. Validasi input data.
2. Validasi output data.

B. Tujuan Pengendalian Keamanan Sistem File:

1. Pengendalian software operasional.
2. Perlindungan terhadap sistem pengujian data.
3. Pengendalian akses terhadap kode sumber program.

Petunjuk implementasi:

- Proses input data kepada aplikasi harus dilakukan validasi untuk memastikan bahwa data ini adalah benar dan tepat.
- Proses output data dari aplikasi harus dilakukan validasi untuk menjamin bahwa data yang disimpan adalah benar dan sesuai dengan keadaan.
- Harus ada prosedur yang berlaku untuk melakukan pengendalian instalasi *software* pada sistem operasional.
- Akses kepada kode sumber program harus dibatasi.

Manajemen Insiden Keamanan Informasi	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK09	

Tujuan:

Untuk memastikan bahwa pendekatan yang efektif dan konsistensi telah diterapkan dalam manajemen keamanan informasi pada TMC PMJ.

A. Tujuan Pengendalian Pelaporan Peristiwa Keamanan Informasi dan Kelemahan:
   1. Pelaporan peristiwa keamanan informasi.
   2. Pelaporan kelemahan keamanan.

B. Tujuan Pengendalian Manajemen Insiden Keamanan Informasi dan Perbaikan:
   1. Prosedur dan pertanggungjawaban.
   2. Belajar dari insiden keamanan informasi.

Petunjuk implementasi:

- Semua peristiwa keamanan informasi harus dilaporkan secara terus-menerus melalui saluran manajemen yang tepat secepat mungkin.
- Semua komponen personel TMC PMJ dibutuhkan untuk mencatat dan melaporkan setiap kelemahan keamanan informasi untuk dilakukan pengamatan dan mengantisipasinya.
- pertanggungjawaban manajemen dan prosedur ini harus diterapkan untuk memastikan respon yang cepat, efektif dan teratur berkaitan dengan insiden keamanan informasi.
- TMC PMJ harus memiliki mekanisme untuk mengukur dan memantau aktifasi terhadap insiden keamanan informasi berkaitan dengan bentuk, jumlah dan kerugian yang ditimbulkan.

Manajemen Kesinambungan Bisnis	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK10	

Tujuan:

A. Tujuan Pengendalian Aspek Keamanan Informasi terhadap Manajemen Keberlangsungan Bisnis:
   1. Memasukkan keamanan informasi dalam proses keberlangsungan bisnis.
   2. Mengembangkan dan menerapkan rencana kesinambungan dalam keamanan informasi pada TMC PMJ

Petunjuk implementasi:

- Sebuah proses yang dikelola akan dikembangkan dan dipelihara untuk kelangsungan aplikasi layanan informasi pada TMC PMJ yang ditujukan pada kebutuhan persyaratan keamanan informasi demi keberlangsungan bisnis TMC PMJ.
- Rencana ini akan dikembangkan dan dilaksanakan untuk memelihara atau memulihkan kegiatan operasional TMC PMJ serta memastikan ketersediaan infromasi pada tingkat yang diperlukan dan dalam skala waktu yang dibutuhkan untuk mengantisipasi terjadinya gangguan atau kegagalan dalam proses operasional TMC PMJ secara keseluruhan.

Pemenuhan	KEBIJAKAN KEAMANAN INFORMASI
Kode: OKK11	

Tujuan:

Untuk memaksimalkan efektifitas dan meminimalkan gangguan ke atau dari proses *audit sistem informasi.*

A. Tujuan Pengendalian Pertimbangan Sistem Audit Informasi:
   1. Audit Sistem Informasi.

Petunjuk implementasi:

- Persyaratan audit dan kegiatannya yang melibatkan pemeriksaan pada sistem operasional harus terencana dengan kehati-hatian serta menyetujui untuk meminimalkan resiko gangguan pada operasional TMC PMJ.

5.3.5. Penerapan Manajemen Keberlangsungan Bisnis Pada TMC PMJ.

Manajemen keberlangsungan bisnis merupakan aktifitas yang ditujukan untuk menentukan operasional setelah terjadi gangguan pada sistem informasi. Penerapan manajemen ini pada organisasi perlu dilakukan untuk menjaga tiga aspek dasar informasi yaitu kerahasiaan, ketersediaan dan keutuhan informasi dari adanya gangguan dan ancaman yang diprakirakan terjadi.

Dalam penentuan penerapan manajemen keberlangsungan bisnis pada TMC PMJ, dilandasi pada hasil analisis strategi keamanan informasi yang telah dilakukan sebelumnya. Berdasarkan tabel 5..... dinyatakan bahwa berdasarkan identifikasi ancaman yang terjadi dan serta pendefinisian resiko terhadap aset kritis pada TMC PMJ diketahui ada beberapa aset kritis yang perlu dilakukan pengendalian terhadap manajemen keberlangsungan bisnis. Aset-aset tersebut adalah: (a). kelompok IT TMC PMJ; (b). server aplikasi SSB; (c). server SSB 01; (d). server SSB KPTI; (e). server back up data SSB; (f). server website; dan (g). sistem database (oracle, mysql, dll).

Kelompok IT TMC PMJ perlu dilakukan upaya pengelolaan keberlangsungan bisnis mengingat peran sentral yang sangat penting dalam pelaksanaan operasional TMC PMJ yang mengandalkan aplikasi layanan online dengan berbasis komputer. Kelompok IT TMC PMJ ini mempunyai peranan penting berkaitan dengan kerahasiaan, ketersediaan dan keutuhan informasi yang berada di dalam TMC PMJ, Melalui kelompok IT TMC PMJ inilah semua aplikasi layanan informasi pada TMC PMJ diinstalasi, sehingga apabila terjadi gangguan terhadap kelompok IT TMC PMJ saat ini maka secara signifikan juga akan mengakibatkan gangguan terhadap keseluruhan operasional TMC PMJ berkaitan dengan pemahaman aplikasi layanan yang ada, kerahasiaan informasi tersebut dan keutuhan data yang berada di dalamnya.

Tindakan penting yang diterapkan dalam penanganan tindakan terhadap kelompok IT TMC PMJ adalah memberlakukan perjanjian kontrak tertulis yang bersifat mengikat dalam melaksanakan tugasnya. Selain itu juga perlu melakukan proses regenerasi terhadap keberadaan mereka melalui upaya pendidikan dan pelatihan terhadap sumberdaya personel lainnya sehingga mampu menggantikan peran dan fungsi mereka dalam mengelola semua aplikasi layanan informasi apabila terjadi gangguan.

Server aplikasi SSB, server SSB 01, server SSB KPTI, server back up data SSB, server website dan sistem database (oracle, mysql, dll) merupakan aset informasi kritis pada TMC PMJ yang juga perlu dilakukan tindakan manajemen keberlangsungan bisnis. Segala informasi penting menyangkut identifikasi kendaraan bermotor seluruh wilayah Jakarta Raya berada di dalamnya. Ditinjau dari aspek kerahasiaan, ketersediaan dan keutuhan informasinya maka apabila terjadi gangguan terhadap kelima aset ini maka akan mengakibatkan terjadi kerugian yang besar berkaitan dengan keamanan kendaraan bermotor.

Tindakan penting yang dapat diterapkan adalah menempatkan peralatan server-server tersebut tidak berada pada satu lokasi gedung yang sama untuk mengantisipasi ancaman dan gangguan yang mungkin timbul (kebakaran, bencana alam, dll). Selain itu tindakan redudansi dengan cara penduplikasian peralatan juga perlu dilakukan seandainya fasilitas ini rusak atau hancur maka TMC PMJ masih memiliki data informasi penting tersebut.

BAB VI
PENUTUP

6.1. Kesimpulan

Dari hasil penelitian dan pembahasan yang telah dilakukan terhadap manajemen keamanan informasi pada TMC PMJ maka dapat ditarik kesimpulan sebagai berikut:

A. Dalam mengelola TMC PMJ, Direktorat Lalu Lintas Polda Metro Jaya telah melakukan kebijakan keamanan informasi terhadap aset-aset informasi yang ada pada TMC PMJ, namun kebijakan keamanan tersebut belum bisa memberikan keamanan seutuhnya terhadap aset-aset informasi yang ada. Hal ini terbukti dengan terjadinya beberapa gangguan keamanan informasi sehingga menghambat pelaksanaan operasional TMC PMJ.

B. Salah satu penyebab terjadinya gangguan tersebut adalah kebijakan keamanan yang diterapkan belum terdokumentasikan secara otentik sehingga masing-masing komponen pada TMC PMJ belum memahami secara lengkap dan komprehensif tentang tugas dan tanggung jawabnya terkait dengan prosedur keamanan informasi. Selain itu, sebagai akibat dari kebijakan kemanan yang belum terdokumentasi mengakibatkan ada beberapa aset informasi pada TMC PMJ yang tidak mendapatkan tindakan keamanan informasi sehingga nilai resiko yang diterima menjadi tinggi.

C. Untuk mengatasi hal tersebut maka Ditlantas Polda Metro Jaya perlu melakukan perubahan terhadap kebijakan keamanan informasi dan menerapkan tahapan manajemen keamanan informasi berdasarkan pengendalian ISO 27001:2005. Tahapan tersebut meliputi strategi keamanan informasi dan manajemen keberlangsungan bisnis pada TMC PMJ. Pada tahapan strategi keamanan informasi, teridentifikasi bahwa ada beberapa aset informasi yang perlu dilakukan penambahan tindakan keamanan informasi. Agar menghasilkan model keamanan informasi yang optimal maka perlu dilakukan penambahan tindakan keamanan yang telah ada dengan pengendalian dari ISO 27001:2005. Artinya, pemilihan

golongan pengendalian, tujuan pengendalian serta pengendalian yang hendak diterapkan mengacu pada penyesuaian pada kondisi di TMC PMJ berkaitan dengan identifikasi ancaman yang terjadi dan pendefinisian resiko yang telah ditetapkan sebelumnya, yaitu: (a). Golongan kebijakan keamanan; (b). golongan organisasi keamanan informasi; (c). golongan manajemen aset; (d). golongan keamanan sumber daya manusia; (e). golongan keamanan fisik dan lingkungan; (f). golongan komunikasi dan manajemen informasi; (g). golongan kendali akses; (h). golongan akuisisi sistem informasi, pengembangan dan pemeliharaan; (i). golongan manajemen insiden keamanan informasi; (j). golongan manajemen kesinambungan bisnis, dan (k). pemenuhan. Dengan dilandasi hal tersebut maka dapat dilakukan penetapan kebijakan keamanan informasi TMC PMJ dengan mendefinisikan peran, tugas pokok, tanggung jawab dan pertanggungjawaban terhadap komponen TMC PMJ sehingga diharapkan dapat menghasilkan kebijakan keamanan informasi yang mampu bekerja secara efektif dan efisien. Hasil penentuan dari kebijakan keamanan tersebut menghasilkan standar operasional prosedur terhadap sistem keamanan informasi yang ada pada TMC PMJ. Untuk menjaga aktifitas keberlangsungan bisnis pada TMC PMJ maka perlu dilakukan tindakan manajemen berdasarkan pengendalian ISO 27001:2005. Hasil analisis menunjukkan ada beberapa aset informasi pada TMC PMJ yang perlu dilakukan tindakan manajemen keberlangsungan bisnis, yaitu: kelompok IT TMC PMJ, server aplikasi SSB, server SSB 01, server SSB KPTI, server back up data SSB, dan sistem database (oracle, mysql, dll).

6.2. Saran

Saran yang dapat diberikan berkaitan dengan tesis ini adalah:

A. Ditlantas perlu melakukan perubahan kebijakan keamanan informasi berkaitan dengan keamanan informasi sensitif yang dimiliki TMC PMJ dan dituangkan ke dalam bentuk otentikasi dokumentasi yang menyeluruh dan komprehensif.

B. Untuk mendukung terselenggaranya keamanan informasi yang optimal perlu dukungan dalam bentuk pemahaman pentingnya arti keamanan informasi pada TMC PMJ dari seluruh komponen organisasi TMC PMJ, termasuk di dalamnya *top level management*, karena proses strategi keamanan informasi yang efektif dan efisien merupakan hasil identifikasi permasalahan yang dilakukan dengan *bottom-up approach* dan diterapkan dengan *top-down approach*.

C. Penyusunan kebijakan keamanan informasi tersebut harus dilakukan secara periodik 1 kali dalam setahun guna memastikan tindakan keamanan yang tepat dalam mengantisipasi ancaman dan gangguan keamanan informasi yang selalu berubah.

D. Mengingat keterbatasan kemampuan dan pengalaman penulis, maka penulis menyarankan dilakukan penilitian lanjutan berkaitan dengan penentuan kebijakan keamanan informasi untuk melengkapi tesis ini.

DAFTAR PUSTAKA

I. BUKU

Albert, Christopher and Dorofee, Audrey (2002). *Managing Information Security Risk, The OCTAVE Approach*. Boston: Pearson Edication.

Bakharuddin. (2009). "Manajemen Polantas Polda Metropolitan Jakarta Raya dalam Mewujudkan dan Memelihara Kamseltibcar Lantas", (Desertasi, Program Studi Kajian Ilmu Kepolisian Program Pasca Sarjana Universitas Indonesia Jakarta).

Bayley, David H (1994). *Police for the Future*. NewYork: Oxford University Press, Inc.

Davis, Gordon B. (1995), *Kerangka Dasar Sistem Informasi Manajemen, Bagian 1 Pengantar*. (Andreas S. Adiwardana, Penerjemah). Jakarta: PT. Gramedia.

Djamin, Awaloedin (1995). *Administrasi Kepolisian RI*. Bandung: Sanyata Sumanasa Wira.

Djamin, Awaloedin, B.W. Umar, B. Siswanto (1995). *Manajemen Sumber Daya Manusia, Kontribusi Teoritis dalam Pembinaan dan Pengembangan Personel di Lingkungan Polri*. Bandung: Sanyata Sumanasa Wira, Sespim Polri.

Dougherty, Ken (2006). Selecting the Right Business Continuity Strategy. In In Tipton, Harold F. and Krause, Micki (Ed.) *Information Security Management Handbook vol.3* (5th ed.) (pp. 451-456). New York: Auerbach Publications.

Felson, Marcus and Cohen, Robert K (1963). Cesare Beccaria on Crime and Punishment. In Saile, Said et al. (Ed.) (2008). *Himpunan Teori/Pendapat*

para Sarjana yang Berkaitan dengan Kepolisian. Jakarta: Tidak dipublikasikan.

Fischer, Robert J. and Green, Gion (1998). *Introduction to Security, Sexth Edition.* Burlington: Butterworth-Heinemann.

Fitzgerald, Todd (2006). Buliding Management Commtment through Security Councils or Security Councils Critical Success Factors. In Tipton, Harold F. and Krause, Micki (Ed.) *Information Security Management Handbook vol.3 (*5th ed.) (pp. 197-212). New York: Auerbach Publications.

Friedmann, Robert. R (1998). *Community Policing, Comparative Perspectives and Prospects.* (Kunarto, Penerjemah). Jakarta: PT. Cipta Manunggal.

Gibson, William (1984). *Neuromancer.* New York:Ace.

John W. Cresswell (2002). *Research Design, Qualitative & Quantitative Approach.* Jakarta: KIK Press.

Kelana, Momo (2004). *Hukum Kepolisian.* Jakarta: PT Grasindo.

Keputusan Kapolri No. Pol.: Kep/07/I/2005 Tanggal 31 Januari 2005 tentang Struktur Organisasi Dit Lantas Polda Metro Jaya.

Keputusan Presiden RI Nomor 70 Tahun 2002 tentang Organisasi dan Tata Kerja Kepolisian Negara Republik Indonesia

Klockars (1985), Carl B. *The Idea of Police, Volume 3.* Newbury Park-London-New Delhi: SAGE Publications.

Kurnia, Aries Fajar (2006). "Perencanaan Kebijakan Keamanan Informasi Berdasarkan *Information Security Management System* (ISMS) ISO 27001 Studi Kasus Bank XYZ". (Tesis, Program Studi Teknologi Informasi Program Magister Fakultas Ilmu Komputer Universitas Indonesia. Jakarta).

McLeod, Raymond, Jr and P.Schell, George (2008). *SIstem Informasi Manajemen, Edisi 10* (Ali Akbar Yulianto & Afia R. Fitriati, Penerjemah). Jakarta: Salemba Empat.

Mustofa, Muhammad (2007). *Kriminologi, Kajian Sosial Terhadap Kriminalitas, Perilaku Menyimpang dan Pelanggaran Hukum*. Jakarta: Fisip UI Press.

Nasir, Moh. (2003). *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Peraturan Kapolri Nomor 7 Tahun 2008 tentang Pedoman Dasar Strategi dan Implementasi Pemolisian Masyarakat dalam Penyelenggaraan Tugas Polri.

Plains, White (1977). *Data Security Controls and Procedures-A Philosophy for DP Installation*. New York: IBM Corporation.

Price, Sean M. (2006) Developing and Conducting a Security Test and Evaluation. In Tipton, Harold F. and Krause, Micki (Ed.) *Information Security Management Handbook vol.3 (*5th ed.) (pp. 213-240).

Pipkins, Donald L (2000). *Information Security Protecting the Global Enterprise*. New Jersey: Prentice Hall PTR.

Robert Mc.Crie (2001). *Security Operations Management*. Wildwood Avenue: Butterworth-Heinemann.

Rockley, L. E and Hill, D. A (1981). *Security Its Management and Control*. London: Hutchinson Publishing Group.

Santoso, Himawan (1998). "Promosi Jabatan bagi Perwira Pertama" (Tesis, Program Pascasarjana Kajian Ilmu Kepolisian Universitas Indonesia. Jakarta).

Shaurette, Ken M. Technology Convergence and Security: A Simple Risk Management Model. In Tipton, Harold F. and Krause, Micki (Ed.) *Information Security Management Handbook vol.3 (*5th ed.) (pp. 233-240). New York: Auerbach Publications.

Siagian, Sondang P (2001). *Sistem Informasi Manajemen*. Jakarta: Bumi Aksara.

Siagian, Sondang P (2000). *Teori Pengembangan Organisasi*. Jakarta: Bumi Aksara.

Seni Internet Hacking (2008). Jakarta: www.jasakom.com/penerbitan.

Snare, John and Kuper, Eva (2005). *Text for ISO/IEC Final DIS 27001 Information Technology -- Security Techniques . Information security management systems – Requirements.* Germany: DIN Deutshc Institute for Normung.

Shinder, Debra Littlejohn (2002). *Science of the Cybercrime*. United States of America: Syngress Publishing.

Sofana, Iwan (2010). *Cisco CCNA dan Jaringan Komputer*. Bandung: Informatika Bandung.

Sterling, Bruce (1990). *The Hacker Crackdown, Law and Disorder on the Electronic Frontier, Massmarket Paperback.* http://www.lysator.liu.se/etexts/hacker.

Suparlan, Parsudi (2009). *Polisi Indonesia dalam rangka Otonomi Daerah*. Makalah Seminar Hukum Nasional VII BPHN. Departemen Kehakiman RI. Jakarta: Tidak dipublikasikan.

Suparlan, Parsudi (1994). *Metodologi Penelitian Kualitatif*. Jakarta: Program Pasca Sarjana Universitas Indonesia.

Susilo, Djoko (2006). *Implementasi Polmas pada Fungsi Lalu Lintas*. Jakarta: Ditlantas Polri.

Thibault, Edward A, Lynch, Lawrence M, Mc.Bride, R. Bruce (2001) *Proactive Police Management, Fourth Edition*. (Kunarto, Penerjemah). Jakarta: PT. Cipta Manuggal.

Tim Penyusun DItlantas Mabes Polri (2005). *Vademikum Polisi Lalu Lintas*. Jakarta: Tidak dipublikasikan.

Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia No. 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia.

Undang-Undang Republik Indonesia No. 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan.

Zamani (1998). *Manajemen*. Jakarta: Badan Penerbit IPWI.

II. SERIAL

Djamin, Awaloedin (2008). Polri dan Perkembangan Industrial Security di Indonesia. Jakarta: Tidak dipublikasikan.

Golose, Petrus Reinhard (2006). Perkembangan Cyber Crime dan Upaya Penanganannya di Indonesia oleh Polri dalam Buletin Hukum Perbankan dan Kebanksentralan. Volume 4 Nomor 2, Agustus 2006.

Hadiman (2009). Pilihan Sekuriti Menghadapi Kejahatan, Kajian Ketahanan Nasional dan Kajian Pascasarjana Universitas Indonesia. Jakarta: Tidak dipublikasikan.

Hadiman (2009). Observasi Fisik. Jakarta: Tidak dipublikasikan.

Hadiman (2009). Resiko dan Manajemen Resiko. Jakarta: Tidak dipublikasikan.

Hadiman (2009). Security Assesment. Jakarta: Tidak dipublikasikan.

Kepolisian Daerah Metropolitan Jakarta Raya (2009). Overview Polda Metropolitan Jakarta Raya. Jakarta: Tidak dipublikasikan.

Suryadi (2009). Naskah Buku Manajemen Sekuriti di Indonesia. Jakarta: Tidak dipublikasikan.

Suryadi (2010). Penentuan Nilai Parameter terhadap Indikator Analisis Resiko. Jakarta: TIdak dipublikasikan.

III. PUBLIKASI ELEKTRONIK

Detikinet.com, "TMC Polda Metro Jaya Dibobol!". 9 September 2008. http://www.detikinet.com/read/2008/09/09/075957/1002692/323/tmc-polda-metro-jaya-dibobol?browse=frommobile.

Forum Pembaca Kompas. 11 September 2009. http://www.mail-archive.com/forum-pembaca-kompas@yahoogroups.com/msg61007.html

Susanto, Arief (2009). "Pengenalan Komputer". http://www.ariefsusanto.at.ua.

Vivanews, "Hacker mencuri Data 130 Juta Kartu Kredit di Amerika". 11 September 2009. http://teknologi.vivanews.com/news/read/83502-hacker_curi_data_130_juta kartu kredit

Website Ditlantas Polda Metro Jakarta Raya (2006), "Layanan BPKB Ditargetkan Raih ISO 9001". 10 November 2009. http://www.lantas.metro.polri.go.id/news/index. php?id=2&nid=6707

Website International Organization for Standardization (ISO). 11 April 2010. http://www.iso.org/iso/home.htm

Yuhefizar (2003). "Tutorial Komputer dan Jaringan". http://www.IlmuKomputer.com

Lampiran 1: Surat Perintah Penelitian di Ditlantas Polda Metro Jaya.

POLRI DAERAH METRO JAYA
DIREKTORAT LALU LINTAS

SURAT PERINTAH
Nomor : Sprin / 690 / III / 2010

Pertimbangan : bahwa dalam rangka membantu penelitian oleh mahasiswa Universitas Indonesia, di pandang perlu mengeluarkan surat perintah.

Dasar : nota dinas Dir Intelkam Polda Metro Jaya Nomor : B/ND-142/III/2010/Dit Intelkam tanggal 21 Maret 2010, perihal rekomendasi permohonan penelitian oleh mahasiswa Universitas Indonesia a.n. Punky Bhuana Santoso.

DIPERINTAHKAN

Kepada : 1. AKBP TEDDY MINAHASA PUTRA, SH, SIK NRP. 78110326
KASUBDIT REG IDENT DIT LANTAS POLDA METRO JAYA

2. PA SIAGA TMC REGU A, B, CDIT LANTAS PMJ

Untuk : 1. tersebut diatas, disamping melaksanakan tugas dan tanggung jawabnya sehari-hari, agar melayani dan mendampingi mahasiswa Universitas Indonesia dalam rangka membantu Penelitian.

2. identitas mahasiswa yang akan melakukan penelitian adalah :

nama : Punky Bhuana Santoso.
NPM : 0906447406
fakultas : (S2) Kajian Ilmu Kepolisian Program Pascasarjana Universitas Indonesia.
judul riset : "Penerapan Manajemen Keamanan Informasi Pada Traffic Management Center Dit Lantas PMJ Dengan Pengendalian ISO 27001".

3. dalam pemberian data tetap mempertimbangkan kerahasiaan dinas.

4. melaksanakan perintah ini dengan sebaik – baiknya dan penuh rasa tanggung jawab.

Selesai

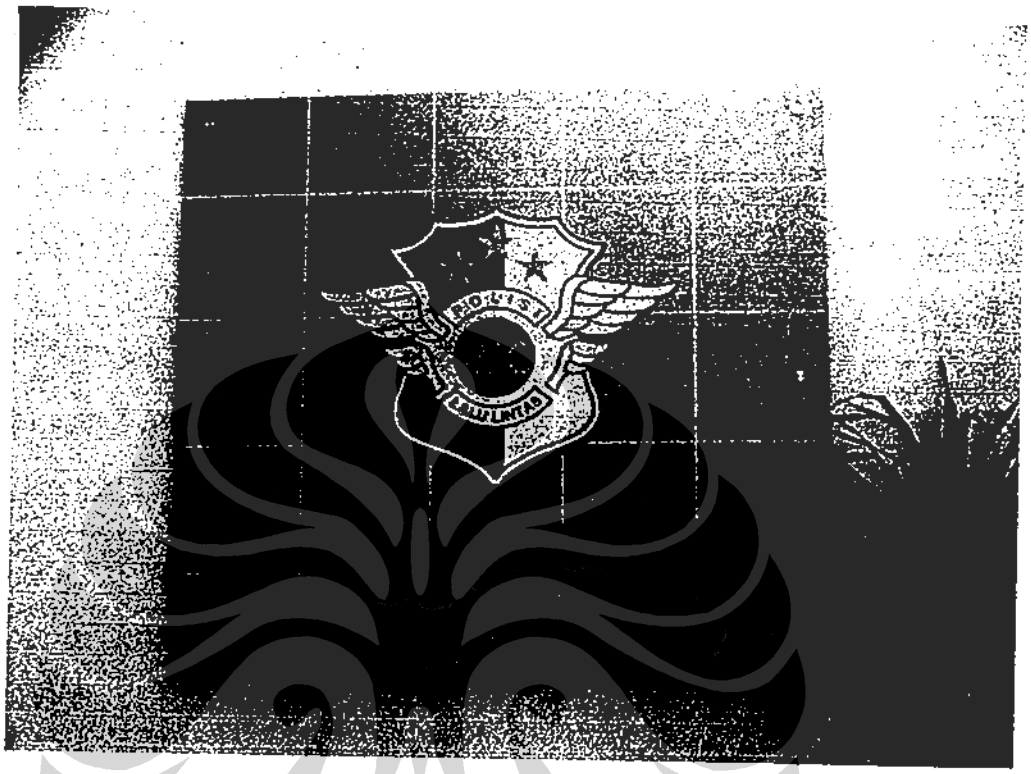
Dikeluarkan di : Jakarta
Pada tanggal : 26 Maret 2010

a.n. DIREKTUR LALU LINTAS POLDA METRO JAYA
WADIR

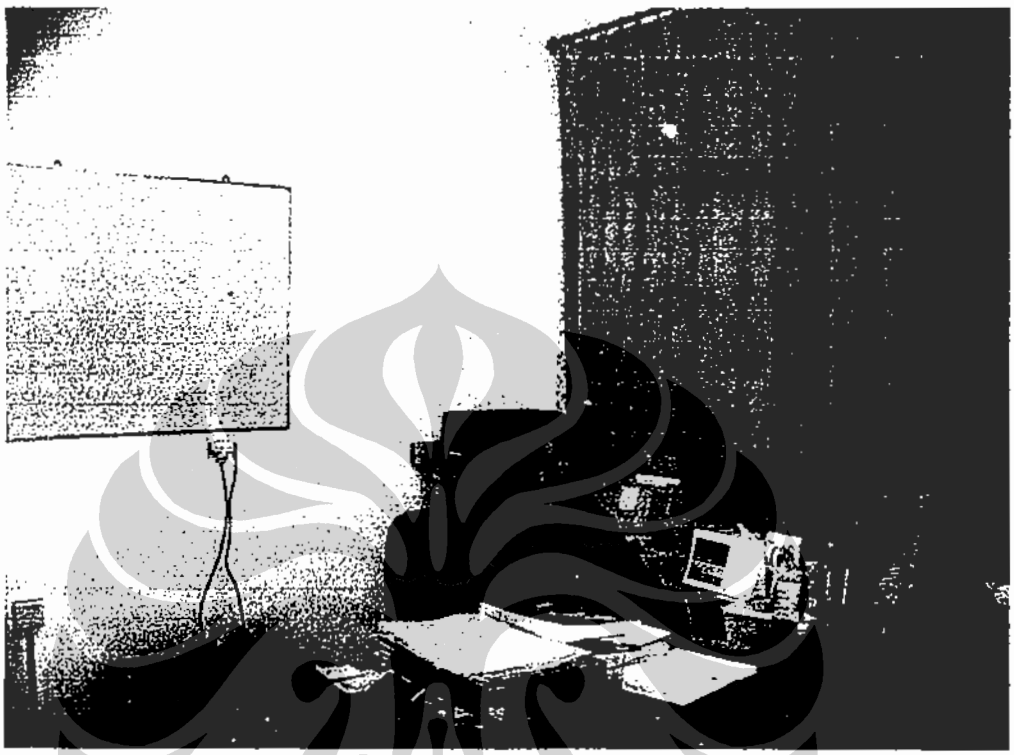
[redacted]
AKBP NRP 67050235

Tembusan :
Dir Lantas Polda Metro Jaya.

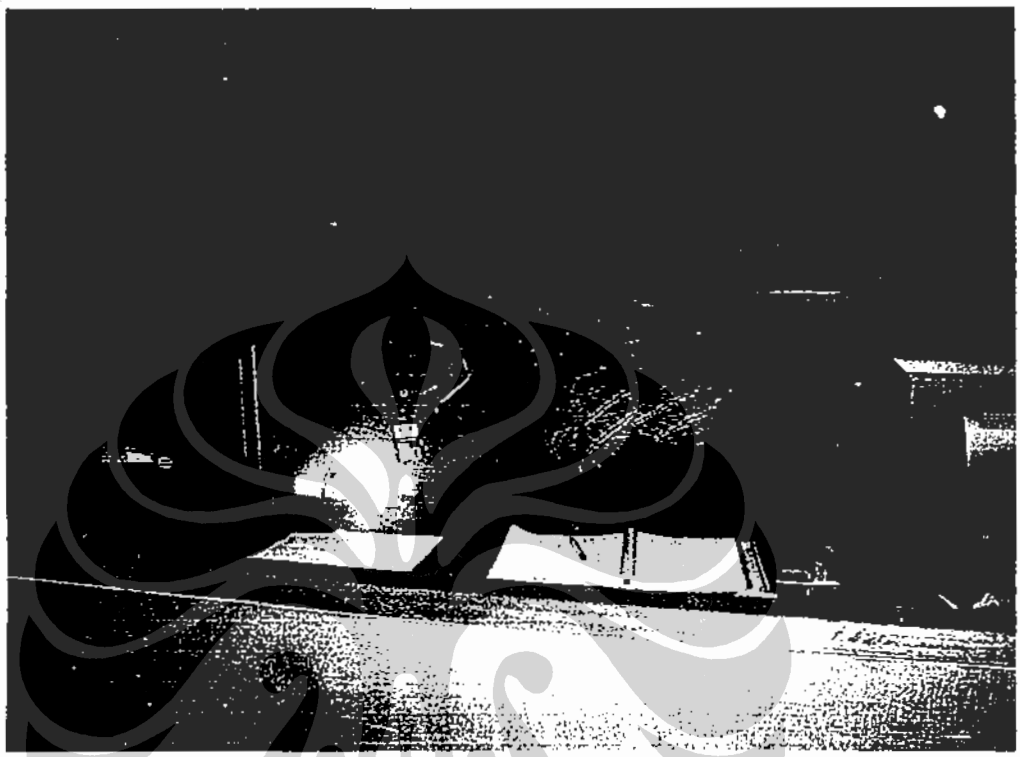
Lampiran 2: Dokumentasi selama Penelitian



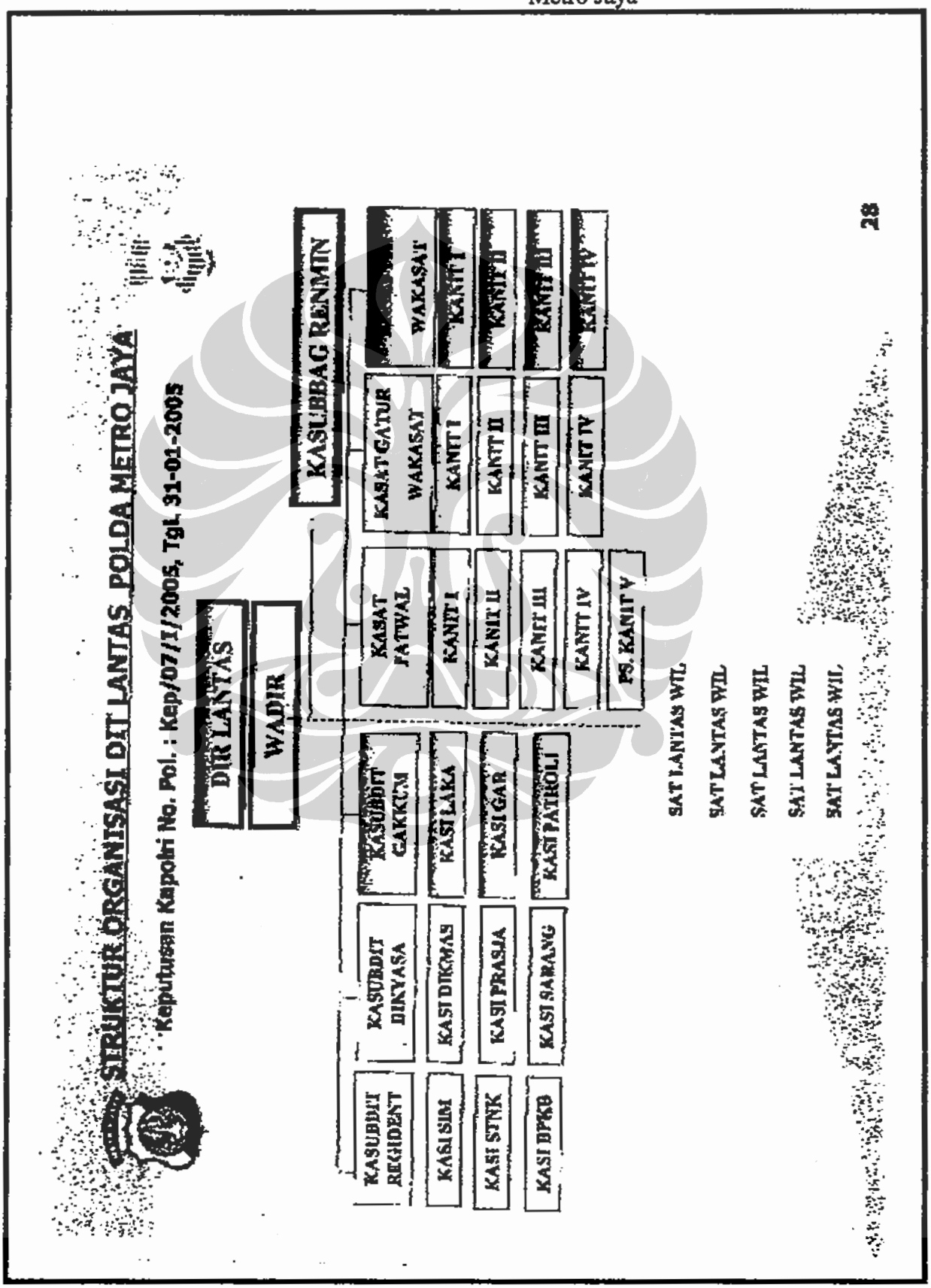
(Lanjutan Lampiran 2)



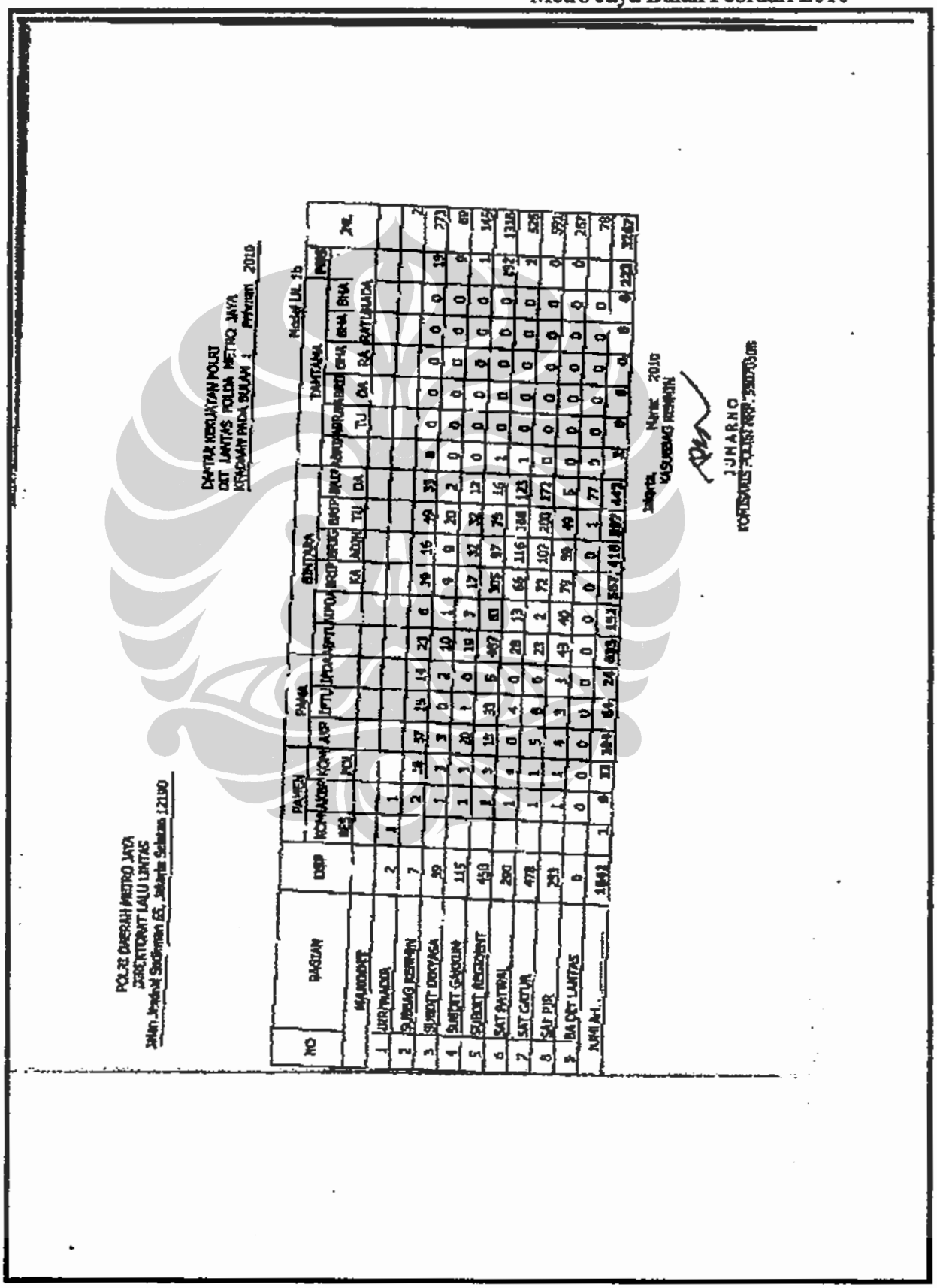
(Lanjutan Lampiran 2)



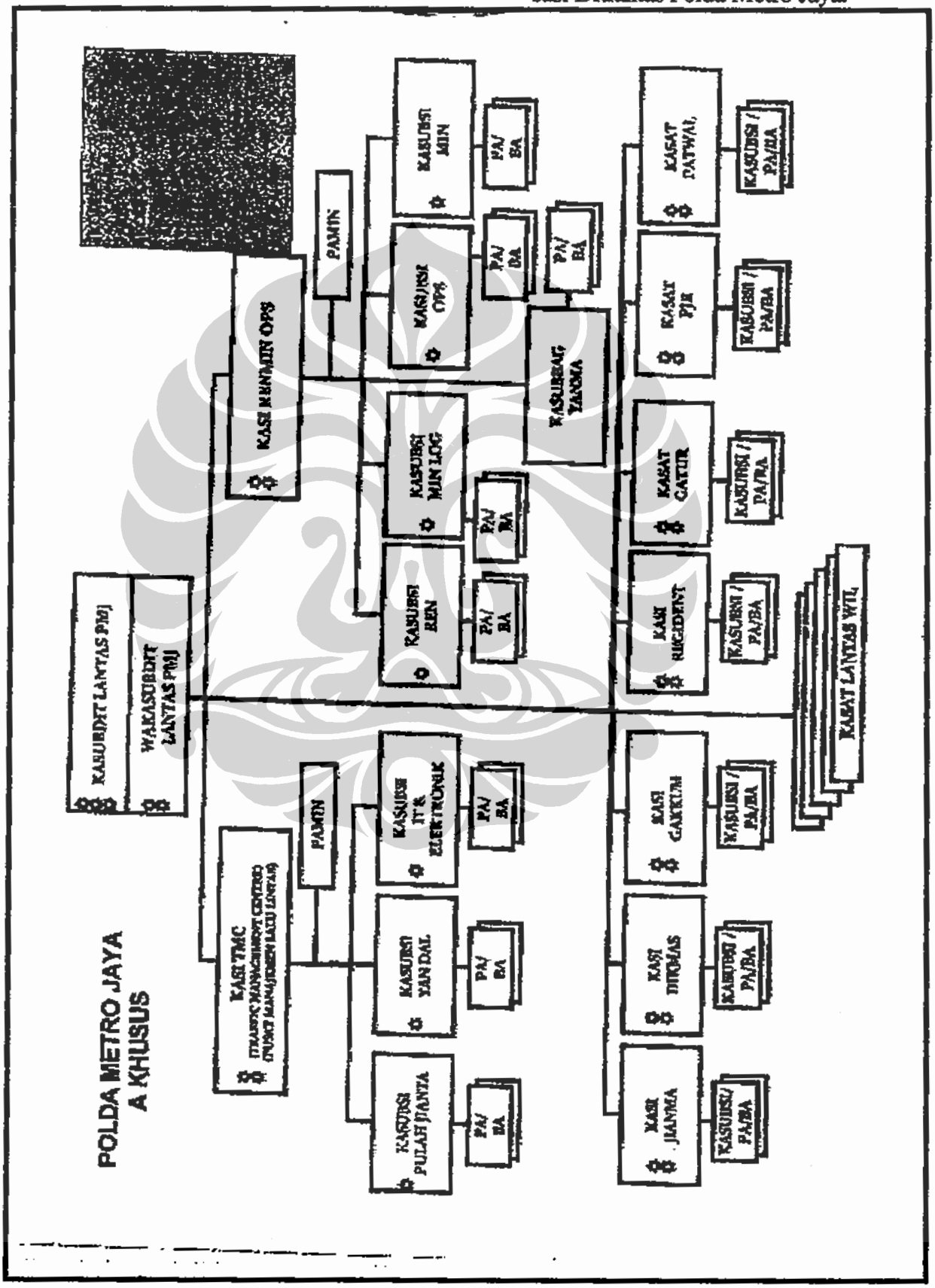
Lampiran 3: Struktur Organisasi Ditlantas Polda Metro Jaya



Lampiran 4: Daftar Kekuatan Polri Ditlantas Polda Metro Jaya Bulan Februari 2010



Lampiran 5: Ajuan Pengembangan Struktur Organisasi Ditlantas Polda Metro Jaya.



Lampiran 6: Surat Perintah Dirlantas tentang Penunjukan Operator Operasional TMC PMJ

POLRI DAERAH METRO JAYA
DIREKTORAT LALU LINTAS

SURAT - PERINTAH
Nomor : Sprin / 39 / I / 2010/Ditlantas

Pertimbangan : Bahwa untuk kepentingan dinas Kepolisian dalam rangka peningkatan pelayanan masyarakat melalui operasional Traffic Management Centre (TMC), dipandang perlu mengeluarkan Surat Perintah.

Dasar :
1. Undang-undang RI No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia.
2. Undang-undang RI No. 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan.
3. Rencana Kerja Ditlantas Polda Metro Jaya Tahun 2010.
4. Rencana Pelaksanaan Quick Wins Ditlantas Polda Metro Jaya Tahun 2010.

DIPERINTAHKAN

Kepada : PARA PAMEN, PAMA DAN BINTARA YANG NAMA DAN PANGKATNYA TERCANTUM DALAM DAFTAR LAMPIRAN SURAT PERINTAH INI

Untuk :
1. disamping melaksanakan tugas dan jabatan sehari – hari, ditunjuk sebagai Operator Operasional TMC.
2. melaksanakan perintah ini dengan sebaik-baiknya serta penuh rasa tanggung jawab.
3. surat perintah ini berlaku sejak tanggal dikeluarkan.

Selesai.

Dikeluarkan di : Jakarta
Pada tanggal : 31 Januari 2010

DIREKTUR LALU LINTAS POLDA METRO JAYA

DIREKTUR

Drs. DJOKO KIROWO, MM
KOMISARIS BESAR POLISI NRP 61120710

Tembusan :
1. Kapolda Metro Jaya
2. Irwasda Polda Metro Jaya
3. Karo Ops Polda Metro Jaya

(Lanjutan Lampiran 6)

POLRI DAERAH METRO JAYA
DIREKTORAT LALU LINTAS

1

LAMPI...d SPRIN DIR LANTAS PMJ
NOMOR : SPRIN/ / I / 2010
TANGGAL : JANUARI 2010

SUSUNAN DAFTAR NAMA OPERATOR TMC

NO.	N A M A	PANGKAT/ N R P	JABATAN	
			STRUKTURAL	BAGIAN
1	2	3	4	5
1.	ARIES SYAHBUDIN, SIK, M. HUM	AKBP 73040251	KASAT PJR	KOORDINATOR TMC
2.	INDRA JAFAR, SIK	KOMPOL 74040421	KASI BPKB	WAKIL KOORDINATOR TMC
3.	ADHIE SANTIKA, SIK	KOMPOL 76120658	KASI SAMAPTA	KATEAM ANALIS
4.	ERWAN KUSBIYANTORO	BRIGADIR 81110208	BA REGIDENT	ANGGOTA
5.	HERU KRISTANTO	BRIPTU 84030357	BA RENMIN	STAF TMC
6.	DODI PURWADI	AIPTU 67060096	BA SNIST JAKTIM	OPR STNK
7.	CATUR	BRIPKA 74030148	BA SNIST JAKBAR	OPR STNK
8.	JOHN SISWANTO	BRIPKA 73060139	BA SNIST JAKSEL	OPR STNK
9.	SUKANTO	BRIPKA 72020194	BA SNIST DEPOK	OPR STNK
10.	KASIL JUMADI K.	BRIPTU 82108636	BA SNIST JAKUT	OPR STNK
11.	SUNARTO	AKP 65060067	PA RENMIN	PA SIAGA A
12.	KRISHAN MENON	AIPTU 62090508	BA RENMIN	OPR CALL CENTRE
13.	MUHAMMAD AR	AIPTU 66120370	BA RENMIN	OPR CALL CENTRE
14.	DAVID GILBERT	BRIPDA 87070599	BA RENMIN	OPR CALL CENTRE
15.	IMAM SUPANGAT	BRIPDA 85082009	BA RENMIN	OPR CALL CENTRE
16.	SUTIMAN	AIPDA 64070026	BA RENMIN	OPR CAKRA (HT)
17.	SUZAN HERBETH SH	BRIPKA 57060679	BA RENMIN	OPR CAKRA (HT)
18.	YUSWANTORO	BRIPKA 66060286	BA RENMIN	OPR CAKRA (HT)
19.	YOKA MULYADI	BRIPTU 82100108	BA RENMIN	OPR CAKRA (HT)
20.	MT. RIDHA	AIPDA 66020251	BA BPKB	OPR CCTV
21.	ARIF RUSY	AIPTU 66030196	BA SIM	OPR CCTV
22.	FAJAR SUBEKTI	BRIPDA 87120227	BA RENMIN	OPR GIS

/ 23. PURWANTO .....

(Lanjutan Lampiran 6)

2

LAMPIRAN "SPRIN DIR LANTAS PMJ
NOMOR : SPRIN/ /I/2010
TANGGAL : JANUARI 2010

NO.	N A M A	PANGKAT/ N R P	JABATAN	
			STRUKTURAL	BAGIAN
23.	PURWANTO	BRIPTU 82120715	BA RENMIN	OPR INTERNET
24.	ARI WIMBO A	BRIPDA 87070916	BA RENMIN	OPR INTERNET
25.	WITRADI	BRIPTU 82060731	BA RENMIN	OPR SMS 1717
26.	SULISTYO TATAK	BRIPTU 87100144	BA RENMIN	OPR SMS 1717
27.	ROMI WIDIATA	BRIPTU 82071006	BA RENMIN	REPORT SMS 1717
28.	CHRISTOPEL	BRIPDA 87080678	BA RENMIN	STAF REGU A
29.	HENDRIK	-	-	TEKNISI TMC A
30.	MUDIANA	AKP 62120479	PA RENMIN	PA SIAGA B
31.	KASMO	AIPTU 59030102	BA SMST BSD	OPR CALL CENTRE
32.	ZULFIKAR	BRIPDA 88020011	BA RENMIN	OPR CALL CENTRE
33.	RIZA RUSHAWAN	BRIPDA 88060098	BA RENMIN	OPR CALL CENTRE
34.	DENI SUMANDAR	BRIPDA 86021836	BA RENMIN	OPR CALL CENTRE
35.	SKIYOKO	AIPTU 61030554	BA RENMIN	OPR CAKRA (HT)
36.	GANDA ARITONANG	AIPDA 65080541	BA RENMIN	OPR CAKRA (HT)
37.	KASYANTO	BRIPKA 63120936	BA RENMIN	OPR CAKRA (HT)
38.	KUSWANDAR	AIPTU 60030554	BA SMST BEKASI	OPR CCTV
39.	MARSONO	BRIPKA 66120471	BA SMST BEKASI	OPR CCTV
40.	LULIK SUPRIYANTO	BRIGADIR 80051211	BA RENMIN	OPR GIS
41.	BROWN PRABOWO	BRIPTU 84080291	BA RENMIN	OPR GIS
42.	HERI NURSIANCA	BRIPTU 83090423	BA RENMIN	OPR INTERNET
43.	ADI KURNIAWAN	BRIPTU 82071411	BA RENMIN	OPR INTERNET
44.	AGUS SUPRIYANTO	BRIPKA 70080178	BA SMST JAKTIM	OPR SMS 1717
45.	IRAWAN PRASETYO	BRIPDA 86021434	BA RENMIN	OPR SMS 1717
46.	RISDIANSYAH	BRIPDA 88061273	BA RENMIN	OPR REPORT SMS 1717
47.	INDRA BANGUN	BRIPDA 87080719	BA RENMIN	STAF REGU B
48	DANY SUDIRMAN	-	-	TEKNISI REGU B

/ 49. SUGENG ....

(Lanjutan Lampiran 6)

3

LAMPIRAN : SPRIN DIR LANTAS PMJ
NOMOR : SPRIN/ /I/ 2010
TANGGAL : JANUARI 2010

NO.	N A M A	PANGKAT/ N R P	JABATAN	
			STRUKTURAL	BAGIAN
49.	SUGENG BUDIONO	AKP 61080484	PA RENMIN	PA SIAGA C
50.	MASRULY F.	BRIPTU 82020899	BA RENMIN .	OPR CALL CENTRE
51.	GARIYANTO	BRIPDA 86101429	BA RENMIN	OPR CALL CENTRE
52.	GANGSAR A.	BRIPDA 87080470	BA RENMIN	OPR CALL CENTRE
53.	FAJAR ANDOYO	BRIPDA 88082272	BA RENMIN	OPR CALL CENTRE
54.	: SENO ADHI B.	BRIPDA 87080361	BA RENMIN	OPR CALL CENTRE
55.	OGAN LOVIANA. APD	BRIPKA 72100207	BA RENMIN	OPR CAKRA (HT)
56.	WIDIA PRAWIRA	BRIPTU 82100265	BA RENMIN	OPR CAKRA (HT)
57.	SUGENG AH.	AIPTU 63020199	BA RENMIN	OPR CAKRA (HT)
58.	TARWONO	AIPTU 59121186	BA RENMIN	OPR CAKRA (HT)
59.	AHMAD MAULANA	BRIPTU 83120714	BA RENMIN	OPR GIS
60.	REZA IRAWAN	BRIPOR 87070452	BA RENMIN	OPR GIS
61.	MASKO VENDS	AIPTU 61090453	BA SMST TGR	OPR CCTV
62.	TARMIN	BRIPKA 71070085	BA SIM	OPR INTERNET
63.	M. IMAM EFENDI	BRIPDA 86121453	BA RENMIN	OPR INTERNET
64.	SATRIO A.	BRIPTU 84100450	BA RENMIN	OPR SMS 1717
65.	DESAB ALQOLLI	BRIPTU 81110782	BA RENMIN	OPR REPORT SMS 1717
66.	M. ANDI PRABOWO	BRIPTU 83010991	BA RENMIN	STAF REGU C
67.	MELWAN FIRDAUS	-	-	TEKNISI REGU C

DIREKTUR LALU LINTAS POLDA METRO JAYA

DIREKTUR

[redacted]
KOMISARIS BESAR POLISI NRP 61120710

Lampiran 7: Absensi Regu Jaga Personel TMC.

POLRI DERAH METRO JAYA
DIREKTORAT LALU LINTAS
TRAFFIC MANAGEMENT CENTRE

ABSENSI PERSONIL TMC REGU A

DINAS : RABU, 14 APRIL 2010
JAM : 07.00—19.00 WIB

NO	NAMA	PANGKAT	OPERATOR	T. TANGAN	KET
1	KRISNAN	AIPTU	CALL CENTRE	1.	
2	ARIFRUBI	AIPTU	CCTV	2.	
3	MUHAMMAD	AIPTU	CALL CENTRE	3.	
4	SUZANSI.M	AIPDA	REPORT&ACTION	4.	
5	M.TRIDIA P	AIPDA	CCTV	5.	
6	SUTIVAN	AIPDA	REPORT&ACTION	6.	
7	YUSWANTORO	BRIPKA	REPORT&ACTION	7.	
8	YOKA M	BRIPTU	REPORT&ACTION	8.	
9	PURWANTO	BRIPTU	PUBLISTER	9.	
10	WIRADI	BRIPTU	SMS	10.	
11	ROBBY W	BRIPTU	REPORT SMS	11.	
12	TATAK	BRIPTU	SMS	12.	
13	GILBERT	BRIPDA	CALL CENTRE	13.	
14	IMAM SUPANGAT	BRIPDA	CALL CENTRE	14.	
15	CHRISTOPEL	BRIPDA	STAF	15.	
16	ARI WIMBO AMARNO	BRIPDA	PUBLISTER	16.	
17	FAJAR SUBERTI	BRIPDA	GIS	17.	
18			STNK	18.	
19			TERMIN	19.	

REKAP ABSEN
JUMLAH :
KURANG :
HADIR :
KETERANGAN
CUTI/IJIN :
SAKIT :

JAKARTA, 14 APRIL 2010

MENGETAHUI:
PA SIAGA "A"

SUNARTO
AKP NRP.65080087

(Lanjutan Lampiran 7)

POLRI DAERAH METRO JAYA
DIREKTORAT LALU LINTAS
TRAFFIC MANAGEMENT CENTRE

ABSENSI PERSONIL TMC REGU B

DINAS : MALAM
HARI / TANGGAL : RABU , 14 APRIL 2010
JAM : 19.00 S/D 07.00 WIB

NO	NAMA	PANGKAT	OPERATOR	TTD
1.	KUSNANDAR	AIPTU	CCTV II	1.....
2.	SRIYOKO	AIPTU	GPS	2.....
3.	KASNO	AIPTU	CALL CENTRE	3.....
4.	G.ARITONANG	AIPDA	CAKRA	4.....
5.	MARSONO	BRIPKA	CCTV I	5..
6.	AGUS.S	BRIPKA	SMS 1717	6
7.	KASYANTO	BRIPKA	CAKRA	7.....
8.	LILIK SUPRIYANTO	BRIGADIR	GIS	8..
9.	HERY M.	BRIPTU	INTERNET	9..
10.	A.KURNIAWAN. SH	BRIPTU	INTERNET	10.
11.	ERWIN.P	BRIPTU	GIS	11.
12.	IRAWAN P	BRIPDA	SMS 1717	12.
13.	INDRA .B	BRIPDA	STAFF	13.
14.	ZULFIKAR ALI M.	DRIPDA	CALL CENTER	14.....
15.	RISDIANSYAH	BRIPDA	GIS	15.
16.	RIZA RUSMAWAN	BRIPDA	CALL CENTER	16.....
17.	DENI SUNANDAR	BRIPDA	CALL CENTER	DIKJUR
18	JIKON.S	BRIPKA	SINK	17.....

REKAP ABSEN
JUMLAH :
KURANG :-
HADIR :
KETERANGAN
DINAS :-
LEPAS DINAS :-
CUTI/IJIN :-
SAKIT :-
TK :-

JAKARTA 15 APRIL 2010
MENGETAHUI
PA SIAGA "B"

MUJIANA
AKP NRP 62120479

Lampiran 8: Rekapitulasi Laporan Masyarakat ke TMC PMJ 1x24 Jam.

POLRI DAERAH METRO JAYA
DIREKTORAT LALU LINTAS

REKAPITULASI LAPORAN MASYARAKAT KE TMC 1 X 24 JAM
MELALUI: SMS1717, CALL CENTRE, INTERNET, RADIO & FAX . HARI/TGL : SELASA , 13 APRIL 2010

SMS 1717	TELEPON	INTERNET	RADIO	FAXIMILE	HT	JUMLAH
1228	341	62	29	4	20	1684

NO.	JENIS LAPORAN	BAG, SAT / WIL																			
		PUO	JTR	RAR	JAL	TOL	TGR KOT	TGR KAB	DPOK	BKS KOT	BKS KAB	JAK.JH	PATWAL	GAKUM	DIKYASA	REG IDENT	GATUR	TL-I	PJR	LAIN-LAIN	JMLH
1	LAKA		4	4	4		1	1											1		18
2	LANGGAR													2							3
3	MACET	2	4	6	22	6													2		42
4	YAN BBN															471					471
5	YAN STNK															427					427
6	YAN BPKB															1					1
7	KK HILANG																				
8	CEK NO POL															308					308
9	SARAN																				
10	KRITIK																				
11	POSITIF																				
12	JUDI				1			1	1											1	4
13	NARKOBA																			1	1
14	PREMANISME		1			1															2
15	ANCMN BOM																				
16	LAIN - LAIN				2									6	2			1	3	398	410
17	JUMLAH	2	9	10	29	7	1	3	1					6	2	1207		1	6	388	1684

Mengetahui
PA SIAGA TMC "C"

SUGENG BUDIONO
AKP NRP 62080462

Mengetahui
PAWAS TMC

JUHARNO
KOMISARIS POLISI NRP 59070808

Jakarta, 14 APRIL 2010
PA REKAP DATA

DESAJI AL CHOILLI
BRIPTU NRP 81110782

Lampiran 9: Laporan Harian TMC PMJ tentang Situasi Kamseltibcar Lantas.

POLRI DAERAH METRO JAYA
DIREKTORAT LALU LINTAS
Jalan Jenderal Sudirman 53, Jakarta 12190

LAPORAN HARIAN
SITUASI KAMSELTIBCAR LANTAS
HARI / TGL : MINGGU, 28 MARET 2010
SELAMA 1 X 24 JAM

1. **DILAPORKAN SITUASI KAMSELTIBCAR LANTAS DI WILAYAH HUKUM POLDA METROPOLITAN JAKARTA RAYA DAN SEKITARNYA , SELAMA 1 X 24 JAM DARI JAM 06.00 S/D 06.00 WIB SEBAGAI BERIKUT :**
   a. **LAKA LANTAS**
      JUMLAH : **3 (TIGA)**
      1). WILAYAH : BEKASI KOTA
      JAM : 05 : 00 WIB
      TKP : JL. . RAYA PERUM JATI SARI JATI ASIH BEKASI KOTA
      YANG TERLIBAT LAKA : SPD MTR B 6903 AN DENGAN PENYEBRANG JALAN
      KORBAN : PENYEBRANG JALAN A/N : LARDI / LK / 24 TH / SWASTA
      ALAMAT : DESA GESING RT 3 / 2 KEC WISMAN TORO WONOKIRI
      TERSANGKA : PENGENDARA KR SPM B 6903 AN A/N : HJ . HERAWATI / PR / 59 TH / SWASTA (MD VER RSUD BEKASI)
      ALAMAT : JL. . SERAYU II BLOK DL 2 NO . 9 BUMI DIRGANTARA CIPAYUNG PAYANGAN
      URAIAN SINGKAT : SPD MTR BERJALAN DARI ARAH UTARA MENUJU ARAH SELATAN SESAMPAINYA DI TKP MENABRAK PENYEBRAG JALAN TSB
      DITANGANI : YANMAS LAKA METRO BEKASI KOTA
      KETERANGAN : KECELAKAAN LALU LINTAS KORBAN MENINGGAL DUNIA (3–3 K)

      2). WILAYAH : JAKARTA PUSAT
      JAM : 15.00 WIB
      TKP : JL . MERDEKA SELATAN DEKAT WISMA ANTARA JAK – PUS
      YANG TERLIBAT LAKA : SPD MTR B 6723 TSV DENGAN PENYEBRANG JALAN
      KORBAN : PENYEBRANG JALAN A/N : ANDI ROHANDI / LK / 20 TH / SWASTA
      ALAMAT : DESIN WAGE RT 3 / 4 CIREBAK KUNINGAN JABAR
      TERSANGKA : PENGENDARA KR SPM B 6723 TSV A/N : HASAN / LK / 62 TH / PEMULUNG (LUKA VER RS . BUDI KEMULIAAN)
      ALAMAT : WATAK PEMULUNG TN . ABANG JAK PUS
      URAIAN SINGKAT : SPD MTR BERJALAN DARI ARAH TIMUR MENUJU ARAH BARAT SESAMPAINYA DI TKP MENABRAK PENYEBRANG JALAN TSB
      DITANGANI : YANMAS LAKA METRO JAKARTA PUSAT
      KETERANGAN : KECELAKAAN LALU LINTAS KORBAN MENGALAMI LUKA (3–3 L)

      3). WILAYAH : JAKARTA PUSAT

(Lanjutan Lampiran 9)

JAM	:	22:00 WIB
TKP	:	TAMAN PERPAKIRAN GEDUNG TVRI
YANG TERLIBAT LAKA	:	KR B 230 DS DENGAN KR B 8848 YW
KORBAN	:	KR B 230 DS A/N H. DIDI SUPRIYANTO, SH.,M9 ANGGOTA DPR-RI
ALAMAT	:	WISMA DPR-RI BLOK D3/28? RT. 8/5 RAWA JATI JAKARTA SELATAN
TERSANGKA	:	KR B 8848 YW A/N KARTO/L/26 TNI/SWASTA
ALAMAT	:	DESA DARMA RADINAN RT. 3/5 KEC. ADI KARANG BANYUMAS
URAIAN SINGKAT	:	PADA WAKTU KR B 230 DS SEDANG PARKIR TIBA-TIBA SATPAM YANG IDENTITASNYA TIDAK DIKETAHUI MENDORONG KR 8848 YW SEHINGGA MENGENAI KR B 230 DS DAN MENGALAMI KERUSAKAN PADA DASHBORD KANAN DEPAN PENYOK DAN PINTU KANAN TIDAK BISA DIBUKA DAN SATPAM YANG MENDORONG KR 8848 YW MENGHILANG SEHINGGA IDENTITASNYA TIDAK DIKETAHUI
DITANGANI	:	LAKA LANTAS PMI
KETERANGAN	:	KECELAKAAN LALU LINTAS KORBAN MENGALAMI KERUGIAN MATERI (3-3 M)

h. PELANGGARAN TILANG DIT LANTAS PMJ

1). PELANGGARAN
- a). TILANG : -
- b). TEGURAN : -

2). BARANG BUKTI YANG DI SITA
- a). SIM : -
- b). STNK : -
- c). KENDARAAN : -
- d). STUK /STCK : -

3). JENIS RANMOR YANG MELANGGAR
- a). BUS : -
- b). TRUCK : -
- c). PICK UP : -
- d). MINIBUS : -
- e). JEEP : -
- f). SEDAN : -
- g). MIKROLET : -
- h). METROMINI : -
- i). TAXI : -
- j). R.3 : -
- k). R.2 : -

4) JENIS PELANGGARAN
- a). RAMBU RAMBU : -
- b). STOP LINE : -
- c). ANGKUTAN PLAT HITAM : -
- d). JALUR BUS WAY : -
- e). NAIK TURUN PENUMPANG : -
- f). LAWAN ARUS : -
- g). 3 IN 1 : -
- h). SAFETY BELT : -
- i). HELM : -
- j). STM LAJUR KIRI : -

(Lanjutan Lampiran 9)

k). TRAFIC LIGHT : -
l). ROTATOR : -
m). MARKA : -
n). MUATAN : -
o) SURAT-SURAT : -
p). KELENGKAPAN KR : -
q) TRUK BUS LAJUR KANAN : -
r). TNKB :
s) LAIN-LAIN : -

c. KEMACETAN LALU LINTAS
1). 08:38 WIB TERJADI KEPADATAN KENDARAAN SEKITAR SENAYAN YANG DISEBABKAN RAMAINYA PENGUNJUNG SENAYAN
2). 10:49 WIB TERJADI KEPADATAN KENDARAAN DEPAN H. SANUSI A ARAH PEJOMPONGAN YANG DISEBABKAN PENUTUPAN JL. SUDIRMAN DAN SELESAI 11:58 WIB
3). 12:53 WIB TERJADI KEPADATAN KENDARAAN SUDIRMAN ARAH BUNDERAN HI YANG DISEBABKAN VOLUME KENDARAAN
4). 13:28 WIB TERJADI KEPADATAN KENDARAAN JATI WARINGIN ARAH PONDOK GEDE YANG DISEBABKAN BANYAKNYA KENDARAAN KELUAR-MASUK TOL.
5). 13.58 WIB TERJADI KEPADATAN KENDARAAN KRANGGAN ARAH GT CIBUBUR YANG DISEBABKAN VOLUME KENDARAAN
6). 14:50 WIB TERJADI KEPADATAN KENDARAAN BLOK TL ASEMKA ARAH HARMONI YANG DISEBABKAN VOLUME KENDARAAN
7). 16:29 WIB TERJADI KEPADATAN KENDARAAN TOL PLUIT ARAH BANDARA TERSENDAT DI GERBANG BANDARA SHITTA YANG DISEBABKAN VOLUME KENDARAAN
8). 16:32 WIB TERJADI KEPADATAN KENDARAAN TOL JAGORAWI ARAH JAKARTA KM 23 YANG DISEBABKAN PEMBANGUNAN PINTU TOL KM 18.6
9). 18:56 WIB TERJADI KEPADATAN KENDARAAN SEMANGGI ARAH PESANGGRAHAN YANG DISEBABKAN VOLUME KENDARAAN
10). 19:06 WIB TERJADI KEPADATAN KENDARAAN JL. LET. JEND. SUPRAPTO ARAH ATRIUM YANG DISEBABKAN VOLUME KENDARAAN
11). 19.09 WIB TERJADI KEPADATAN KENDARAAN JL. KRAMAT RAYA ARAH JL. LET. JEND. SUPRAPTO YANG DISEBABKAN VOLUME KENDARAAN
12). 19:10 WIB TERJADI KPADATAN KENDARAAN POIOK INDAH ARAH LEBAK BULUS YANG DISEBABKAN VOLUME KENDARAAN
13). 19:18 WIB TERJADI KEPADATAN KENDARAAN JL. SALEMBA UI ARAH MATRAMAN YANG DISEBABKAN VOLUME KENDARAAN
14). 19:30 WIB TERJADI KEPADATAN KENDARAAN JL. PROKLAMASI YANG DISEBABKAN VOLUME KENDARAAN

d. UNJUK RASA
- NIHIL

e. GIAT VIP / VVIP
1). PRESIDEN RI : 16:35 WIB START HALIM LANJUT ISTANA NEGARA
16:50 WIB TIBA ISTANA NEGARA
- 17:50 WIB START ISTANA NEGARA LANJUT KEDIAMAN CIKEAS
18:30 WIB TIBA KEDIAMAN CIKEAS

2). IBU PRESIDEN RI : 13:00 WIB START KEDIAMAN CIKEAS LANJUT ISTANA NEGARA
13:30 WIB TIBA ISTANA NEGARA

3). PUTRA - PUTRI PRESIDEN RI : TIDAK ADA LAPORAN

4). WAKIL PRESIDEN RI : TIDAK ADA LAPORAN

(Lanjutan Lampiran 9)

5).	IBU WAKIL PRESIDEN RI	: TIDAK ADA LAPORAN
6)	BAPAK YUSUF KALLA	: TIDAK ADA LAPORAN
7).	IBU YUSUF KALLA	: TIDAK ADA LAPORAN
8).	IBU MEGAWATI	: TIDAK ADA LAPORAN
9).	KETUA MPR RI	: TIDAK ADA LAPORAN
.0).	KETUA DPR RI	: TIDAK ADA LAPORAN
'1).	DELEGASI MALAYSIA	: TIDAK ADA LAPORAN
'2).	KETUA MK	: TIDAK ADA LAPORAN
.3).	IBU DIN	: TIDAK ADA LAPORAN
.4).	POLKAM	: TIDAK ADA LAPORAN
15).	MENDAGRI	: TIDAK ADA LAPORAN
16).	MENPORA	: TIDAK ADA LAPORAN
17).	MENDIKNAS	: TIDAK ADA LAPORAN
18).	PANGLIMA TNI	: TIDAK ADA LAPORAN
19).	KAPOLRI	: 19:55 WIB START KEDIAMAN LANJUT HOTEL DARMAWANGSA : 20:00 WIB TIBA HOTEL DARMAWANGSA : 20:15 WIB START HOTEL DARMAWANGSA LANJUT KEDIAMAN : 2020 WIB TIBA KEDIAMAN
20).	IBU KAPOLRI	: TIDAK ADA LAPORAN
21).	WAKA POLRI	: 18:50 WIB START KEDIAMAN LANJUT TAMIN : 19:00 WIB TIBA TAMIN : 19:20 WIB START TAMIN LANJUT HOTEL DARAMAWANSA : 20:15 WIB TIBA HOTEL DARMAWANGSA : 20:20 WIB START HOTEL DARMAWANGSA LANJUT KEDIAMAN : 20:28 WIB TIBA KEDIAMAN
22).	KEPALA STAF ANGKATAN UDARA	: TIDAK ADA LAPORAN
23).	KASAD AD	: TIDAK ADA LAPORAN
24).	KAPOLDA METRO JAYA	: 19:57 WIB START HOTEL SANGRILA LANJUT KEDIAMAN : 20:15 WIB TIBA KEDIAMAN
25).	WAKA POLDA METRO JAYA	: TIDAK ADA LAPORAN
26).	GUBERNUR DKI JAKARTA	: TIDAK ADA LAPORAN

(Lanjutan Lampiran 9)

33). WAKIL GUBERNUR DKI JAKARTA : TIDAK ADA LAPORAN

f. GANGGUAN TRAFFIC LIGHT
   1). TL. AL AZHAR BRAWIJAYA : 10.00 S/D 14.00 WIB JAKARTA SELATAN

g. POHON TUMBANG
   - NIHIL.

h. BANJIR / GENANGAN AIR / DAM BOCOR
   - NIHIL.

i. KEBAKARAN
   - NIHIL

j. GANGGUAN KENDARAAN RODA DUA / RODA EMPAT
   NIHIL.

k. ANCAMAN BOM
   - NIHIL.

l. JALAN BERLUBANG DAN GALIAN
   1). BERLUBANG
   JAKARTA PUSAT
   1. JL.KRAMAT RAYA SAMPING FLY OVER ARAH UTARA MENJELANG TL SIMPANG 5
   2. JL.LETJEN SUPRAPTO TURUNAN GALUR ARAH SENEN
   3. JL.KRAMAT RAYA SEBELUM TANJAKAN PO
   4. JL.SALEMBA RAYA ARAH TIMUR TL.MATRAMAN
   5. TL.PINTU BESI
   6. JL. LETJEN SUPRAPTO JALUR LAMBAT ARAH SIMPANG LIMA SENEN

   JAKARTA BARAT
   1. JL.DAAN MOGOT DEPAN JAYA MIX
   2. SEPANJANG JL.RAYA DAAN MOGOT DEPAN SAMSAT
   3. JL.ASEMKA DEKAT TL
   4. PERLINTASAN KERETA API TAMBORA
   5. JL.S.PARMAN DEPAN TWIN PLAZA
   6. JL.TUBAGUS ANGKE MENJELANG REL KERETA
   7. GROGOL ARAH ROXY JL. RUSAK
   8. KOLONG GROGOL ARAH LATEMENTEN
   10. DEPAN MEDIKA ARAH PESING
   11. JL. KAMAL RAYA ARAH TOL / CENGKARENG

   JAKARTA UTARA
   1. CILINCING SEBELUM RUKOTAN
   2. KOJA BOULEVARD SEMPER ARAH UI
   3. KELUAR TERMINAL TERPADU
   4. RS.MITADINATA DEPAN PLTU KIRI DAN KANAN
   5. PIT DEPAN MASJID AL KHUSNAH
   6. PEDEMANGAN KAMPUNG BANDAN
   7. KELAPA GADING PINTU 3

   JAKARTA TIMUR
   1. JL.RAYA BEKASI PINTU I KAWASAN INDUSTRI PULO GADUNG SAMPING PTC
      JALUR BUSWAY SEBELUM TL MATRAMAN
   2. JUALUR BUS WAY SEBELUM TL MATRAMAN
   3. JL RAYA BOGOR DEPAN MAYASARI ARAH SELATAN TUTUP GORONG JEBLOS
   4. DEPAN PGC ARAH SELATAN

(Lanjutan Lampiran 9)

5. PERTIGAAN BUDAYA CONDET
6. JL. MATRAMAN ARAH KAMPUNG MELAYU

JAKARTA SELATAN
1. JL.PAL ATRIHAN
2. JL.PUTIAT RAYA JL.INDEX PASAR JUMAT
3. SETIABUDI TL CILUAMI ARAH CILEDUK

2). GALIAN
JAKARTA TIMUR
- NIHIL

JAKARTA PUSAT
- NIHIL

JAKARTA UTARA
- NIHIL

JAKARTA BARAT
- NIHIL

JAKARTA SELATAN
1. JL.BLANGIT RAYA DEPAN GRAHA INTI FAYZI ARAH SELATAN (GALIAN KABEL)
2. JL. RAYA RADIO DALAM

2. LAPORAN MASYARAKAT MELALUI TMC
a. JUMLAH LAPORAN

1).	SMS 1717	:	442
2).	TELEPHONE	:	129
3).	INTERNET	:	37
4).	RADIO	:	15
5).	FAXIMILE	:	-
6).	HT	:	10

b. JENIS LAPORAN YANG DI SAMPAIKAN
1). MASALAH LALU LINTAS

LAKA	:	3
- LANGGAR	:	3
KEMACETAN	:	32
- PELAYAN SIM	:	90
PELAYANAN STNK	:	55
- PELAYANAN BPKB	:	-
- KR HILANG	:	-
- CEK NOPOL	:	177
- SARAN MASYARAKAT	:	-
- KRITIK POLRI	:	2
- PENILAIAN POSITIF	:	-

2). MASALAH DI LUAR LALU LINTAS

- JUDI	:	3
- MIRAS / NARKOBA	:	1
- PREMANISME	:	2
ANCAMAN BOM	:	-
- LAIN – LAIN	:	265

3). LAPORAN INTERNET

- JUMLAH PENGUNJUNG	:	3.169
- BERITA YANG DI INPUT		

(Lanjutan Lampiran 9)

OLEH ANGGOTA TMC	:	8
- KONSULTASI MASYARAKAT	:	5
- FORUM	:	2
- ENTOSIS	:	14
- GALERI FOTO	:	-
- OPINI MASYARAKAT	:	-
- LINK	:	-
- HEADLINE NEWS	:	-
HILANG TEMU RANMOR	:	
- EMAIL	:	3
- LAIN- LAIN	:	-

3. DEMIKIAN LAPORAN INI DI BUAT SEBAGAI BAHAN PERTIMBANGAN PIMPINAN LEBIH LANJUT

Jakarta , 29 Maret 2010
PA SIAGA " A "

SUNARTO
AKP NRP. 65080087

Lampiran 10: Kendala dan Saran dari Masing-Masing Operator TMC PMJ.

KENDALA DAN SARAN DARI MASING – MASING OPERATOR TMC

NO	OPERATOR	KENDALA	SARAN
1.	SMS	1. JARINGAN SMS KADANG LAMBAT. 2. OPERATOR SMS KESULITAN DALAM MENJAWAB PERTANYAAN YANG MENYANGKUT BIAYA (SIM , STNK & BPKB). 3. DATA SSB MASIH ADA YANG TIDAK VALID DENGAN DATA KPTI PADAHAL DATA SSB SERING DIGUNAKAN OLEH PETUGAS DI LAPANGAN UNTUK MELAKUKAN PENINDAKAN, SEHINGGA ADA BEBERAPA KENDARAAN MASYARAKAT YANG DITANGKAP PADAHAL DATANYA SUDAH BENAR. 4. TIDAK BISA CEK JUMLAH SMS MASUK KATEGORI CEK NOPOL YANG DIFORMAT OTOMATIS OLEH KOMPUTER.	1. DIBENAHI MASALAH JARINGAN AGAR LEBIH CEPAT. 2. MOHON PETUNJUK KEPADA PIMPINAN. 3. AGAR DATA SSB SELALU DI UPDATE. 4. DAPAT CEK JUMLAH SMS MASUK KATEGORI CEK NOPOL YANG DIFORMAT OTOMATIS KOMPUTER.
2.	CALL CENTRE	1. NADA TELEPON MASUK TAPI TIDAK BUNYI. 2. OPERATOR CALL CENTRE KESULITAN DALAM MENJAWAB PERTANYAAN YANG MENYANGKUT BIAYA (SIM , STNK & BPKB). 3. KURANG MENGUASAI [illegible] RADIO.	1. PERBAIKAN LINE TELEPON. 2. MOHON PETUNJUK PIMPINAN. 3. AGAR DILAKUKAN PELATIHAN ON AIR.

(Lanjutan Lampiran 10)

3.	INTERNET	1. JARINGAN KADANG LAMBAT. 2. RAM KURANG SEHINGGA LOADING KOMPUTER SANGAT LAMA. 3. OPERATOR INTERNET KESULITAN DALAM MENJAWAB PERTANYAAN YANG MENYANGKUT BIAYA (SIM , STNK & BPKB). 4. KURANG MAHIR DALAM PEMBUATAN BERITA 5. TIDAK ADA KAMERA UNTUK DOKUMENTASI. 6. TIDAK ADA SARANA TRANSPORTASI PENUNJANG UNTUK DATANG KE TKP APABILA ADA KEJADIAN MENONJOL. 7. JARANG DAPAT TEMBUSAN TENTANG KEGIATAN DARI SATKER / SUBDIT.	1. PERBAIKAN JARINGAN. 2. TAMBAH RAM. 3. MOHON PETUNJUK PIMPINAN. 4. AGAR PERSONIL INTERNET DIBERIKAN PEMBEKALAN TENTANG JURNALISTIK. 5. INVENTARIS KAMERA. 6. AGAR TAMPILAN/TAMPLATE DESIGN WEBSITE DIPERBAHARUI 7. DITAMBAH PAGELINK KHUSUS PHOTO AGAR MASYARAKAT MUDAH / BISA MENGIRIM GAMBAR PERISTIWA YANG TERJADI KE WIBESITE LANTAS. 8. MEMBUAT WIBESITE VERSI MOBILE AGAR MUDAH DIBUKA DISEMUA JENIS HANDPHONE 10. HARDISK POKET UNTUK PENYIMPINAN DATA / BACKUP DATA (BELUM ADA) 12. SETIAP ADA KEGIATAN SATKER / SUBDIT TMC DAPAT TEMBUSAN AGAR LANGSUNG BISA DI INFORMASIKAN KEPADA MASYARAKAT (CONTOH: GOES TO CAMPUS, INOVASI LAYANAN REGIDENT, SOSIALISASI)

4.	GIS	1. PROGRAM TRAFFIC LIGHT DI PETA GIS MASIH ADA YANG KURANG. 2. LAKA YANG SUDAH DISIMPAN DI GIS TIDAK BISA DIHAPUS APABILA INGIN DILAKUKAN PENGEDITAN JIKA TERJADI KESALAHAN INPUT. 3. LAKA ONLINE SELALU TERLAMBAT DIINPUT OLEH PETUGAS LAKA WILAYAH. 4. DATA PLOTING POS TETAP WILAYAH MASIH SERING TERLAMBAT DIINPUT OLEH OPERATOR WILAYAH	1. PENAMBAHAN TITIK TRAFFIC LIGHT PADA PETA GIS. 2. DILAKUKAN PERBAIKAN. 3. AGAR PETUGAS LAKA WILAYAH SEGERA INPUT KE LAKA ONLINE SETELAH KEJADIAN KECELAKAAN YG SUDAH DILAKUKAN PENYIDIKAN. 4. AGAR PLOTING POS TETAP WILAYAH DI ISI TEPAT WAKTU.
5.	CCTV	1. CCTV MILIK POLDA YANG BERFUNGSI HANYA 1 (SATU) DARI 50 KAMERA CCTV. 2. TIDAK BISA MENGGERAKKAN CCTV MILIK PEMDA DKI.	1. AGAR DILAKUKAN PERBAIKAN. 2. BISA MENGGERAKAN CCTV MILIK PEMDA DKI.
6.	GPS	1. GPS KURANG MAKSIMAL KARENA BANYAK YANG TIDAK BERFUNGSI. 2. TEKNISI GPS JARANG KONTROL KE TMC. 3. KENDARAAN YANG DIPASANGI GPS MASIH ADA YANG TIDAK SESUAI DENGAN NO BODY.	1. AGAR DILAKUKAN PERBAIKAN. 2. TEKNISI SERING KONTROL GPS. 3. NO BODY KENDARAAN HARUS SESUAI DENGAN GPS.
7.	HT	1. HT YANG ADA KURANG MAKSIMAL DAN JUMLAHNYA KURANG (HT BELUM PERNAH DIGANTI).	1. PENAMBAHAN 2 HT DAN 3 BATRE AGAR MEMAKSIMALKAN OPERATOR DALAM BERKOORDINASI DENGAN PETUGAS DI LAPANGAN SEKALIGUS BISA MEMONITOR JALUR ATAS DAN JALUR BAWAH.

(Lanjutan Lampiran 10)

8.	STAFF	1. KOMPUTER SERING OVERHEAT (APABILA PANAS SERING MATI) 2. TIDAK ADA JARINGAN LAN YANG TERHUBUNG DENGAN KOMPUTER STAFF	1. AGAR KOMPUTER DIPERBAIKI 2. AGAR DIPASANG JARINGAN UNTUK MEMUDAHKAN PENGAMBILAN DATA / LAPORAN DARI MASING-MASING OPERATOR 3. SETIAP AKAN ADA KUNJUNGAN KE TMC SELALU DIKASIH TEMBUSAN SEBELUMNYA.
9	TEKNISI	1 SERING KELUAR KANTOR TMC TANPA BERKOORDINASI TERLEBIH DAHULU DENGAN PA SIAGA SEHINGGA KETIKA DIBUTUHKAN SULIT DICARI. 2 JIKA DIMINTA TOLONG OLEH ANGGOTA TMC PERIHAL PERBAIKAN KOMPUTER / JARINGAN INTERNET TERKESAN PASIF TANPA ADA TINDAK LANJUT	1. STATUS TEKNISI AGAR DIPERHARTIKAN KARENA SELAMA INI MASIH BELUM ADA KEJELASAN. (PHL)
10	PA SIAGA	1 PENGAWASAN KEPADA OPERATOR TMC LEMAH SEHINGGA BANYAK ALAT PENDUKUNG YANG BERUBAH FUNGSI. 2. APLAUSE PIKET SERING TERLAMBAT KHUSUSNYA YANG PIKET MALAM.	1. PENINGKATAN PENGAWASAN KEPADA OPERATOR TMC UNTUK MENGGUNAKAN ALAT SEBAGAI MESTINYA & APLAUSE PIKET MALAM SESUAI DENGAN JAM NYA YANG TELAH DITENTUKAN
11	TMC	1. MEJA ANGGOTA CAKRA JANGAN DIBIARKAN KOSONG HAL INI MENYULITKAN JIKA OPERATOR SMS ATAU CAL CENTRE MENINDAKLANJUTI LAPORAN DARI MASYARAKAT. 2. ALAS KAKI DILEPAS KETIKA MEMASUKI RUANGAN TMC. 3. BUANG LUDAH , ABU & PUNTUNG ROKOK JANGAN DIBUANG SEMBARANGAN	1. ARAHAN DARI PIMPINAN.

(Lanjutan Lampiran 10)

(Lanjutan Lampiran 10)

JAKARTA, 29 MARET 2010

STAFF TMC

HERU KRISTANTO
BRIPTU NRP 84030337

MENGETAHUI
PA SIAGA TMC

MUJIANA
AKP NRP 62120479

ISO/IEC JTC 1/SC 27 **N4472**

ISO/IEC JTC 1/SC 27/WG 1 **N14472**

REPLACES: N4186

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Text for FDIS ballot

TITLE: **Text for ISO/IEC Final DIS 27001[1] Information technology — Security techniques — Information security management systems — Requirements**

SOURCE: Project Editors: John Snare and Eva Kuiper

DATE: 2005-04-15

PROJECT: 27001

STATUS: In accordance with resolution 13 (contained in SC27 N4599) of the 17th SC27 Plenary meeting held in Vienna, Austria, 2005-04-18/19 this document has been sent to the ISO Central Secretariat (ITTF) for 2-month FDIS letter ballot.

It is circulated within SC27 for information.

ACTION ID: ITTF

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC27 Chairman
M. De Soete, SC27 Vice-Chair
T. Humphreys, K. Naemura, M. Ohlin, WG Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 42 + 1 (ATTACHMENT 1 = explanatory report)

[1] document renumbered from 24743 to 27001
(Vienna resolution 7 of 17th SC 27 Plenary, April 2005)

Secretariat ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.ni.din.de/sc27

Reference number of working document: ISO/IEC JTC/1SC 27 N 4472

Date: 2005-05-14

Reference number of document: ISO/IEC FDIS 27001

Committee identification: ISO/IEC JTC 1/SC 27/WG 1

Secretariat: DIN

Information technology — Security techniques — Information security management systems — Requirements

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: Final Draft International Standard
Document language: English

Contents

Page

Foreword iv

0 Introduction v
0.1 General v
0.2 Process approach v
0.3 Compatibility with other management systems vi

1 Scope 1
1.1 General 1
1.2 Application 1

2 Normative references 1

3 Terms and definitions 2

4 Information security management system 3
4.1 General requirements 3
4.2 Establishing and managing the ISMS 3
4.2.1 Establish the ISMS 3
4.2.2 Implement and operate the ISMS 5
4.2.3 Monitor and review the ISMS 6
4.2.4 Maintain and improve the ISMS 7
4.3 Documentation requirements 7
4.3.1 General 7
4.3.2 Control of documents 8
4.3.3 Control of records 8

5 Management responsibility 8
5.1 Management commitment 8
5.2 Resource management 9
5.2.1 Provision of resources 9
5.2.2 Training, awareness and competence 9

6 Internal ISMS audits 9

7 Management review of the ISMS 10
7.1 General 10
7.2 Review input 10
7.3 Review output 10

8 ISMS improvement 11
8.1 Continual improvement 11
8.2 Corrective action 11
8.3 Preventive action 11

Bibliography 34

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

0 Introduction

0.1 General

This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

This International Standard can be used in order to assess conformance by interested internal and external parties.

0.2 Process approach

This International Standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the following process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a) understanding an organization's information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;

c) monitoring and reviewing the performance and effectiveness of the ISMS; and

d) continual improvement based on objective measurement.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) process model, which is applied to structure all ISMS processes. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6, 7 and 8.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002)[1)] governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

---

1) OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

EXAMPLE 1

A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2

An expectation might be that if a serious incident occurs — perhaps hacking of an organization's eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.

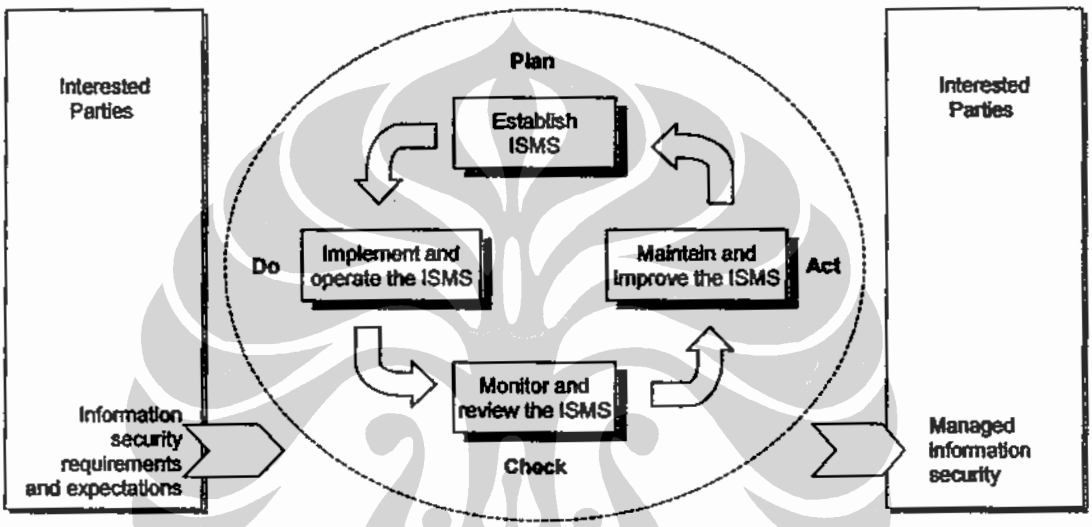


Figure 1 — PDCA model applied to ISMS processes

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

0.3 Compatibility with other management systems

This International Standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards. Table C.1 illustrates the relationship between the clauses of this International Standard, ISO 9001:2000 and ISO 14001:2004.

This International Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

Information technology — Security techniques — Information security management systems — Requirements

IMPORTANT - This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application. Compliance with an ISO/IEC Standard does not in itself confer immunity from legal obligations.

1 Scope

1.1 General

This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the *context of the organization's overall business risks. It specifies requirements for the implementation of security* controls customized to the needs of individual organizations or parts thereof.

The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

NOTE 1: References to 'business' in this standard should be interpreted broadly to mean those activities that are core *to the purposes for the organization's existence.*

NOTE 2: ISO/IEC 17799 provides implementation guidance that can be used when designing controls.

1.2 Application

The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature. Excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard.

Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons. Where any controls are excluded, claims of conformity to this International Standard are not acceptable unless such exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements.

Note: If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this Standard within this existing management system.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
asset
anything that has value to the organization

[ISO/IEC 13335-1:2004]

3.2
availability
the property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 13335-1:2004]

3.3
confidentiality
the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-1:2004]

3.4
information security
preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

[ISO/IEC 17799:2005]

3.5
information security event
an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

[ISO/IEC TR 18044:2004]

3.6
information security incident
a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[ISO/IEC TR 18044:2004]

3.7
information security management system (ISMS)
that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.8
integrity
the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004]

3.9
residual risk
the risk remaining after risk treatment

[ISO/IEC Guide 73:2002]

3.10
risk acceptance
decision to accept a risk

[ISO/IEC Guide 73:2002]

3.11
risk analysis
systematic use of information to identify sources and to estimate the risk

[ISO/IEC Guide 73:2002]

3.12
risk assessment
overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002]

3.13
risk evaluation
process of comparing the estimated risk against given risk criteria to determine the significance of risk

[ISO/IEC Guide 73:2002]

3.14
risk management
coordinated activities to direct and control an organization with regard to risk

[ISO/IEC Guide 73:2002]

3.15
risk treatment
process of selection and implementation of measures to modify risk

[ISO/IEC Guide 73:2002]

NOTE: In this International Standard the term "control" is used as a synonym for "measure".

3.16
statement of applicability
documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.

NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security.

4 Information security management system

4.1 General requirements

The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization's overall business activities and the risks they face. For the purposes of this International Standard the process used is based on the PDCA model shown in Figure 1.

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS

The organization shall do the following.

a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets, technology, and including details of and justification for any exclusions from the scope (see 1.2).

b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that:

   1) *includes a framework for setting objectives and establishes an overall sense of direction and* principles for action with regard to information security;

   2) takes into account business and legal or regulatory requirements, and contractual security obligations;

   3) aligns with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place;

   4) establishes criteria against which risk will be evaluated (see 4.2.1c)); and

   5) has been approved by management.

   NOTE: For the purposes of this document, the ISMS policy is considered as a superset of the information security policy. These policies can be described in one document.

c) Define the risk assessment approach of the organization.

   1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

   2) *Develop criteria for accepting risks and identify the acceptable levels of risk. (see 5.1f)).*

   The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

   NOTE: There are different methodologies for risk assessment. Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3 (Guidelines for the Management of IT Security: Techniques for the Management of *IT Security).*

d) Identify the risks.

   1) Identify the assets within the scope of the ISMS, and the owners[2] of these assets.

   2) Identify the threats to those assets.

   3) Identify the vulnerabilities that might be exploited by the threats.

   4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

e) Analyse and evaluate the risks.

   1) Assess the business impact upon the organization that might result from a security failure, taking into *account the consequences of a loss of confidentiality, integrity or availability of the assets.*

   2) Assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

---

[2] The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.

3) Estimate the levels of risks.

4) Determine whether the risk is acceptable or requires treatment using the risk acceptance criteria established in 4.2.1c)2).

f) Identify and evaluate options for the treatment of risks.

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policies and the criteria for risk acceptance (see 4.2.1c)2));

3) *avoiding risks; and*

4) transferring the associated business risks to other parties, e.g. insurers, suppliers.

g) Select control objectives and controls for the treatment of risks.

Controls objectives and controls shall be selected and implemented to meet the requirements identified *by the risk assessment and risk treatment process. This selection shall take account of the criteria for* accepting risks (see 4.2.1c)) as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover these requirements.

The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

NOTE: Annex A contains a comprehensive list of control objectives and controls that have been found to be commonly relevant in organizations. Users of this International Standard are directed to Annex A as a starting point for control selection to ensure that no important control options are overlooked.

h) Obtain management approval of the proposed residual risks.

i) Obtain management authorization to implement and operate the ISMS.

j) Prepare a Statement of Applicability.

A Statement of Applicability shall be prepared that includes the following:

1) the control objectives and controls, selected in 4.2.1g) and the reasons for their selection;

2) the control objectives and controls currently implemented (see 4.2.1e)2)); and

3) the exclusion of any control objectives and controls in Annex A and the justification for their exclusion.

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

4.2.2 Implement and operate the ISMS

The organization shall do the following.

a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5).

b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) Implement controls selected in 4.2.1g) to meet the control objectives.

d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3c)).

NOTE: Measuring the effectiveness of controls allow managers and staff to determine how well controls achieve planned control objectives.

e) Implement training and awareness programmes (see 5.2.2).

f) Manage operations of the ISMS.

g) Manage resources for the ISMS (see 5.2).

h) Implement procedures and other controls capable of enabling prompt detection of and response to security incidents (see 4.2.3).

4.2.3 Monitor and review the ISMS

The organization shall do the following.

a) Execute monitoring and review procedures and other controls to:

1) promptly detect errors in the results of processing;

2) promptly identify attempted and successful security breaches and incidents;

3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) help detect security events and thereby prevent security incidents by the use of indicators; and

5) determine whether the actions taken to resolve a breach of security were effective.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, effectiveness measurements, suggestions and feedback from all interested parties.

c) Measure the effectiveness of controls to verify that security requirements have been met.

d) Review risk assessments at planned intervals and review the level of residual risk and identified acceptable risk, taking into account changes to:

1) the organization;

2) technology;

3) business objectives and processes;

4) identified threats;

5) effectiveness of the implemented controls; and

6) external events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate.

e) Conduct internal ISMS audits at planned intervals (see 6).

NOTE: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for internal purposes.

f) Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified (see 7.1).

g) Update security plans to take into account the findings of monitoring and reviewing activities.

h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).

4.2.4 Maintain and improve the ISMS

The organization shall regularly do the following.

a) Implement the identified improvements in the ISMS.

b) Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.

c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

d) Ensure that the improvements achieve their intended objectives.

4.3 Documentation requirements

4.3.1 General

Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and the recorded results are reproducible.

It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

The ISMS documentation shall include:

a) documented statements of the ISMS policy (see 4.2.1b)) and objectives;

b) the scope of the ISMS (see 4.2.1a));

c) procedures and controls in support of the ISMS;

d) a description of the risk assessment methodology (see 4.2.1c));

e) the risk assessment report (see 4.2.1c) to 4.2.1g));

f) the risk treatment plan (see 4.2.2b));

g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3c));

h) records required by this International Standard (see 4.3.3); and

i) the Statement of Applicability.

NOTE 1: Where the term "documented procedure" appears within this International Standard, this means that the procedure is established, documented, implemented and maintained.

NOTE 2: The extent of the ISMS documentation can differ from one organization to another owing to:

- the size of the organization and the type of its activities; and
- the scope and complexity of the security requirements and the system being managed.

NOTE 3: Documents and records may be in any form or type of medium.

4.3.2 Control of documents

Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

a) approve documents for adequacy prior to issue;

b) review and update documents as necessary and re-approve documents;

c) ensure that changes and the current revision status of documents are identified;

d) ensure that relevant versions of applicable documents are available at points of use;

e) ensure that documents remain legible and readily identifiable;

f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification;

g) ensure that documents of external origin are identified;

h) ensure that the distribution of documents is controlled;

i) prevent the unintended use of obsolete documents; and

j) apply suitable identification to them if they are retained for any purpose.

4.3.3 Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.

Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS.

EXAMPLE

Examples of records are a visitors' book, audit reports and completed access authorization forms.

5 Management responsibility

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing an ISMS policy;

b) ensuring that ISMS objectives and plans are established;

c) establishing roles and responsibilities for information security;

d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;

e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1);

f) deciding the criteria for accepting risks and for acceptable risk levels;

g) ensuring that internal ISMS audits are conducted (see 6); and

h) conducting management reviews of the ISMS (see 7).

5.2 Resource management

5.2.1 Provision of resources

The organization shall determine and provide the resources needed to:

a) establish, implement, operate, monitor, review, maintain and improve an ISMS;

b) ensure that information security procedures support the business requirements;

c) identify and address legal and regulatory requirements and contractual security obligations;

d) maintain adequate security by correct application of all implemented controls;

e) carry out reviews when necessary, and to react appropriately to the results of these reviews; and

f) where required, improve the effectiveness of the ISMS.

5.2.2 Training, awareness and competence

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are *competent to perform the required tasks by:*

a) determining the necessary competencies for personnel performing work effecting the ISMS;

b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;

c) evaluating the effectiveness of the actions taken; and

d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

6 Internal ISMS audits

The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

a) conform to the requirements of this International Standard and relevant legislation or regulations;

b) conform to the identified information security requirements;

c) are effectively implemented and maintained; and

d) perform as expected.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results (see 8).

NOTE: ISO19011:2002, Guidelines for quality and/or environmental management systems auditing, may provide helpful guidance for carrying out the internal ISMS audits.

7 Management review of the ISMS

7.1 General

Management shall review the organization's ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. *The results of the reviews shall be clearly documented and records shall be maintained* (see 4.3.3).

7.2 Review input

The input to a management review shall include:

a) *results of ISMS audits and reviews;*

b) feedback from interested parties;

c) techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;

d) *status of preventive and corrective actions;*

e) vulnerabilities or threats not adequately addressed in the previous risk assessment;

f) results from effectiveness measurements;

g) follow-up actions from previous management reviews;

h) any changes that could affect the ISMS; and

i) recommendations for improvement.

7.3 Review output

The output from the management review shall include any decisions and actions related to the following.

a) Improvement of the effectiveness of the ISMS.

b) Update of the risk assessment and risk treatment plan.

c) Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:

   1) business requirements;

   2) security requirements;

   3) business processes effecting the existing business requirements;

   4) regulatory or legal requirements;

   5) contractual obligations; and

   6) levels of risk and/or risk acceptance criteria.

d) Resource needs.

e) Improvement to how the effectiveness of controls is being measured.

8 ISMS improvement

8.1 Continual improvement

The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).

8.2 Corrective action

The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. The documented procedure for corrective action shall define requirements for:

a) identifying nonconformities;

b) determining the causes of nonconformities;

c) evaluating the need for actions to ensure that nonconformities do not recur;

d) determining and implementing the corrective action needed;

e) recording results of action taken (see 4.3.3); and

f) reviewing of corrective action taken.

8.3 Preventive action

The organization shall determine action to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

a) identifying potential nonconformities and their causes;

b) evaluating the need for action to prevent occurrence of nonconformities;

c) determining and implementing preventive action needed;

d) recording results of action taken (see 4.3.3); and

e) reviewing of preventive action taken.

The organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment.

NOTE: Action to prevent nonconformities is often more cost-effective than corrective action.