BAB V

PERANCANGAN TATA KELOLA TI

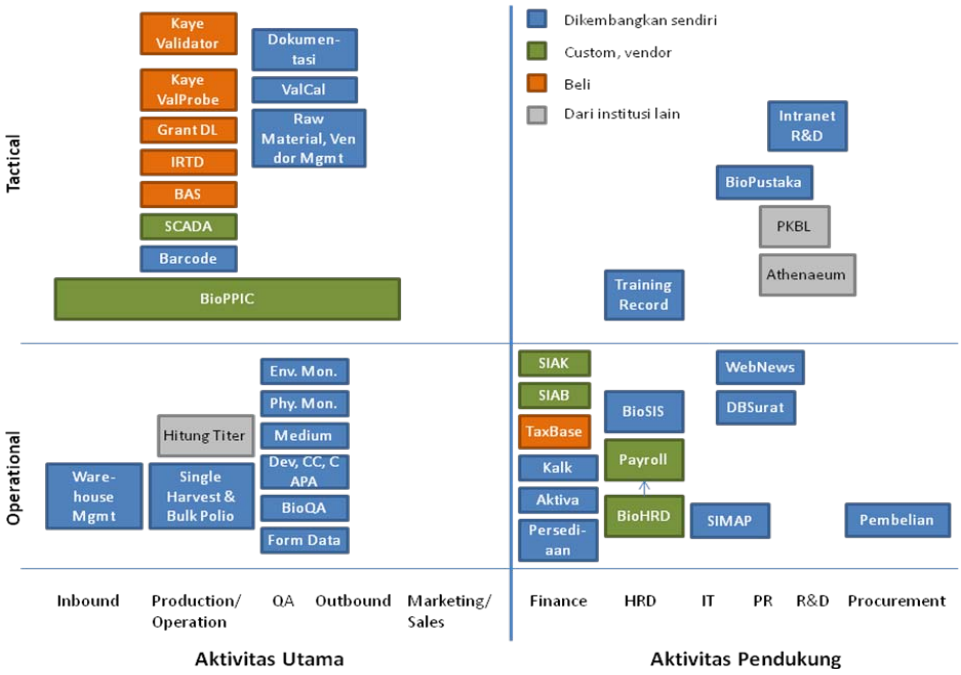
Pada bagian ini akan menjelaskan tentang kondisi dan analisis TI, pengukuran kinerja TI, tingkat kematangan proses DS5 beserta rekomendasi jangka pendek dan jangka panjang yang perlu dilakukan untuk meningkatkan tingkat kematangan.

V.1 Kondisi Teknologi Informasi

Kondisi TI perlu dijelaskan baik dari segi arsitektur, infrastruktur dan kebijakannya sebagai dasar analisis kondisi TI secara umum maupun yang terkait dengan proses memastikan keamanan sistem.

V.1.1 Arsitektur Sistem Informasi

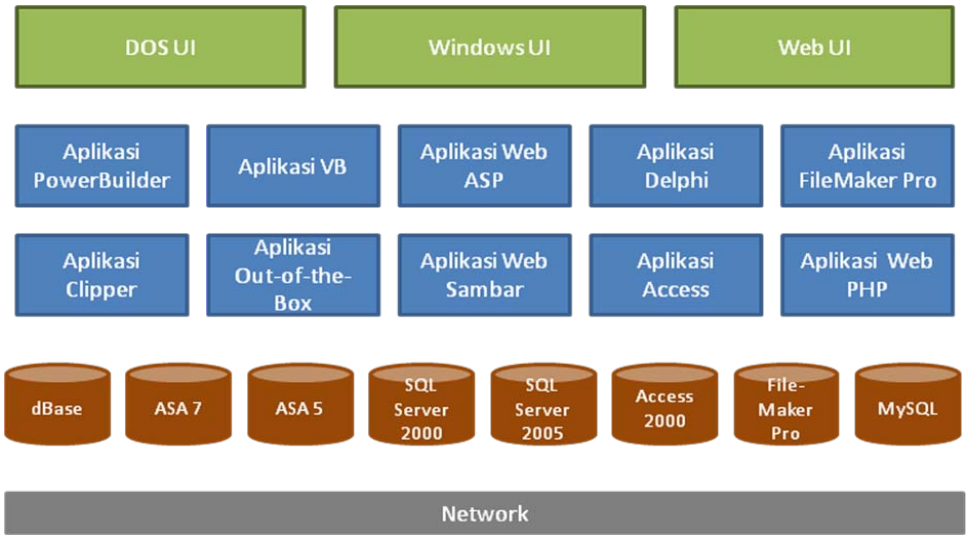
Arsitektur sistem informasi PT Bio Farma (Persero) saat ini dapat dilihat pada Gambar IV.1. Pada gambar tersebut memperlihatkan pemetaan aplikasi yang ada dilihat dari dua sudut pandang, yaitu tingkat manajemen dan proses bisnis. Tingkat manajemen memperlihatkan tingkat strategik (*strategic*), taktis (*tactical*) dan operasional (*operational*). Saat ini belum ada aplikasi yang dapat ditempatkan di tingkat strategik. Proses bisnis dibedakan menjadi proses utama dan proses pendukung, yang kemudian memperlihatkan unit-unit kerja dalam organisasi.



Gambar V.1 Arsitektur Sistem Informasi PT Bio Farma

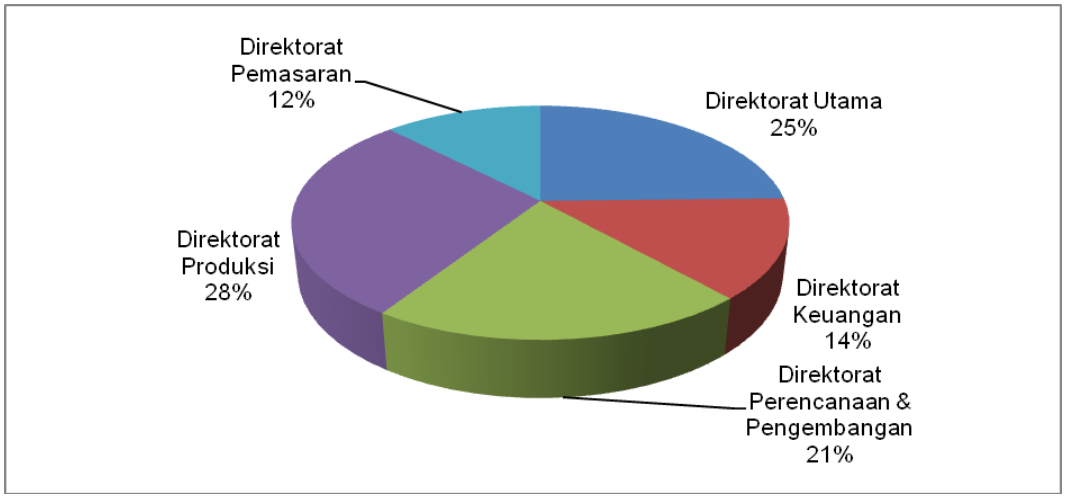
V.1.2 Infrastruktur Teknologi Informasi

Arsitektur TI di PT Bio Farma saat ini dapat dilihat pada Gambar IV.2. Pada gambar tersebut bahwa terdapat berbagai antarmuka pengguna, *platform* pembuatan aplikasi/bahasa pemprograman dan *database*.



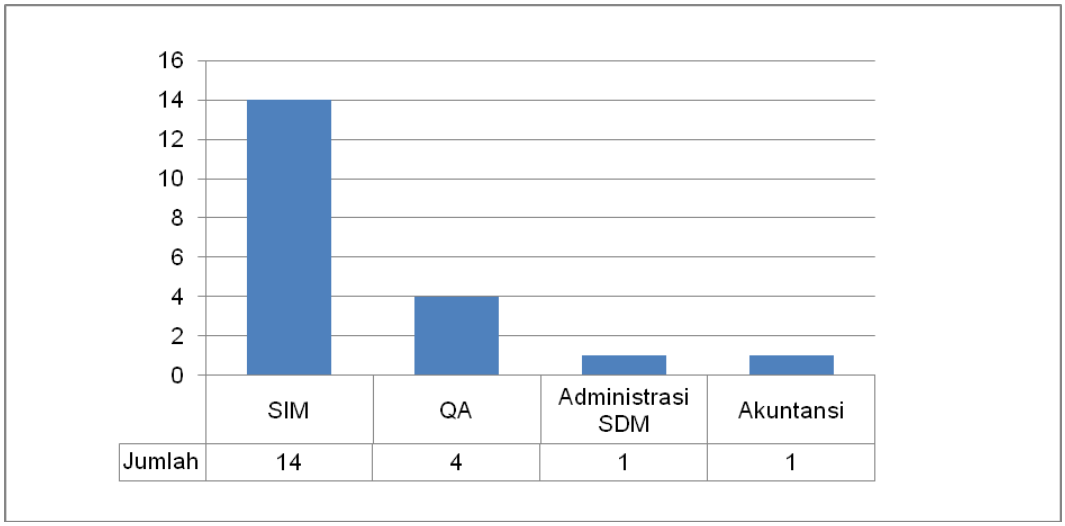
Gambar V.2 Arsitektur TI PT Bio Farma

Penyebaran komputer *end user* di PT Bio Farma dapat dilihat pada Gambar IV.3.



Gambar V.3 Penyebaran Komputer *end user*

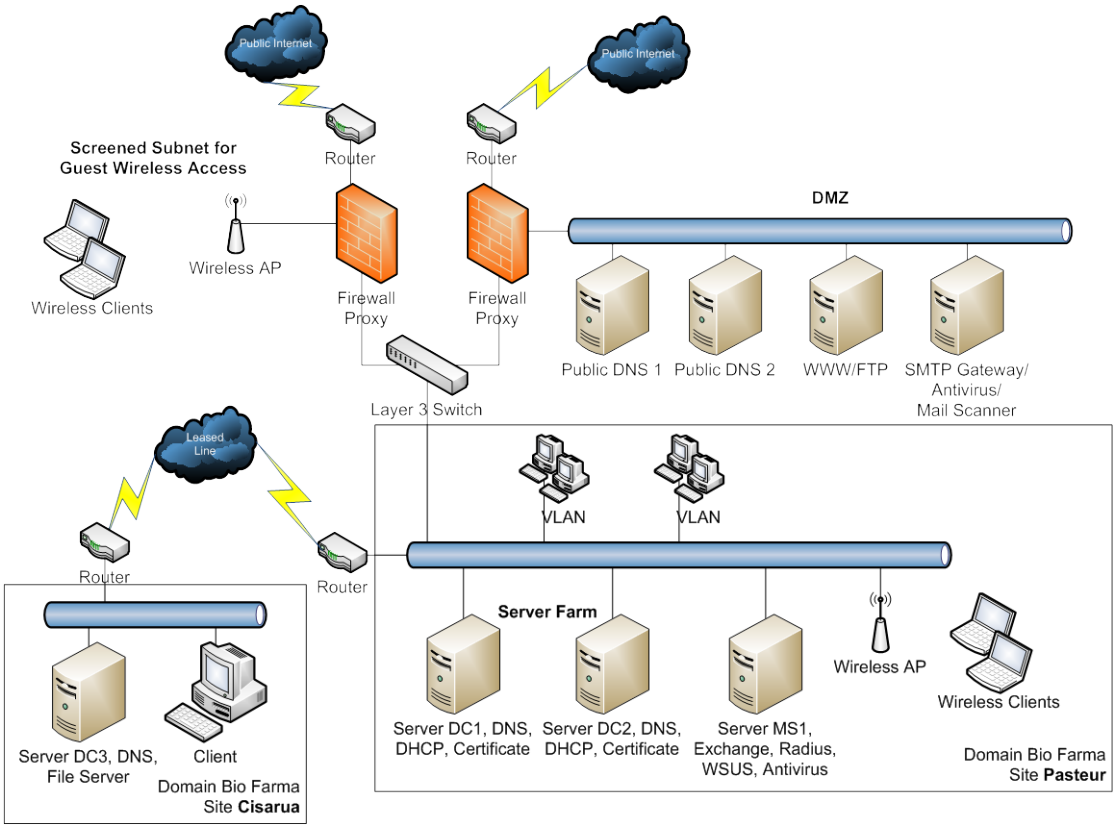
Saat ini di PT Bio Farma terdapat 20 server dengan penyebaran seperti diperlihatkan pada Gambar IV.4. Dari ke-20 server tersebut terdapat 10 komputer dengan spesifikasi yang memang ditujukan server, yaitu berprosesor Intel Xeon. Sisanya sebuah Pentium D, 2 Pentium 4, dan 8 Pentium III.



Gambar V.4 Penyebaran Server

Diagram jaringan komputer PT Bio Farma dapat dilihat pada Gambar IV.5. Beberapa hal yang perlu diperhatikan :

1. Saat ini PT Bio Farma menggunakan dua penyedia jasa Internet (ISP), yaitu Indonet dan Jalawave.
2. Jaringan terdiri dari dua situs yaitu Pasteur dan kantor cabang Cisarua.
3. Jaringan di Pasteur dibagi menjadi beberapa VLAN, terdapat pula *wireless access point* untuk akses nirkabel bagi pengguna *mobile* dan tamu.
4. Terdapat *Demilitarized Zone* (DMZ) yang menampung *DNS public*, *web server*, *FTP server*, serta *mail server* beserta antivirus.



Gambar V.5 Jaringan Komputer PT Bio Farma

V.1.3 Kebijakan yang dimiliki sehubungan dengan TI

Berikut adalah daftar dari prosedur (SOP) dan kebijakan atau sistem manual yang berhubungan dengan TI di lingkungan PT Bio Farma :

1. Prosedur *Backup* Data (Dok.# : 215K-Back-Up) - merupakan pedoman untuk melaksanakan *backup database* di komputer dan server.
2. Prosedur Penanganan Masalah Komputer (Dok.# : 215K-Mslh-Komp) - merupakan penjelasan tentang penanganan masalah yang terjadi dengan komputer dan lingkungan infrastruktur TI PT Bio Farma.
3. Prosedur Baku *Update* Antivirus (Dok.# : 215K-SIS-04) - mengatur *update* antivirus yang digunakan di lingkungan PT Bio Farma.
4. Prosedur Baku Pembuatan Email (Dok.# : 215K-SIS-02) - mengatur tata cara pembuatan email bagi pengguna di PT Bio Farma.
5. *Backup* Data (Dok.# : SM-S13.1).
6. Penanganan Masalah Komputer (Dok.# : SM-S13.5).

V.1.4 Layanan Pihak Ketiga

Saat ini kerja sama dengan pihak ketiga masih terbatas. Berikut adalah daftar layanan pihak ketiga yang diberikan kepada PT Bio Farma sebagai bagian dari strategi *outsourcing* perusahaan.

Tabel V.1 Daftar Layanan Pihak Ketiga

No.	Layanan	*Vendor*
1.	Akses Internet 128 Kbps	PT. Indonet
2.	Akses Internet 512 Kbps	PT. JalaWave Cakrawala
3.	Desain, Konfigurasi dan Instalasi Infrastruktur Jaringan Komputer	PT. Sidola
4.	Pemeliharaan Infrastruktur Jaringan Komputer	PT. IT Vision

V.2 Analisis Kondisi Teknologi Informasi

Berdasarkan kondisi TI baik secara umum dan yang terkait dengan proses memastikan keamanan sistem dilakukan analisis sebagai dasar pembuatan rekomendasi.

V.2.1 Analisis Kondisi TI Secara Umum

Gambaran umum TI di PT Bio Farma di mana sebagian besar aplikasi bisnis yang digunakan berasal dari kebutuhan operasional di suatu unit (departemen yang memiliki inisiatif) yang kemudian dikembangkan oleh masih-masing unit kerja melalui mekanisme dikerjakan internal atau dikerjakan oleh pihak ketiga, jadi proses investasi dan proyek masih sangat bergantung pada pengguna.

Hal ini cukup riskan mengingat untuk memilih solusi serta melakukan implementasi dibutuhkan suatu kompetensi yang memadai pada hal-hal seperti perumusan kebutuhan, penyusunan spesifikasi, penentuan *vendor* atau teknologi, implementasi, hingga ke manajemen proyek.

Pendekatan dalam pengembangan berbagai kegiatan TI masih bersifat *bottom-up* tanpa diawasi oleh suatu fungsi manajemen yang sifatnya strategis, hal ini bisa berakibat kegiatan TI bersifat parsial tanpa melihat efektifitas kolektif di level perusahaan, kegiatan TI yang melibatkan berbagai unit kerja sulit diwujudkan, karena hanya mengandalkan komunikasi antara unit-unit kerja tersebut tanpa arahan dari manajemen yang lebih tinggi.

Dari sudut arsitektur infrastruktur TI, aplikasi masih terpisah-pisah dan belum terintegrasi satu sama lain, belum adanya standardisasi mulai dari lapisan (*layer*) antarmuka pengguna, aplikasi, hingga database, komputer *PC desktop* dan *laptop* serta *server* yang digunakan, namun saat ini PT Bio Farma sedang dalam tahap penerapan ERP (*Enterprise Resource Planning*).

V.2.2 Analisis Kondisi DS5 (Memastikan Keamanan Sistem)

Divisi TI yang ada di PT Bio Farma belumlah lama dibentuk, sebelumnya berbentuk bagian dengan nama SIM (*System Information Management*). Pembentukkan ini merujuk pada *IT Master Plan* yang telah dibuat, dengan penunjukkan ahli madya yang khusus mengelola *IT Policy & Governance* dan terdapatnya tujuan TI, tujuan bisnis, proses TI, rencana strategis TI dan risiko TI yang di dokumentasikan dengan jelas pada *IT Master Plan*, hal ini menegaskan bahwa PT Bio Farma memiliki kesadaran dan kepedulian akan Tata Kelola TI.

Sesuai dengan misi Divisi TI yang mengedepankan keamanan data, hal ini menambah bahwa Divisi TI memiliki kepedulian dan kewajiban dalam mengedepankan keamanan data guna menyediakan solusi pelayanan informasi secara cepat dan tepat waktu sehingga dapat dimanfaatkan seluruh karyawan maupun stakeholder sebagai alat mempermudah proses kerja dan pengambilan keputusan dengan tetap mengikuti *Quality System* yang berlaku di PT Bio Farma.

Namun untuk saat ini, belum ada personil yang khusus mengelola keamanan seperti *Security Engineer* atau *Information Security Administrator* dan panitia pengarah keamanan sebagai fungsi garis pelaporan untuk keamanan informasi di struktur organisasi Divisi TI.

Kebijakan yang dimiliki PT Bio Farma baik berupa prosedur maupun sistem manual seperti Prosedur *BackUp* Data, *Update* Antivirus, Pembuatan Email dan Penanganan Masalah Komputer belumlah memadai bila dilihat dari sudut keamanan, namun saat ini PT Bio Farma telah mempunyai rencana pembuatan kebijakan dan prosedur keamanan dan sedang dalam tahap pembuatan. Rencana pembuatan kebijakan dan prosedur keamanan TI yang sedang dibuat memperhatikan kebutuhan bisnis, resiko, infrastruktur TI, standar kebijakan keamanan informasi, investasi sumber daya keamanan dan dikomunikasikan kepada *stakeholder* lalu ke pengguna.

Kebijakan dan prosedur manajemen pengguna belum ada dan belum terdokumentasi karena masih dalam tahap pembuatan, belum adanya perjanjian atau pernyataan tertulis yang ditandatangani untuk benar-benar menjaga kerahasiaan *password* masing-masing, kurangnya kesadaran untuk pengetahuan karyawan terhadap pentingnya menjaga rahasia *password*, kecuali tersebut di atas pelaksanaan berjalan cukup baik, hal ini terlihat dari hak akses pengguna yang diminta disetujui oleh pihak yang bertanggung jawab terhadap keamanan, pengelolaan pengguna dan hak akses disimpan dalam tempat penyimpanan

utama yang secara spesifik teridentifikasi melalui mekanisme otentik; pembagian dan pembatasan dalam mengakses aplikasi, file dan data bagi tiap-tiap operator (proses instalasi berlaku untuk *administrator*); pengguna masing-masing telah memiliki *username* dan *password* yang berbeda, dengan kriteria seperti panjang maksimum, kadaluarsa, penggunaan kembali, kombinasi karakter, angka, dan simbol; proses pembuatan pengguna berlaku untuk semua pengguna termasuk vendor, penyedia layanan dan mitra bisnis; sistem memiliki catatan atau *log* otomatis untuk mencatat segala aktivitas..

Sudah adanya kebijakan dan prosedur *backup data* dapat dilihat seperti database telah di *backup* secara otomatis dan periodik oleh sistem, *database* memiliki tabel otorisasi atau sehingga terlindung dari akses yang tak terotorisasi, data-data sensitif telah ter-enkripsi, pengelolaan kunci sandi (kriptografi) otomatis melalui sistem, data perusahaan diklasifikasikan sesuai dengan tingkat rahasia dan sensitif, tetapi belum terdapat pembatasan penggunaan alat simpan *portable*.

Kebijakan dan prosedur penanganan virus dan *malicious software* hanya berupa prosedur *update antivirus* namun belum terdokumentasi, namun *malicious software prevention* dan *virus protection tool* telah berjalan dan didistribusikan terpusat dan ter-*update* otomatis, e-mail yang masuk disaring melalui *mail server*. Kebijakan keamanan jaringan belum ada seperti *firewalls, security appliances, network segmentation, intrusion detection,* jaringan yang diperbolehkan, jenis koneksi yang diijinkan, namun dalam pelaksanaannya telah berjalan baik, seperti

adanya *Firewall Demilitarized Zone* (DMZ), *Wireless Access Point* menggunakan *password,* proses log-on untuk masuk ke jaringan, server berada dilokasi yang aman dan terlindungi, instalasi fisik telah dipasang secara baik dan menjamin keamanan jaringan, dimungkinkan akses jaringan dari luar gedung oleh pengguna tertentu, proses memonitor *traffic* jaringan dan pengamanannya bila terjadi masalah atas gangguan jaringan, persyaratan keamanan fisik seperti pencatatan suhu, pencatatan akses ke ruang server, alat pemadam kebakaran.

Standar pengembangan perangkat lunak (*software development*) masih bersifat khusus belum mencakup semua perangkat lunak, juga belum adanya suatu mekanisme keputusan untuk *outsourcing* (kompetensi maupun proses) ke pihak ketiga, maupun standar dalam manajemen vendor, namun dalam setiap pengembangan perusahaan maupun pengembangan TI di perusahaan memperhatikan aspek keamanan sistem dan sesuai dengan tujuan utama perusahaan, bila ada sistem baru (hasil pengembangan atau dari pihak luar) sebelum diaplikasikan dilakukan pengujian kompatibilitas *software* dan *hardware*, perbaikan dan modifikasi terhadap program atas sepengetahuan dan diotorisasi pimpinan, *source code* disimpan terpisah dan dilindungi dari akses yang tidak terotorisasi.

Belum terdapatnya kebijakan dan prosedur penanggulangan insiden keamanan dan tim tanggap darurat komputer (CERT/*computer emergency response team*) untuk mengelola keadaan darurat.

Kebijakan penanganan masalah komputer di PT Bio Farma sudah ada, seperti adanya pemeliharaan *hardware* dan *software*, penggantian *hardware* dan *software* bila timbul kerusakan atau keusangan melalui *help desk* (SIMAP), inventarisasi semua perangkat jaringan, layanan dan aplikasi, serta masing-masing komponen telah diberikan peringkat resiko keamanan.

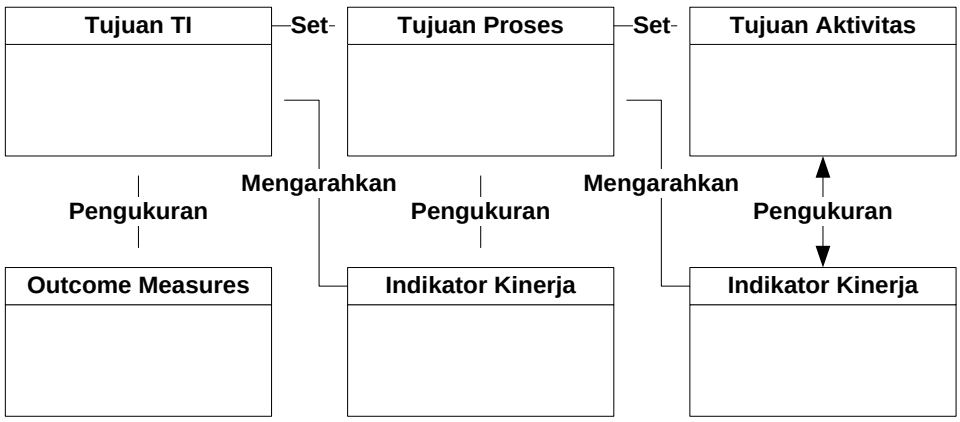
Belum terdapat mekanisme *audit* untuk semua kegiatan implementasi TI, yang bertujuan memberikan umpan balik (*feedback*) terhadap kebijakan atau prosedur sehubungan dengan TI, namun mekanisme *audit* hanya dilakukan oleh pihak internal di lingkungan Divisi TI itu sendiri.

V.3 Pengukuran Kinerja TI

Pemahaman akan ukuran-ukuran kinerja dalam TI diperlukan agar pihak manajemen mengetahui ukuran proses-proses yang baik sehingga dapat dijadikan panduan dalam penentuan hal-hal yang ingin dicapai melalui pelaksanaan proses terkait dalam tujuan pengelolaan TI. Pengukuran kinerja TI sendiri akan mencakup pengukuran pada Tujuan TI, Tujuan Proses dan Tujuan Aktivitas. Pemenuhan Tujuan TI tersebut akan diukur melalui sebuah ukuran kinerja, yang selanjutnya akan disebut sebagai *Outcome Measures*. Sedangkan pemenuhan Tujuan Proses beserta aktivitas-aktivitas yang terlibat, akan diukur melalui ukuran-ukuran kinerja yang selanjutnya akan disebut sebagai Indikator Kinerja.

Outcome Measures pada Tujuan TI menggambarkan ukuran dari hal-hal yang ingin dicapai melalui penyediaan TI. Sedangkan Indikator Kinerja pada Tujuan Proses menggambarkan Proses TI yang apa yang seharusnya diberikan sebagai dukungan terhadap Tujuan TI. Kemudian secara lebih spesifik tujuan tersebut dijabarkan ke dalam Tujuan Aktivitas yang menggambarkan hal-hal yang seharusnya ada dalam aktivitas yang dilakukan demi pencapaian kinerja yang diharapkan. Keterkaitan antara Tujuan TI, Tujuan Proses dan Tujuan Aktivitas dalam pengukuran kinerja dapat dilihat pada Gambar V.1. Tujuan TI akan menentukan Tujuan Proses dan Tujuan Proses akan menentukan Tujuan Aktivitas.

Ketiga tujuan tersebut memiliki indikator pengukuran masing-masing. Kinerja Tujuan TI diukur dengan *Outcome Measures,* sedangkan Tujuan Proses dan Tujuan Aktivitas akan diukur dengan Indikator Kinerja. Indikator Kinerja sebagai variabel pengukuran Tujuan Aktivitas akan mendorong dan mengarahkan Tujuan Proses. Hal yang sama berlaku pada Indikator Kinerja sebagai variabel pengukuran Tujuan Proses akan mendorong dan mengarahkan Tujuan TI.



Gambar V.6 Indikator Kinerja Proses TI DS5

Tujuan Aktivitas dari Proses TI DS5 (Memastikan Keamanan Sistem) meliputi kegiatan sebagai berikut :

1. Memahami persyaratan keamanan, kerentanan dan ancaman.
2. Mengelola identitas pengguna dan otorisasi secara standar.
3. Mendefinisikan insiden keamanan.
4. Pengujian keamanan secara berkala.

Untuk dapat menilai atau mengukur seberapa baik aktivitas di atas telah dilaksanakan, didefinisikan Indikator Kinerja terhadap Tujuan Aktivitas, yaitu:

1. Frekuensi dan tinjauan terhadap jenis kejadian keamanan yang perlu diawasai.
2. Jumlah dan jenis akun yang usang.
3. Jumlah *IP address*, *port* dan jenis *traffic* yang dilarang yang tidak terotorisasi.
4. Persentase kunci kriptografi yang disetujui dan dicabut.
5. Jumlah hak akses yang terotorisasi, ditarik, di-*reset* atau diubah.

Hasil pengukuran Indikator Kinerja terhadap Tujuan Aktivitas tersebut akan mendorong dan mengarahkan keberhasilan Tujuan Proses, yaitu:

1. Ijin akses terhadap data sensitif dan kritis hanya kepada pengguna yang berhak.
2. Pengidentifikasian, monitoring dan pelaporan kerentanan dan insiden keamanan.
3. Pendeteksian dan keputusan akan akses informasi, aplikasi dan infrastruktur yang tidak berhak.
4. Meminimalkan dampak kerentanan dan insiden keamanan.

Untuk dapat mengukur keberhasilannya diperlukan Indikator Kinerja terhadap Tujuan Proses yang didefinisikan sebagai berikut :

1. Jumlah dan jenis pelanggaran akses aktual dan yang dicurigai.
2. Jumlah pelanggaran dalam pemisahan tugas.
3. Persentase pengguna yang tidak mematuhi standar *password*.
4. Jumlah dan jenis pencegahan kode berbahaya (*malicious code*).

Hasil pengukuran Indikator Kinerja terhadap Tujuan Proses akan mendorong dan mengarahkan keberhasilan dalam pencapaian Tujuan TI, yaitu:

1. Jaminan bahwa informasi kritis dan rahasia akan disembunyikan dari pihak-pihak yang tidak berkepentingan.
2. Kepastian bahwa transaksi bisnis dan pertukaran informasi dapat dipercaya.
3. Menjaga integritas informasi dan pengeloalan infrastruktur.
4. Kemampuan memberikan penjelasan dan melindungi semua aset TI.
5. Jaminan layanan dan infrastruktur TI dapat menahan dan mengembalikan kegagalan karena kesalahan, serangan yang disengaja maupun bencana alam.

Untuk mengukur keberhasilan Tujuan TI dibutuhkan *Outcome Measures,* yaitu:

1. Jumlah insiden yang berpengaruh terhadap bisnis.
2. Jumlah sistem yang persyaratan keamanannya tidak terpenuhi.
3. Waktu untuk memberikan, mengubah dan menghapus akses hak istimewa.

Untuk melakukan pengawasan pada proses memastikan keamanan sistem, maka perlu dilakukan pengukuran secara berkelanjutan terhadap indikator yang telah ditetapkan dalam Indikator Kinerja dan *Outcome Measures*, dan membandingkan realisasi hasil pengukuran dengan suatu target tingkat kinerja. Penentuan besaran target tingkat kinerja dibuat untuk tiap indikator (Indikator Kinerja dan *Outcome Measures*), dilakukan dengan mempertimbangkan beberapa hal yang dipandang perlu untuk diperhatikan dalam penetapannya. Adapun nilai besaran target kinerja yang telah ditetapkan secara periodik dapat dan perlu dievaluasi disesuaikan dengan kebutuhan perusahaan. Terkait dengan realisasi hasil pengukuran yang tidak memenuhi target tingkat kinerja, akan segera dilakukan langkah-langkah perbaikan dan penyempurnaan yang diperlukan. Indikator dan target tingkat kinerja dibuat berdasarkan Indikator Kinerja dan *Outcome Measures* yang sudah digunakan beserta usulan terhadap target tingkat kinerja yang diharapkan akan tercapai sebagai indikasi keberhasilan pada pencapaian tujuan dalam rangkaian proses memastikan keamanan sistem.

V.4 Tingkat Kematangan Proses Memastikan Kemanan Sistem

Tingkat model kematangan Proses TI DS5 (Memastikan Kemanan Sistem) terdiri atas 6 tingkat, tingkat model kematangan itu antara lain :

Level 0 : (*Non-Existen*)

Ketika perusahaan belum menyadari kebutuhan akan keamanan TI. Tanggung jawab dan penanggung jawab belum ditentukan untuk kepastian keamanan. Pengukuran yang mendukung pengelolaan keamanan TI tidak diimplementasikan.

Tidak terdapatnya laporan keamanan TI dan tidak ada proses respon terhadap pelanggaran keamanan TI. Terdapatnya banyak kekurangan terhadap proses administrasi keamanan sistem yang ada.

Level 1 : (*Initial/Ad Hoc*)

Saat perusahaan belum menyadari kebutuhan keamanan TI. Kesadaran akan kebutuhan keamanan terutama bergantung pada tiap individu. Keamanan TI ditempatkan berdasar pada kemampuan reaktif. Keamanan TI tidak diukur. Pelanggaran keamanan TI yang terdeteksi menyebabkan respon saling menunjuk karena tanggung jawab yang tidak jelas. Respon terhadap pelanggaran keamanan TI tidak dapat diprediksi.

Level 2 : (*Repeatable but Intuitive*)

Ketika tanggung jawab dan penanggung jawab keamanan TI ditentukan dalam koordinator keamanan TI, walaupun manajemen otoritasnya terbatas. Kesadaran akan kebutuhan keamanan terpecah dan terbatas. Walaupun informasi terkait dengan keamanan diproduksi oleh sistem, namun tidak dianalisis. Layanan dari pihak ketiga mungkin tidak memenuhi kebutuhan keamanan perusahaan secara spesifik. Kebijakan keamanan sedang dikembangkan tetapi keahlian dan peralatan tidak mencukupi. Pelaporan keamanan TI tidak lengkap, cenderung membingungkan atau tidak berhubungan. Pelatihan keamanan tersedia namun dilakukan umumnya karena inisiatif individu. Keamanan TI terutama terlihat sebagai tanggung jawab dan area TI sementara bisnis tidak melihat keamanan TI dalam areanya.

Level 3 : (*Defined Process*)

Jika kesadaran akan kemanan dan dipertimbangkan oleh pihak manajemen. Prosedur keamanan TI didefinisikan dan diselaraskan dengan kebijakan keamanan TI. Tanggung jawab keamanan TI ditentukan dan dipahami namun tidak diselenggarakan secara konsisten. Rencana keamanan TI dan solusi keamanan tersedia sebagai dorongan analisis resiko. Pelaporan keamanan tidak terdiri dari fokus bisnis yang jelas. Pengetesan keamanan adhoc (contoh: pengetesan gangguan) dilaksanakan. Pelatihan keamanan tersedia untuk TI dan bisnis, tetapi hanya secara informal dijadwalkan dan dikelola.

Level 4 : (*Managed and Measurable*)

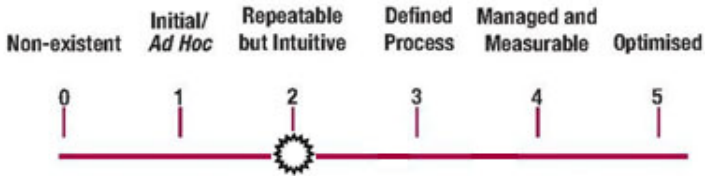
Saat tanggung jawab keamanan TI secara jelas ditentukan, dikelola dan diselenggarakan. Analisis resiko dan dampak keamanan secara konsisten dilakukan. Kebijakan dan prosedur keamanan dilengkapi dengan dasar keamanan yang spesifik. Metode untuk promosi kesadaran (*awareness*) keamanan adalah hal yang wajib. Identifikasi pengguna, otentifikasi, otorisasi distandarkan. Sertifikasi keamanan diikuti oleh anggota staf yang bertanggung jawab terhadap audit dan pengelolaan keamanan. Pengetesan keamanan dilengkapi menggunakan standar dan proses yang formal sehingga dapat meningkatkan level keamanan. Proses keamanan TI dikoordinasikan dengan fungsi keseluruhan keamanan organisasi. Pelaporan keamanan TI dikaitkan dengan Tujuan Bisnis. Pelatihan keamanan TI dilakukan di area bisnis dan TI. Pelatihan tersebut direncanakan dan dikelola dalam tata cara yang sesuai dengan kebutuhan bisnis dan riwayat resiko keamanan

yang terdefinisi. Tujuan dan metrik untuk pengelolaan keamanan sudah terdefinisi namun belum diukur.

Level 5 : (*Optimised*)

Jika keamanan TI tanggung jawab bersama dari pengelolaan bisnis dan TI serta diintegrasikan dengan Tujuan Bisnis keamanan perusahaan. Kebutuhan keamanan TI secara jelas terdefinisi, dioptimasi dan termasuk dalam rencana keamanan yang disetujui. Pengguna dan pelanggan secara meningkat bertanggung jawab dalam mendefinisikan kebutuhan keamanan dan fungsi keamanan terintegrasi dengan aplikasi di tahap desain. Insiden keamanan ditempatkan secara tepat dengan prosedur respon insiden formal yang didukung dengan perangkat otomatis. Penilaian keamanan periodik dilaksanakan untuk pengevaluasian efektivitas implementasi rencana keamanan. Informasi perihal *threats* dan kerentanan secara sistematis dikumpulkan dan dianalisis. Kontrol yang cukup untuk mitigasi risiko secara tepat dikomunikasikan dan diimplementasikan. Pengetesan keamanan, analisis penyebab dasar (*root cause analysis*) dari insiden keamanan dan identifikasi proaktif dari resiko digunakan untuk peningkatan proses yang berkelanjutan. Proses dan teknologi keamanan diintegrasikan di keseluruhan perusahaan. Metrik untuk pengelolaan keamanan diukur, dikumpulkan dan dikomunikasikan. Pihak manajemen menggunakan pengukuran ini untuk membenahi rencana keamanan dalam proses perbaikan berkelanjutan.

Berdasarkan perhitungan tingkat kematangan Proses TI DS5 (Memastikan Keamanan Sistem) yang ada pada tingkat 2 – *Repeatable But Intuitive*, maka model kematangan proses memastikan keamanan sistem seperti pada Gambar V.7.



Gambar V.7 Model Kematangan DS5 (Memastikan Keamanan Sistem)

Berdasarkan model kematangan tersebut bila dibandingkan dengan kondisi saat ini dapat digambarkan sebagai berikut, tanggung jawab dan penanggung jawab keamanan TI belum ditentukan dalam koordinator keamanan TI. Kesadaran akan kebutuhan keamanan sudah ada. Informasi yang terkait dengan keamanan dihasilkan oleh sistem, namun tidak dianalisis. Layanan dari pihak ketiga mungkin memenuhi kebutuhan keamanan perusahaan. Kebijakan keamanan sedang dikembangkan tetapi keahlian dan peralatan tidak mencukupi. Pelaporan keamanan TI tidak lengkap. Pelatihan keamanan tersedia namun dilakukan umumnya karena inisiatif individu. Keamanan TI terlihat sebagai tanggung jawab dan area TI serta bisnis mulai melihat keamanan TI sebagai kebutuhan.

V.5 Rekomendasi Proses Memastikan Kemanan Sistem

Rekomendasi yang perlu dilakukan untuk perbaikan proses memastikan keamanan sistem dibagi dua, yaitu rekomendasi jangka pendek dan rekomendasi jangka panjang.

V.5.1 Rekomendasi Jangka Pendek

Berikut rekomendasi jangka pendek yang perlu dilakukan untuk dapat meningkatkan tingkat kematangan ke tingkat – 3 (*Defined Proces*s) :

1. Tanggung jawab dan penanggung jawab keamanan TI sebaiknya ditentukan dalam koordinator keamanan TI dan diselenggarakan secara konsisten.
2. Kesadaran akan kebutuhan keamanan tetap dipertahankan baik dari manajemen maupun pengguna.
3. Rencana dan solusi keamanan TI diterapkan dan diperbarui melalui kebijakan dan prosedur keamanan dengan analisis resiko.
4. Informasi terkait dengan keamanan yang dihasilkan oleh sistem sebaiknya dianalisis dan dilaporkan agar sesuai dengan tujuan bisnis.
5. Layanan dari pihak ketiga sebaiknya sesuai kebutuhan keamanan perusahaan.
6. Kebijakan dan prosedur keamanan yang sedang dikembangkan diikuti dengan ketersediaan keahlian dan peralatan yang mencukupi.
7. Melakukan pengujian keamanan secara periodik untuk menjamin mutu keamanan tetap terpelihara.
8. Pelatihan keamanan tersedia untuk manajemen TI dan bisnis, dijadwalkan dan dikelola secara formal.

V.5.2 Rekomendasi Jangka Panjang

Berikut rekomendasi jangka panjang yang perlu dilakukan terkait dengan proses memastikan keamanan :

1. Pengembangan struktur organisasi dengan membentuk Komite Pengarah TI (*IT Steering Committee*) yang merupakan forum lintas sektoral yang melakukan persetujuan prinsip akan aspek strategis TI.
2. Menunjuk personil sebagai *Information Security Administrator* yang bertugas menerapkan, memantau, menegakkan kebijakan keamanan informasi, serta melaporkan masalah yang berhubungan dengan keamanan informasi.
3. Menunjuk personil sebagai *Security Engineer* yang bertugas melakukan pengaturan keamanan di piranti-piranti seperti firewall dan proxy, memantau log keamanan dan kondisi keamanan fisik, melakukan pengujian keamanan, melakukan pelatihan yang berhubungan dengan keamanan informasi, serta melaporkan masalah-masalah yang berhubungan dengan keamanan informasi.
4. Menyusun kebijakan dan prosedur manajemen pengguna. Dilakukan secara terpusat menggunakan *Active Directory* sebagai *directory services.* Pembuatan, perubahan, dan penghapusan pengguna harus tercatat serta pengguna yang berupa karyawan harus terkait dengan kebijakan SDM, *Group policy* perlu diterapkan untuk menegakkan kebijakan keamanan informasi.
5. Menyusun Kebijakan Keamanan Informasi. Menyatakan komitmen manajemen menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal merupakan payung kebijakan lain yang berhubungan dengan keamanan informasi.

Kebijakan keamanan informasi mencakup :

a. Definisi, sasaran dan ruang lingkup keamanan informasi.
b. Persetujuan terhadap kebijakan dan program keamanan informasi.
c. Kerangka kerja penetapan sasaran kontrol dan kontrol.
d. Struktur dan metodologi manajemen risiko.
e. Organisasi dan tanggungjawab keamanan informasi.

6. Menyusun Kebijakan Penggunaan Aset Teknologi Informasi. Panduan bagi karyawan tentang apa yang boleh dan yang tidak boleh dilakukan dengan aset teknologi informasi, Menjamin penggunaan sesuai dengan tujuan bisnis.
7. Menyusun Kebijakan Organisasi, Peran dan Tanggungjawab Keamanan Informasi. Uraian organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi serta uraian peran dan tanggung jawabnya.
8. Menyusun Kebijakan Klasifikasi Informasi. Klasifikasi informasi yang ada dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi, baik yang dihasilkan secara intenal maupun diterima dari pihak eksternal.
9. Menyusun Kebijakan Manajemen Risiko. Ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.
10. Menyusun Kebijakan Strategi Penanggulangan Bencana atau *Busineess Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP), yang meliputi analisis dampak terhadap bisnis (*Business Impact Analysis*), pemusatan

pengolahan data di *data center*, redundansi fasilitas, situs pengolahan informasi dan lokasi *backup offsite,* pengujian dan pemeliharaan BCP.

11. Menyusun Prosedur *Outsourcing*. Penanganan kontrak *outsourcing* proses ke luar lingkungan perusahaan, *Service Level Agreement*, Pengamanan proses yang dilakukan secara *outsourcing.*
12. Menyusun Prosedur *Tele-working* dan *Mobile Computing*. Pengendalian dan pengamanan penggunaan hak akses secara *remote*. Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.
13. Menyusun Prosedur Pemeliharaan dan Penanganan Masalah Perangkat Keras dan Lunak. Inventarisasi perangkat keras dan lunak, *Patching*, *Upgrade*, Pembuangan perangkat lunak yang tidak digunakan lagi, Relokasi perangkat keras, Pengamanan fisik dan datanya, Pembuangan perangkat keras.
14. Menyusun Prosedur Pengendalian Instalasi Perangkat Lunak & Hak Kekayaan Intelektual. Daftar perangkat lunak standar yang diijinkan, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan perangkat lunak yang tidak diizinkan.
15. Menyusun Prosedur Pengelolaan *Removable* Media & Disposal Media. Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan, informasi (*tape/hard disk/flashdrive/CD*) dan penghapusan informasi ataupun penghancuran media.
16. Menyusun Prosedur Pengelolaan Hak Akses Pengguna. Pendaftaran, penghapusan, pemantauan dan peninjauan hak akses pengguna, terhadap sumber daya informasi (aplikasi, sistem operasi, database, jaringan, intranet,

internet, ekstranet, email, *remote*), Panduan pemilihan password, Prosedur login, Manajemen password, Identifikasi dan autentikasi.

17. Menyusun Prosedur Pengendalian Akses Fisik dan Kondisi Lingkungan Fasilitas TI. Pengamanan atas fasilitas TI seperti *data center* dari akses yang tidak diinginkan, Isolasi *data center* dan fasilitas sensitif lainnya, Pengaturan suhu dan kelembapan, Pencegahan kebakaran.
18. Menyusun Prosedur Manajemen Jaringan. Konfigurasi jaringan, Manajemen jaringan, Perlindungan terhadap Serangan pada Jaringan, Pengaturan pengamanan dan kabel jaringan.
19. Menyusun Prosedur Penggunaan Kriptografi. Menjaga dan memelihara kriptografi, Enkripsi, Manajemen kunci elektronik, Tanda tangan digital.
20. Menyusun Prosedur Penggunaan Internet dan *Email*. Pedoman tingkah laku yang aman di Internet, *Download file*, Pengiriman, penerimaan, *forwarding email*, Prinsip keamanan dan non-repudiasi, Retensi *email*.
21. Menyusun Prosedur Manajemen Data dan Dokumen. Pengelolaan penyimpanan data, Manajemen database, Perubahan data dalam keadaan darurat, Retensi dan pengarsipan data, Pengamanan data dan dokumen sensitif ketika dikirimkan, Penanganan cetakan *hard copy*, Fotokopi, Pembuangan dokumen sensitif.
22. Menyusun Prosedur Pengembangan Perangkat Lunak. Metodologi pengembangan, Standar penulisan kode, Penyimpanan kode sumber, Analisis kebutuhan, Dokumentasi, Perubahan Darurat, Pengujian dan validasi.

23. Menyusun Prosedur Perlindungan terhadap Virus dan *Malware*. Menangani virus atau *malware*, Melaporkan kejadian virus, Penggunaan antivirus atau *antispyware*.
24. Menyusun Prosedur Penanganan Insiden TI. Pelaporan insiden, Pelaporan kebocoran/celah keamanan TI (*security vulnerabilities*), Investigasi masalah, Penanganan masalah, Tindakan korektif, Tim Tanggap Darurat Komputer.
25. Menyusun Prosedur Audit Sistem Informasi. Periode audit, Proses audit TI internal dan eksternal, Rencana, ruang lingkup, pelaksanaan dan pelaporan, Tindak lanjut hasil audit, Persyaratan kompetensi auditor.
26. Menyusun prosedur atau rencana pelatihan dan pengembangan SDM untuk manajemen, staf TI dan staf non-TI.
    a. Pelatihan untuk manajemen meliputi Keamanan Informasi bagi Manajemen, Perencanaan Kelangsungan Usaha (*Business Continuity Planning* dan *Disaster Recovery Plan*).
    b. Pelatihan untuk staf TI meliputi Keamanan Informasi, Proses Pengembangan Software, Dukungan Pengguna/*helpdesk*, *IT Outsourcing*, Audit Sistem Informasi.
    c. Pelatihan untuk staf non-TI meliputi Kesadaran Keamanan Informasi, Penggunaan Internet dan Email.
27. Sertifikasi bagi staf TI yang meliputi *Security*+, CISSP, CISM, CISA, CSIH dan *Cisco Career Certifications*.