TESIS - PM147501

PERENCANAAN TATA KELOLA MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN *INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY* (ITIL) v3. pada D~NET SURABAYA

ADI TIATAMA
NRP 9114205321

DOSEN PEMBIMBING
Dr.Tech, Ir. R. V. Hari Ginardi, MSc

PROGRAM MAGISTER MANAJEMEN TEKNOLOGI
BIDANG KEAHLIAN MANAJEMEN TEKNOLOGI INFORMASI
PROGRAM PASCA SARJANA
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2016

LEMBAR PENGESAHAN

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar
Magister Manajemen Teknologi (M.MT)
di
Institut Teknologi Sepuluh Nopember

Oleh :

ADI TIATAMA
NRP. 9114205321

Tanggal Ujian : 28 Juni 2016
Periode wisuda : September 2016

Disetujui oleh :

1. **Dr. Ir. R.V. Hari Ginardi, M.Sc.**
   NIP.19650518 199203 1 003 (Pembimbing)

2. **Prof. Dr. Drs. Mohammad Isa Irawan, M.T.**
   NIP. 19631225 198903 1 001 (Penguji)

3. **Erma Suryani, S.T., M.T., Ph.D.**
   NIP.19700427 200501 2 001 (Penguji)

Direktur Program Pascasarjana

Prof. Ir. Djauhar Manfaat, M.Sc., Ph.D.
NIP. 19601202 198701 1 001

PERENCANAAN TATA KELOLA MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN *INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY* (ITIL) v3. PADA D~NET SURABAYA

Nama Mahasiswa : Adi Tiatama
NRP : 9114.205.321
Dosen Pembimbing : Dr.Tech, Ir. R. V. Hari Ginardi, MSc

ABSTRAK

D~Net Surabaya merupakan salah satu perusahaan yang bergerak pada bidang jasa internet di surabaya. Pemanfaatan teknologi informasi yang *up-to-date* merupakan suatu keharusan bagi perusahaan. Resiko ancaman terhadap keamanan informasi terus meningkat seiring berjalannya waktu. Kerugian finansial yang ditimbulkan sangat besar yang terjadi dalam berbagai bentuk seperti hilangnya pendapatan, besarnya biaya perbaikan, hilangnya data dan kepercayaan pelanggan serta bentuk-bentuk kerugian lain. Kenyataan ini mengharuskan pengguna teknologi informasi baik sebagai pribadi maupun institusi harus siap menghadapi ancaman keamanan informasi ini.

Tata kelola manajemen keamanan informasi diperlukan untuk menjaga kerahasiaan, integritas dan ketersediaan informasi yang ada di perusahaan. Dalam penelitian ini diperlukan pemahaman keamanan informasi yang sedang berlangsung di perusahaan, selanjutnya tahap analisa sesuai dengan standar *security management* dan diakhiri dengan tahap perencanaan tata kelola manajemen keamanan informasi. Standar yang digunakan adalah manajemen keamanan ITIL berdasar pada standar ISO 27001.

Hasil dari penelitian ini menunjukkan bahwa masih terdapat beberapa kebijakan keamanan informasi yang belum ada dan terdokumentasi dengan baik diantaranya kebijakan tentang penggunaan dan penyalahgunaan aset TI, kebijakan tentang pengklasifikasian informasi dan dokumen, kebijakan tentang akses penyedia layanan TI, informasi dan komponen dan kebijakan tentang pelepasan aset. Manajemen kemanan informasi sangat menunjang tercapainya SLA yang diberikan oleh D~Net ke pelanggan, sehingga dalam proses dan penerapannya D~Net dapat bersaing tinggi dalam kemajuan teknologi internet dengan perusahaan lain. Peningkatan kualitas layanan berbanding lurus dengan *improvement* dan kebijakan keamanan informasi yang diterapkan.

Kata Kunci: Information Technology Infrastructure Library, Manajemen Keamanan Informasi

(Halaman ini sengaja dikosongkan)

INFORMATION SECURITY MANAGEMENT GOVERNANCE PLANNING USING *INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY* (ITIL) v3. IN D~NET SURABAYA

Student Name	: Adi Tiatama
NRP	: 9114.205.321
Advisor	: Dr.Tech, Ir. R. V. Hari Ginardi, MSc

ABSTRACT

D~Net Surabaya is one of the companies engaged in the field of Internet services in Surabaya. The use of up to date information technology is a necessary for the company, since the risk of threats toward information security continues to increase over time. The financial losses caused by those threats are very big that are being happened in many forms such as loss of income, the cost of repairs, loss of data and the trusted of customers as well as other forms of losses.

Governance of information security management is required to maintain the confidentiality, integrity and availability of information in the company. This study discussed an understanding of information security which is going on in the company, furthermore, stage of the analysed in accordance with the standards of security management and ended by planning phase of governance of information security management. The standard which's used is security management of ITIL based on ISO 27001 standard.

The results of this study indicate that there are still some information security policies that are not exist and are well documented including the policy on use and misuse of IT assets, the policy on the classification of information and documents, policies on access to IT service providers, information and components and policies on the release of assets, Information security management does support the achievement of Service Level Agreement which is provided by D~Net to customers, so that in the process and its application D~Net can be highly competitive in the advancement of internet technology to other companies. Improved quality of service is directly proportional to the improvement and information security policy which's applied.

Keywords: Information Technology Infrastructure Library, Information Security Management

(Halaman ini sengaja dikosongkan)

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan mengucapkan puji syukur kehadirat Allah SWT atas segala rahmat dan ridho-Nya sehingga penulis dapat menyelesaikan penelitian ini. Terwujudnya penelitian ini tidak lepas dari dukungan tanpa henti dari Ayahanda Nurkolis dan Ibunda tercinta Siti Nurjanah yang senantiasa memberikan nasihat, do'a, dukungan, semangat, dan kasih sayangnya kepada penulis. Adapun bimbingan, motivasi maupun masukan positif dari berbagai pihak turut mengisi kelancaran dalam proses penyelesaian penelitian ini dapat terselesaikan dengan baik. Oleh karena itu, dalam kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Dr. Tech, Ir. R. V. Hari Ginardi, MSc, sebagai dosen pembimbing yang telah membimbing penulis dengan sangat baik dalam menyelesaikan penelitian ini.
2. Pimpinan MMT ITS Prof. Dr. Ir. Udisubakti Ciptomulyono, MEngSc, beserta jajaran pimpinan MMT ITS dan seluruh civitas MMT ITS.
3. Adelia Rochma yang telah berbagi tawa dan dukungan serta doa untuk penulis menyelesaikan tesis ini.
4. Putri Junifinata Anggraini, selaku istri penulis atas segala kasih sayang dan rasa pengertiannya dalam meluangkan waktu dan menyemangati untuk menyelesaikan penelitian ini.
5. Andi Surya Pranata dan Bastian Ardhi Nugraha yang telah meluangkan waktunya untuk untuk menjadi responden untuk penelitian penulis.
6. Seluruh jajaran manajemen puncak di D~Net Surabaya serta rekan-rekan kerjaurusan TI maupun rekan-rekan kerja di bidang lain.
7. Teman-teman di MMT ITS khususnya MTI yang senantiasa menjadi tempat bertukar pikiran dalam menyelesaiakan penelitian ini.

Kami menyadari masih banyak kekurangan dalam penulisan pelaporan ini, sehingga besar harapan kami adanya kritik dan saran yang membangun dari semua pihak untuk perbaikan penelitian selanjutnya.

Wassalamu'alaikum Wr. Wb.

Surabaya, Juni 2016

Penulis

DAFTAR ISI

(Halaman ini sengaja dikosongkan)

DAFTAR GAMBAR

(Halaman ini sengaja dikosongkan)

DAFTAR TABEL

(Halaman ini sengaja dikosongkan)

BAB 1

PENDAHULUAN

Bab pendahuluan ini berisi pembahasan fakta dan masalah yang melatarbelakangi dilakukannya penelitian. Isi dari bab ini terdiri dari sub bab: latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

1.1 Latar Belakang

Meningkatnya kemajuan teknologi informasi begitu pesat, menjadikan perkembangan dan keakuratan informasi semakin menjadi tuntutan dalam menjalankan bisnis perusahaan. Perusahaan yang telah berkembang maupun yang sedang berkembang membutuhkan teknologi informasi yang modern guna mendukung dalam kinerja perusahaan. Namun dalam proses berkembang suatu teknologi memiliki banyak ancaman dan kerentanan terhadap keamanan informasi data yang bersifat rahasia dan sensitif. Penerapan standar keamanan informasi diperlukan untuk mengelola keamanan informasi data yang ada di perusahaan. Sesuai dengan standar keamanan informasi dan praktek terbaik, dapat dipastikan bahwa informasi dari perusahaan yang dijamin keamanannya dapat membantu mengurangi/menghindari *downtime* terhadap sistem dan layanan perusahaan.

Aktivitas pengguna tak dikenal sebagai potensi serangan dan ancaman terhadap organisasi. Sejak keamanan informasi memiliki peran yang sangat penting dalam mendukung kegiatan organisasi, organisasi membutuhkan standar atau dasar yang mengatur tentang keamanan informasi. Beberapa organisasi swasta dan pemerintah mengembangkan badan standar yang berfungsi untuk perbandingan, standar dalam beberapa kasus, peraturan hukum tentang keamanan informasi untuk memastikan bahwa keamanan informasi sesuai dengan tingkatannya, untuk memastikan bahwa sumber daya digunakan dengan cara yang benar, dan untuk memastikan praktik keamanan terbaik diterapkan dalam suatu organisasi.

Ada beberapa standar untuk tata kelola teknologi informasi yang mengarah pada keamanan informasi seperti PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO 27001, BS7799, PCIDSS, COSO, SOA, ITIL dan COBIT. Standar-standar tersbut memiliki kekuatan dan fokus masing-masing, komponen utamanya dan standarisasinya berdasarkan ISMS.

Salah satu perusahaan yang menjadi obyek dalam penilitian ini adalah perusahaan D~Net, merupakan salah satu perusahaan yang bergerak pada bidang jasa dimana selalu berinovasi pada produk dan layanan demi memberikan solusi terbaik bagi konsumen, khususnya sektor perusahaan. Salah satunya dengan menjadikan kepentingan konsumen sebagai prioritas utama. D~NET merupakan *Internet Service Provider* (ISP) pertama yang menyediakan Technical Support siaga 24 jam yang kemudian didukung oleh Divisi Network Monitoring Center. Kombinasi teknologi tercanggih dan teknisi bersertifikat internasional memberikan jaminan agar konsumen tetap nyaman menikmati akses internet stabil dan berkualitas (www.sby.dnet.net.id).

Pada perusaahaan yang berbasis jasa dalam penanganan internet ini telah menggunakan ITIL sebagai acuan, dimana bisnis utamanya adalah layanan teknologi informasi. D~Net melakukan perubahan proses bisnisnya secara bertahap, ini dikarenakan sangat sulit untuk menata ulang proses bisnis yang sudah ada dan sedang berjalan. Proses dan fungsi *Service Operation* yang sesuai dengan tujuan perusahaan dipilih untuk diterapkan di perusahaan karena bersifat operasional, sedangkan *issue* yang lain diterapkan secara bertahap.

Untuk menjaga informasi yang dimiliki oleh perusahaan dari ancaman dari luar maupun internal, maka D~Net perlu menerapkan Sistem Manajemen Keamanan Informasi. Sehingga informasi yang ada masih terjaga kerahasiaannya, terjaga integritasnya dan data akan tersedia saat dibutuhkan.

Berdasarkan uraian latar belakang diatas, ITIL dipilih karena berfokus pada teknologi informasi yang ada di suatu organisasi dan staf-staf nya. ITIL tidak fokus terhadap bisnis dan produk. ITIL menjamin organisasi dapat cepat untuk mengintegrasikan, membuat prosedur dan praktek terbaik untuk meningkatkan keuntungan dalam melakukan bisnisnya. Manajemen keamanan ITIL berdasar

pada standar ISO 27001 (https://en.wikipedia.org). Hasil yang diharapkan dari penelitian ini mampu mencegah adanya ancaman atau ketidakamanan informasi data perusaahan yang dapat merugikan konsumen dan perusahaan. Memetakan kebijakan dan tata kelola tentang keamanan informasi data di D~Net sesuai dengan ITIL. Sehingga dalam proses dan penerapannya, D~Net mampu meningkatkan kualitas layanan dan dapat bersaing tinggi dalam kemajuan teknologi internet dengan perusahaan lain.

1.2 Perumusan Masalah

Berdasarkan paparan latar belakang di atas, perumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengatasi ancaman yang ada di D~Net terkait dengan masalah keamanan informasi data.
2. Bagaimana menentukan kebijakan-kebijakan tentang keamanan informasi data agar sesuai dengan kebutuhan D~Net.

1.3 Batasan Masalah

Dalam pembahasan penelitian ini lebih difokuskan pada Tata Kelola Manajemen Keamanan Informasi menggunakan ITIL v3 yang dikhususkan pada bagian *Security Management* pada D~Net Surabaya, dimana outputnya berupa kebijakan keamanan informasi.

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah yang ada maka tujuan yang ingin dicapai dari penelitian ini adalah:

1. Menyusun Tata Kelola Manajemen Keamanan Informasi Data yang sesuai dengan kebutuhan D~Net sebagai pedoman atau panduan dalam menangani ancaman yang mungkin terjadi.
2. Memberikan rekomendasi yang sesuai dengan kebutuhan D~Net tentang temuan keamanan informasi data saat ini sebagai panduan dimasa mendatang.

1.5 Manfaat Penelitian

Dari hasil penelitian ini diharapkan dapat memberikan kontribusi dan manfaat bagi D~Net saat ini maupun di masa mendatang, adapun beberapa manfaat yang diharapkan oleh peneliti adalah sebagai berikut:

1. Mempermudah perusahaan dalam mengidentifikasi masalah dan penanganannya tentang keamanan informasi data.
2. Mengetahui apakah penerapan ITIL menambah *value added service* bagi perusahaan?
3. Mendukung pencapaian tata kelola perusahaan yang sesuai dengan tujuan perusahaan.

1.6 Sistematika Penulisan

Adapun sistematika penulisan penelitian ini disajikan dengan penjelasan sebagai berikut:

BAB 1 Pendahuluan

Bab ini memuat latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaaat penelitian, dan sistematika penulisan.

BAB 2 Kajian Pustaka dan Dasar Teori

Bab ini membahas mengenai kajian pustaka dan dasar teori berfungsi sebagai sumber dalam memahami permasalahan yang berkaitan dengan penelitian yang dilakukan.

BAB 3 Metodologi Penelitian

Pada bab ini menjelaskan mengenai tahapan-tahapan yang akan digunakan dalam proses penelitian ini.

BAB 4 Analisa dan Pembahasan

Bab ini membahas tentang analisa dan perancangan kebijakan keamanan informasi sesuai dengan ITIL *security management.*

BAB 5 Saran dan Kesimpulan

Bab ini membahas tentang hasil penelitian dan saran yang bisa digunakan sebagai bahan pengembangan dari penelitian selanjutnya.

BAB 2

KAJIAN PUSTAKA DAN DASAR TEORI

Pada bab ini menguraikan tentang kajian pustaka dan teori yang digunakan sebagai dasar dari penelitian, mulai dari pengertian mendasar mengenai manajemen keamanan informasi menggunakan ITIL beserta literatur-literatur yang terkait dengan penelitian ini.

2.1 Keamanan Informasi Data di D~Net

Keamanan Informasi adalah suatu upaya untuk mengamankan aset-aset informasi yang dimiliki perusahaan dari ancaman-ancaman dunia maya. Ancaman-ancaman tersebut termasuk kejahatan dunia maya, yang menurut wikipedia merupakan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, confidence fraud, penipuan identitas, pornografi anak, dll

Ancaman-ancaman yang biasanya terjadi di D~Net antara lain adalah:

1. Serangan *Denial of Service* (DoS) dan *Distributed* DoS (DDos)

   DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (*hang, crash*) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan layanan sehingga ada kerugian finansial.

2. Virus

   Virus sudah menjamur di indonesia. Penyebaran biasanya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus juga dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan menyisipkan salinannya ke dokumen lain sehingga merusak informasi yang ada pada dokumen.

3. Spam

   Biasanya dilakukan pada perangkat elektronik mail (email), dimana pelaku mengirimkan pesan secara bertubi-tubi tanpa dikehendaki penerimanya. Biasanya berisi informasi-informasi yang tidak kita inginkan. Ini sangat merugikan bagi penyelenggara jasa internet, khusunya D~Net.

4. Phising

   Merupakan penyalahgunaan email dimana berbentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi yang penting, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang tepercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. Jika suatu perusahaan sangat mengandalkan transaksi email dalam proses bisnisnya ini merupakan ancaman yang serius dan perusahaan harus sadar akan hal ini, salah satu cara menghindari ancaman ini adalah dengan saling konfirmasi lagi dengan telpon atau mengirim pesan untuk memastikan transaksi tersebut.

5. Probing dan port scanning

   Merupakan suatu cara para hacker sebelum masuk ke mesin server yang ditargetkan dimana dilakukan pengintaian. Yang dilakukan adalah melakukan port scanning untuk melihat service-service apa saja yang ada di server target. Misal program web server Apache, mail server Sendmail, dan lain-lain.

Dengan adanya beberapa ancaman-ancaman yang dapat terjadi, D~Net sudah melakukan beberapa pencegahan atau tindakan preventif, yaitu:

1. Setiap karyawan wajib melakukan reset password setiap 3 bulan, dimana system sudah mengatur semuanya dan terpusat.
2. Setiap server sudah terinstall firewall.

   Menghindari adanya ancaman untuk mail server seperti (phising, spamming dll) D~Net telah memasang sistem keamanan, seperti:

a. *Throttling*, jadi ketika pengirim melakukan pengiriman email dalam jumlah besar, D~Net selaku ISP membatasi jumlah email yang dikirim setiap beberapa detik (bisa diubah sesuai keinginan), seperti sistem antrean. Ini dilakukan untuk menghindari email yang dikirim dibaca sebagai spam oleh mail server lain yang dapat merugikan pelanggan.

b. DKIM (*Domain Keys Identified Mail*)

   Mail server yang terinstall DKIM melakukan verifikasi email dan mencegah SPAM yang masuk. Fitur ini memastikan bahwa email yang masuk tidak dimodifikasi dan benar benar asli dari pengirimnya.

c. SPF (*Sender Policy Framework*)

   Dengan adanya SPF memungkinkan anda untuk mengotorisasi server dan alamat IP untuk untuk mengirim email dari domain anda. Fitur ini untuk mencegah email SPAM yang keluar. SPF dapat membantu mencegah spoofing dan phishing dengan memverifikasi nama domain yang mengirim pesan email.

d. Antivirus

   Digunakan untuk melindungi email dari virus yang menyebabkan kerusakan dokumen.

3. Setiap laptop atau komputer PC terinstall antivirus dan untuk autentikasi sudah terpusat.
4. Adanya sistem monitoring untuk mengetahui, menganalisa ancaman-ancaman yang terjadi. Ini juga membantu mendesain keamanan untuk evaluasi berikutnya.
5. Memiliki sistem log yang terpusat, berfungsi untuk membantu analisa dimana merupakan kumpulan asal usul atau riwayat jika terjadi kerusakan server atau adanya penyerangan/penyusupan dari pihak luar.

2.2 Pengertian Tata Kelola Informasi

Menurut IT Governance Institute 2003, tata kelola teknologi informasi adalah tanggung jawab dewan direksi dan manajemen eksekutif organisasi yang merupakan bagian terintegrasi dari pengelolaan perusahaan yang mencakup kepemimpinan, struktur serta proses organisasi yang memastikan bahwa teknologi informasi perusahaan dapat dipergunakan untuk mempertahankan dan memperluas strategi dan tujuan organisasi.

Peter Weill dan Jeanne W. Ross 2004, mendefinisikan tata kelola teknologi informasi sebagai aktifitas dalam pengambilan keputusan dan kerangka kerja yang dapat dipertanggungjawabkan untuk mendorong perilaku yang diinginkan dalam pengunaan teknologi informasi.

Sehingga dapat didefinisikan tata kelola teknologi informasi merupakan pengelolaan teknologi informasi secara terstruktur dan proses-proses yang ada di dalamnya untuk mendukung tujuan bisnis dari perusahaan, mengendalikan sumber daya teknologi informasi dan mengelola resiko-resiko teknologi informasi yang dilakukan oleh seluruh pemangku kepentingan.

2.3 Tujuan Penerapan Tata Kelola Teknologi Informasi

Dikembangkannya tata kelola teknologi informasi bertujuan untuk mengatur pemakaian teknologi informasi dan memastikan bahwa teknologi informasi memenuhi dan sesuai dengan tujuan, sebagai berikut:

1. Menyelaraskan teknologi informasi dengan strategi perusahaan serta realisasi dari keuntungan-keuntungan yang telah dijanjikan dari penerapan teknologi informasi.
2. Penggunaan teknologi informasi memungkinkan perusahaan mengambil peluang-peluang yang ada, serta memaksimalkan pemanfaatan teknologi informasi dalam memaksimalkan keuntungan dari penerapan teknologi informasi tersebut.
3. Bertanggungjawab terhadap seluruh penggunaan sumber daya teknologi informasi.
4. Menegelola resiko-resiko yang terkait teknologi informasi dengan tepat.

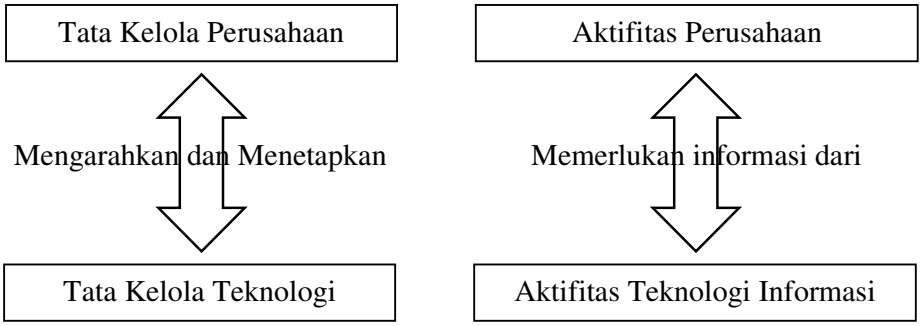
2.4 Hubungan Tata Kelola Teknologi Informasi dan Tata Kelola Perusahaan

Berdasarkan definisi tata kelola teknologi informasi di dikemukakan bahwa tata kelola teknologi informasi adalah tanggung jawab dari direksi dan manajemen eksekutif, sehingga tata kelola teknologi informasi merupakan bagian yang penting dari tata kelola perusahaan.

Ketergantungan bisnis terhadap teknologi informasi akan membuat teknologi informasi mengambil peranan penting dalam penyelesaian isu yang berkaitan dengan tata kelola perusahaan

Tata kelola perusahaan akan mengarahkan dan mengatur tata kelola teknologi informasi. Sebagai gantinya teknologi informasi dapat memberi peluang strategi dan menghasilkan masukan perbaikan bagi perencanaan strategi perusahaan. Dalam hal ini, tata kelola teknologi informasi memungkinkan perusahaan atau organisasi untuk mengambil keuntungan maksimal atas informasi.

Hubungan antara tata kelola teknologi informasi dengan tata kelola perusahaan dapat dilihat pada gambar 2.1.



Gambar 2.1 Tata Kelola Perusahaan dan Tata Kelola Teknologi Informasi (Surendro, 2009)

2.5 Standar Tata Kelola Teknologi Informasi

Dalam menerapkan tata kelola teknologi informasi, diperlukan sebuah model standar tata kelola yang *representatif* dan menyeluruh, yang mencakup masalah perencanaan, implementasi, operasional dan pengawasan terhadap

seluruh proses teknologi informasi. Penggunaan standar tata kelola teknologi informasi akan memberikan keuntungan-keuntungan sebagai berikut (IT Governance Institute, 2003)

a. *The Wheel exist* - Penggunaan standar yang sudah ada dan matang akan sangat efisien. Perusahaan tidak perlu mengembangkan sendiri suatu kerangka kerja dengan mengandalkan pengalamannya sendiri yang tentunya sangat terbatas.
b. *Structured* - Standar menyediakan suatu kerangka kerja yang terstruktur yang mudah dipahami dan diikuti manajemen. Kerangka kerja yang terstruktur dengan baik akan memberikan stiap orang pandangan yang realtif sama.
c. *Best Practices* - Standar telah dikembangkan dalam jangka waktu yang relative lama dan melibatkan ratusan orang dan organisasi diseluruh dunia. Pengalaman yang direfleksikan dalam model-model tata kelola yang ada tidak dapat dibandingkan dengan suatu usaha daru satu perusahaan tertentu.
d. *Knowledge Sharing* - Dengan mengikuti standar yang umum, manajemen akan dapat berbagi ide dan pengalaman antar organisasi melelui user groups, majalah, buku dan media informasi lainnya.
e. *Audible* - Tanpa standar baku, akan sulit bagi auditor, terutama auditor dari pihak ketiga untuk melakukan kontrol secara efektif. Dengan adanya standar, maka baik manajemen maupun auditor memiliki dasar yang sama dalam melakukan pengelolaan teknologi informasi dan pengukurannya.

Setiap model standar tata kelola teknologi informasi memiliki fokus penekanan yang berbeda-beda serta kelebihan dan kekurangan masing-masing. Beberapa model standar tata kelola teknologi informasi yang banyak digunakan pada saat ini, antara lain:

a. *Committee of Sponsoring Organozation of the Treadway Commision* (COSO).
b. *The International Organozation for Standarization The International Electrotechnical Commission* (ISO/IEC 17799).

c. *The Information Technology Infrastructure Library* (ITIL).

d. *Control Objectives for Information and Related Technology* (COBIT).

2.6 Model Standar Tata Kelola Teknologi Informasi

2.6.1 *Committee of Sponsoring Organozation of the Treadway Commision* (COSO)

COSO merupakan inisiatif bersama dari lima organisasi sektor swasta yang dibentuk pada tahun 1985. Tujuan utamanya adalah untuk mengidentifikasi faktor-faktor yang menyebabkan penggelapan laporan keuangan dan membuat rekomendasi untuk mengurangi kejadian tersebut. COSO telah menyusun suatu definisi umum untuk pengendalian, standar, dan kriteria internal yang dapat digunakan perusahaan untuk menilai sistem pengendalian mereka.

COSO disponsori dan didanai oleh 5 asosiasi dan lembaga akuntansi profesional:

1. American Institute of Certified Public Accountants (AICPA),
2. American Accounting Association (AAA),
3. Financial Executives Institute (FEI), The Institute of Internal Auditors (IIA) dan,
4. The Institute of Management Accountants (IMA)

Definisi dari kontrol internal menurut COSO adalah suatu proses yang dijalankan oleh dewan direksi, manajemen, dan staff, untuk menyediakan "*reasonable assurance*" mengenai:

- Efektifitas dan efisiensi operasional
- Reliabilitas pelaporan keuangan
- Kepatuhan atas hukum dan peraturan yang berlaku
- Pengamanan Aset

Menurut kerangka kerja COSO, kontrol internal terdiri dari 5 komponen yang saling terkait, yaitu:

- *Control Environment*
- *Risk Assessment*
- *Control Activities*
- *Information and communication*
- *Monitoring*

Gambar 2.2 5 komponen COSO

Pada tahun 2004, COSO mengeluarkan *report* '*Enterprise Risk Management – Integrated Framework*', COSO percaya kerangka kerja ini dapat memperluas kontrol internal, memberikan fokus yang lebih kuat dan luas pada subjek manajemen risiko perusahaan.

COSO '*Enterprise Risk Management – Integrated Framework*' memiliki 4 kategori tujuan bisnis:

1. Strategis
2. Operasional
3. Pelaporan dan
4. Kepatuhan

Komponen dalam *Enterprise Risk Management*, yaitu:

- *Internal Environment*
- *Objective Setting*
- *Event Identification*
- *Risk Assessment*
- *Risk Response*
- *Control Activities*
- *Information and Communication*
- *Monitoring*

Gambar 2.3 '*Enterprise Risk Management – Integrated Framework*'

2.6.2 ISO/IEC 17799

International Standards Organization (ISO) mengelompokkan standar keamanan informasi yang umum dikenali secara internasional ke dalam struktur penomoran yang standar yakni ISO 17799. ISO/IEC 17799 tahun 2005, resmi dipublikasikan pada tanggal 15 Juni 2005. Pada tanggal 1 Juli 2007, nama itu secara resmi diubah menjadi ISO/IEC 27002 tahun 2005. Konten tersebut masih persis sama. Standar ISO/IEC 17799: 2005 (sekarang dikenal sebagai ISO/IEC 27002:2005) dikembangkan oleh *IT Security Subcommittee dan Technical Committee on Information Technology* (ISO/IEC 27002, 2005).

ISO 27002:2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan didalam ISO/IEC 27001. Sarno dan Iffano (2009:187) mengatakan kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol, 39 objektif kontrol dan 133 kontrol keamanan/ kontrol.

ISO 27002:2005 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhanya, dengan mempertimbangkan hasil kajian resiko yang telah dilakukanya (Direktorat Keamanan Informasi, 2011).

Standar tersebut memiliki fungsi dan peran masing-masing dan berkembang ke seri lain yang paparan lebih lanjutnya akan dijelaskan sebagai berikut:

1. ISO/IEC 27000: merupakan dokumen yang berisikan definisi-definisi dalam bidang keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
2. ISO/IEC 27001: berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.
3. ISO/IEC 27002: merupakan panduan praktis pelaksanaan, teknik, dan implementasi sistem manajemen keamanan informasi perusahaan berdasarkan ISO/IEC 27001.
4. ISO 27003: berisi panduan untuk perancangan dan penerapan SMKI agar meemenuhi persyaratan ISO 27001.
5. ISO 27004: berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.
6. ISO 27005: dokumen panduan pelaksanaan manajemen resiko.
7. ISO 27006: dokumen panduan untuk sertifikasi SMKI perusahaan.
8. ISO 27007: dokumen panduan audit SMKI perusahaan.

2.6.3 ITIL v3

ITIL adalah kerangka kerja yang berdasar pada proses dan menyediakan manager teknologi informasi panduan untuk kegiatan yang berkaitan dengan divisi teknologi informasi dan organisasi secara keseluruhan. Proses terdiri dari kegiatan formal yang dirancang untuk menghasilkan hasil yang spesifik. ITIL kini diakui sebagai standar global manajemen keamanan teknologi informasi yang berdasar pada ISO / IEC 20000, (Iden dan Langeland 2010).

Kerangka kerja ITIL berfokus pada teknologi informasi yang ada pada suatu organisasi dan staf-staffnya. ITIL tidak berfokus pada bisnis dan produk. ITIL menjamin organisasi dapat cepat untuk mengintegrasikan, membuat prosedur dan praktek terbaik untuk meningkatkan keuntungan dalam menjalankan bisnisnya (https://en.wikipedia.org/wiki/ITIL).

ITIL menyediakan kerangka kerja untuk tata kelola teknologi informasi, manajemen dan pengendalian layanan teknologi informasi. Ini berfokus pada pengukuran secara terus-menerus dan peningkatan kualitas layanan teknologi informasi yang diberikan, baik dari bisnis dan perspektif pelanggan. Fokus ini merupakan faktor utama dalam keberhasilan ITIL di seluruh dunia dan telah memberikan kontribusi kepada penggunaan. Beberapa manfaat yang diperoleh oleh organisasi meliputi:

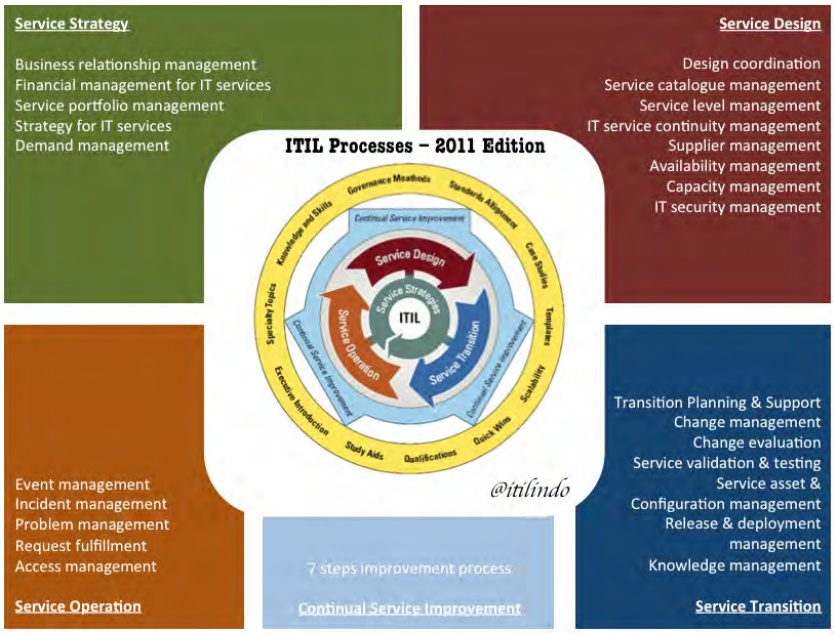
1. Peningkatan pengguna dan kepuasan pelanggan dengan layanan teknologi informasi.
2. Peningkatan ketersediaan layanan, langsung mengarah ke peningkatan keuntungan bisnis dan pendapatan.
3. Penghematan keuangan dari berkurangnya pengerjaan ulang atau kehilangan waktu dan dari peningkatan manajemen sumber daya dan penggunaan.
4. Peningkatan waktu ke pasar untuk produk dan layanan baru.
5. Peningkatan pengambilan keputusan dan mengurangi risiko.

ITIL diterbitkan dalam suatu rangkaian buku yang masing-masing membahas suatu topik pengelolaan teknologi informasi. ITIL merupakan merek dagang terdaftar dari *Office of Government Commerce* (OGC) Britania Raya. ITIL memberikan deskripsi detail tentang beberapa praktik teknologi informasi dengan daftar cek, tugas, serta prosedur menyeluruh yang dapat disesuaikan dengan segala jenis organisasi teknologi informasi.

Walaupun dikembangkan sejak dasawarsa 1980-an, penggunaan ITIL baru meluas pada pertengahan 1990-an dengan spesifikasi versi keduanya (ITIL v2) yang paling dikenal dengan dua set bukunya yang berhubungan dengan Manajemen Layanan Teknologi Informasi, yaitu Antar Layanan dan Dukungan Layanan.

Pada 30 Juni 2007, OGC menerbitkan versi ketiga ITIL (ITIL v3) yang intinya terdiri dari lima bagian dan lebih menekankan pada pengelolaan siklus hidup layanan yang disediakan oleh teknologi informasi. Kelima bagian tersebut

adalah Strategi layanan, Desain layanan, Transisi layanan, Operasi layanan dan Peningkatan layanan terus menerus.



Gambar 2.4 Siklus Layanan ITIL

2.6.3.1 Strategi Layanan

Strategi layanan merupakan aset yang strategis bagi perusahaan atau organisasi karena bukan hanya sekedar kemampuan dalam memberikan, mengelola dan mengoperasikan layanan TI. Bagi perusahaan, panduan untuk menentukan tujuan/sasaran serta ekspektasi nilai kinerja dalam mengelola layanan TI dan rencana operasional ditentukan pada tahap ini. Strategi layanan mencakup pembentukan pasar untuk menjual layanan, menentukan tipe-tipe dan karakteristik penyedia layanan baik internal maupun eksternal, aset-aset layanan, konsep portofolio layanan dan strategi untuk implementas secara keseluruhan.

Proses-proses yang dicakup dalam strategi layanan antara lain:

1. Manajemen Hubungan Bisnis *(Business Relationship Management)*
2. Manajemen Keuangan *(Financial management for IT Services)*
3. Manajemen Portofolio Layanan *(Service portfolio management)*
4. Strategi untuk layanan TI *(Strategy for IT Services)*
5. Manajemen Permintaan *(Demand management)*

2.6.3.2 Desain Layanan

Layanan teknologi informasi dapat memberikan manfaat yang maksimal bagi perusahaan, jika di desain secara sistematis dan praktek terbaik dengan acuan tujuan bisnis yang sudah ditetapkan. Desain layanan berisi prinsip-prinsip dan metode-metode desain untuk mengkonversi tujuan-tujuan strategis organisasi teknologi informasi dan bisnis menjadi portofolio/koleksi layanan teknologi informasi .

Objektif dari desain layanan adalah membuat desain layanan teknologi informasi yang tepat dan inovatif, termasuk arsitektur, proses, kebijakan dan dokumentasi, untuk memenuhi kesepakatan dari kebutuhan bisnis untuk saat ini dan masa depan. (OGC: Desain Layanan)

- Layanan baru atau perubahan layanan.
- Alat penunjang untuk sistem manajemen layanan, terutama layanan portofolio, termasuk di dalamnya katalog layanan.
- Arsitektur teknologi dan sistem manajemen.
- Proses-proses yang dibutuhkan.
- Metode dan metriks pengukuran.

Proses-proses yang dicakup dalam *Service Design* antara lain:

1. Desain Koordinasi *(Design Coordination)*
2. Manajemen Katalog Layanan *(Service Catalogue Management)*
3. Manajemen Tingkat Layanan *(Service Level Management)*
4. Manajemen Kelangsungan Layanan TI *(IT Service Continuity Managemen)t*
5. Manajemen Penyedia *(Supplier Management)*
6. Manajemen Ketersediaan *(Availability Management)*
7. Manajemen Kapasitas *(Capacity Management)*
8. Manajemen Keamanan Teknologi Informasi *(IT Security Management)*

2.6.3.3 Transisi Layanan

Transisi layanan merupakan proses pengembangan dari layanan TI yang sudah di desain untuk direalisasikan ke tahap berikutnya yaitu operasi layanan.

Proses-proses yang dicakup dalam transisi layanan yaitu:

1. Perancanaan dan Dukungan Transisi *(Transition Planning and Support)*
2. Manajemen Perubahan *(Change management)*
3. Manajemen Konfigurasi dan Layanan Aset *(Service Asset & Configuration management)*
4. Manajemen Rilis dan Penempatan *(Release & Deployment management)*
5. Validasi dan Uji Coba Layanan *(Service Validation and Testing)*
6. Evaluasi Perubahan *(Change Evaluation)*
7. Manajemen Pengetahuan *(Knowledge Management)*

2.6.3.4 Operasi Layanan

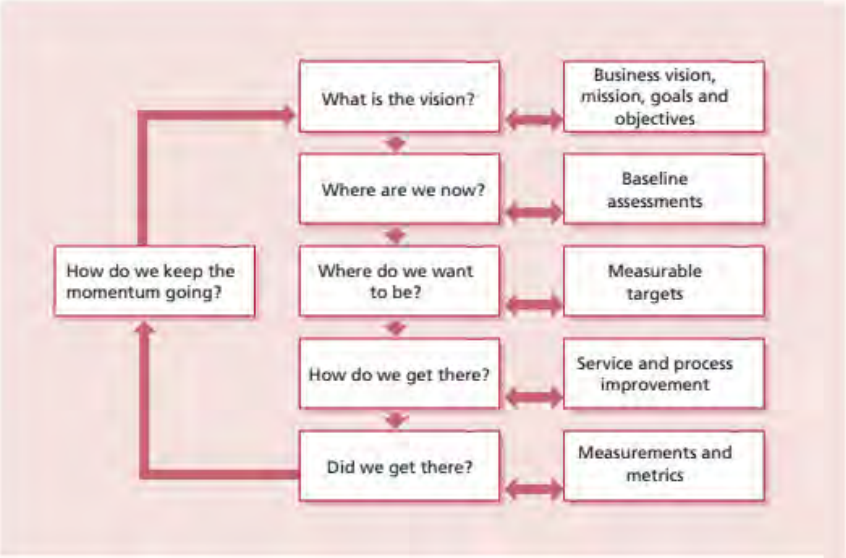
Operasi layanan merupakan tahapan yang mencakup semua kegiatan operasional pengelolaan layanan-layanan teknologi informasi. Di dalamnya terdapat berbagai panduan bagaimana mengelola layanan teknologi informasi secara efisien dan efektif serta menjamin tingkat kinerja yang telah ditentukan. Panduan-panduan ini mencakup bagaiman menjaga kestabilan operasional layanan teknologi informasi serta pengelolaan perubahan desain, skala, ruang lingkup serta target kinerja layanan teknologi informasi. Proses-proses yang dicakup dalam operasi layanan yaitu:

1. Manajemen Peristiwa *(Event Management)*
2. Manajemen Insiden *(Incident Management)*
3. Manajemen Masalah *(Problem Management)*
4. Pemenuhan Permintaan *(Request Fulfillment)*
5. Manajemen Akses *(Access Management)*

2.6.3.5 Peningkatan Layanan Terus menerus

Merupakan tahapan terakhir dari siklus hidup layanan ITIL, pada tahapan ini dilakukan evaluasi terhadap layanan teknologi informasi yang telah berjalan. Peningkatan layanan terus menerus bertujuan untuk memeriksa / memastikan dan meningkatkan kualitas layanan teknologi informasi yang dianggap perlu setelah dilakukan identifikasi, agar dapat berjalan secara terus menerus. Hal ini dilakukan

untuk mengatasi perubahan kebutuhan bisnis dan teknologi sehingga keselarasan dan peningkatan terhadap layanan teknologi informasi tetap berkelanjutan.



Gambar 2.5 Model Peningkatan Layanan Terus menerus

Proses-proses yang dicakup dalam peningkatan layanan terus menerus yaitu:

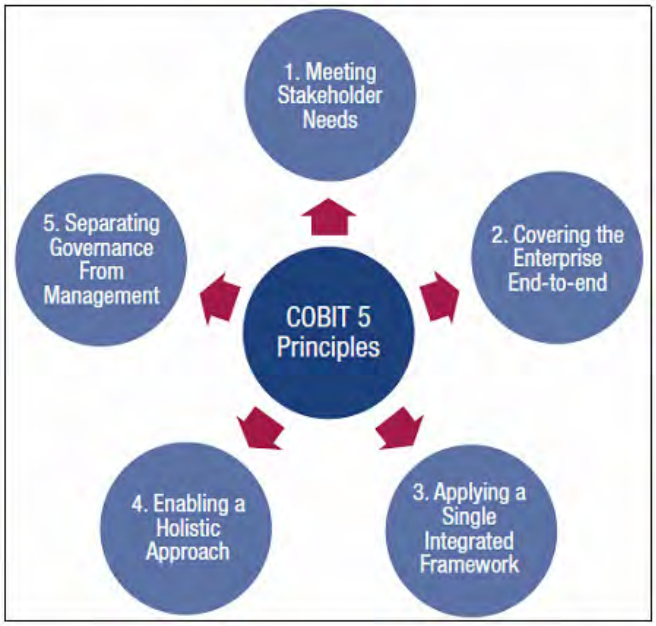
1. 7 Langkah proses perbaikan
2. Pengukuran Layanan
3. Pelaporan Layanan

2.6.4 COBIT

COBIT adalah kerangka kerja tata kelola teknologi informasi yang ditujukan kepada manajemen, staf pelayanan teknologi informasi, departemen kontrol, fungsi audit dan lebih penting lagi bagi pemilik proses bisnis adalah untuk memastikan kerahasiaan, integritas dan ketersediaan data serta informasi yang sensitif dan kritikal. COBIT telah berkembang menjadi kerangka kerja tata kelola tata kelola yang paling signifikan, karena COBIT menyediakan pedoman yang komprehensif di lingkungan proses-proses teknologi informasi dan hubungannya dengan tujuan bisnis.

COBIT 5 memiliki lima prinsip kunci untuk tata kelola dan manajemen teknologi informasi perusahaan. Kelima prinsip ini memungkinkan perusahaan

untuk membangun sebuah kerangka tata kelola dan manajemen yang efektif, yang dapat mengoptimalkan investasi dan penggunaan teknologi informasi untuk mendapatkan keuntungan bagi para pemangku kepentingan.

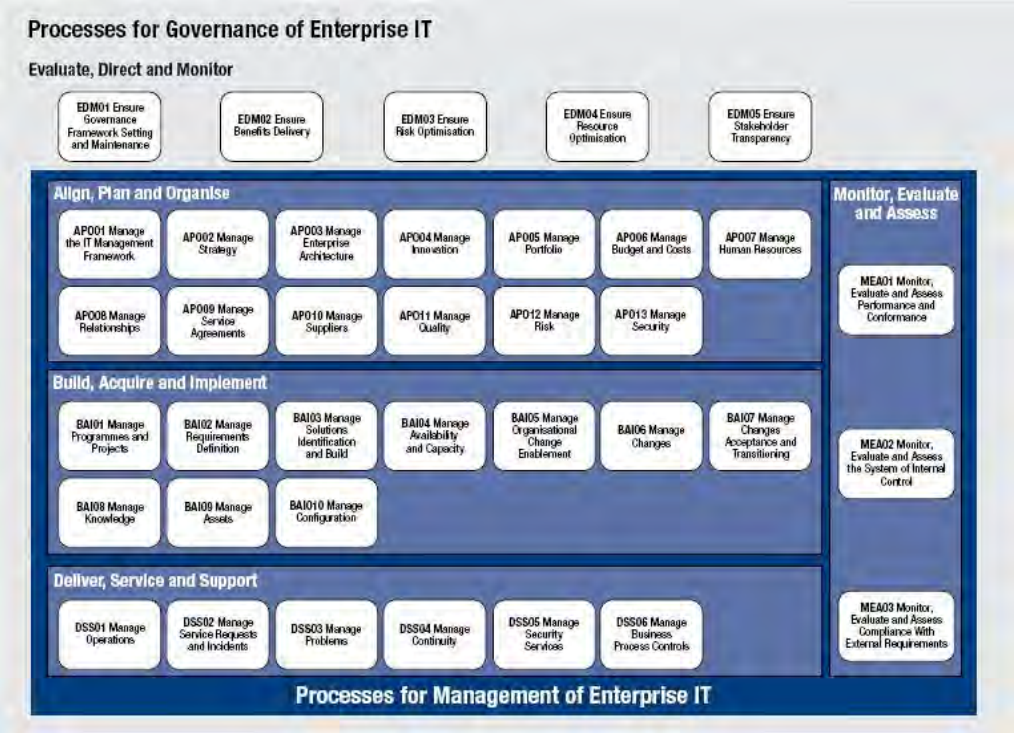


Gambar 2.6 Lima prinsip dalam COBIT 5

COBIT 5 memiliki 5 domain yang terbagi dalam domain *governance* dan *management*, masing-masing domain memiliki proses yang memungkinkan untuk mencapai tujuannya. Satu domain berasal dari *governance* dan empat lainnya berasal dari *management*. Domain yang berasal dari area *governance of enterprise* IT adalah (*Evaluate, Direct*, dan *Monitor*) EDM yang terdiri dari 5 proses. Sedangkan domain yang berasal dari *management of enterprise* IT sejalan dengan tanggung jawab pada area *plan, build, run, and monitor* (PBRM).

Terdapat 32 proses yang dipecah kedalam masing-masing domain sebagai berikut:

1. *Align, Plan and Organize* (APO) dengan13 proses.
2. *Build, Acquire and Implement* (BAI) dengan 10 proses.
3. *Deliver, Service and Support* (DSS) dengan 6 proses.
4. *Monitor, Evaluate and Assess* (MEA) dengan 3 proses.



Gambar 2.7 Domain dalam COBIT 5

2.7 Manajemen Keamanan Informasi

2.7.1 Kerangka Kerja Tata Kelola Keamanan

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisasi resiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis.

Keamanan bisa dicapai dengan beberapa cara atau strategi yang bisa dilakukan secara simultan atau dilakukan kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Contoh dari keamanan informasi antara lain (Whitman dan Mattord, 2011)

1. *Physical Security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik

dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi dan bencana alam.

2. *Personal Security* adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup *physical security*.
3. *Operational Security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
4. *Communication Security* adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

2.7.2 Aspek Keamanan Informasi

Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Kebanyakan orang mungkin akan bertanya, mengapa "keamanan informasi" dan bukan "keamanan teknologi informasi". Kedua istilah ini sebenarnya sangat terkait, namun mengacu pada dua hal yang sama sekali berbeda. Keamanan teknologi informasi mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan.

Berbeda dengan "keamanan informasi" yang fokusnya justru pada data dan informasi milik perusahaan. Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

Berdasarkan penjelasan tersebut, "kemananan teknologi informasi" merupakan bagian dari keseluruhan aspek "keamanan informasi". Karena teknologi informasi merupakan salah satu alat penting yang digunakan untuk mengamankan akses serta penggunaan dari data dan informasi perusahaan. Dari pemahaman ini pula, kita akan mengetahui bahwa teknologi informasi bukanlah satu-satunya aspek yang memungkinkan terwujudnya konsep keamanan informasi di perusahaan.

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut (Whitman dan Mattord, 2009):

1. *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity* (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

Gambar 2.8 Elemen - elemen keamanan informasi

(Sumber: Sarno dan Iffano, 2009)

Selain dari aspek kerahasiaan, integritas dan ketersediaan terdapat beberapa aspek lain dari keamanan informasi, yaitu:

1. *Privacy*

   Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain.

2. *Identification*

   Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan *user name* dan *user ID*.

3. *Authentication*

   Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang di klaim.

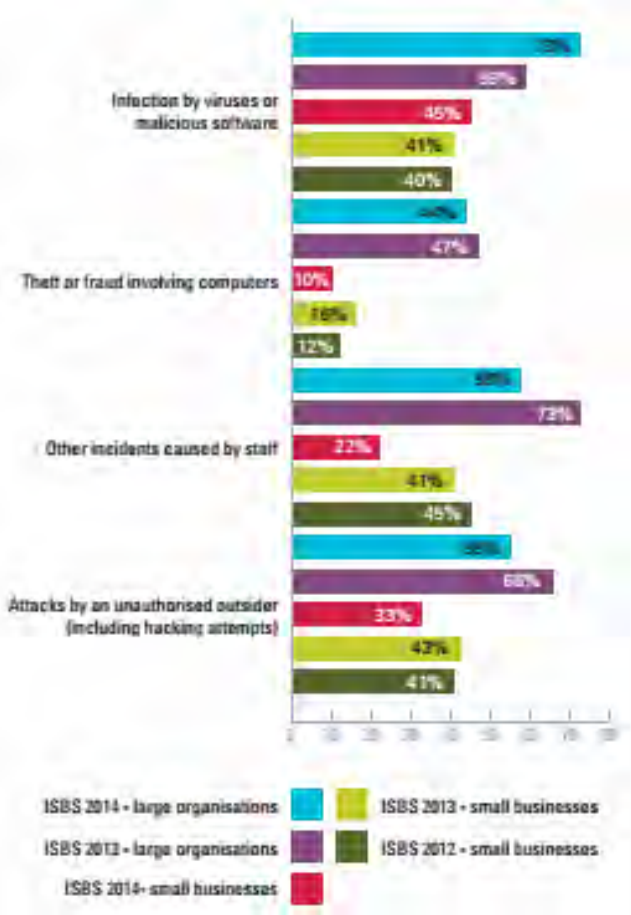
4. *Authorization*

   Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari informasi.

5. *Accountability*

   Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu.

2.7.3 Alasan dibutuhkan keamanan informasi



Gambar 2.9 Jenis pelanggaran yang diderita oleh beberapa organisasi
(Sumber: ISBS 2014)

Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil kerugian perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga

diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar. Hasil survey ISBS tahun 2014 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara atau terlindungi sehingga menimbulkan kerawanan. Hasil survei yang terkait dengan hal ini dapat dilihat pada Gambar 2.9. Survei pada Gambar 2.9 menunjukkan bahwa lebih dari 50% organisasi besar mengalami serangan atau kerusakan data karena kelemahan dalam sistem keamanan baik pada tahun 2013 maupun 2013. Hanya pencurian atau penipuan yang hanya 44% di tahun 2014. Setiap tahun jumlah pelanggaran terhadap keamanan informasi akan semakin meningkat karena diikuti juga mengenai perkembangan teknologi yang semakin maju. Untuk itulah maka haruslah ada mengenai suatu pengontrolan keamanan informasi.

Menurut Lin, dkk (2011) bahwa dengan mengetahui ilmu dan pengetahuan mengenai pengontrolan keamanan informasi yang saat ini sedang diimplementasikan dalam organisasi, seseorang dapat menetapkan pedoman organisasi untuk perusahaan sehingga dapat efektif dalam pengelolaan keamananan informasi. Dalam meningkatkan sistem pengendalian internal dan keamanan informasi pada organisasi dapat membantu organisasi dalam meningkatkan keamanan informasi.

2.7.4 Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Infromasi merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan. Dan sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut:

1. **Struktur organisasi**, biasarnya berupa keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi. Misalnya; *Chief Security Officer* dan beberapa lainnya.
2. **Kebijakan keamanan,** atau dalam bahasa Inggris disebut sebagai *Security Policy*. Contoh kebijakan keamanan ini misalnya adalah sebagai berikut:

Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk logon pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terkoneksi ke jaringan.

3. **Prosedur dan proses,** yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur permohonan ijin akses aplikasi, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.

4. **Tanggung jawab**, yang dimaksud dengan tanggung jawab atau responsibility di sini adalah tercerminnya konsep dan aspek-aspek keamanan informasi perusahaan di dalam job description setiap jabatan dalam perusahaan. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamaan informasi perusahaan untuk staf dan karyawannya.

5. **Sumber daya manusia**, adalah pelaksana serta obyek pengembangan keamanan informasi di perusahaan. Manusia yang bisa memperbaiki serta merusak semua usaha-usaha tersebut.

Sangat penting bagi organisasi untuk menggunakan sistem manajemen keamanan informasi (SMKI) untuk secara efektif mengelola aset informasi mereka. SMKI pada dasarnya terdiri dari sekumpulan kebijakan oleh sebuah organisasi untuk menentukan, membangun, mengembangkan dan memelihara keamanan komputer mereka berdasarkan hardware dan software sumber daya. Kebijakan ini mengontrol di mana sumber daya komputer dapat digunakan.

Sejak keamanan informasi memiliki peran yang sangat penting dalam mendukung kegiatan organisasi, organisasi membutuhkan standar atau dasar yang mengatur tentang keamanan informasi. Beberapa organisasi swasta dan pemerintah mengembangkan badan standar yang berfungsi untuk perbandingan, standar dalam beberapa kasus, peraturan hukum tentang keamanan informasi untuk memastikan bahwa keamanan informasi sesuai dengan tingkatannya, untuk memastikan bahwa sumber daya digunakan dengan cara yang benar, dan untuk memastikan praktik keamanan terbaik diterapkan dalam suatu organisasi.

Ada beberapa standar untuk tata kelola teknologi informasi yang mengarah ke keamanan informasi seperti PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL dan COBIT. Standar-standar tersbut memiliki kekuatan dan fokus masing-masing, komponen utamanya dan standarisasinya berdasarkan ISMS.

ITIL berfokus pada implementasi teknologi informas dan didukung dengan manajemen layanan yang baik diharapkan dapat memberikan nilai ke perusahaan yang nantinya nilai tersebut juga dirasakan oleh pelanggan yang dapat diukur melalui kepuasan terhadap produk dan layanan profesional yang diberikan.

2.7.5 Manajemen Keamanan ITIL

Konsep dasar dari manajemen keamanan adalah keamanan informasi. Tujuan utama dari keamanan informasi adalah untuk menjamin keamanan informasi. Ketika melindungi informasi itu adalah nilai informasi yang harus dilindungi. Nilai nilai tersebut adalah kerahasiaan, integritas dan ketersediaan. Terdiri dari aspek *privacy*, *anonymity* dan *verifability*.

Tujuan dari manajemen keamanan dibagi dua:

1. Realisasi persyaratan keamanan yang ditetapkan dalam *Service Level Agreement* (SLA) dan persyaratan lainnya yang ditentukan dalam kontrak, undang undang dan kemungkinan kebijakan internal atau eksternal.
2. Realisasi pada tingkat dasar keamanan. Hal ini diperlukan untuk menjamin kelangsungan organisasi manajemen. Hal ini juga

diperlukan untuk mencapai penyederhanaan *service level management* untuk kamanan informasi, sehingga menjadi lebih mudah untuk mengelola beberapa SLA daripada mengelola SLA dalam jumlah yang besar.

Input dari proses manajemen keamanan dibentuk oleh SLA dengan persyaratan keamanan tertentu, undang-undang dokumen (jika ada) dan lainnya (eksternal) kontrak yang mendukung. Persyaratan ini juga dapat bertindak sebagai indikator kinerja utama (KPI) yang dapat digunakan untuk manajemen proses dan untuk pembenaran hasil dari proses manajemen keamanan. Hasil akhir memberikan informasi pembenaran untuk realisasi SLA dan laporan penyimpangan dari persyaratan. Menurut ITIL kebijakan keamanan meliputi:

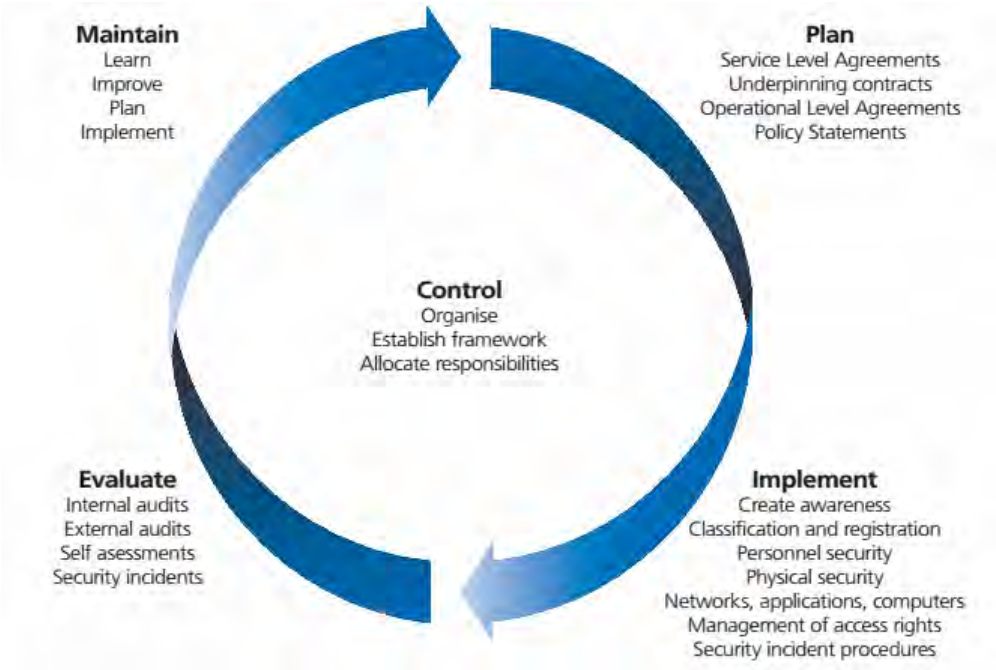
1. Kebijakan tentang penggunaan dan penyalahgunaan aset TI,
2. Kebijakan tentang akses kontrol,
3. Kebijakan tentang kontrol password,
4. Kebijakan tentang email,
5. Kebijakan tentang internet,
6. Kebijakan tentang penanganan virus,
7. Kebijakan tentang pengklasifikasian informasi,
8. Kebijakan tentang pengklasifikasian dokumen,
9. Kebijakan tentang akses remote,
10. Kebijakan tentang akses penyedia layanan TI, informasi dan komponen,
11. Kebijakan tentang pelepasan aset.

Manajemen keamanan ITIL menggambarkan proses keamanan yang terstruktur di dalam organisai manajemen. Manajemen keamanan ITIL berdasar pada standar ISO 27001. Menurut ISO.ORG "ISO/IEC 27001:2005 mencakup semua jenis organisasi (misalnya: perusahaan komersial, instansi pemerintah, organisasi bukan nirlaba). ISO/IEC 27001:2005 menetapkan persyaratan untuk mendirikan, menerapkan, pengoperasian, pemantauan, peninjauan, pemeliharaan dan meningkatkan pendokumentasian Sistem Manajemen Keamanan Informasi dalam konteks resiko bisnis dalam sebuah organisasi secara keseluruhan. Ini persyaratan spesifik untuk melaksanakan kontrol keamanan yang disesuaikan

dengan kebutuhan organisasi atau bagiannya. ISO/IEC 27001:2005 dirancang untuk memastikan pemilihan kontrol keamanan yang memadai dan proporsional yang melindungi aset informasi dan memberikan kepercayaan kepada pihak yang berkepentingan.

2.7.6 Proses Manajemen Keamanan ITIL

Proses manajemen keamanan terdiri dari kegiatan yang dilakukan oleh manajemen keamanan atau kegiatan yang dikendalikan oleh manajemen keamanan. Karena organisasi dan sistem informasi mereka terus-menerus berubah, kegiatan dalam proses manajemen keamanan harus direvisi terus menerus, agar tetap *up-to-date* dan efektif. Manajemen keamanan merupakan proses yang berkesinambungan dan dapat dibandingkan dengan Siklus Kualitas W. Edwards Deming (*Plan, Do, Check, Act*). Berikut siklus dari proses manajemen keamanan ITIL:



Gambar 2.10 Kerangka kerja Sistem Manajemen Keamanan Informasi pada ITIL

1. Control

Kontrol bertujuan menciptakan kerangka kerja manajemen untuk mengatur dan mengelola proses manajemen keamanan itu sendiri. Dimulai dengan mendefinisikan proses keamanan informasi, struktur organisasi untuk persiapan, persetujuan dan pelaksanaan kebijakan keamanan informasi dan alokasi tanggung jawab beserta kontrol dokumentasi yang diperlukan.

2. Plan

Perencanaan berfokus pada desain dan rekomendasi dari langkah-langkah keamanan yang tepat berdasarkan persyaratan organisasi. Persyaratan ini diperoleh dari sumber seperti penjualan dan risiko layanan, rencana dan strategi, SLA dan OLA (Perjanjian Tingkat Operasional), dan hukum, moral dan tanggung jawab etis untuk keamanan informasi.

3. Implementation

Tahap implementasi memastikan bahwa semua langkah-langkah yang sudah ditentukan dalam rencana dilaksanakan dengan benar untuk mendukung kebijakan keamanan informasi.

4. Evaluation

Evaluasi diperlukan mengawasi kebijakan keamanan informasi dan untuk mengukur keberhasilan dari implementasi dan perencanaan keamanan. Hasil dari evaluasi dapat menyebabkan kebijakan baru atau mempertahankan kebijakan yang sebelumnya.

5. Maintenance

Pada tahap ini digunakan untuk meningkatkan pelaksanaan langkah-langkah keamanan informasi yang didasarkan pada hasil evaluasi.

2.7.7 Kerangka kerja yang terkait

Menurut penelitian Franky dan Joko Lianto (2011) yang berjudul "Perancangan Tata Kelola Teknologi Informasi dengan Framework COBIT pada Infrastruktur dan Keamanan Jaringan Universitas X", berkesimpulan bahwa pengelolaan infrastruktur jaringan di Universitas X untuk tahap evaluasi tingkat kematangan berada dalam tingkat terdefinisi. Artinya, sebagian besar prosedur

standar sudah ada dan terkomunikasikan dengan baik, namun masih sering terjadi penyimpangan karena tidak dimonitor dengan baik. Dimana proses-proses yang dipakai adalah sebagai berikut: AI5, AI3, PO3, DS3, DS7, dan DS9. Sedangkan untuk pengelolaan keamanan jaringan proses-proses yang dipakai adalah sebagai berikut: PO9, PO6, AI7, DS4, DS5, DS9, DS12, DS13 dan ME2 dimana sesuai dengan *IT Goals*. Dari hasil evaluasi tingkat kematangan dapat disimpulkan secara umum, pengelolaan keamanan jaringan saat ini mengikuti pola berulang dan intuitif. Artinya, aktifitas yang ada belum sepenuhnya terarah dan terdefinisi secara formal. Akibatnya, terdapat beberapa ketidak konsistenan yang memungkinkan terjadinya masalah di kemudian hari.

Farroh Sakinah dan Bambang Setiawan (2014) dengan penelitian yang bejudul "Indeks Penilaian Kematangan (*Maturity*) Manajemen Keamanan Layanan TI", Kombinasi antara metodologi manajemen TI menggunakan ITIL, COBIT dan ISO / IEC 27002 akan memberikan hasil yang lebih komprehensif dan efisien baik dari sisi persiapan hingga pengimplementasian fitur-fitur yang sebelumnya tidak dipertimbangkan oleh organisasi yang hanya menggunakan satu buah metodologi. Indeks penilaian yang dibuat memiliki fitur yang dikhususkan untuk organisasi penyelenggara layanan publik, terutama di perguruan tinggi sehingga fitur/pertanyaan yang ada di dalam indeks lebih bersifat khusus.

Yu Xiaozhong, Liu Jian dan Yang Yong (2015) dengan penelitian yang bejudul "*Study on the IT Service Evaluation System in ITIL-based Small and Medium-sized Commercial Banks*", berdasarkan KPI manajemen ITIL, tidak bisa dipungkiri pemangku kepentingan terikat dengan sistem evaluasi kepuasan. Karena beberapa indikator dari sistem indikator sulit untuk diukur, jaringan BP berdasarkan optimasi GA diterapkan dalam melakukan evaluasi. Berdasarkan analisis simulasi, dapat dilihat bahwa algoritma genetika secara efektif dapat meningkatkan proses evaluasi dan hasil dari algoritma tradisional BP, mencapai konvergensi lebih cepat, presisi tinggi, dan representasi yang lebih baik dari pengetahuan dan pengalaman para ahli. Selain itu, algoritma dapat digunakan untuk melatih dan menyesuaikan model sesuai dengan kebutuhan evaluasi, sehingga memiliki penerapan yang lebih tinggi dan kecerdasan.

Luís Velez Lapão (2011) dengan penelitian yang berjudul "*Organizational Challenges and Barriers to Implementing IT Governance in a Hospital*" , peneliti menilai manajemen layanan TI menggunakan kuesioner OGC 2001 untuk memahami seberapa baik kinerja HISD dibandingkan dengan ITIL berdasarkan praktik terbaik. Secara umum, ketika proses manajemen layanan TI berada pada tahap awal, berada pada tingkat kematangan 1. Di penelitian ini, baik Insiden dan tingkat manajemen layanan gagal untuk mencapai tingkat minimum prasyarat (tingkat kematangan 0). Ini berarti bahwa, proses manajemen layanan TI adalah ad-hoc. Sedangkan untuk insiden manajemen HSS process dan technology berada pada tingkat kematangan 2, Vision dan Steering, People dan Culture berada pada tingkat kematangan 1.

Berdasarkan jurnal-jurnal yang telah dipaparkan diatas dapat disimpulkan, bahwa ITIL, COBIT dan ISO / IEC 27002 digunakan sebagai dasar pembuatan tata kelola manajemen keamanan sistem informasi. Penelitian ini akan menggunkan *framework* ITIL khususnya menggunakan siklus dari proses manajemen keamanan informasi ITIL itu sendiri. yang membahas tentang keamanan informasi menggunakan ITIL.

2.8 Gambaran Umum Obyek Penelitian

2.8.1 Sejarah Singkat D~Net

D~Net merupakan salah satu perusahaan yang bergerak dibidang jasa, khususnya layanan internet yang berdiri di tahun 1997. D~Net berkembang menjadi salah satu penyedia layanan internet berkualitas terbaik di Surabaya. Sejalan dengan moto kami yaitu "*The Quality Internet Service Provider*", D~Net kini telah memperkuat posisinya sebagai penyedia layanan internet terdepan di areanya.

Seiring pesatnya perkembangan teknologi informasi, D~Net selalu berinovasi pada produk dan layanan demi memberikan solusi terbaik bagi pelanggan, khususnya sektor perusahaan. Terlebih lagi D~Net telah memiliki sambungan fiber optic ke *International Backbone* dan *Indonesia Internet Exchange* (IIX) untuk menyediakan koneksi internet yang lebih cepat dan handal.

Meletakkan kepentingan pelanggan sebagai prioritas utama, D~Net adalah ISP pertama yang menyediakan Technical Support siaga 24 jam yang kemudian didukung divisi Network Monitoring Center. Kombinasi teknologi tercanggih dan teknisi bersertifikat internasional memberikan jaminan agar pelanggan tetap nyaman menikmati akses internet stabil dan berkualitas.

Sebagai kontribusi kepada komunitas, lewat program CSR (*Corporate Social Responsibility*), D~Net telah melakukan beberapa kegiatan amal meliputi sektor pendidikan, budaya, olah raga, dan memberikan bantuan pada korban bencana alam.

2.8.2 Profil Umum D~Net

D~Net pusat yang beralamatkan di Graha Bumi Surabaya Jl. Basuki Rahmad 106 - 128 Kota Surabaya, Kode Pos 60271 merupakan salah satu perusahaan yang bergerak di bidang jasa, terutama sebagai penyedia layanan internet sebagai bisnis utamanya. Tidak hanya di Surabaya, D~Net juga memiliki cabang di Jakarta, Malang dan Denpasar untuk memperluas area pelayanannya. Untuk memperkuat posisi sebagai penyedia layanan internet yang terdepan, D~Net dituntut untuk melakukan inovasi produk dan layanannya. Dimana, yang dahulunya masih menggunakan teknologi yang lama sekarang bertransformasi menggunakan teknologi *cloud computing* dan otomatisasi untuk mempermudah pemeliharaan terhadap perangkat lunaknya.

Gambar 2.11 Wilayah jangkauan D~Net Surabaya

2.8.3 Visi dan Misi

Menurut Wibisono (2006, p.43), Visi merupakan rangkaian kalimat yang menyatakan cita-cita atau impian sebuah organisasi atau perusahaan yang ingin dicapai di masa depan. Atau dapat dikatakan bahwa visi merupakan pernyataan *want to be* dari organisasi atau perusahaan. Visi juga merupakan hal yang sangat krusial bagi perusahaan untuk menjamin kelestarian dan kesuksesan jangka panjang.

Steiss (2003), menyatakan bahwa pernyataan visi harus mencakup misi organisasi, filosofi dan nilai-nilai inti dasar, strategi dasar, kriteria kinerja, pengambilan keputusan, dan standar etika. Pernyataan tersebut harus menekankan tujuan sosial, yang penting organisasi berfungsi dan yang membenarkan keberadaannya. Selain itu, pernyataan itu harus pendek dan inspiratif.

Wibisono (2006, p.46), Misi merupakan rangkaian kalimat yang menyatakan tujuan atau alasan eksistensi organisasi, yang memuat apa yang disediakan oleh perusahaan kepada masyarakat, baik berupa produk ataupun jasa.

Indrajit (2008), Misi masih merupakan sesuatu yang memiliki arti global dan cenderung generik. Oleh karena itu, beberapa ditentukan beberapa obyektif yang ingin dicapai dalam beberapa hal sehubungan dengan misi yang dicanangkan tersebut. Sebuah perusahaan yang memiliki misi untuk menjadi perusahaan kurir tercepat di dunia, memiliki beberapa obyektif yang harus dicapai. Biasanya obyektif yang ditetapkan bersifat customer oriented seperti:

1. Memberi kepuasan pelanggan individu dengan cara melakukan pengiriman barang barang ke seluruh dunia secara cepat dan aman.
2. Memberikan fasilitas-fasilitas khusus kepada pelanggan korporat yang secara periodik mengirimkan barang-barangnya ke seluruh penjuru dunia.

Sedangkan contoh obyektif yang lebih bersifat internal (*back office*) adalah:

1. Menjadikan seluruh kantor-kantor cabang di dunia sebagai perusahaan dengan fasilitas pelayan pelanggan terbaik.
2. Meningkatkan kompetensi sumber daya manusia perusahaan sehingga memiliki tingkat profesionalisme yang tinggi.

Berdasarkan pengertian-pengertian diatas D~Net membuat Visi Misi sebagai landasan dalam menjalankan perusahaan.

Visi

Menjadi Internet Service Provider pilihan di Surabaya, Jawa Timur, dan Bali dengan mengedepankan kualitas produk dan layanan.

Misi

Memenuhi kebutuhan internet berkualitas yang bernilai lebih untuk area Surabaya, Jawa Timur, dan Bali.

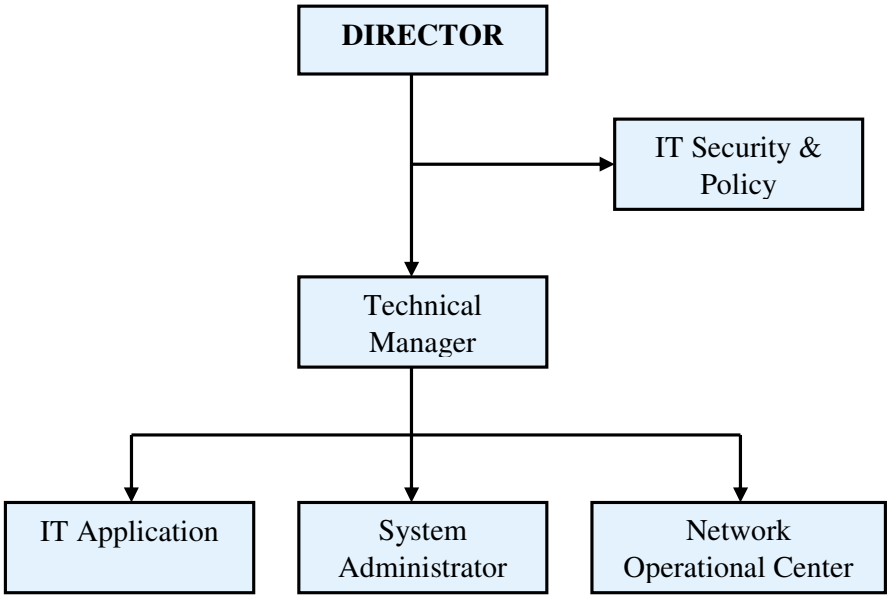
Kebijakan Mutu

Menyediakan layanan internet dengan kualitas & nilai tambah terbaik setiap saat untuk mendukung kelancaran bisnis pelanggan.

2.8.4 Struktur Organisasi TI di D~Net

Sebagai pendukung keamanan informasi dalam perusahaan, diperlukan kesadaran dari manajemen untuk menentukan tujuan yang jelas, memiliki komitmen, mendukung masalah keamanan dengan memangku tanggung jawab keamanan informasi serta menerapkan strategi dan kebijakan. Menjaga keamanan informasi dari kerentanan akan sulit jika manajemen tidak mendukung kebijakan tersebut. Kegiatan keamanan informasi harus dikoordinasikan oleh perwakilan dari berbagai divisi yang terkait dan memiliki fungsi pekerjaan yang terkait.

Berdasarkan observasi dan wawancara dengan D~Net, dapat disimpulkan berikut divisi-divisi yang terkait dengan keamanan informasi :



Gambar 2.12 Struktur Organisasi TI di D~Net

D~Net memberikan peran dan tanggung jawab yang berkaitan dengan keamanan informasi yang bertujuan untuk menjaga, mengoperasikan, mengelola dan memberi dukungan terhadap operasional yang ada. Peran dan tanggung jawab ditugaskan kepada perorangan. Tidak menuntut kemungkinan setiap perorangan memiliki beberapa peran dan tanggung jawab asalkan jelas antara peran dan tanggung jawabnya, sehingga mengurangi adanya kemungkinan melakukan kecurangan dan tidak menyebabkan konflik kepentingan.

1. *IT Policy & Security*

   Merupakan pemegang tanggung jawab utama untuk menjamin keamanan informasi di D~Net, bertanggungjawab atas pengembangan, pemeliharaan informasi dan sistem informasi terkait serta melakukan koordinasi terkait program keamanan informasi. Beberapa tugas *IT Policy & Security* antara lain:

   a. Mengembangkan, mengelola kebijakan keamanan informasi dan secara berkala menilai apakah kebijakan dilaksanakan sesuai dengan standar.

b. Memastikan bahwa semua sistem teknologi infomrasi dan data telah diklasifikasikan.
c. Memberi solusi atas permasalahan tentang keamanan inforamasi.
d. Meningkatkan keahlian karyawan yang terkait tentang keamanan informasi.
e. Menjaga semua karyawan supaya tetap sadar akan pentingnya keamanan informasi.
f. Mengumpulkan data terhadap kondisi keamanan informasi, yang digunakan sebagai bahan analisa untuk evaluasi keamanan informasi kedepannya.
g. Melakukan mitigasi dan melaporkan semua insiden keamanan teknologi informasi.

2. *Technical Manager*

Teknikal manager bertanggung jawab atas segala aktifitas dari *IT Application*, Sistem Administrator dan *Network Operational Center*. Selain itu bertanggung jawab untuk melakukan penelitian dan pengembangan teknologi yang berkembang pada saat ini serta melakukan perencanaan produk terkait TI.

3. *IT Application*

Memiliki tanggung jawab dalam pembuatan, pengembangan serta maintenance aplikasi internal maupun eksternal. Keamanan informasi dari aplikasi sangat diperlukan agar kerahasiaan informasi tetap terjaga.

4. *System Administrator*

Sistem administrator merupakan seorang analis, teknisi yang melaksanakan, mengelola dan mengoperasikan sistem yang ada di perusahaan. Sistem administrator membantu administrasi operasional teknologi informasi perusahaan, mengimplementasikan kontrol keamanan untuk melindungi informasi perusahaan dan memastikan bahwa informasi perusahaan tidak hilang.

5. *Network Operation Center* (NOC)

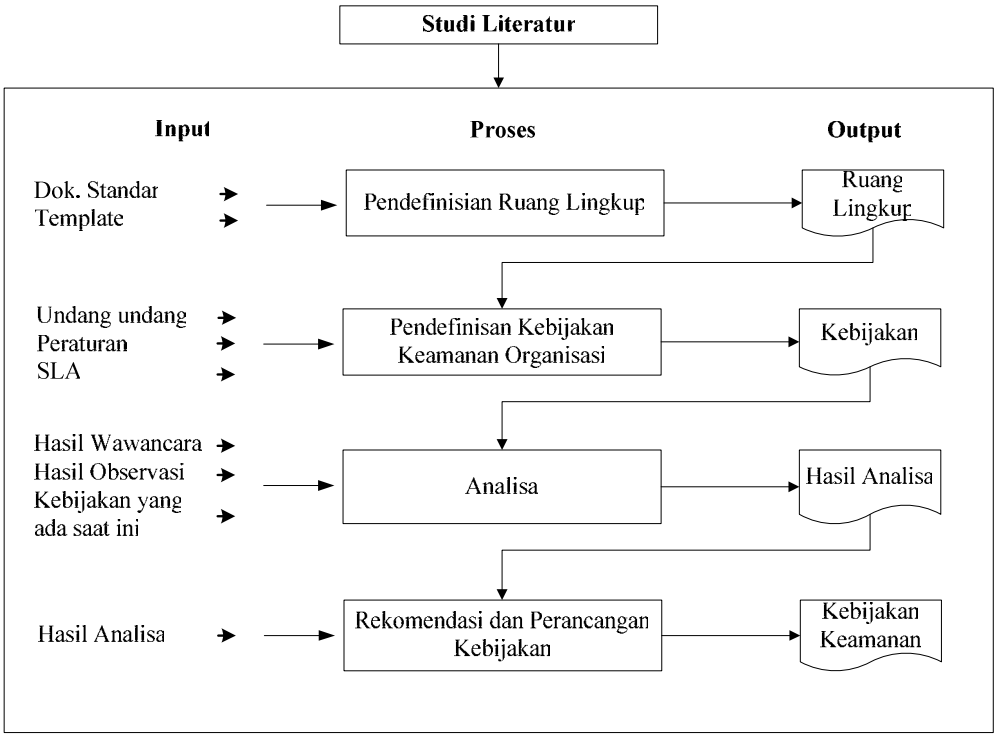
   NOC memiliki tanggung jawab untuk menangani konfigurasi dan perubahan manajemen jaringan, keamanan jaringan, memonitor performansi jaringan, pelaporan, jaminan kualitas, serta memastikan bahwa produk yang ditawarkan D~Net sudah siap untuk diberikan ke pelanggan.

(Halaman ini sengaja dikosongkan)

BAB 3

METODOLOGI PENELITIAN

Pada bab ini akan menjelaskan mengenai tahapan pelaksanaan penelitian tentang tata kelola Sistem Informasi Keamanan Data di D~Net Surabaya. Tahapan pelaksanaan pada penelitian ini secara garis besar adalah: studi literatur, tahap pengumpulan data dan informasi untuk pendefinisian kebijakan keamanan organisasi, analisis, rekomendasi dan perancangan kebijakan keamnanan informasi. Tahapan tersebut seperti yang terlihat pada gambar 3.1. berikut.



Gambar 3.1 Tahapan Pelaksanaan Penelitian

3.1 Tahap Studi Literatur

Studi literatur dilakukan dengan mengumpulkan dan mempelajari teori yang berhubungan perancangan tata kelola yang didapat dari buku, jurnal ilmiah serta penelitian terdahulu, dan materi mengenai perusahaan yang akan diteliti. Penulis mengaplikasikan metode ITIL v3 tentang *security management*.

Referensi tentang *security management* yang diperoleh merupakan dasar bagi peneliti untuk melakukan penelitian, sehingga memberikan jaminan bahwa penelitian dilakukan dengan landasan teori yang telah teruji dan diakui secara ilmiah. Selain itu juga menjadi panduan dalam mengidentifikasi masalah dan merumuskan langkah-langkah untuk menyelesaikan permasalahan tersebut.

3.2 Tahap Pendefinisian Ruang Lingkup

Proses kedua adalah tahapan pendefinisian ruang lingkup yaitu mengidentifikasi ruang lingkup yang berhubungan dengan kebutuhan perencanaan keamanan informasi ini. Ruang lingkup perencanaan keamanan sistem informasi ini tidak hanya pada sistem informasi yang ada pada perusahaan, tetapi juga berdasarkan keamanan dalam memanajemen seluruh kemungkinan kelemahan informasi yang dapat dimungkinkan berasal dari faktor di luar sistem itu sendiri. Penentuan ruang lingkup dilakukan dengan cara melakukan observasi di D~Net Surabaya.

Tahapan ini menghasilkan dokumen ruang lingkup keamanan informasi yang ditawarkan. Dokumen tersebut menentukan unit bisnis, departmen, dan atau sistem apa saja yang akan dicakup melalui penerapan keamanan informasi yang telah ditentukan dan disepakati oleh peneliti dengan D~Net Surabaya.

3.3 Tahap Pendefinisain Kebijakan Keamanan Organisasi

Dalam tahap ini mendefinisikan kebijakan keamanan informasi yang sesuai dengan kondisi D~Net Surabaya. Dimana untuk proses justifikasi melibatkan orang yang memilik kewenangan dalam menentukan kebijakan teknologi informasi di D~Net Surabaya. Adapun hasil dari proses tahapan ini

adalah suatu dokumen kebijakan keamanan informasi. Mennurut ITIL kebijakan kemanan informasi meliputi :

1. Kebijakan tentang penggunaan dan penyalahgunaan aset TI

   Kebijakan ini mengharuskan organisasi untuk mengidentifikasi semua aset informasi yang penting, menyusun dan menginventarisasi aset tersetbut. Aset-aset tersebut termasuk perangkat lunak dan untuk menggambarkannya jumlah aset yang telah dialokasikan, data yang lengkap (model, jenis, nomor seri, tanggal akuisisi dan nomor lain), dimana lokasinya dan lain-lain.

2. Kebijakan tentang akses kontrol

   Akses kontrol merupakan suatu tindakan untuk mengizinkan atau tidak mengizinkan pengguna dan membatasi pengguna dalam mengakses sistem, sumber daya dan informasi tertentu. Pengguna harus seseorang yang terpercaya dan memiliki identitas sebelum diberi hak akses. Resiko dalam pemberian dan pembatasan hak akses adalah ketidaknyamanan dan kehilangan informasi jika sampai disalahgunakan, oleh karena itu backup setiap hari diperlukan. Akses kontrol meliputi autorisasi, autentikasi, enkripsi, sistem monitoring dan otomatisasi.

   Menurut Calder dan Watkins, 2008. sesuai dengan standar, organisasi menentukan akses kontrol, pendokumentasian yang jelas tentang akses kontrol, tentang kebijakannya dan membatasi hak akses dari kebijakan yang telah dibuat. Akses kontrol yang baik memperhitungkan berbagai resiko dari ancaman-ancaman yang ada. Terkait pengaturan akses kontrol harus selaras atau berkaitan dengan tujuan bisnis, pendokumentasian yang jelas dan kesadaran dari pengguna. Kegagalan dalam menerapkan kebijakan ini bisa menyebabkan tidak terkontrolnya pengguna yang mengakses informasi, informasi tidak terjaga kerahasiaannya, banyaknya akses yang tidak sah dan terungkapnya informasi rahasia ke pihak ketiga.

3. Kebijakan tentang kontrol password

   Dalam organisasi disarankan memiliki sistem manajemen password yang menjamin dari kualitas password. Password yang baik biasanya terdiri dari huruf besar dan kecil, angka, karakter khusus dan terdapan minimal jumlah karakternya. Password haruslah terenkripsi tidak boleh menyimpan *plain text* dari password. Setiap pengguna dalam mengakses informasi harus memasukkan password dan ada batas waktu tertentu terkait masa aktif password sehingga mengharuskan pengguna untuk mengganti password tersebut.

4. Kebijakan tentang email

   Kebijakan tentang email diperlukan karena banyaknya organisasi yang menggunakan email sebagai sarana komunikasi setiap transaksinya. Email harus dijaga kerahasiaannya karena bersifat pribadi. Email yang bagus harus ada perlindungan terhadap kerahasiaannya, misalnya menggunakan antivirus, antispam, filtering email dll.

5. Kebijakan tentang internet

   Penyalahgunaan penggunaan internet dapat mengakibatkan hilangnya produktivitas disuatu organisasi, karena waktu dihabiskan untuk *'Surfing'* di internet. Akses ke internet diberikan kepada pengguna untuk mendukung dari kegiatan bisnis organsisasi dan hanya atas dasar untuk melakukan pekerjaan mereka dan peran profesional. Sebagai keamanan dari ancaman yang ada di internet seharusnya organisasi meningkatkan keamanan yang ada di organisasinya, misal dengan merubah ke teknologi keamanan yang terbaru (seperti enkripsi, autentikasi dan monitoring jaringan).

6. Kebijakan tentang penanganan virus

   Kebijakan ini bertujuan untuk melindungi perangkat lunak dari serangan virus komputer dengan memastikan perangkat lunak anti-virus telah terinstal, digunakan dan diperbarui dengan frekuensi yang tepat.

7. Kebijakan tentang pengklasifikasian informasi

   Menetapkan suatu standar kebijakan untuk perlindungan terhadap aset informasi dari akses tidak sah / tanpa kompromi atau keterbukaan merupakan hal yang penting bagi suatu organisasi. Dengan demikian, organisasi yang telah mengadopsi kebijakan klasifikasi informasi sangat terbantu dalam mengelola dan melindungi aset informasinya. Tingkatan klasifikasi informasi sesuai dengan tingkat kebutuhan akan pengklasifikasian informasi yang ada di organisasi itu sendiri. Semakin kompleks suatu organisasi maka tingkat klasifikasi akan kerahasiaan informasi semakin banyak.

8. Kebijakan tentang pengklasifikasian dokumen

   Hampir sama dengan kebijakan pengklasifikasian informasi, tetapi yang diklasifikasikan adalah dokumentasinya. Kebijakan ini memastikan dokumen yang dikelola, ditangani, disimpan dan diklasifikasikan dengan benar. Pengklasifikasian ini dalam rangka untuk menjaga keamanan dokumen.

9. Kebijakan tentang akses remote

   Kebijakan ini bertujuan untuk memberikan panduan mengenai bekerja dengan aman dari luar jaringan organisasi. Organisasi menyediakan kemudahan bagi teknisi untuk bekerja dari luar dimana tingkat keamanan harus tetap dijaga agar kerahasiaan informasi yang ada di organisasi tetap terjaga. Tidak semua pengguna bisa mendapat akses remote, setiap pengguna yang akan menggunakan akses remote diharuskan melakukan permintaan terlebih dahulu ke divisi terkait agar semuanya dapat terpantau dan terdokumentasi.

10. Kebijakan tentang akses penyedia layanan TI, informasi dan komponen

    Kebijakan ini mengatur tentang hak akses penyedia layanan TI agar keamanan informasi tetap terjaga. Menurut Järveläinen, 2012. Meskipun perusahaan dapat menggunakan jasa outsourcing dalam infrastruktur TI dan memiliki sistem informasi antarorganisasi, mereka tidak bisa mengabaikan risiko yang mungkin terjadi demi reputasi mereka

jika mitra eksternal mereka gagal untuk memberikan pelayanan yang dibutuhkan. Dari hasil penelitian Järveläinen telah ditemukan bahwa beberapa metode seperti kontrak, audit dan standar yang diterapkan dapat menyeimbangkan hubungan kekuasaan antara organisasi atau mentransfer tanggung jawab kepada pihak lain.

11. Kebijakan tentang pelepasan aset

    Kebijakan ini diperlukan untuk memastikan bahwa prosedur untuk pelepasan aset mencapai nilai terbaik dan dilakukan dengan cara yang efisien, efektif dan transparan. Pelepasan aset selalu harus selalu didokumentasikan agar bisa dilacak dan harus disetujui oleh divisi yang terkait.

3.4 Tahap Analisa

Pada tahapan ini memerlukan sejumlah input yang berupa hasil studi dokumen perusahaan, wawancara dan observasi lapangan pada D~Net Surabaya. Kelengkapan dokumen pendukung digunakan sebagai acuan dalam melakukan analisa baik berupa peraturan maupun prosedur. Output yang dihasilkan melalui tahap ini adalah dokumen atau rumusan tentang hasil analisa.

3.5 Tahap Rekomendasi dan Perancangan Kebijakan

Tahapan ini merupakan implementasi dari tahap sebelumnya yaitu tahap analisa. Pada tahap ini berisi tentang rekomendasi yang disampaikan ke D~Net untuk meningkatkan keamanan informasinya dimana sesuai dengan ITIL *security management.* Kebijakan yang belum ada atau belum sempurna akan di rancang pada tahap ini.

3.6 Metode Pengumpulan Data

Merupakan tahap dimana data dan informasi mengenai objek penelitian dikumpulkan dan digunakan sebagai bahan analis. Data-data yang diperlukan dalam penelitian ini dapat diperoleh dengan cara studi dokumen perusahaan,

wawancara dan observasi terhadap pihak-pihak yang terkait dalam objek penelitian ini.

3.6.1 Studi Dokumen Perusahaan

Data sumber penelitian salah satunya diperoleh dari mempelajari dokumen perusahaan. Dokumen-dokumen tersebut antara lain dokumen-dokumen yang berisikan tentang visi, misi, sasaran dan tujuan, strategi, program utama perusahaan, prosedur-prosedur dan kebijakan yang sudah diterapkan di perusahaan.

3.6.2 Wawancara

Menurut Sugiyono (2011: 317), wawancara digunakan sebagai teknik pengumpulan data apabila peneliti ingin melakukan studi pendahuluan untuk menemukan permasalahan yang harus diteliti, dan juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam dan jumlah respondennya sedikit. Teknik pengumpulan data dengan wawancara dapat dilakukan secara terstruktur maupun tidak terstruktur dan dapat dilakukan melalui tatap muka maupun dengan menggunakan telepon.

Dalam penelitian ini peneliti melakukan wawancara langsung tatap muka dengan beberapa pihak yaitu:

Tabel 3.1 Pihak yang terlibat dalam Pengumpulan Informasi dan Analisa

Pihak	Peran
Technical Manager	Memberikan informasi terkait pentingnya semua informasi yang ada di perusahaaan dan pentingnya informasi untuk dipelihara serta beberapa solusi yang bisa diterapkan.
System Engineer Manager	Memberikan informasi dan penjelasan mengenai proses-proses yang terjadi dalam penanganan keamanan informasi di D~Net.
Network Operational Center Staff	Memberikan informasi aktivitas-aktivitas nyata dari proses operasional NOC yang sedang terjadi.

Dimana membahas permasalahan apa saja yang ada di perusahaan tentang keamanan informasi data perusahaan serta kemungkinan beberapa solusi yang bisa diterapkan oleh perusahaan.

Analisis data dalam penelitian kualitatif dilakukan sejak sebelum memasuki lapangan, selama di lapangan, dan setelah selesai di lapangan (Sugiyono, 2009:89). Dalam penelitian ini, metode uji pengolahan data yang digunakan adalah pengujian substantif (*Substantive Test*). Pengujian substantif adalah perosedur yang digunakan untuk menguji kekeliruan atau kesalahan data yang kita ajukan ke responden yang berpengaruh terhadap kebenaran akan data tersebut.

Peneliti melakukan pengujian substantif untuk menguji apakah data yang dicatat benar-benar ada (terdokumentasi) atau ada bukti penunjang yang meyakinkan, jika peneliti merasa yakin bahwa data-data tersebut telah dicatat (terdokumentasi) atau ada bukti penunjang, auditor dapat meyakini bahwa data yang didapat adalah benar. Data yang didapat dari wawancara yang dilakukan oleh peneliti adalah data teknikal dimana untuk outputnya hanya ada dua, yaitu: apakah sudah dilaksanakan atau belum dilaksanakan ('Ya' atau 'Tidak').

3.6.3 Observasi

Observasi dilakukan dengan melakukan pengamatan langsung ke lapangan untuk memperoleh proses bisnis yang ada di perusahaan dan penerapan keamanan informasi yang sudah ada di D~Net Surabaya.

BAB 4

ANALISA DAN PEMBAHASAN

Pada bab ini menjelaskan mengenai perancangan tentang tata kelola Sistem Informasi Keamanan Data di D~Net Surabaya. Perancangan tersebut dapat diketahui dengan melakukan analisa terhadap kondisi yang ada saat ini. Analisa ini dilakukan dengan mempelajari kondisi internal dari D~Net Surabaya yang ada saat ini. Kondisi internal D~Net Surabaya selanjutnya akan dijadikan acuan atau dasar dalam melakukan perancangan kebijakan keamanan informasi.

4.1 Pendefinisian Ruang Lingkup

4.1.1 Produk dan Layanan D~Net

D~Net pusat yang beralamatkan di Graha Bumi Surabaya Jl. Basuki Rahmad 106 - 128 Kota Surabaya, Kode Pos 60271 merupakan salah satu perusahaan yang bergerak di bidang jasa, terutama sebagai penyedia layanan internet sebagai bisnis utamanya. Tidak hanya di Surabaya, D~Net juga memiliki cabang di Jakarta, Malang dan Denpasar untuk memperluas area pelayanannya. Untuk memperkuat posisi sebagai penyedia layanan internet yang terdepan, D~Net dituntut untuk melakukan inovasi produk dan layanannya. Dimana, yang dahulunya masih menggunakan teknologi yang lama sekarang bertransformasi menggunakan teknologi *cloud computing* dan otomatisasi untuk mempermudah pemeliharaan terhadap perangkat lunaknya.

Produk dan layanan yang ditawarkan oleh D~Net terdiri dari:

1. *Dedicated Connectivity*

   Dedicated Connectivity merupakan kategori layanan utama yang dimiliki D~Net. Layanan ini memberikan koneksi pribadi untuk pelanggan sehingga koneksi akan lebih terjamin dan stabil. Berbeda dengan kategori produk yang lain, Target pasar untuk *Dedicated Connectivity* adalah korporat, manufaktur, pendidikan, dan kesehatan yang membutuhkan akses yang lebih terjamin. Terdapat 4 buah layanan yakni:

a. D~Net Premium

D~Net Premium merupakan solusi layanan internet dedicated untuk mendukung kegiatan operasional bisnis, kebutuhan pribadi, ataupun game online yang menggunakan akses internet global. Salah satu keunggulan layanan ini yaitu fitur 100% capacity redundant yang memberikan jaminan backup koneksi agar Anda dapat menikmati layanan internet stabil dan berkualitas. D~Net Premium tersedia melalui jaringan dan infrastruktur D~Net dengan kenyamanan akses selama 24 jam dan layanan purna jual.

b. D~Net Corporate

D~Net Corporate adalah solusi untuk kebutuhan layanan internet berkualitas dengan harga ekonomis. Layanan ini memberikan koneksi stabil dan berkecepatan tinggi sehingga Anda dapat menikmati layanan internet selama 24 jam non stop. Koneksi internet dapat digunakan untuk mendukung kegiatan operasional bisnis, kebutuhan pribadi ataupun bermain game online yang membutuhkan koneksi internet global.

c. D~Net IIX

D~Net IIX merupakan layanan internet dedicated premium untuk korporasi yang hanya membutuhkan koneksi internet domestik. Dengan menggunakan media wireless melalui jaringan dan infrastruktur D~Net, pelanggan akan selalu terhubung dengan jaringan Indonesia Internet eXchange di Jakarta selama 24 jam.

d. D~Net Loop

Layanan D~Net Loop sangat tepat bagi perusahaan yang ingin menghubungkan kantor pusat dengan beberapa kantor cabang yang berada di satu wilayah ataupun lintas wilayah. Layanan ini menghubungkan jaringan WAN pelanggan melalui jaringan D~Net. Media yang akan digunakan tersedia dalam berbagai pilihan, Wireless, ADSL, dan Fiber Optic.

2. *Broadband Internet Connectivity*

Sebuah kategori layanan untuk memenuhi kebutuhan internet dengan skala pemakaian lebih kecil. *Broadband* sendiri berarti penggunaan jalur internet berbagi dengan pengguna lainnya, lebih dikenal dengan istilah "*up to*" karena D~Net selaku penyedia jasa internet tidak dapat menjamin jumlah bandwidth yang akan diterima pelanggan.

Broadband Internet Connectivity menyasar segmen yang berbeda dengan kategori *Dedicated Connectivity*, target pasar lebih mengarah ke pelanggan personal, usaha kecil, dan industri wisata skala kecil. Maka dari itu, terdapat 4 buah layanan yaitu:

a. D~Net Apartment

D~Net Apartment adalah pengganti produk *Internet Service Package for Apartment* (ISPA), sebuah layanan internet broadband untuk penghuni apartemen di Kota Surabaya, Memiliki skema berupa kerja sama dengan manajemen apartemen untuk sharing revenue. Kebijakan harga dan besaran presentasi bagi hasil ditentukan oleh kedua belah pihak melalui nota kerjasama. Layanan ini tersedia melalui jaringan POP yang ada di gedung-gedung apartemen dalam cakupan area layanan D~Net, melalui media wireless.

b. D~Net Office

D~Net Office merupakan layanan internet yang tersedia melalui jaringan POP (*Point Of Presence*) D~Net di gedung perkantoran maupun lokasi coverage area D~Net. Didukung oleh infrastruktur Fiber Optic yang didistribusikan lewat jaringan kabel di dalam gedung, pelanggan akan menikmati layanan internet berkecepatan tinggi. D~Net Office menggunakan metode sharing *revenue* untuk bekerja sama dengan gedung perkantoran mitra. Kebijakan harga dan besaran presentasi bagi hasil ditentukan oleh kedua belah pihak melalui nota kerjasama.

c. D~Net Visol

D~Net Visol adalah layanan internet broadband untuk pelanggan Villa dan personal (rumahan) yang hanya berlaku di area Bali. Berbagai kemudahan prosedur instalasi, koneksi internet unlimited hingga 4Mbps serta Technical Support yang siaga 24 jam akan menjamin bandwidth pelanggan sesuai SLA.

d. D~Net SOHO

D~Net SOHO adalah layanan internet broadband untuk pelanggan *Small Office* and *Home Office,* bisnis UKM, dan Rumah Toko, yang hanya berlaku di area Bali. Layanan ini memiliki kontrak selama minimal 1 tahun.

3. Layanan email, domain dan hosting

D~Net mengembangkan layanan email server handal dan aman. Untuk melengkapinya, D~Net juga menawarkan kebutuhan domain-hosting untuk keperluan bisnis. Terdapat 2 buah layanan yaitu:

a. DREAMS

DREAMS merupakan layanan server email handal, terpercaya, dan unik. Mudah digunakan dan mengedepankan sisi keamanan server email untuk meningkatkan operasional bisnis mulai dari segment SOHO hingga Korporasi.

b. Domain dan Hosting

Layanan domain D~Net merupakan layanan registrasi domain untuk keperluan perusahaan ataupun pribadi sebagai identitas unik. Pilihan layanan domain meliputi domain Indonesia (.id) dan domain internasional (.com, .net, .tv dst). Sedangkan, Layanan hosting D~Net terhubung dengan jaringan IIX dan Internasional selama 24 jam, Layanan ini digunakan mengatur konfigurasi website perusahaan atau website pribadi.

4. Layanan lainnya

Merupakan kumpulan produk *add-ons* dari layanan *Dedicated Connectivity*, Mulai dari layanan manajemen bandwidth, access point yang terintegrasi, hingga ketersediaan server handal dan aman untuk menyimpan data. Terdapat 4 layanan yaitu:

a. *Smart Gateway*

Layanan ini merupakan solusi untuk menjaga koneksi internet tetap lancar, mengatur traffic bandwidth, hingga mengatur akses ke situs di Internet dan sosial media. Menggunakan Routerboard MikroTik dan ditangani oleh teknisi handal dan bersertifikat, sehingga *resource* yang ada dapat dimaksimalkan secara tepat.

b. Colocation

Layanan yang menyediakan tempat untuk server maupun perangkat lain termasuk koneksi Internet ke Backbone Internet/IIX (Optional) dan tenaga listrik di Data Center milik D~Net. Perangkat pelanggan akan terjaga selama 24 jam, serta diawasi Technical Support berpengalaman. Data Center D~Net memiliki standar Internasional serta didukung jaminan keamanan serta tenaga listrik cadangan, yang menjamin server Anda berfungsi penuh selama 24 jam setiap harinya selama setahun penuh. Temperatur ruangan yang terjaga akan menjamin perangkat beroperasi pada suhu yang tepat, sehingga mengurangi resiko kerusakan akibat panas berlebih.

c. Officewifi

D~Net menghadirkan layanan internet cepat nirkabel (WIFI) dengan akses terpercaya. D~Net Officewifi mendukung kegiatan perusahaan, sekolah hingga perhotelan dalam meningkatkan kenyamanan berinternet secara mobile dan fleksibel.

d. Smart Wifi Monitoring

D~Net Smart WiFi Monitoring merupakan layanan manajemen Access Point guna mengidentifikasi *traffic* dan penggunaan internet. Layanan ini meningkatkan kenyamanan berinternet dan sangat cocok diterapkan mulai dari segmen SOHO, perhotelan, hingga korporasi.

4.1.2 Persetujuan Tingkat Layanan produk D~Net

Merupakan perjanjian layanan secara keseluruhan antara kedua belah pihak (pihak pelanggan dan pihak provider) untuk peningkatan kinerja D~Net. Persetujuan Tingkat Layanan atau SLA diberikan sebagai jaminan atas layanan yang diberikan kepada pelanggan, sehingga pelanggan tersebut merasa puas atas layanan yang diberikan. Salah satu aspek informasi yang harus dilindungi adalah menjamin a*vailability* atau ketersediaan, sehingga pihak pelanggan merasa terbantu dengan ketersediaan layanan yang diberikan oleh pihak provider karena proses pengelolaan data/informasi dengan pihak-pihak terkait (*customer*/vendor) berjalan lancar dan tidak terganggu karena layanan mengalami *down*.

- Cara menghitung SLA

Sebagai contoh D~Net memberikan SLA 99% atas layanan yang diberikan ke pelangan, artinya dalam 1 bulan D~Net menjamin bahwa layanan standar yang diberikan 99% dalam 1 bulan, dan 1% dianggap wajar jika terjadi *down* dalam layanan tersebut.

- 1 hari = 24 jam, 1 bulan = 30 hari
- 30 hari x 24 jam = 720 jam (merupakan layanan 100%)
- 99% * 720 jam = 712.8 jam (layanan standar dari D~Net, sisanya 7.2 jam dianggap wajar jika layanan mengalami *down*).

Sehingga batas akhir atau tolerensi yang di berikan apabila layanan mengalami *down* adalah 7.2 jam, jika layanan mengalami *down* lebih dari 7.2 jam maka pihak D~Net wajib memberikan restitusi kepada pelanggan tersebut.

Restitusi adalah mengganti kerugian, ganti kerugian yang diberikan kepada pelanggan oleh D~Net. Ganti rugi yang diberikan kepada pelanggan adalah potongan harga dari biaya bulanan.

- Cara menghitung Restitusi

Contoh : PT ABC membayar 1 juta per bulan kepada pihak D~Net, kemudian satu bulan pertama D~Net hanya bisa memberikan SLA 95%, sedangkan didalam kontrak seharunsya memberikan SLA 98%. Sehingga pihak D~Net harus memberikan restitusi kepada PT ABC.

- 98% – 90% = 8% (merupakan hak penggantian yang diterima oleh pelanggan, penggantian dalam bentuk pengurangan pembayaran).
- 1 bulan Rp. 1.000.000 = untuk layanan 98% (1% sekitar Rp. 10.204)
- Maka untuk layanan hanya 95% = 1.000.000 – (8% x Rp. 10.204)
- Rp. 1.000.000 – Rp. 81.632 = Rp. 918.368, Artinya dalam bulan ini PT ABC hanya punya kewajiban membayar sekitar Rp. 918.368

SLA sangat di butuhkan oleh pihak pelanggan karena dengan SLA dapat menjadi tolak ukur ketersedian layanan internet yang di berikan oleh D~Net. Apabila pelanggan sangat tergantung dengan komunikasi online seperti email, chat, dll atau system yang ada di perusahaan tersebut sudah online maka wajib memilih kualitas ISP yang memberikan layanan terbaik.

Berikut merupakan SLA yang diberikan D~Net ke pelanggan untuk setiap produk-produk D~Net:

Tabel 4.1 SLA Produk dan Layanan D~Net

No.	Layanan	SLA	Backup Upstream
1.	**D~Net Premium**	99.5%	100%
2.	**D~Net Corporate**	99%	50%
3.	**D~Net IIX**	99%	100%
4.	**D~Net Loop**	99%	-
5.	**D~Net Office**	98%	10%
6.	**D~Net SOHO**	90%	10%

Manager produk telah menganalisa selama setahun, berapa rata-rata jaringan di D~Net mengalami *down* sehingga itu menjadi acuan utama dalam pembentukan SLA selain itu ada keyakinan dari D~Net karena telah melakukan perbaikan dari segi keamanan jaringan.

Selama satu bulan pelanggan mendapatkan jaminan SLA yang telah diberikan D~Net, jika SLA tidak tercapai maka akan ada restitusi ke pelanggan dengan mengkonversi berapa total jam yang tidak mencapai SLA kemudian dilakukan pengurangan tagihan ke pelanggan. D~Net akan menyertakan bukti-bukti dan menginformasikan ke pelanggan terkait tidak tercapainya SLA.

Kebijakan keamanan informasi diperlukan untuk mendukung kegiatan operasional D~Net sehingga SLA yang diberikan ke pelanggan dapat tercapai 100%.

4.2 Analisa

4.2.1 Analisa Kelengkapan Dokumen Pendukung

Kelengkapan dokumen pendukung digunakan sebagai acuan dalam melakukan analisa baik berupa peraturan maupun prosedur. Setelah dilakukan wawancara dan observasi di lapangan, berikut hasil analisa kebijakan keamanan informasi beserta bukti pendukung:

Tabel 4.2 Dokumen Pendukung Kebijakan tentang penggunaan dan penyalahgunaan aset TI

Assessment	Bukti / Dokumen Pendukung	Memenuhi
Mengidentifikasi semua aset yang perlu dilindungi seperti aset informasi, aset software, aset fisik, layanan serta ditentukan pemilik / penanggung jawabnya dan dicatat agar dilindungi secara tepat.	Terdapat sebagian aset yang teridentifikasi dan disimpan di aplikasi D~Net manajemen.	✘ Tidak
Melakukan klasifikasi aset yang telah diidentifikasi.	Tidak ada bukti	✘ Tidak

Penilaian resiko terkait aset-aset yang ada dan *criticalities* sistem aset.	Tidak ada bukti	✘ Tidak
Melakukan review dan optimasi aset pada kondisi saat ini.	Tidak ada bukti	✘ Tidak
Melakukan penilaian dan pencatatan.	Tidak ada bukti	✘ Tidak

Tabel 4.3 Dokumen Pendukung Kebijakan tentang akses kontrol

Assessment	**Bukti / Dokumen Pendukung**	**Memenuhi**
Mengendalikan/membatasi akses *user* terhadap informasi-informasi yang ada di D~Net seperti akses jaringan, akses sistem operasional, akses aplikasi.	Prosedur akses kontrol.	✓Ya
Mengawasi sistem akses dan pemakaian akses kontrol oleh user terhadap informasi.	Prosedur pengawasan akses kontrol.	✓Ya
Sanksi yang tegas jika terbukti melakukan pelanggaran.	Prosedur *Performance Appraisal.*	✓Ya
Melakukan monitoring atau pengawasan.	Terdapat aplikasi monitoring *logging system*.	✓Ya

Tabel 4.4 Dokumen Pendukung Kebijakan tentang kontrol password

Assessment	**Bukti / Dokumen Pendukung**	**Memenuhi**
Menetapkan prosedur pengendalian *password* sebagai berikut: 1. User mendapatkan password awal sesuai dengan standar D~Net; 2. Password awal harus diganti saat pertama kali login; 3. Password awal bersifat (*unique*) untuk setiap user dan susah ditebak; 4. Memaksa *user* untuk mengubah	Prosedur instalasi laptop / komputer untuk karyawan baru.	✓Ya

*password*nya setelah 6 bulan dan menolak bila *user* memasukkan password yang sama dengan yang digunakan sebelum saat mengganti *password;* 5. Semua akses aplikasi, dan login komputer menggunakan *password* yang sama.		
Penggunaan *password* yang digunakan seharusnya: 1. Kumpulan dari huruf besar dan kecil, angka dan karakter khusus; 2. Minimal 8 karakter.	Menggunakan sistem login terpusat (*Active Directory*).	✔Ya
Kerahasiaan akan password *user* harus tetap terjaga.	Menggunakan sistem login terpusat (*Active Directory*).	✔Ya
User dan *password* yang digunakan untuk koneksi ke server atau jaringan harus *request* / mengirim tiket ke bagian terkait menggunakan aplikasi *ticketing*.	Terdapat di aplikasi *ticketing.*	✔Ya
Melakukan monitoring atau pengawasan.	Terdapat aplikasi monitoring *logging system*.	✔Ya

Tabel 4.5 Dokumen Pendukung Kebijakan tentang email

Assessment	**Bukti / Dokumen Pendukung**	**Memenuhi**
Akses email hanya dapat digunakan ketika menggunakan jaringan internal D~Net.	Prosedur operasional keamanan jaringan.	✔Ya
Adanya antisipasi dan menerapkan pengendalian pengamanan yang memadai dari ancaman dari pihak yang tidak bertanggung jawab, seperti *spamming, phising, mail relay*, virus dll. Untuk pengamanan bisa menggunakan antivirus atau *antispam.*	Prosedur untuk antisipasi dan pengendalian ancaman untuk email.	✔Ya

Filtering konten email yang tidak bertanggung jawab supaya tidak sampai ke *user.*	Prosedur *filtering* konten berdasarkan peraturan pemerintah.	✓ Ya
Melakukan monitoring atau pengawasan.	Terdapat aplikasi monitoring untuk email.	✓ Ya

Tabel 4.6 Dokumen Pendukung Kebijakan tentang internet

Assessment	**Bukti / Dokumen Pendukung**	**Memenuhi**
Adanya antisipasi dan menerapkan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, database dan jaringan, termasuk ancaman dari pihak yang tidak bertanggung jawab, seperti DDOS, *malicious code, Packet Sniffing*, *IP Spoofing* dll.	Prosedur operasional keamanan jaringan.	✓ Ya
Prosedur untuk melakukan *update*, pengujian dan instalasi.	Prosedur untuk *update* dan *resarch.*	✓ Ya
Akses ke server dan perangkat jaringan lainnya diharuskan menggunakan autentikasi dan teknik kriptografi untuk mengamankan proses transaksi informasi. Teknik kriptografi yang bisa digunakan antara lain menggunakan *enkripsi* dan *digital signatures* (menggunakan *public key*) disesuaikan dengan informasi yang akan diakses.	• Prosedur instalasi server baru. • Prosedur konfigurasi server.	✓ Ya
Adanya *logging system* / *syslog* yang terpusat untuk semua server. Digunakan untuk analisa jika terdapat anomali.	Terdapat aplikasi monitoring *logging system*.	✓ Ya
Adanya *Intrusion Detection System* (IDS).	Tidak ada bukti	✘ Tidak
Adanya *Intrusion Prevention System* (IPS).	Tidak ada bukti	✘ Tidak
Semua aplikasi yang terhubung dengan	Tidak semua aplikasi	✘ Tidak

IP Public harus menggunakan *Secure Socket Layer* (SSL)	menggunakan SSL	
Backup System	• Prosedur *backup* sistem Sistem *backup* sudah tersentralisasi dan sebagian *backup* ada di amazone	✓Ya
Melakukan monitoring atau pengawasan.	Terdapat aplikasi monitoring internet.	✓Ya

Tabel 4.7 Dokumen Pendukung Kebijakan tentang penanganan virus

Assessment	Bukti / Dokumen Pendukung	Memenuhi
Setiap perangkat harus terinstal antivirus yang *up-to-date* (jika memungkinkan diinstal).	Prosedur instalasi laptop / komputer untuk karyawan baru.	✓Ya
Antivirus harus selalu diperbarui.	Prosedur untuk *auto update* antivirus.	✓Ya
Melakukan monitoring atau pengawasan.	Terdapat aplikasi monitoring.	✓Ya

Tabel 4.8 Dokumen Pendukung Kebijakan tentang pengklasifikasian informasi

Assessment	Bukti / Dokumen Pendukung	Memenuhi
Mengidentifikasi semua sumber daya informasi yang perlu dilindungi.	Tidak ada bukti	✘ Tidak
Informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya.	Tidak ada bukti	✘ Tidak
Strandarisasi penamaan informasi dan pelabelan.	Tidak ada bukti	✘ Tidak

Tabel 4.9 Dokumen Pendukung Kebijakan tentang pengklasifikasian dokumen

Assessment	Bukti / Dokumen Pendukung	Memenuhi
Mengidentifikasi semua dokumen yang perlu dilindungi.	Tidak ada bukti	✘ Tidak
Dokumen perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya.	Terdapat di aplikasi D~Net manajemen.	✔ Ya
Standarisasi penamaan dan pelabelan dokumen.	Tidak ada bukti	✘ Tidak

Tabel 4.10 Dokumen Pendukung Kebijakan tentang akses remote

Assessment	Bukti / Dokumen Pendukung	Memenuhi
Permintaan tentang hak akses remote harus melalui prosedur yaitu melakukan *request* / mengirim tiket ke bagian terkait menggunakan aplikasi *ticketing.*	Terdapat di aplikasi *ticketing.*	✔ Ya
Diharuskan menggunakan metode *tunneling*, bisa menggunakan VPN (*Vitual Private Network*).	Prosedur konfigurasi *tunneling*.	✔ Ya
Untuk *user collocation* tergantung mereka sendiri apakah menyediakan akses remote atau tidak menyediakan akses remote.	MOU (*Memorandum of Understanding*) dengan *user.*	✔ Ya
Melakukan monitoring atau pengawasan.	Terdapat aplikasi monitoring *logging system*.	✔ Ya

Tabel 4.11 Dokumen Pendukung Kebijakan tentang akses penyedia layanan TI, informasi dan komponen

Assessment	Bukti / Dokumen Pendukung	Memenuhi
Identifikasi semua penyedia layanan TI / *supplier.*	Tidak ada bukti	✘ Tidak
Pembatasan hak akses penyedia layanan TI / *supplier.*	Tidak ada bukti	✘ Tidak
Dokumentasi dan pelaporan terkait kegiatan penyedia layanan TI / *supplier.*	Tidak ada bukti	✘ Tidak

Tabel 4.12 Dokumen Pendukung Kebijakan tentang pelepasan aset

Assessment	Bukti / Dokumen Pendukung	Memenuhi
Identifikasi aset yang sudah tidak digunakan.	Tidak ada bukti	✘ Tidak
Analisa aset, apakah bisa dimanfaatkan ke perangkat lain.	Analisa dilakukan ketika membutuhkan suku cadang.	✘ Tidak
Semua transaksi terkait perpindahan harus disetujui oleh manager.	Persetujuan hanya sebatas lisan.	✘ Tidak
Dokumentasi aset yang sudah tidak digunakan beserta transaksinya.	Tidak ada bukti	✘ Tidak

4.2.2 Hasil Analisa Kelengkapan Dokumen Kebijakan Keamanan Informasi

Berdasarkan pada penelitian analisa kualitatif kelengkapan dokumen pendukung kebijakan keamanan informasi, menunjukkan bahwa sebagian besar masih terdapat beberapa proses manajemen keamanan informasi perlu dilakukan pembenahan dan dibuatkan kebijakannya sesuai dengan kerangka kerja ITIL v3. Dari hasil analisa tersebut maka dapat diketahui hasil review sebagai berikut:

a. Kebijakan tentang penggunaan dan penyalahgunaan aset TI, menunjukkan tidak ada dokumen pendukung yang dilengkapi dari 5 dokumen pendukung yang seharusnya ada (0%).
b. Kebijakan tentang akses kontrol, menunjukkan bahwa dokumen pendukung semuanya sudah terlengkapi dari 4 dokumen pendukung yang seharusnya ada (100%).
c. Kebijakan tentang kontrol password, menunjukkan bahwa dokumen pendukung semuanya sudah terlengkapi dari 5 dokumen pendukung yang seharusnya ada (100%).
d. Kebijakan tentang email, menunjukkan bahwa dokumen pendukung semuanya sudah terlengkapi dari 4 dokumen pendukung yang seharusnya ada (100%).
e. Kebijakan tentang internet, menunjukkan 6 dokumen pendukung lengkap (67%) dan 3 dokumen pendukung tidak lengkap (33%).
f. Kebijakan tentang penanganan virus, menunjukkan bahwa dokumen pendukung semuanya sudah terlengkapi dari 3 dokumen pendukung yang seharusnya ada (100%).
g. Kebijakan tentang pengklasifikasian informasi, menunjukkan tidak ada dokumen pendukung yang dilengkapi dari 3 dokumen pendukung yang seharusnya ada (0%).
h. Kebijakan tentang pengklasifikasian dokumen, menunjukkan 1 dokumen pendukung lengkap (33%) dan 2 dokumen pendukung tidak lengkap (77%).
i. Kebijakan tentang akses remote, menunjukkan bahwa dokumen pendukung semuanya sudah terlengkapi dari 4 dokumen pendukung yang seharusnya ada (100%).
j. Kebijakan tentang akses penyedia layanan TI, informasi dan komponen, menunjukkan tidak ada dokumen pendukung yang dilengkapi dari 3 dokumen pendukung yang seharusnya ada (0%).

k. Kebijakan tentang pelepasan aset, menunjukkan tidak ada dokumen pendukung yang dilengkapi dari 4 dokumen pendukung yang seharusnya ada (0%).

Tabel 4.13 Review kelengkapan dokumen pendukung

No.	Kebijakan	Jumlah Dokumen Pendukung	Kelengkapan Dokumen Pendukung	Prosentase
1.	Penggunaan dan penyalahgunaan aset TI	5	0	0%
2.	Akses kontrol	4	4	100%
3.	Kontrol password	5	5	100%
4.	Email	4	4	100%
5.	Internet	9	6	67%
6.	Penanganan virus	3	3	100%
7.	Pengklasifikasian informasi	3	0	0%
8.	Pengklasifikasian dokumen	3	1	33%
9.	Akses remote	4	4	100%
10.	Akses penyedia layanan TI, informasi dan komponen	3	0	0%
11.	Pelepasan aset	4	0	0%

Dari total 47 dokumen pendukung, 27 dokumen sudah terlengkapi (57%) dan 20 dokumen pendukung belum terlengkapi (43%). Tidak lengkapnya dokumen pendukung dikarenakan belum terdokumentasikannya semua proses dengan baik dan tidak adanya kebijakan tersebut dalam kegiatan operasional. Sehingga diperlukan adanya perbaikan terhadap dokumentasi manajemen keamanan informasi yang ada saat ini dan pembuatan kebijakan keamanan informasi menurut ITIL dan apa yang diharapkan oleh manajemen terkait manajemen keamanan informasi dapat tercapai.

4.3 Evaluasi Dokumen Pendukung Kebijakan Keamanan Informasi

Perencanaan berfokus pada desain dan rekomendasi dari langkah-langkah keamanan yang tepat berdasarkan kebutuhan organisasi. Persyaratan ini diperoleh dari sumber seperti penjualan dan risiko layanan, rencana dan strategi, SLA (*Service Level Agreements*) dan OLA (*Operational Level Agreement*), hukum, moral dan etika untuk keamanan informasi.

Berdasarkan hasil analisa di atas, kebijakan keamanan informasi di D~Net sudah ada, tetapi masih ada beberapa yang harus diperbaiki dan ditambahkan.

Tabel 4.14 Daftar kekurangan Dokumen Pendukung Kebijakan

No.	Kekurangan Dokumen Pendukung Kebijakan	Yang harus dilakukan
1	Belum adanya kebijakan tentang pengklasifikasian informasi dan dokumen. • Hal ini dapat berdampak pada tidak adanya perlindungan khusus terhadap informasi yang ada karena untuk masing-masing informasi tingkat kerahasiaannya sama.	• Divisi IT melakukan pendokumentasian dan pengklasifikasian informasi sesuai dengan tingkat kepentingannya.
2	Belum adanya kebijakan tentang pelepasan aset. • Hal ini akan berdampak tidak ada dokumentasi yang jelas terhadap aset-aset yang sudah tidak terpakai dan terjual.	• Divisi IT membuat kebijakan terkait pelepasan aset-aset yang sudah tidak terpakai dan dilakukan pendokumentasian secara berkala.
3	Belum adanya sanksi yang tegas bagi staf yang memberikan informasi user passwordnya ke staf lain. • Hal ini dapat mengakibatkan kecurangan terkait informasi penting yang ada di perusahaan.	• Divis terkait membuat suatu peraturan terkait pelanggaran-pelanggaran dan sanksi yang akan diterima jika melakukan pelanggaran tersebut.

4	Belum terdapat *transfer knowledge* yang baik antar staff ketika merancang, mengaplikasikan serta memelihara keamananan informasi. • Hal ini dapat mengakibatkan proses fitur baru maupun pengembangan dari fitur yang sudah ada berjalan dengan waktu yang cukup lama karena perlu pemahaman terlebih dahulu.	• Divisi IT menerapkan *transfer knowledge* ke *end user*. • Pendokumentasian *knowledge.*
6	Belum terdapat perangkat keamanan jaringan TI yang memadai (*firewall*, IPS, IDS). • Hal tersebut dapat berpotensi menimbulkan celah keamanan informasi.	• Divisi IT melakukan fungsi terkait untuk merancang design keamanan jaringan TI, kemudian mengimplementasikan rancangan yang telah dibuat.
7	Belum terdapat perencanaan pelatihan keamanan informasi secara *continuity*. • Hal tersebut dapat berpotensi keahlian staff tidak *up-to-date*.	• Divisi TI melakukan penjadwalan secara rutin terkait dengan pelatihan keamanan informasi dan *sharing knowledge* antar staff TI.
8	Belum teridentifikasinya dan terdokumentasikannya semua aset informasi yang ada di perusahaan serta belum ter-*update*. • Hal tersebut dapat menimbulkan ketidaktransparanan informasi.	• Divisi TI melakukan identifikasi semua aset yang berhubungan dengan TI dan mendokumentasikan secara berkala.
9	Belum adanya analisa resiko terkait aset-aset yang dimiliki perusahaan. • Hal tersebut dapat berdampak negatif terhadap kualitas layanan yang diberikan kepada para pelanggan.	• Divisi TI menentukan fungsi yang bertugas melakukan analisa resiko terhadap aset-aset yang dimiliki perusahaan secara berkala. • Divisi TI menetukan mitigasi dari hasil analisa resiko tersebut kemudian memonitor dan mengevaluasi secara

		berkala.
10	Tidak semua aplikasi yang terhubung dengan *IP Public* menggunakan SSL • Hal tersebut dapat berpotensi menimbulkan celah keamanan informasi.	• Divisi TI menambahkan SSL kesemua aplikasi khususnya aplikasi yang terhubung dengan IP Public / jaringan internet.
11	Belum terdapat dan terdokumentasi dengan baik sebagai acuan untuk pengelolaan preses keamanan TI. a. Dokumentasi terkait proses keamanan informasi: • Berita acara • User manual • Dokumen teknis b. Pelaporan hasil realisasi dan evaluasi. c. Arsitektur TI: • Informasi • Infrastruktur Jaringan • Infrastruktur *Hardware*	• Semua aktifitas operasional divisi TI dilakukan pendokumentasian secara detail.
12	Belum adanya kebijakan tentang akses penyedia layanan TI, informasi dan komponen. Hal ini akan berdampak tidak ada informas dan dokumentasi yang jelas terhadap akses penyedia layanan TI.	• Divisi IT membuat kebijakan terkait akses penyedia layanan TI, informasi dan komponen serta dilakukan pendokumentasian secara berkala.

Untuk menunjang kegiatan operasional dari temuan-temuan diatas, berikut beberapa rekomendasi yang dapat dilaksanakan, yaitu:

1. Melakukan sosialisasi yang menekankan terhadap Pedoman Keamanan Informasi yang ada di perushaan kepada seluruh staff secara berkala.
2. Agar Divisi TI menentukan mekanisme pengukuran keberhasilan proses-proses TI yang ada di dalamnya / KPI.

3. Agar Divisi TI mengoptimalkan penggunaan website perusahaan dan portal internal dalam peyampaian informasi baik untuk internal perusahaan maupun untuk pelanggan D~Net.
4. Agar D~Net memperketat pengamanan fisik di area kantor supaya tidak dapat dimasuki oleh pihak yang berwenang, seperti: menempatkan *security* di area kantor, menyediakan *log book* untuk ruang server, akses masuk ke ruang server menggunakan *fingerprint*.
5. Agar Divisi TI memilliki struktur organisasi yang sesuai dengan kebutuhan dan fungsi-fungsi untuk menjalankan kegiatan operasional.
6. Agar Divisi TI melakukan *research* untuk pengembangan sistem keamanan informasi yang sudah ada.
7. Agar Divisi TI mendapatkan pelatihan keamanan informasi secara berkala untuk meningkatkan *skill* tiap individu.
8. Agar Divisi TI melakukan otamatisasi disetiap proses TI yang dijalankan. Sangat bermanfaat jika melakukan pemeliharan dalam jumlah yang banyak.
    a. Dapat meningkatkan efisiensi waktu pengerjaan,
    b. Meminimalkan pengeluaran pada biaya,
    c. Penggabungan dan penerapan teknologi baru,
    d. Memperbarui proses operasional divisi TI,
    e. Meningkatkan produktivitas,
    f. dan peningkatan komunikasi dapat menghasilkan keputusan yang lebih baik dan lebih cepat.
9. Agar Divisi TI mengimplementasikan server untuk autentikasi terpusat atau yang biasa disebut AAA (*Authentication, Authorization, Accounting*). Server AAA digunakan untuk mengontrol hak akses masuk ke server. Diharapkan dapat meningkatkan kemanan terhadap server-server yang dimiliki D~Net.
10. Agar Divisi TI menerapkan sistem *cloud computing*, dimana semua data tersimpan di server secara terpusat, flexibilitas dan skalabilitas tinggi dan untuk investasi jangka panjang.

4.4 Perancangan Kebijakan Keamanan Informasi

Kebijakan keamanan informasi dirancang untuk mendukung pencapaian tingkat kapabilitas yang diharapkan perusahaan. Rancangan dibuat untuk bisa dijadikan acuan oleh D~Net untuk mencapai tujuan dari setiap proses kegiatan operasional. Pada proses verfikasi kebijakan keamanan informasi ini diwakilkan oleh *System Enginer Manager* dengan melakukan pengecekan apakah sudah sesuai dengan tujuan TI yang ada di perusahaan.

Berdasarkan hasil analisa yang telah dilakukan terhadap kebijakan keamanan informasi yang ada di D~Net, hingga pada proses verifikasi dokumen, berikut rancangan kebijakan keamanan informasi sesuai dengan kerangka kerja ITIL v3:

4.4.1 KEBIJAKAN ASET

4.4.1.1 PENDAHULUAN

Aset seharusnya dapat dilacak dengan mudah. Salah satu alasan utama melacak aset, yaitu untuk pengendalian perangkat dan untuk keamanan aset. Kebijakan pengendalian aset tidak hanya memungkinkan aset perusahaan untuk dilacak mengenai lokasinya dimana dan siapa yang menggunakan tetapi juga akan melindungi data yang tersimpan pada aset tersebut.

4.4.1.2 TUJUAN

Kebijakan ini dirancang untuk melindungi dan mengendalikan aset perusahaan pada jaringan. Kebijakan ini akan membantu mencegah hilangnya data atau aset perusahaan dan mengurangi risiko kehilangan data karena tidak terdokumentasikannya aset perusahaan.

4.4.1.3 RUANG LINGKUP

Semua karyawan yang memiliki akses ke sistem komputer perusahaan harus mematuhi kebijakan pengendalian aset untuk melindungi keamanan jaringan, melindungi integritas data, dan melindungi aset perusahaan lainnya.

4.4.1.4 KEBIJAKAN

- Semua aset harus teridentifikasi:
    1. Nama aset.
    2. ID unik dari aset tersebut.
    3. Siapa yang bertanggung jawab terhadap aset tersebut.
    4. Dimana lokasi aset sekarang berada.
    5. Terdapat serah terima aset.
    6. Jika terjadi perpindahan aset, data/informasi aset sebelumnya tetap disimpan sebagai history.
    7. Status / kondisi.

- Semua aset yang teridentifikasi harus memiliki atau dibuatkan satu kode unik untuk identitasnya.
- Semua informasi tentang aset harus disimpan di database (mencakup semua informasi secara detail) supaya mudah dilakukan pelacakan.
- Dilakukan pengecekan atau identifikasi aset secara berkala baik pencocokan data dari database dan pencocokan secara fisik di lapangan.
- Semua aset harus diklasifikasikan.
- Melakukan penilaian resiko terhadap aset-aset yang telah teridentifikasi.
- Dikenakan sanksi jika terbukti menyalahgunakan aset perusahaan.

4.4.2 KEBIJAKAN AKSES KONTROL

4.4.2.1 PENDAHULUAN

Keamanan informasi adalah perlindungan terhadap informasi baik kegiatan yang disengaja maupun tidak disengaja dan modifikasi atau perusakan. Informasi adalah aset berharga dari perusahaan yang harus dikelola dengan hati-hati. Semua informasi memiliki nilai, namun tidak semua informasi memiliki nilai yang sama atau memerlukan tingkat perlindungan yang sama.

4.4.2.2 TUJUAN

Kontrol akses bertujuan melindungi informasi dengan mengendalikan hak-hak pengguna untuk menggunakan sumber daya informasi yang berbeda dan menjaga informasi terhadap penggunaan yang tidak sah.

4.4.2.3 RUANG LINGKUP

Kebijakan ini berlaku untuk semua karayawan D~Net dimana memiliki hak untuk mengakses informasi dan sistem informasi.

4.4.2.4 KEBIJAKAN

- Mengidentifikasi pengguna resmi dari aset informasi dan menentukan hak akses / pembatasan penggunaan (misalnya: individu, kelompok, sistem, aplikasi, anonim, dan sementara).
- Menonaktifkan akun yang sudah tidak diperlukan (termasuk karyawan telah keluar dari perusahaan).
- Tidak boleh terdapat akses ganda dalam mengakses aset informasi.
- Memberikan akses ke sistem berdasarkan otorisasi yang berlaku dan terkait kebutuhan akan sistem yang diakses.
- Penambah akses ke sistem harus menggunakan sistem *ticketing* yang telah disediakan D~Net.

- Memberi sanksi yang tegas jika terdapat akun yang terbukti melakukan pelanggaran.
- Setiap ruang kerja, ruang server, ruang rapat harus memiliki keamanan fisik untuk bisa masuk ke dalam ruangan tersebut, seperti: CCTV, menempatkan *security* di area kantor, *fingerprint* dan *log book*.
- Melakukan pemantauan terhadap akun yang mengakses secara tidak sah ke aset informasi.

4.4.3 KEBIJAKAN KONTROL PASSWORD

4.4.3.1 PENDAHULUAN

Password merupakan aspek penting dalam keamanan komputer. Pemilihan password yang salah dapat mengakibatkan membahayakan seluruh jaringan perusahaan. Dengan demikikan semua karyawan D~Net, kontraktor maupun vendor yang memiliki akses ke D~Net bertanggung jawab untuk mengambil langkah-langkah yang tepat dalam mengamankan password.

4.4.3.2 TUJUAN

Tujuan dari kebijakan ini adalah menetapkan standar dalam pembuatan password yang kuat, melindungi password dan melakukan perubahan password secara berkala.

4.4.3.3 RUANG LINGKUP

Ruang lingkup kebijakan ini mencakup semua karyawan yang memiliki tanggung jawab terhadap akunnya masing-masing, dimana memilliki akses ke jaringan perusahaan atau yang dapat mengakses informasi perusahaan.

4.4.3.4 KEBIJAKAN

A. Umum

- Setiap sistem memiliki tingkatan level password (misalnya: administrator, admin, user dll).
- Setiap password harus diubah setidaknya setiap 6 bulan.
- Akun pengguna yang memiliki hak istimewa diberikan melalui proses *approval* harus memiliki password yang unik.
- Password tidak boleh ditulis di kertas, disimpan di email maupun perangkat lain.

- Password untuk server harus benar-benar dijaga kerahasiaannya (untuk akses lokal server), sedangkan untuk mengakses server harus menggunakan *digital signature* (menggunakan *public key*).
- User dan password untuk serever harus *request* menggunkan aplikasi *ticketing*.
- Melakukan pemantauan terhadap user dan password.

B. Pedoman

1. Pedoman Pembuatan Password

Password di D~Net digunakan untuk berbagai tujuan, misalnya: untuk masuk ke portal, login ke laptop/komputer, akun untuk email dan untuk aplikasi-aplikasi internal. Oleh karena itu harus disadari bagaimana memilih password yang bagus dan kuat.

Password harus memiliki karakteristik sebagai berikut:

- Mengandung karakter huruf besar dan kecil.
- Memiliki angka dan tanda baca, misalnya: 0-9, @ # $% ^ & * () _ + | ~ -! = \ ` { } []:?."; '<>, /)
- Panjang password minimal 8 karakter.
- Semestinya bukan berupa informasi pribadi, nama keluarga dll.
- Password setidaknya mudah diingat tetapi memiliki karakteristik yang kuat.

2. Standar Perlindungan Password

- Tidak boleh berbagi password dengan siapa pun.
- Password tidak boleh ditulis dan disimpan.
- Jika sedang menggunakan aplikasi jangan menggunakan *"Remember Password"*.
- Perubahan password dilakukan maksimal 6 bulan, jika tidak melakukan perubahan password maka tidak bisa mengakses semua informasi yang ada di D~Net.

4.4.4 KEBIJAKAN EMAIL

4.4.4.1 PENDAHULUAN

Hampir semua perusahaan menggunakan email sebagai alat komunikasi utama dalam bisnis mereka, oleh karena itu perlu adanya kesadaran dari pengguna dalam menggunakan email. Penyalahgunaan pemakaian email dapat dibawa ke ranah hukum, melanggar privasi seseorang dan memiliki resiko terkait keamanan, sehingga penting bagi pengguna untuk memahami penggunaan yang tepat dari email.

4.4.4.2 TUJUAN

Tujuan dari kebijakan ini adalah memastikan penggunaan yang tepat dari email perusahaan dan membuat karyawan menyadari apa yang dilakukan sudah baik dan diterima oleh sistem email.

4.4.4.3 RUANG LINGKUP

Kebijakan ini mencakup penggunaan yang tepat dari email perusahaan dan berlaku untuk semua karyawan yang melakukan pekerjaan atas nama perusahaan.

4.4.4.4 KEBIJAKAN

A. Umum

- Semua pengguna email harus berperilaku etis dan sesuai dengan hukum yang berlaku dalam mengirim email.
- Akun email harus digunakan terutama untuk tujuan bisnis perusahaan, tetapi untuk tujuan komersial dilarang.
- Semua data yang terdapat dalam email atau lampiran harus diamankan.
- Dilarang mengirim konten-konten yang berisi tentang SARA dan Pornografi, jika terdapat karyawan yang menerima email yang berisi konten-konten tersebut karyawan bisa melapor ke divisi terkait.

- Dilarang secara otomatis meneruskan email ke pihak ketiga yang tidak berkaitan dengan perusahaan.
- Semua transaksi email yang terkait dengan proses bisnis perusahaan harus menggunakan email perusahaan.

B. Persyaratan

- Divisi TI harus mengamankan semua transaksi email perusahaan dari pihak yang tidak bertanggung jawab.
- Divisi TI memastikan bahwa email perusahaan hanya dapat diakses dan digunakan ketika terhubung jaringan internal D~Net.
- Divisi TI melakukan *filtering* konten agar tidak sampai ke pelanggan.
- Divisi TI melakukan monitoring terhadap email server.

4.4.5 KEBIJAKAN INTERNET

4.4.5.1 PENDAHULUAN

Koneksi internet memiliki berbagai resiko untuk perusahaan dan harus diatasi untuk mengamankan aset informasi yang penting bagi perusahaan. Akses internet secara berlebihan dapat mempengaruhi produktivitas kerja karena waktu habis digunkan untuk internet. Semestinya akses internet diberikan kepada karyawan untuk mendukung kegiatan bisnis perusahaan.

4.4.5.2 TUJUAN

Tujuan dari kebijakan ini adalah untuk menentukan penggunaan yang tepat dari internet bagi karyawan D~Net.

4.4.5.3 RUANG LINGKUP

Kebijakan penggunaan internet ini berlaku untuk semua pengguna internet (individu yang bekerja untuk perusahaan, termasuk karyawan paruh waktu, pekerja kontrak, mitra bisnis dan vendor) yang mengakses internet melalui komputer atau jaringan internal perusahaan.

4.4.5.4 KEBIJAKAN

A. Umum

- Akses layanan internet akan diberikan berdasarkan tanggung jawab pekerjaan karyawan saat ini.
- Persyaratan akses pengguna internet akan ditinjau secara berkala oleh divisi terkait.
- Menggunakan sumber daya perusahaan komputer dengan mengakses internet untuk keperluan pribadi secara tidak wajar, tanpa persetujuan dari manajer pengguna dan departemen IT, dapat dipertimbangkan untuk tindakan disiplin.

- Penggunaan internet diberikan dengan tujuan untuk mendukung kegiatan bisnis perusahaan. Terkait penggunaan internet yang diberikan yaitu:
    1. Untuk komunikasi antar karyawan atau pihak ketiga untuk tujuan bisnis.
    2. Untuk mendukung operasional TI, seperti upgrade software dan download *patch*.
    3. Untuk mendukung pekerjaan tiap-tiap divisi.
    4. dan untuk penelitian.

B. Persyaratan

- Divisi TI harus melakukan pengamanan yang ketat terhadap jaringan internet agar tidak disalahgunakan oleh pihak ketiga.
- Divisi TI harus melakukan *update* secara rutin, melakukan pengujian dan instalasi.
- Divisi TI melakukan monitoring terhadap jaringan internet perusahaan.
- Divisi TI melakukan tindakan koreksi, korektif dan pencegahan terkait ancaman yang ada di internet.
- Divisi TI memastikan semua akses ke server menggunakan metode *digital signatures.*

4.4.6 KEBIJAKAN PENANGANAN VIRUS

4.4.6.1 PENDAHULUAN

Virus merupakan program perangkat lunak berbahaya yang dirancang untuk menghancurkan atau merusak informasi, mencuri data pengguna dan merusak sistem. Infeksi oleh virus dapat mengurangi kelancaran proses bisnis perusahaan, karena bisa beresiko kehilangan data dan memerlukan waktu untuk pemulihan / mengalami keterlambatan dalam melakukan pekerjaan yang dirasa itu penting.

4.4.6.2 TUJUAN

Kebijakan ini dibuat untuk membantu mencegah komputer/laptop D~Net dari infeksi virus, mengamankan jaringan dan kode berbahaya. Kebijakan ini dimaksudkan untuk membantu mencegah kerusakan aplikasi pengguna, data, file, dan perangkat keras.

4.4.6.3 RUANG LINGKUP

Semua karyawan D~Net yang terlibat akses ke komputer kantor, jaringan dan sistem aplikasi internal harus mematuhi kebijakan ini.

4.4.6.4 KEBIJAKAN

- Semua perangkat komputer/laptop yang terhubung ke jaringan internal harus memiliki antivirus dan sudah dikonfigurasi sehingga dapat mendeteksi virus.
- Secara rutin dan otomatis antivirus diperbarui.
- Semua file pada perangkat komputer akan di*scan* secara berkala untuk pencegahan dari infeksi virus.
- Jika perangkat komputer/laptop ditemukan sudah terinfeksi virus maka tidak boleh terhubung ke jaringan lokal dan diberikan ke *IT Infrastructure* untuk dilakukan pemulihan.

4.4.7 KEBIJAKAN PENGKLASIFIKASIAN INFORMASI DAN DOKUMEN

4.4.7.1 PENDAHULUAN

Informasi telah menjadi aset penting yang menentukan kelangsungan sebuah perusahaan, pengamanan informasi menjadi lebih diperlukan dari sebelumnya. Tidak semua informasi mempunyai nilai guna yang sama atau memiliki resiko yang sama sehingga dalam proses perlindungannya berbeda, sehingga agar efisien informasi harus diklasifikasikan.

4.4.7.2 TUJUAN

Tujuan dari kebijakan ini adalah untuk menentukan kewajiban karyawan dalam mengidentifikasi, mengklasifikasi, dan menjaga informasi dalam rangka untuk melindungi privasi, kerahasiaan, integritas dan ketersediaan aset informasi yang ada di D~Net .

4.4.7.3 RUANG LINGKUP

Kebijakan ini berlaku bagi semua karyawan D~Net yang bertanggung jawab untuk memberikan semua informasi yang mereka ketahui dan didokummentasikan ke aplikasi *project management*.

4.4.7.4 KEBIJAKAN

A. Umum

- Setiap hasil atau laporan dari kegiatan yang berupa informasi harus di informasikan, disimpan di *project management* dan dikelompokkan.
- Sistem teknologi informasi yang digunakan di perusahaan saat ini harus di informasikan dan disimpan di *project management* dan dikelompokkan.

- Dalam menerapkan klasifikasi informasi dan dokumen, yang dilakukan adalah:
    1. Melakukan labeling terhadap informasi.
    2. Menyimpan informasi.
    3. Menghapus informasi yang tidak dibutuhkan.
    4. Melindungi integritas informasi.
    5. Membangun akuntabilitas.

B. Klasifikasi Informasi dan Dokumen

1 Informasi Umum

Informasi yang dibuat dalam kegiatan proses bisinis perusahaan dan jika terdapat kebocoran informasi tidak menyebabkan kerusakan dan tidak mempengaruhi proses bisnis perusahaan. Informasi ini tersedia untuk umum, karyawan dan pihak ketiga.

Contoh Informasi Umum:

1. Informasi yang ada di website perusahaan.
2. Posisi dan deskripsi pekerjaan setiap karyawan.
3. Laporan berkala (*newsletter*).
4. Iklan dan brosur terkait produk D~Net.
5. Pemberitahuan ke pelanggan.

2 Informasi Internal

Informasi yang dibuat untuk kebutuhan internal perusahaan. Hanya karyawan D~Net yang dapat mengakses informasi ini.

Contoh Informasi Internal:

1. Posisi dan deskripsi pekerjaan setiap karyawan.
2. Nomor ekstensi telepon tiap divisi.
3. User manual.
4. *Standard Operating Procedure* (SOP) tiap divisi .

3 Informasi Rahasia

Merupakan informasi yang dilindungi perusahaan, hanya divisi tertentu yang dapat mengakses informasi tersebut.

Contoh Informasi Rahasia:

1. Informasi pembelian.
2. Draft gaji karyawan.
3. Laporan audit.
4. Informasi keuangan perusahaan / laporan *budgeting*.

4 Informasi Terbatas

Merupakan informasi yang sangat sensitif. Akses informasi yang tidak sah atau tidak disengaja ke informasi ini akan berdampak pada kelangsungan proses bisnis perusahaan.

Contoh Informasi Terbatas:

1. User dan password server-server D~Net.
2. Strategi perusahaan.

4.4.8 KEBIJAKAN AKSES REMOTE

4.4.8.1 PENDAHULUAN

Dengan adanya akses remote perusahaan dapat memberikan dukungan dan respon yang lebih baik kepada pelanggan. Kelebihan kompetitif lainnya adalah membuat karyawan menjadi lebih produktif dan efisien.

4.4.8.2 TUJUAN

Tujuan dari kebijakan ini adalah menentukan standar untuk menghubungkan koneksi dari luar ke jaringan lokal perusahaan. Standar ini dirancang untuk meminimalkan potensi kerusakan dari penggunaan yang tidak sah. Kerusakan meliputi hilangnya data sensitif atau rahasia perusahaan, kekayaan intelektual, kerusakan citra publik, kerusakan sistem internal, dll.

4.4.8.3 RUANG LINGKUP

Ruang lingkup kebijakan ini mencakup semua karyawan yang melakukan koneksi dari luar ke jaringan lokal perusahaan. Kebijakan ini berlaku untuk koneksi akses remote yang digunakan untuk melakukan pekerjaan kantor dari luar.

4.4.8.4 KEBIJAKAN

A. Umum

- Hak akses remote hanya diberikan kepada teknisi D~Net untuk kegiatan operasional seperti troubleshooting, maintenance dll.
- Dalam pemberian hak akses remote, teknisi terlebih dahulu melakukan *request* hak akses melalui aplilasi *ticketing*.
- Teknisi menerima segala konsekuensi jika hak akses yang telah diberikan terbukti disalahgunakan.
- Untuk menggunakan akses remote teknisi dapat menggunkan VPN (*Virtual Private Network*) yang telah disediakan oleh D~Net.

B. Persyaratan

- Untuk keamanan akses remote, harus dimonitoring secara ketat. Untuk autentikasi user password menggunakan user LDAP yang sudah terdaftar.
- Semua host yang terhubung ke jaringan internal perusahaan yang melalui akses remote harus menggunakan software anti-virus yang paling *up-to-date*.
- Teknisi yang menggunakan akses remote harus memastikan bahwa mereka tidak terhubung ke jaringan lain pada saat yang sama, dengan pengecualian dari jaringan pribadi yang berada di bawah kendali penuh dari pengguna.
- Server yang digunakan untuk akses remote harus memenuhi persyaratan minimum autentikasi.
- *Split-tunneling* tidak diizinkan.
- Konfigurasi hardware yang tidak standar harus melalui persetujuan divisi terkait agar keamanan akses remote tetap terjaga.

4.4.9 KEBIJAKAN AKSES PENYEDIA LAYANAN TI, INFORMASI DAN KOMPONEN

4.4.9.1 PENDAHULUAN

Kebijakan ini memberi batasan kepada penyedia layanan TI / *supplier* dalam mengakses informasi yang ada di perusahaan. Sehingga meminimalisir resiko-resiko yang kemungkinan terjadi.

4.4.9.2 TUJUAN

Kebijakan ini mengatur tentang hak akses penyedia layanan TI / *supplier* agar keamanan informasi tetap terjaga.

4.4.9.3 RUANG LINGKUP

Kebijakan ini berlaku untuk semua penyedia layanan TI / *supplier*.

4.4.9.4 KEBIJAKAN

- Mengidentifikasi dan mendokumentasikan semua penyedia layanan TI / *supplier*.
- Hak akses penyedia layanan TI / *supplier* terhadap jaringan lokal D~Net harus dibatasi.
- Semua kegiatan penyedia layanan TI / *supplier* harus atas sepengetahuan dan persetujuan manager.
- Semua kegiatan operasional penyedia layanan TI / *supplier* harus dilaporkan dan terdokumentasi.
- Semua kegiatan operasional penyedia layanan TI / *supplier* harus ada pendamping dan yang bertanggung jawab.

4.4.10 KEBIJAKAN PELEPASAN ASET

4.4.10.1 PENDAHULUAN

Semua aset perusahaan baik aset yang terpakai maupun yang tidak terpakai seharusnya terdokumentasi dengan baik. Sehingga memungkinkan untuk melacak atau melihat *history* dari aset tersebut. Aset yang sudah tidak dipergunakan harus dievaluasi, kemudian diambil sebuah keputusan apakah masih bisa dimanfaatkan di lain tempat atau diserah terimakan ke divisi warehouse.

4.4.10.2 TUJUAN

Tujuan dari kebijakan ini adalah untuk menentukan standar penyelesaian ketika aset sudah tidak dipergunakan lagi. Kebijakan ini dirancang untuk menjamin penggunaan yang efisien dari perangkat, memaksimalkan perangkat, kelengkapan laporan dan meminimalisir resiko-resiko yang kemungkinan terjadi.

4.4.10.3 RUANG LINGKUP

Kebijakan ini berlaku untuk semua karyawan yang melakukan transaksi terhadap perangkat milik perusahaan.

4.4.10.4 KEBIJAKAN

- Mengidentifikasi dan mendokumentasikan semua aset yang sudah tidak digunakan.
- Menganalisa aset apakah masih bisa dipergunakan atau tidak (dipindah ke perangkat lain atau bisa menjadi suku cadang untuk perangkat lain). Jika sudah benar-benar tidak bisa di manfaatkan, atas sepengetahuan dan persetujuan manager, aset diserah terimakan ke divisi warehouse.
- Semua transaksi terkait perpindahan aset harus sepengetahuan atau harus disetujui oleh manager divisi terkait.

- Untuk semua transaksi terkait perpindahan aset harus melalui dan tersimpan di aplikasi *asset management*.

LAMPIRAN

Wawancara untuk mengetahui tingkat keamanan informasi di D~Net

1. Apakah anda pernah menerima pelatihan tentang keamanan informasi?
   Belum pernah menerima palatihan tentang keamanan informasi yang secara resmi dan bersertifikat dari D~Net, selama ini melakukan keamanan informasi belajar secara otodidak (trial and error) dari internet atau sumber-sumber terpercaya lainnya dan sesuia best practice pada umumnya.

2. Sertifikasi atau kualifikasi apa yang anda miliki?
   Belum memiliki sertifikasi khusus tentang keamanan informasi.

3. Apakah D~Net memiliki kebijakan keamanan informasi?
   D~Net memiliki kebijakan tersendiri tentang keamanan informasi yang disesuaiakan dengan kebutuhan perusahaan, misal: karyawan tidak bisa mengakses jaringan kantor dari luar.

4. Apakah D~Net memiliki program tentang kesasdaran dalam keamanan informasi buat karyawannya?
   Belum ada, selama ini masih dilakukan sesuai dengan best practice yang disesuaikan dengan kebutuhan D~Net, selain itu juga belum adanya sertifikasi.

5. Bagaimana menggambarkan kebijakan keamanan informasi yang ada di D~Net
   - Kebijakan keamanan informasi telah disetujui oleh top manajemen?
     Jadi dari System Administrator melakukan riset tentang keamanan informasi, kemudaian hasil riset tersebut diajukan ke top manajemen melalui problem managemen yang dilaksanakan setiap minggu. Jika disetujui oleh top manajemen maka kebijakan keamanan informasi tersebut dilaksanakan.

- Kebijakan keamanan informasi telah dikomunikasikan kepada seluruh karyawan dan pihak eksternal yang relevan?

  Tidak semua kebijakan diinformasikan ke pelanggan, hanya kebijakan yang memliki efek tinggi yang dikomunikasikan dengan pelanggan D~Net. Misal: reset password untuk seluruh pelanggan D~Net yang menggunakan DREAMS karena ada perubahan dari segi keamanan maka D~Net mengkomunikasikan dengan pelanggannya .

- Adanya hukuman jika melakukan pelanggaran terkait kebijakan keamanan informasi?

  D~Net memberi hukuman kepelanggan jika terbukti melakukan pelanggaran. Misal: user email ketahuan melakukan spamming maka D~Net akan memblokir user tersebut untuk tidak kirim email selama 1 minggu, website pelanggan di deface maka pelanggan harus membetulkan websitenya terlebih dahulu kemudian D~Net memberi akses lagi.

- Kebijakan keamanan informasi diinformasikan secara online melalui website?

  Kebijakan keamanan informasi di D~Net tidak diinformasikan secara online.

- Apakah anda telah membaca dan memahami kebijakan keamanan informasi yang ada di D~Net?

  Iya sudah memahami kebijakan yang ada di D~Net.

6. Apakah D~Net memberikan akses jaringan remote?

   D~Net menyediakan akses jaringan remote / VPN kepada teknisinya, dengan cara teknisi request/tiket ke divisi terkait untuk membuka akses jaringan remote. Untuk user yang collocation tergantung user itu sendiri untuk menyediakan akses remote atau tidak

7. Apakah semua aset-aset penting sudah diidentifikasi dan inventarisasi dengan jelas dan dipelihara?

Belum ada indentifikasi dan inventarisai aset, teapi sudah ada rencana untuk melakukan inventarisasi dan menunggu aplikasi Warehouse.

8. Jelaskan kondisi saat ini tentang pendekatan D~Net terhadap keamanan informasi
   - Jaringan firewall?
     Sudah memiliki firewall, di pelihara oleh NOC. Firewall yang dimiliki D~Net terletak pada level menengah kebawah karena disesuaikan dengan jumlah traffic yang ada di D~Net dan menyesuaikan dengan kebutuhan.
   - Intrusion Detection System (IDS) ?
     *Sudah ada IDS. Aplikasi yang digunakan adalah **fail2ban** dengan custom scripting, jadi jika terdeteksi malicious code maupun virus baru akan diupdate dan dimasukkan ke dalam firewall dengan melakukan pengecekan atau analisa melalui syslog.*
   - Intrusion Prevention System (IPS) ?
     Sudah ada. IPS yang digunakan adalah firewall, tetapi dirasa masih kurang smart karena belum sampai menganalisa apakah paket yang dikirim mengandung virus atau tidak. Selama ini yang dilakukan adalah pemblokiran port yang ada di server.
   - VPN untuk akses jarak jauh?
     Suda ada. Hanya teknisi yang bisa memakai VPN dengan request/tiket ke divisi terkait.
   - Secure Socket Layer (SSL) untuk transaksi keamanan Web?
     Sudah ada. Untuk aplikasi internal menggunakan Self Signed Certificated sedangkan exteranal menggunakan SSL yang terdaftar.
   - Manajemen ancaman terpadu (ITM)?
     Ancaman yang sudah kita ketahui sudah di manage.

- Sentralisasi sistem backup?
  Sistem backup yang ada di D~Net sudah tersentralisasi, untuk kedepannya akan diubah supaya lebih skalabilitas.

- Enkripsi?
  Untuk enkripsi dari server ke server harus melalui Public Key/RSA, sedangkan untuk enkripsi ke aplikasi tergantung aplikasi yang diakses misal: TLS, SMTP, HTTPS dll memiliki enkripsi, sedangakan koneksi ke database PostgreSQL tidak ada enkripsi. Untuk enkirpsi dari aplikasi berbasis web enkripsi yang digunakan tergantung kebutuhan (SHA256-CRYPT, SHA512-CRYPT, BLF-CRYPT, SSHA256, SSHA512 dll).

- Monitoring atau penyaringan konten-konten yang aktif?
  D~Net memliki monitoring terhadap jaringan yang dimiliki, dimana sudah terpusat dan customizable untuk semua server.

9. Sudahkah D~Net melakukan penilaian resiko untuk menentukan nilai dari aset TI dan risiko aset tersebut?
   Belum ada.

10. Apakah D~Net sudah memiliki kebijakan ISMS?
    Belum ada.

11. Apakah ada karyawan dimana memiliki hak akses untuk melakukan investigasi TI melalui jalur belakang?
    Tidak ada, semua akses lewat jalur depan. Dimana semua aktivitas masuk ke syslog server.

12. Apakah D~Net melakukan audit tentang keamanan TI dan penilaian tentang kerentanan TI secara teratur?
    ● Bulanan ● Triwulan ● Setiap Tahun ● Tidak ada audit ● Lainnya (Jelaskan):
    Tidak ada audit tentang keamnana informasi.

13. Apakah D~Net memiliki prosedur yang formal dalam menangani insiden keamanan IT? Jelaskan!

    Semua prosedur tentang penanganan insiden keamanan informasi ada di Wiki yang dimiliki D~Net, misal: prosedur penanganan tentan email spamming, deface website, email kena hack dll.

14. Apa hambatan utama keamanan TI yang diterapkan di D~Net?
    - Penegakan kebijakan
    - Teknologi
    - Kesadaran
    - Dukungan dari manajemen
    - Sumber Daya Manusia
    - Adanya kebijakan/aturan

    Hambatan yang dimiliki adalah tentang pengetahuan sekitar 40%, biaya untuk menunjang keamanan informasi 35%, sumber daya manusia 15% dan kesadaran 10%

15. Adakah rencana untuk pengembangan dan penerapan untuk memlihara atau memulihkan operasional D~Net dan memastikan ketersediaan informasi dalam rentang skala waktu yang diperlukan untuk menangani gangguan atau kegagalan terhadap proses bisnis penting?

    Masih belum ada, memaksimalkan yang sudah ada misal custom script fail2ban.

16. Apakah D~Net siap untuk kejadian yang tak terduga
    - D~Net telah menerapkan rencana tanggap insiden (IRP/Incident Response Plan)

      Dengan melakukan backup system secara otomatis dan berkelanjutan, untuk kedepannya ditingkatkannya skalabilitas dan adanya system redundant.
    - D~Net menerapkan rencana pemulihan bencana (DRP/Disaster Recovery Plan)

Sebagian besar server yang ada di D~Net ada di amazon untuk backupnya. Ini dilakukan jika sewaktu-waktu terjadi musibah dengan D~Net, kita dapat memulihkan secepat mungkin dan seperti semula.

- D~Net menerapkan rencana kesinambungan bisnis (BCP/Business Continuity Plan)
  Belum ada.

17. Apakah ada prosedur formal tentang pendaftaran dan penghapusan user di D~Net untuk pemberian dan pencabutan akses ke semua sistem informasi dan layanan?
    Ada. Semua permintaan harus melalui aplikasi ticketing yang dimiliki D~Net.

18. Seberapa sering Anda melakukan back-up?
    Daily dan dilakukan secara otomatis.

19. Adakah pihak keamanan untuk menjaga kantor, kamar dan fasilitas kantor? Jelaskan!
    Tidak ada. Karena D~Net bertempat di gedung bersama, maka untuk pihak keamanan mengikuti pihak penyedia gedung. Untuk ruang server dan pintu masuk kantor terdapat fingerprint.

20. Apakah D~Net memiliki perlindungan fisik terhadap kerusakan dari kebakaran, banjir, gempa bumi, ledakan, dan bencana alam lainnya atau dari kesalahan manusia yang telah dirancang dan diterapkan?
    Tidak ada.

21. Apakah semua komputer/laptop karyawan sudah terinstall anti-virus?
    Semua komputer karyawan sudah terinstall anti-virus.

22. Seberapa sering anti-virus diperbarui dan apakah otomatis?
    Up to date.

23. Apa prosedur di D~Net untuk memperbarui perangkat lunak dan perangkat keras, jelaskan!

    Sudah ada. Rencana kedepan untuk update OS diserver bisa mudah dan cepat dilakukan.

24. Apakah peran dan tanggung jawab keamanan sudah jelas dan dinyatakan dalam syarat dan kondisi kerja di D~Net?

    Belum ada.

25. Setelah pemutusan hubungan kerja terhadap karyawan, apakah D~Net memastikan bahwa karyawan tersebut telah mengembalikan aset informasi D~Net yang dimiliknya dan kemudian menghapus hak aksesnya dengan cara yang tepat?

    Sudah dilakukan, tetapi masih dilakukan secara manual. Untuk kedepannya dibuat suatu proses termination secara otomatis.

26. Apakah menurut Anda D~Net telah berbuat cukup untuk melindungi sistem informasi?

    Saya mencoba melakukan yang terbaik.

27. Apakah ada proses dimana menjamin karyawan mengikuti praktik keamanan yang baik dalam pemilihan dan penggunaan password?

    Ada sesuai dengan standar D~Net.

28. Digambarkan seperti apa password yang baik?

    Merupakan kumpulan dari huruf besar dan kecil, angka, karakter khusus dan minimal 8 karakter.

29. Kapan Anda terakhir mengubah kata sandi Anda?

    Selama 6 bulan sekali secara system karyawan diwajibkan mengganti password, jika tidak diubah maka karyawan tidak bisa tersambung dengan server.

30. Mengapa anda mengubah password anda?

    Karena suatu keharusan dan jika tidak mengubah password tidak memiliki akses masuk.

31. Apakah informasi yang terdapat di email sudah dilindungi? Apa langkah-langkah keamanan yang ada di D~Net? Jelaskan!

    Iya, email di D~Net terpasang antivirus, antispam, autentikasi dengan SPF dan DKIM, memiliki BRBL (Baracuda Reputation Block List) jadi semua IP yang masuk list di BRBL secara otomatis akan di block dan custom filtering.

32. Apakah D~Net memeriksa status operasional dari langkah-langkah keamanan yang sudah diterapkan, seperti merekam dan memelihara akses log, melakukan pemeriksaan terhadap operasional yang tidak sah untuk mengakses informasi penting?

    Sudah ada prosedur untuk memonitoring dan analisa terhadap operasional yang tidak semestinya.

BAB 5

KESIMPULAN DAN SARAN

Bagian akhir dari tesis ini merupakan kesimpulan dan saran sebagai pelengkap agar konsep yang dijabarkan dalam tesis ini dapat terimplementasi dalam kondisi sesungguhnya.

5.1 Kesimpulan

Dari hasil penelitian yang telah dilakukan dapat diambil beberapa kesimpulan sebagai berikut:

1. Berdasarkan pada penelitian analisa kualitatif kelengkapan dokumen pendukung kebijakan keamanan informasi, kebijakan tentang akses kontrol, kebijakan tentang kontrol password, kebijakan tentang email, kebijakan penanganan virus dan kebijakan tentang akses remote sudah 100% terlengkapi untuk dokumen pendukung kebijakan keamanan informasi. Sedangakan kebijakan yang lain masih dibawah 100%, kebijakan tentang penggunaan dan penyalahgunaan aset TI (0%), kebijakan tentang internet (67%), kebijakan tentang pengklasifikasian informasi (0%), kebijakan tentang pengklasifikasian dokumen (33%), kebijakan tentang akses penyedia layanan TI, informasi dan komponen (0%) dan kebijakan tentang pelepasan aset (0%).
2. Dari total 47 dokumen pendukung, 27 dokumen sudah terlengkapi (57%) dan 20 dokumen pendukung belum terlengkapi (43%).
3. Berdasarkan hasil analisa peneliti menggunakan standar keamanan informasi menggunakan ITIL, kebijakan-kebijakan keamanan informasi yang di D~Net masih ada kekurangan-kekurangan kelengkapan dokumen, diantaranya yang harus dipenuhi adalah:
    a. Kebijakan tentang penggunaan dan penyalahgunaan aset TI,
    b. Kebijakan tentang internet,
    c. Kebijakan tentang pengklasifikasian informasi dan dokumen,

d. Kebijakan tentang akses penyedia layanan TI, informasi dan komponen,
e. Kebijakan tentang pelepasan aset.

5.2 Saran

Dari hasil penelitian yang telah dilakukan dapat diperoleh beberapa saran sebagai berikut:

1. Perlu adanya suatu standar keamanan informasi tersertifikasi yang digunakan oleh D~Net supaya meningkatkan nilai dari layanan yang diberikan, serta membentuk rasa aman dan percaya akan layanan yang diberikan oleh D~Net.
2. Diharapkan pihak yang berkaitan dengan keamanan informasi melakukan inventarisasi aset-aset perusahaan yang dirasa penting, melakukan penilaian resiko dan melaksanakan operasional keamanan informasi sesuai dengan kebijakan yang telah dibuat.
3. Dalam membantu implementasi keamanan informasi diperluakan suatu cara atau metode untuk mengelola server-server yang dimiliki D~Net, dimana yang jumlahnya tidak sedikit. Otomatisasi merupakan suatu cara yang pas dalam mengelola server dalam jumlah banyak, juga dapat membuat kegiatan operasional jauh lebih efektif dan efisien.

DAFTAR PUSTAKA

Ali, S. M., Soomro, T. R., & Brohi, M. N. (2013). "*Mapping Information Technology Infrastructure Library with other Information Technology Standards and Best Practices"*. Journal of Computer Science, 9 (9), 1190.

Wibisono, Dermawan, (2006). "*Manajamen Kinerja & Organisasi, Panduan Penyusunan Indikator"*, Jakarta: Erlangga.

Indrajit, (2008), "*Visi Perusahaan dan Strategi Sistem Informasi"*, www.eko-indrajit.com. Diakses 24 Desember 2015.

Steiss, Allan W. (2003). "*Strategic Management for Public and Nonprofit Organizations*", Virgina Polytechnic Institute and State University Blacksburg, Virginia, USA.

IT Service Management Forum, (2011), "*An Introductory Overview of ITIL 2011*", IT Service Management Forum.

Chess, D. M., Hanson, J. E., Pershing, J. A., Jr., White, S. R. (2007). "*Prospects for simplifying ITSM-based management through self-managing resources"*. IBM Systems Journal; Jul-Sep 2007; 46, 3.

Pollard, C., and Cater-Steel, A. (2009). "*Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. And Australian Companies: An Exploratory Study*", Information Systems Management (26:2), Spring 2009, pp. 164-175.

Iden, J., and Langeland, L. (2010). "*Setting the Stage for a Successful ITIL Adoption: A Delphi Study of IT Experts in the Norwegian Armed Forces",* Information Systems Management (27:2), Spring 2010, pp. 103-112.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). "*Information security management system standards: A comparative study of the big five*". International Journal of Electrical & Computer Sciences, 11(5), 2011.

Munteanu, A. (2006). "*Information Security Risk Assessment: Qualitative Versus Quantitative Dilemma*", 6th IBIMA conference.

Surendro, K. (2009). "*Implementasi Tata Kelola Teknologi Informasi",* Bandung: Informatika.

Weill, P., and Ross, J. (2004). "*IT Governance; How Top Performers Manage IT Decision Rights for Superior Results*", Harvard Business School Press, Boston.

ITGI. (2003). *"Board Briefing on IT Governance, 2nd Edition"*, 2ed. Rolling Meadows, IL, USA: IT Governance Institute.

Järveläinen, J. (2012). "*Information Security and Business Continuity Management in Interorganizational IT Relationship*", Information Management & Computer Security, Vol. 20 Iss: 5, pp.332 - 349.

Kitheka, P. (2013). "*Information Security Management System In Public Universities In Kenya: A Gap Analysis Between Common Practices And Industry Best Practices"*, Unversity of Nairobi, School of Computing and Informatics.

Abdellateef, L. (2014). "*Information Security Management in Palestinian Banking*", An-Najah National University.

Pricewaterhouse Coopers (PwC). (2014). "*Technical Report - Information Security Breaches Survey*".

Clinch, J. (2009). "*ITIL V3 and Information Security*". OGC Best Management Practice

Sugiyono. (2009). *"Memahami Penelitian Kualitatif"*. Bandung: Alfabeta.

http://www.itgovernance.co.uk/itsm.aspx diakses 25 Desember 2015 07.40

http://www.sby.dnet.net.id diakses 03 Januari 2016 17:45

BIOGRAFI PENULIS

Adi Tiatama, lahir di Bojonegoro pada 29 Juni 1988 sebagai anak pertama dari pasangan Bpk. Nurkolis dan Ibu Siti Nurjanah. Setelah menempuh pendidikan formal di SDN Kepatihan Bojonegoro, SMP Negeri 1 Bojonegoro dan SMK Telkom Sandhy Putra Malang, penulis melanjutkan pendidikan tinggi di S1 Teknik Informatika ITATS pada 2007.

Penulis kemudian melanjutkan pendidikan ke jenjang S2 di Institut Teknologi Sepuluh Nopember Surabaya dengan mengambil konsentrasi Manajemen Teknologi Informasi pada Magister Manajemen Teknologi (MMT-ITS).

Penulis telah bekerja sebagai Technical Support di perusahaan telekomunikasi, Telkom Flexi dan sekarang sebagai Software Developer pada sebuah perusahaan yang bergerak di bidang jasa internet (ISP) yaitu D~Net Surabaya.

Data Pribadi Penulis :
Nama : Adi Tiatama
Email : aditiatama@gmail.com