A2806/H/11

PERPUSTAKAAN ITS

ITS
Institut
Teknologi
Sepuluh Nopember

RSSI
005.74
Har
P-1
2011

TUGAS AKHIR - KS091336

PEMBUATAN DOKUMEN TATA KELOLA TI PADA PROSES PENGELOLAAN KEAMANAN SISTEM INFORMASI BERDASARKAN ISO/IEC 17799 STUDI KASUS: BIDANG PENGEMBANGAN TI, DINAS KOMUNIKASI DAN INFORMATIKA JAWA TIMUR

Willis Hardyansyah
NRP 5207 100 027

Dosen Pembimbing
Ir. Aris Tjahyanto, M.Kom
Bekti Cahyo H, S. Si., M.Kom

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2011

PERPUSTAKAAN ITS
Tgl Terima 10-2-2011
Terima Dari H
No Agenda Prp. -

ITS
Institut
Teknologi
Sepuluh Nopember

FINAL PROJECT - KS091336

DESIGNING IT GOVERNANCE DOCUMENT ON SECURITY MANAGEMENT INFORMATION SYSTEM PROCESS BASED ON ISO/IEC 17799 CASE STUDY OF IT DEVELOPMENT SECTOR COMMUNICATION AND INFORMATION TECHNOLOGY DEPARTMENT OF EAST JAVA

Willis Hardyansyah
NRP 5207 100 027

Supervisor
Ir. Aris Tjahyanto, M.Kom
Bekti Cahyo H, S. Si., M.Kom

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Sepuluh Nopember Institute of Technology
Surabaya 2011

PEMBUATAN DOKUMEN TATA KELOLA TI PADA PROSES PENGELOLAAN KEAMANAN SISTEM INFORMASI BERDASARKAN ISO/IEC 17799 STUDI KASUS: BIDANG PENGEMBANGAN TI, DINAS KOMUNIKASI DAN INFORMATIKA JAWA TIMUR

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Pada
Bidang Studi Perencanaan dan Pengembangan Sistem Informasi
(PPSI)
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya

Oleh :

WILLIS HARDYANSYAH
NRP 5207 100 027

Surabaya, 08 Februari 2011

KETUA
JURUSAN SISTEM INFORMASI

Ir. A. Holil Noor Ali M.Kom
NIP 196606021992031002

PEMBUATAN DOKUMEN TATA KELOLA TI PADA PROSES PENGELOLAAN KEAMANAN SISTEM INFORMASI BERDASARKAN ISO/IEC 17799 STUDI KASUS: BIDANG PENGEMBANGAN TI, DINAS KOMUNIKASI DAN INFORMATIKA JAWA TIMUR

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Pada
Bidang Studi Perencanaan dan Pengembangan Sistem Informasi (PPSI)
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya
Oleh :

WILLIS HARDYANSYAH
NRP 5207 100 027

Disetujui Tim Penguji: Tanggal Ujian : 31 Januari 2011
Periode Wisuda : Maret 2011

Ir. Aris Tjahyanto, M.Kom **(Pembimbing 1)**

Bekti Cahyo H, S.Si., M.Kom **(Pembimbing 2)**

Ir. Khakim Ghozali, M.MT **(Penguji 1)**

Apol Pribadi Subriadi, S.T., M.T **(Penguji 2)**

PEMBUATAN DOKUMEN TATA KELOLA TI PADA PROSES PENGELOLAAN KEAMANAN SISTEM INFORMASI BERDASARKAN ISO/IEC 17799 STUDI KASUS: BIDANG PENGEMBANGAN TI, DINAS KOMUNIKASI DAN INFORMATIKA JAWA TIMUR

Nama Mahasiswa	:	**Willis Hardyansyah**
NRP	:	**5207 100 027**
Jurusan	:	**Sistem Informasi FTIf - ITS**
Dosen Pembimbing	:	**Ir. Aris Tjahyanto, M.Kom**
		Bekti Cahyo H, S.Si., M.Kom

Abstrak

Sekarang ini TI banyak digunakan oleh berbagai perusahaan/institusi untuk mendukung proses bisnis baik utama maupun pendukung yang ada di perusahaan. Sayangnya masalah keamanan yang merupakan salah satu aspek dari sebuah teknologi informasi ini sering kali kurang mendapat perhatian. Karena apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan. Pada hakikatnya keamanan itu tidak dapat muncul demikian saja, dia harus direncanakan.

Oleh karena itu pengelolaan TI yang berbasis risiko yang dituangkan dalam tata kelola menjadi bagian yang penting untuk menangani semua ancaman yang muncul dari sebuah sistem informasi. Pembuatan dokumen tata kelola TI dalam tugas akhir ini akan dilakukan dengan menggunakan ISO/IEC 17799 sebagai framework sistem manajemen keamanan informasi.

Hasil penelitian ini berupa dokumen kerja dan prosedur tata kelola TI yang dapat digunakan sebagai pedoman dalam menangani setiap permasalahan yang berhubungan dengan proses pengelolaan keamanan sistem informasi berdasarkan prinsip CIA (confindetiality, integrity, availability).

Kata kunci: Tata kelola TI, Keamanan sistem informasi, ISO/IEC 17799.

Halaman ini sengaja dikosongkan.

DESIGNING IT GOVERNANCE DOCUMENT ON SECURITY MANAGEMENT INFORMATION SYSTEM PROCESS BASED ON ISO/IEC 17799 CASE STUDY OF IT DEVELOPMENT DIVISION, COMMUNICATION AND INFORMATION TECHNOLOGY DEPARTMENT OF EAST JAVA

Name	:	**Willis Hardyansyah**
NRP	:	**5207 100 027**
Department	:	**Sistem Informasi FTIf - ITS**
Supervisor	:	**Ir. Aris Tjahyanto, M.Kom**
		Bekti Cahyo H, S.Si., M.Kom

Abstract

Today IT is widely used by various companies / institutions to support both business process and supporting the existing main in the company. Unfortunately, security issues, which is one aspect of an information technology is often receive less attention. Because if the disturbing performance of the system, security is often reduced or eliminated. In essence that security can not come so easily, it should be planned.

Therefore, risk-based IT management as outlined in the IT governance becomes an important part of dealing with the threats that arise from an information system. The design of IT governance in this final task will be done by using the ISO / IEC 17799 as a framework for information security management system.

The result of this final project is IT governance documents that can be used as guidelines in dealing with any issues relating to process safety management information system based on the principle of the CIA (confindetiality, integrity, availability).

Keywords: *IT Governance*, *Information system security*, ISO/IEC 17799

Halaman ini sengaja dikosongkan.

KATA PENGANTAR

Alhamdulillahirabbilalamiin atas segala rahmat,pertolongan dan kasih sayang-NYA, sehingga tugas akhir berjudul "PEMBUATAN DOKUMEN TATA KELOLA TI PADA PROSES PENGELOLAAN KEAMANAN SISTEM INFORMASI BERDASARKAN ISO/IEC 17799 STUDI KASUS: BIDANG PENGEMBANGAN TI, DINAS KOMUNIKASI DAN INFORMATIKA JAWA TIMUR " dapat terselesaikan dan menghantarkan penulis menjadi sarjana komputer dari Jurusan Sistem Informasi, Fakutas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya. Terima kasih dan penghargaan setinggi-tingginya juga penulis sampaikan kepada:

1. Kedua Orang Tua penulis, Mami, Papi dan seluruh keluarga besar atas restu, doa serta dukungan moril maupun material yang diberikan kepada penulis.
2. Bapak. Ir. Aris Tjahyanto, M.Kom dan bapak Bekti Cahyo H, S.Si., M.Kom selaku dosen pembimbing atas kesabaran dalam membimbing penulis menyelesaikan tugas akhir.
3. Bapak Ir. Khakim Ghozali, M. MT dan Bapak Apol Subriadi, S.T., M.T selaku dosen penguji sidang tugas akhir.
4. Bapak dan Ibu dosen pengajar jurusan Sistem Informasi atas ilmu dan pengalaman yang telah dibagikan.
5. Admin lab PPSI Agung, Donna dan Trino yang telah dengan sabar mendengar keluhan, umpatan, serta luapan emosi ketika mengerjakan TA.
6. Admin lab PPSI Trino (Genesis) atas kebaikannya menata *caption* yang berantakan.
7. Para penghuni lab. PPSI atas kesediaannya berbagi gosip,canda tawa, dan makanan bersama.

8. Penghuni lab DSS yang bersedia menampung jika lab PPSI tidak dibuka.
9. Untuk Genesis atas kesediaannya menjadi teman seperjuangan yang saling menguatkan dan mendukung.
10. Pihak-pihak yang belum sempat penulis sebutkan jasa-jasanya dalam mendukung penyusunan tugas akhir ini.

Penulis menyadari bahwa tugas akhir ini belum sempurna. Oleh karena itu penulis mengharapkan komentar, kritik, dan saran dari berbagai pihak.

Akhirnya, penulis berharap semoga keberadaan tugas akhir ini bermanfaat bagi ilmu pengetahuan dan berbagai pihak.

Surabaya, 28 Januari 2011

Penulis

DAFTAR ISI

Halaman ini sengaja dikosongkan.

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan.

DAFTAR TABEL

Halaman ini sengaja dikosongkan.

BAB I
PENDAHULUAN

Pada bab ini akan dijelaskan beberapa sub-bab, antara lain: latar belakang, perumusan masalah, batasan masalah, tujuan tugas akhir, dan relevansi atau manfaat tugas akhir. Dari uraian-uraian yang ada diharapkan gambaran umum permasalahan serta pemecahan yang ditawarkan melalui tugas akhir ini dapat mudah dipahami.

1.1. Latar Belakang

Perkembangan dunia terutama bidang teknologi informasi pada era globalisasi telah melaju dengan pesat. Sekarang ini banyak perusahaan-perusahan baik swasta maupun instansi pemerintah sangat bergantung dengan teknologi informasi (TI) guna mencapai tujuan bisnisnya. TI banyak digunakan untuk mendukung proses bisnis baik utama maupun pendukung yang ada di perusahaan.

Sayangnya masalah keamanan yang merupakan salah satu aspek dari sebuah teknologi informasi ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola perusahaan atau instansi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Karena apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan, dengan kata lain semakin tinggi tingkat keamanan, maka semakin sulit (tidak nyaman) untuk mengakses informasi.

Keamanan yang dimaksudkan ialah pengelolaan keamanan akan informasi yang berada dalam suatu sistem informasi. Karena informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Maka kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, institusi pemerintahan, maupun individual (pribadi).

Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima sekaligus berdasarkan prinsip *CIA (confindetiality, integrity, availability)* di setiap informasi yang dikandungnya.

Oleh karena itu, keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi, yang dimaksudkan untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat segala kerusakan sistem.

Secara garis besar, ancaman terhadap sistem informasi dapat dibagi menjadi dua macam, yaitu ancaman aktif dan ancaman pasif. Ancaman aktif mencakup kecurangan dan kejahatan terhadap komputer, sedangkan ancaman pasif mencakup kegagalan sistem, kesalahan manusia, dan bencana alam. Kegagalan sistem menyatakan kegagalan dalam peralatan-peralatan komponen.

Tetapi, pada hakikatnya keamanan itu tidak dapat muncul demikian saja, itu harus direncanakan. Oleh karena itu pengelolaan TI yang berbasis risiko yang dituangkan dalam sebuah tata kelola menjadi bagian yang penting. Yang kemudian dapat disebut dengan *IT governance. IT governance* merupakan gabungan (*best practice*) dari perencanaan dan pengorganisasian TI, pembangunan dan pengimplemantasian, *delivery* dan *support*, serta memonitor kinerja TI untuk memastikan kalau informasi perusahaan dan teknologi yang saling berhubungan demi mendukung tujuan bisnis perusahaan.

Tata kelola TI pada proses pengelolaan keamanan sistem informasi dalam prakteknya masih banyak memberikan indikasi peluang munculnya beberapa permasalahan seperti kelemahan (*vulnerabilities*) yang dapat memicu terjadinya ancaman (*threat*) terhadap keberadaan informasi yang berada di dalamnya sebagai

aset yang penting dari suatu perusahaan. Beberapa bentuk ancaman seperti: kehilangan, pencurian, penggandaan dan perusakan terhadap data yang penting bagi institusi dapat menimbulkan dampak yang serius terhadap proses bisnis yang dijalankan.

Berdasarkan paparan di atas memunculkan nilai penting kebutuhan mendasar bagi Dinas Komunikasi Dan Informatika Jawa Timur akan adanya suatu kerangka Tata Kelola TI terkait pengelolaan keamanan sistem informasi sehingga semua ancaman yang teridentifikasi dapat dicegah sekaligus mengoptimalkan kinerja TI agar lebih mempunyai nilai tambah bagi proses bisnis yang dijalankan.

Dengan demikian, dalam tugas akhir ini akan dirancang sebuah pedoman tata kelola TI untuk Dinas Komunikasi Dan Informatika Jawa Timur terutama Bidang Pengembangan TI dengan menggunakan *framework* ISO/IEC 17799 yang merupakan contoh *framework* yang dapat digunakan dalam proses Tata Kelola TI terutama dalam fokusnya akan membahas masalah teknis keamanan yang akan dihadapi.

ISO/IEC 17799 adalah sebuah standar untuk sistem manajemen keamanan informasi. Standar kebutuhan ISO/IEC 17799 meliputi: dokumen kebijakan keamanan informasi, alokasi tanggungjawab keamanan informasi, menyediakan semua para pemakai dengan pendidikan dan pelatihan di dalam keamanan informasi, dan lain-lain.

Pada tugas akhir ini, penulis berharap dokumen tata kelola teknologi informasi yang dibuat dapat menjadi acuan dalam melakukan pengelolaan TI terutama pada proses pengelolaan keamanan sistem informasi di Dinas Komunikasi Dan Informatika Jawa Timur Bidang Pengembangan TI untuk mencapai keselarasan bisnis dan TI yang akan mengarahkan pada pemenuhan nilai bisnis yang notabene adalah kunci dari Tata Kelola TI itu sendiri.

1.2. Perumusan Masalah

Permasalahan yang akan diselesaikan dalam tugas akhir ini adalah:

1. Bagaimana kondisi tata kelola teknologi informasi yang diterapkan saat ini dalam pengamanan sistem informasi di Dinas Komunikasi Dan Informatika Jawa Timur terutama pada Bidang Pengembangan TI?
   a) Risiko apa saja yang muncul selama proses pengelolaan keamanan sistem informasi di Bidang Pengembangan TI Dinas Komunikasi Dan Informatika Jawa Timur?
   b) Apakah ada kontrol keamanan yang sudah diterapkan pada proses pengelolaan keamanan sistem informasi di Bidang Pengembangan TI Dinas Komunikasi Dan Informatika Jawa Timur?
   c) Dampak apa saja yang ditimbulkan bagi risiko pada proses pengelolaan keamanan sistem informasi yang sudah teridentifikasi di Bidang Pengembangan Ti Dinas Komunikasi Dan Informatika Jawa Timur?
   d) Apakah ada metode pengelolaan risiko pada proses pengelolaan keamanan sistem informasi yang diterapkan di Bidang Pengembangan TI Dinas Komunikasi Dan Informatika Jawa Timur?
2. Kondisi tata kelola teknologi informasi seperti apa yang diharapkan dalam pengelolaan keamanan sistem informasi di Bidang Pengembangan TI Dinas Komunikasi Dan Informatika Jawa Timur?

1.3. Batasan Masalah

Batasan pemasalahan dalam tugas akhir ini adalah:

1. Penggunaan *Internasional Organisation for Standardization* (ISO) / IEC 17799 sebagai *framework* untuk membantu dalam pemenuhan pembuatan komponen tata kelola TI yang dikhususkan pada

klausul ke-8 yaitu **Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi.**

2. Penyusunan tata kelola teknologi informasi ini difokuskan kepada aspek pengelolaan TI yang dikhususkan pada keamanan sistem informasi.
3. Dokumen pedoman tata kelola TI yang akan dibuat hanya dapat digunakan pada proses pengelolaan keamanan sistem informasi di Bidang Pengembangan TI Dinas Komunikasi Dan Informatika Jawa Timur.

1.4. Tujuan Tugas Akhir

Beberapa tujuan yang diharapkan dalam penelitian tugas akhir ini adalah sebagai berikut:

1. Melakukan analisis terhadap kondisi tata kelola teknologi informasi pada proses pengelolaan keamanan sistem informasi di Bidang Pengembangan TI, sehingga diperoleh informasi berupa identifikasi ancaman yang berpotensial untuk menciptakan risiko bagi TI beserta dampak yang akan dihasilkan, kontrol keamanan yang diterapkan dan metode pengelolaan risiko yang ada untuk dijadikan acuan perbaikan serta strategi yang dapat diimplementasikan pada tata kelola teknologi informasi yang akan dibuat.
2. Membuat sebuah dokumen tata kelola teknologi informasi berupa dokumen kerja dan prosedur dengan mengidentifikasi tindakan perbaikan, fokus area perbaikan yang diperlukan.

1.5. Relevansi atau Manfaat Tugas Akhir

Tugas akhir ini diharapkan dapat memberikan dua manfaat, yakni untuk pihak internal (dalam hal ini Dinas Komunikasi Dan Informatika Jawa Timur) dan pihak eksternal.

Manfaat bagi pihak internal:

1. Memberikan kesadaran (*awareness*) bagi Dinas Komunikasi Dan Informatika khususnya Bidang

Pengembangan TI akan kebutuhan untuk melakukan langkah-langkah perbaikan secara terus menerus pada tata kelola teknologi informasi khususnya pada proses pengelolaan keamanan sistem informasi.

2. Dengan memberikan suatu dokumen tata kelola TI yang tepat dan baik, sehingga diharapkan akan meningkatkan kualitas operasional dalam pengembangan dan pemeliharaan sistem informasi, yang berkontribusi positif bagi peningkatan kinerja instansi Dinas Komunikasi Dan Informatika Jawa Timur

Sedangkan manfaat bagi pihak eksternal adalah sebagai panduan bagi instansi lain yang akan melakukan penilaian dan pengembangan tata kelola teknologi informasi pada proses pengelolaan keamanan sistem informasi.

1.6. Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini terbagi menjadi lima bab, yaitu:

BAB I: PENDAHULUAN

Bab ini akan menjelaskan tentang latar belakang, perumusan masalah, batasan masalah, tujuan tugas akhir, dan relevansi manfaat tugas akhir.

BAB II: TINJAUAN PUSTAKA

Pada bab ini akan dibahas tentang teori-teori, temuan dan bahan penelitian lain yang menjadi landasan informasi untuk mengerjakan tugas akhir ini, yang nantinya diharapkan akan menjadi kerangka berpikir untuk mengerjakan tugas akhir ini meliputi: pengertian teknologi informasi serta sistem informasi, keamanan informasi, masalah keamanan dalam sistem informasi, pengendalian sistem informasi, tata kelola, tata kelola perusahaan vs tata kelola TI, tata kelola TI, ancaman keamanan sistem informasi, ISO/IEC 17799, panduan umum tata kelola TIK nasional, pengendalian dokumen, *standard operating procedures*.

BAB III: METODE PENELITIAN

Bab ini menjelaskan urutan langkah-langkah yang dilakukan penulis untuk menyelesaikan tugas akhir ini. Metode penyelesaian tugas akhir ini meliputi lima tahap dan masing-masing tahap dibagi menjadi dua langkah atau lebih.

BAB IV: HASIL PENELITIAN DAN ANALISIS DATA

Bab ini menjabarkan hasil penelitian mengenai tata kelola teknologi informasi pada Dinas Komunikasi Dan Informatika Jawa Timur, khususnya pada Bidang Pengembangan TI. Identifikasi sistem informasi yanga ada di instansi serta proses bisnis yang didukung oleh sistem informasi tersebut. Tidak lupa juga adanya identifikasi risiko yang muncul karena kelemahan sistem, penilaian risiko yang didasarkan pada dampak bagi yang dihasilkan pada instansi, serta pengelolaan mitigasi risiko yang optimal sebagai tujuan perbaikan yang diperlukan agar rancangan tata kelola TI yang disusun dapat mencapai hasil yang diinginkan.

BAB V: PEMBUATAN DOKUMEN TATA KELOLA TEKNOLOGI INFORMASI

Bab ini merupakan tahapan pembuatan dokumen tata kelola teknologi informasi. Tahapan yang dilakukan yaitu menyusun pedoman tata kelola TI yang berupa tugas pokok dan fungsi aparatur negara sebagai representasi dokumen kerja yang ada di institusi pemerintahan, serta dokumen prosedur yang didalamnya terdapat struktur tata kelola, rancangan kebijakan keamanan dan sebuah pedoman yang memuat instruksi kerja serta prosedur yang harus dilakukan sebagai rancangan dokumen tata kelola teknologi informasi pada Bidang Pengembangan Teknologi Informatika.

BAB VI: KESIMPULAN DAN SARAN

Kesimpulan yang didapat selama pengerjaan Tugas Akhir ini serta saran perbaikan yang dapat dilakukan untuk penelitian lanjutan ditulis pada bab ini.

Halaman ini sengaja dikosongkan.

BAB II
TINJAUAN PUSTAKA

Pada bab ini akan dibahas tentang teori-teori, temuan dan bahan penelitian lain yang menjadi landasan informasi untuk mengerjakan tugas akhir ini, yang nantinya diharapkan akan menjadi kerangka berpikir untuk mengerjakan tugas akhir ini meliputi: pengertian teknologi informasi serta sistem informasi, keamanan informasi, masalah keamanan dalam sistem informasi, pengendalian sistem informasi, tata kelola, tata kelola perusahaan vs tata kelola TI, tata kelola TI, ancaman keamanan sistem informasi, ISO/IEC 17799, panduan umum tata kelola TIK nasional, pengendalian dokumen, *standard operating procedures*.

2.1 Teknologi Informasi

Istilah teknologi informasi sering rancu dengan istilah sistem informasi itu sendiri dan kadang menjadi bahan perdebatan. Ada yang menggunakan istilah teknologi informasi untuk menjabarkan sekumpulan sistem informasi, pemakai, dan manajemen (Turban, Efraim., McClesn, Ephraim., Wetherbe, James, 1999). Pendapat ini menggambarkan teknologi dalam perspektif yang luas.

Menurut (Alter, 2002), teknologi informasi mencakup perangkat keras dan perangkat lunak untuk melaksanakan satu atau sejumlah tugas pemrosesan data seperti menangkap, mentransmisikan, menyimpan, mengambil, memanipulasi, atau menampilkan data. (Martin, 1999) mendefinisikan teknologi informasi tidak hanya terbatas pada teknologi komputer (perangkat keras dan perangkat lunak) yang digunakan untuk memproses dan menyimpan informasi, melainkan juga mencakup teknologi komunikasi untuk mengirimkan informasi.

Secara lebih umum, (Lucas, 2000) menyatakan bahwa teknologi informasi adalah segala bentuk teknologi yang diterapkan untuk memproses dan mengirimkan informasi dalam bentuk elektronis. Dapat disimpulkan bahwa teknologi informasi

merupakan teknologi komputer yang terdiri atas perangkat lunak, perangkat keras, manusia, jaringan, dan manajemen yang digunakan untuk melaksanakan satu tugas atau lebih terkait proses penyimpanan, pemrosesan dan mendistribusikan informasi sebagai hasilnya kepada pengguna.

2.2 Sistem Informasi

Sesungguhnya yang dimaksud dengan sistem informasi tidak harus melibatkan komputer. Sistem informasi yang menggunakan komputer biasa disebut sistem informasi berbasis komputer (*Computer – Based Information System* atau CBIS). Dalam prakteknya, istilah sistem informasi lebih sering dipakai tanpa kata berbasis komputer walaupun dalam kenyataannya komputer merupakan bagian yang penting.

Ada beragam definisi sistem informasi, sebagaimana tercantum pada tabel 2.1. Dari berbagai definisi tersebut, dapat disimpulkan bahwa sistem informasi mencakup jumlah komponen (manusia, komputer, teknologi informasi, dan prosedur kerja), ada sesuatu yang diproses (data menjadi informasi), dan dimaksudkan untuk mencapai suatu sasaran atau tujuan.

Tabel 2.1 Definisi Sistem Informasi

Sumber	Definisi
(Alter, 1992)	Sistem informasi adalah kombinasi antara prosedur kerja, informasi, orang, dan teknologi informasi yang diorganisasikan untuk mencapai tujuan dalam sebuah organisasi.
(Bonar, George H., Hopwood, William S, 1993)	Sistem informasi adalah kumpulan perangkat keras dan perangkat lunak yang dirancang untuk mentransformasikan data ke dalam bentuk informasi yang berguna.

Tabel 2.1 Definisi Sistem Informasi

(Gelinas, Ulric J., Oram, Allan E., Wiggins, William P., 1990)	Sistem informasi adalah suatu sistem buatan manusia yang secara umum terdiri atas sekumpulan komponen berbasis komputer dan manual yang dibuat untuk menghimpun, menyimpan, dan mengelola data serta menyediakan informasi keluar-an kepada para pemakai.
(Hall, 2001)	Sistem informasi adalah sebuah rangkaian prosedur formal dimana data dikelompokkanm diproses menjadi informasi, dan didisribusikan kepada pemakai.
(Turban, Efraim., McClesn, Ephraim., Wetherbe, James, 1999)	Sebuah sistem informasi mengumpulkan, memproses, menyimpan, menganalisis, dan menyebarkan informasi untuk tujuan yang spesifik.
(Wilkinson, 1992)	Sistem informasi adalah kerangka kerja yang mengkoordinasikan sumber daya (manusia, komputer) untuk mengubah masukan (*input*) menjadi keluaran (informasi), guna mencapai sasaran-sasaran perusahaan.

2.3 Keamanan Informasi

Keamanan informasi adalah upaya untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan

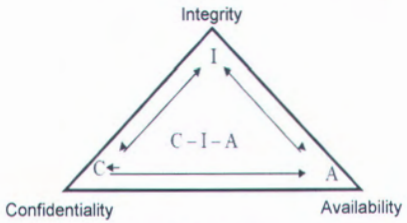
keuntungan yang didapat dari investasi dan kesempatan bisnis. Keamanan informasi dapat dicapai dengan mengimplementasikan sekumpulan kendali keamanan informasi yang sesuai, termasuk di dalamnya, kebijakan, proses, prosedur, struktur organisasi serta fungsi hardware dan software. Kendali-kendali tersebut perlu dibuat, diimplementasikan, dimonitor, ditinjau ulang dan ditingkatkan untuk memastikan kesesuaian antara kendali keamanan yang ada dengan tujuan bisnis organisasi. Keamanan informasi dapat diklasifikasikan sebagai berikut (Triantono, 2007):

- *Physical Security*. Merupakan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- *Personal Security*. Termasuk di dalamnya adalah identifikasi risiko dari pengguna yang memiliki akses kepada informasi.
- *Operation Security*. Merupakan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
- *Communications Security*. Bertujuan untuk mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan media-media tersebut untuk mencapai tujuan organisasi.
- *Network Security*. Fokus pada pengamanan peralatan jaringan data organisasi, jaringan dan isi data organisasi, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Aspek-aspek keamanan informasi dalam suatu organisasi meliputi tiga hal berikut (Triantono, 2007):

- *Confidentiality* (kerahasiaan). Merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
- *Integrity* (integritas). Merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi beserta metode prosesnya.
- *Availability* (ketersediaan). Merupakan aspek yang memberi jaminan atas ketersediaan data saat dibutuhkan, kapan pun dan di mana pun. Aspek ini juga memastikan hanya pengguna yang berhak saja yang dapat menggunakan informasi dan perangkat terkait.

Ketiga aspek tersebut dapat digambarkan sebagai berikut :



Gambar 2.1 Aspek-aspek Keamanan Informasi

Selain ketiga aspek utama di atas, kemanan informasi juga memiliki aspek-aspek lain seperti berikut ini (Triantono, 2007):

- *Privacy* (pribadi). 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.
- *Identification* (identifikasi). Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali individu

pengguna. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi secara umum dilakukan dalam penggunaan *user name* atau *user ID.*

- *Authentication* (autentifikasi). Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
- *Authorization* (autorisasi). Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia ataupun komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari aset informasi.
- *Accountability* (akuntabilitas). Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktifitas terhadap aset informasi yang telah dilakukan, dan siapa yang melakukan aktifitas itu. Aspek ini berupaya memastikan seseorang tidak dapat menyangkal perbuatan yang telah dilakukannya.

2.4 Masalah Keamanan Sistem Informasi

Keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi, yang dimaksudkan untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat segala kerusakan sistem.

Secara garis besar, ancaman terhadap sistem informasi dapat dibagi menjadi dua macam, yaitu ancaman aktif dan ancaman pasif. Ancaman aktif mencakup kecurangan dan kejahatan terhadap komputer, sedangkan ancaman pasif mencakup kegagalan sistem, kesalahan manusia, dan bencana alam. Kegagalan sistem menyatakan kegagalan dalam peralatan-

MILIK PERPUSTAKAAN ITS

peralatan komponen. Berbagai bentuk ancaman terhadap sistem informasi diperlihatkan pada tabel 2.2 (Kadir, 2003) berikut ini.

Tabel 2.2 Ancaman Terhadap Sistem Informasi

Macam Ancaman	Contoh
Bencana alam dan politik	Gempa bumi, banjir, kebakaran dan perang.
Kesalahan manusia	Kesalahan pemasukan data. Kesalahan penghapusan data. Kesalahan operator (salah memberi label pada pita magnetik).
Kegagalan perangkat lunak dan perangkat keras	Gangguan listrik. Kegagalan peralatan. Kegagalan fungsi perangkat lunak.
Kecurangan dan kejahatan komputer	Penyelewengan aktivitas. Penyalahgunaan kartu kredit. Sabotase. Pengaksesan oleh orang yang tidak berhak.
Program yang jahat / usil	Virus, cacing, bom waktu, dll.

Bencana alam merupakan faktor yang tidak terduga yang bisa mengancam sistem informasi. Banjir, badai, gempa bumi, dan kebakaran dapat meluluhlantahkan sumber daya pendukung sistem informasi dalam waktu yang singkat.

Kesalahan pengoperasian sistem oleh manusia juga dapat mengancam integritas sistem dan data. Pemasukan data yang salah dapat mengacau sistem. Begitu juga penghapusan data (sebagaimana terjadi pada kasus penghapusan nomor keamanan sosial yang dibahas di depan). Pelabelan yang salah terhadap pita

magnetik yang berisi backup sistem juga membawa dampak yang buruk kalau terjadi gangguan dalam sistem (misalnya data harus dikembalikan ke dalam sistem).

Gangguan listrik, kegagalan peralatan dan kegagalan fungsi perangkat lunak dapat menyebabkan data tidak konsisten, transaksi tidak lengkap, atau bahkan data rusak. Selain itu, variasi tegangan listrik yang terlallu tajam dapat membuat peralatan-peralatan terbakar.

Metode yang umum digunakan oleh orang dalam melakukan penetrasi terhadap sistem berbasis komputer ada 6 macam (Bonar, George H., Hopwood, William S, 1993), yaitu:

1. Pemanipulasian masukan.
2. Penggantian program.
3. Penggantian berkas secara langsung.
4. Pencurian data.
5. Sabotase.
6. Penyalahgunaan dan pencurian sumber daya komputasi.

2.5 Pengendalian Sistem Informasi

Berkaitan dengan kemanan sistem informasi, diperlukan tindakan berupa pengendalian terhadap sistem informasi. Kontrol-kontrol yang dilakukan untuk pengamanan sistem informasi dapat dilihat pada tabel 2.3 (Kadir, 2003) berikut ini.

Tabel 2.3 Pengendalian Sistem Informasi

Macam Kontrol	Contoh Tindakan
Kontrol administratif	Mempublikasikan kebijakan kontrol secara formal. Mempublikasikan prosedur dan standar. Perekrutan personel secara berhati-hati.

Tabel 2.3 Pengendalian Sistem Informasi

	Pemisahan tugas dalam suatu pekerjaan. Membuat rencana pemulihan terhadap bencana.
Kontrol pengembangan dan pemeliharaan sistem	Melakukan audit terhadap proses untuk menjamin pengendalian dan penelusuran sistem. Mengkaji pasca implementasi. Memastikan bahwa pemeliharaan yang dilakukan terotorisasi. Mengaudit dokumentasi.
Kontrol operasi	Mengontrol akses terhadap pusat data. Mengontrol personel pengoperasi. Mengontrol pemeliharaan peralatan-peralatan. Mengontrol penyimpanan arsip. Melindungi dari virus.
Proteksi terhadap pusat data secara fisik	Mengontrol lingkungan. Melindungi terhadap kebakaran dan banjir. Menyiapkan sumber listrik darurat (misalnya UPS – *uninterruptable power supply*).
Kontrol perangkat keras	Sistem komputer *fault – tolerant*.
Kontrol terhadap akses komputer	Mengidentifikasi dan melakukan otentikasi terhadap pemakai. *Firewall*.

Tabel 2. 4 Pengendalian Sistem Informasi

Kontrol akses informasi	Enkripsi.
Kontrol terhadap perlindungan terakhir	Rencana pemulihan terhadap bencana Asuransi
Kontrol aplikasi	Kontrol terhadap masukan, pemrosesan, dan keluaran. Kontrol terhadap basis data. Kontrol terhadap telekomunikasi.

2.6 Tata Kelola Perusahaan dan Tata Kelola Teknologi Informasi

Berdasarkan definisi tata kelola teknologi informasi *(IT governance)* dari *IT Governance Institut (ITGI)* dikemukakan bahwa *IT governance* adalah tanggungjawab dari dewan direksi dan menajemen eksekutif, oleh karenanya *IT governance* harus menjadi bagian yang tidak terpisahkan dari tata kelola korporat *(corporate governance)* (Surendro, 2009). *Corporate governance* merupakan suatu sistem yang mengarahkan dan mengendalikan entitas-entitas korporat.

Ketergantungan bisnis dan teknologi informasi telah membuatnya tidak dapat menyelesaikan isu pengeloaan korporat tanpa mempertimbangkan teknologi informasi. Hal ini dikarenakan tata kelola korporat mengarahkan dan mengatur tata kelola teknologi informasi (Surendro, 2009). Dan sebagai gantinya teknologi informasi dapat mempengaruhi peluang strategi dan menghasilkan kritik atas perencanaan strategis yang telah dibuat. Dalam hal ini tata kelola teknologi informasi memungkinkan korporat untuk mengambil keuntungan maksimal

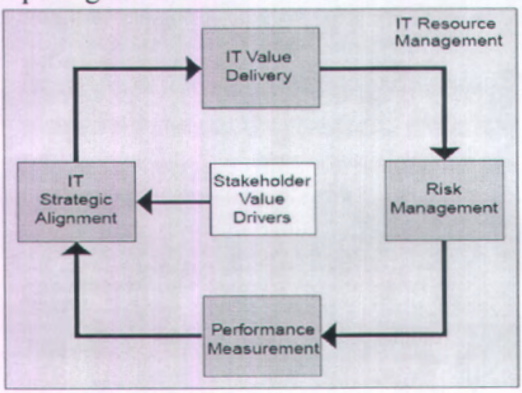
2.7 Tata Kelola Teknologi Informasi

Definisi tata kelola teknologi informasi telah dikemukakan oleh para ahli, diantaranya sebagai berikut:

- Kapasitas organisasi untuk mengendalikan formulasi dan implementasi strategi teknologi informasi dan mengarahkan kepada kepentingan daya saing korporasi (Industry, 1999).
- Tata kelola teknologi informasi adalah pertanggungjawaban dewan direksi dan manajemen eksekutif. Hal ini, merupakan bagian yang terintegrasi dengan tata kelola perusahaan dan berisi kepemimpinan dan struktur serta proses organisasi yang menjamin bahwa organisasi teknologi informasi mengandung dan mendukung strategi serta tujuan bisnis (ITGI, 2001)
- Menurut (Peterson, 2003), tata kelola TI lebih luas cakupannya dari pada manajemen TI (*IT Management*). Manajemen TI fokus pada penyediaan layanan dan produk TI yang efektif untuk internal organisasi dan pengelolaan operasi TI saat ini. Sedangkan, tata kelola TI fokus pada menampilkan dan mentransformasikan TI untuk memenuhi kebutuhan bisnis (*internal focus*) saat ini dan masa depan serta untuk memenuhi kebutuhan customer (*external focus*).
- Tata kelola teknologi informasi adalah penilaian kapasitas organisasi oleh dewan direksi, manajemen eksekutif, manajemen teknologi informasi untuk mengendalikan formulasi dan implementasi strategi teknologi informasi dalam rangka mendukung bisnisnya (Van Grembergen, 2002).

Oleh karena itu, tata kelola TI bertujuan untuk memaksimalkan potensi sumber daya yang ada, dan menghindari tumpang tindih alokasi waktu, biaya dan sumber daya manusia, serta mengurangi risiko dalam pengembangan TI sehingga menjamin investasi TI dapat memberikan hasil yang optimal (Arbiansyah, G., Kristianto, D., Neneng, 2010).

Hal ini mengarah pada lima area utama untuk tata kelola TI yang didorong oleh nilai yang diberikan kepada stakeholder (*stakeholder value drivers*). Dua diantara area tersebut merupakan hasil, yaitu pengiriman nilai (*value delivery*) dan manajemen risiko (*risk management*). Tiga area lainnya merupakan pendorong, yaitu keselarasan strategis (*strategic alignment*), manajemen sumberdaya (*resource management*), dan pengukuran performa (*performance measurement*). Hubungan kelima area ini dapat dilihat pada gambar 2.2 berikut ini.



Gambar 2.2 Fokus Bidang Tata Kelola TI

Dari gambar di atas dapat disimpulkan bahwa dalam pelaksanaan tata kelola TI pada suatu organisasi digerakkan oleh pemberian nilai tambah bagi stakeholder. Untuk memberikan nilai tambah ini dilakukan penyelarasan strategis dan penentuan solusi-solusi yang kolaboratif antara TI dan bisnis.

Dari proses tersebut ditentukan nilai tambah TI yang kemudian dilakukan pengoptimalan pengeluaran dan pembuktian nilai tambah TI tersebut bagi bisnis (Rahmana, 2009). Pemberian nilai tambah ini membutuhkan manajemen risiko yang bertujuan untuk penyelamatan asset TI, pemulihan dari bencana dan keberlangsungan operasi TI. Selanjutnya dibutuhkan manajemen

sumberdaya untuk mengoptimalkan pengetahuan (*knowledge*) dan infrastruktur TI. Keseluruhan area ini dapat dikelola dengan tepat melalui pengukuran performa dengan penelusuran penyelesaian proyek dan memonitor layanan TI.

Tata kelola teknologi informasi dapat dianggap juga sebagai sebuah proses dimana strategi teknologi informasi mengendalikan kumpulan proses-proses yang dilakukan dengan teknologi informasi, mengumpulkan sumber daya yang dibutuhkan untuk melaksanakan kewajibannya. Laporan dari proses teknologi informasi mencakup kewajiban dari proses yang telah dilakukan, kinerja, risiko yang diterima dan ditangani, beserta sumber daya yang telah digunakannya.

Saat ini isu pengelolaan teknologi informasi mengalami pergeseran fokus dari fokus pada teknologi menjadi fokus pada area yang terkait dengan manajemen. Isu ini mengarah pada area tata kelola teknologi informasi:

- Penyelerasan strategis, berfokus pada penyelarasan bisnis dan solusi kolaborasi.
- Penyampaian nilai, berkosentrasi pada optimasi pengeluaran dan nilai teknologi informasi.
- Manajemen risiko, bertujuan untuk menjaga aset teknologi informasi dan pemulihan dari bencana.
- Manajemen sumber daya, berfokus pada optimasi pengetahuan dan infrastruktur teknologi informasi.

Implementasi tata kelola teknologi informasi terdiri dari beberapa langkah utama, yaitu mengidentifikasi kebutuhan, memperkirakan solusi, merencanakan solusi, mengimplementasikan solusi, dan mengoptimalkan solusi.
Dalam menerapkan langkah-langkah tersebut, manajemen harus:

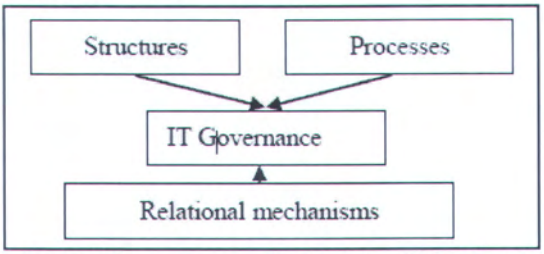
- Memperlakukan inisiatif implementasi sebagai suatu aktivitas program dengan seurutan fase. Dalam hal ini,

jangan memperlakukan inisiatif implementasi sebagai suatu langkah '*one-off*'.

- Mengingat bahwa implementasi melibatkan perubahan budaya serta proses baru. Dengan demikian, kunci sukses utama adalah manajemen perubahan organisasional yang efektif.
- Memastikan terdapat pemahaman yang jelas akan sasaran-sasaran yang ada.
- Mengelola ekspektasi. Pada sebagian besar perusahaan, mencapai pengawasan teknologi informasi yang berhasil memerlukan waktu dan merupakan proses perbaikan yang berkelanjutan.
- Memfokuskan terlebih dahulu pada bagian yang termudah dalam membuat perubahan dan memberikan perbaikan, dan secara inkremental membangun sukses dari sana.
- Mendapatkan *buy-in* dan *ownership* dari manajemen tingkat atas. Kebutuhan ini didasarkan pada prinsip mengelola investasi dalam teknologi informasi dan perubahan karena teknologi informasi.
- Menghindari inisiatif menjadi dipandang sebagai sesuatu yang bersifat birokrasi semata.
- Menghindari pendekatan *checklist* yang tidak fokus.

Stuktur adalah mekanisme yang melibatkan fungsi atau jabatan yang bertanggung jawab seperti Eksekutif TI dan berbagai komisi TI untuk membuat keputusan TI (Guldentops, E., Van Grembergen, W., & De Haes, S, 2002). Pada gambar 2.3 berikut ini adalah mekanisme struktur yang paling umum ada dalam pengimplementasian tata kelola TI (Putra, Risma Bayu, Sesuse, Indra Dana, 2009): *Executives or Senior management Commitee, IT Leadership commitee comprising IT executives, Process teams with IT members, Business/IT relationship managers, IT council*

comprising business and IT excecutives, Architecture committee, Capital approval committee.



Gambar 2.3 Struktur, Proses, Mekanisme Tata Kelola TI

Penerapan tata kelola TI menurut (Guldentops, E., Van Grembergen, W., & De Haes, S, 2002) serta (Peterson, 2003) memerlukan kombinasi Struktur, Proses dan Mekanisme Hubungan untuk keduanya (*structures and proseses*). Setiap organisasi pasti akan berbeda satu dengan yang lain dalam penerapan struktur, proses dan mekanisme hubungannya, tergantung dari kondisi, situasi dan tantangan yang dihadapi masing-masing organisasi.

Proses adalah mekanisme yang menggambarkan proses pengambilan dan pengawasan keputusan strategis TI (Guldentops, E., Van Grembergen, W., & De Haes, S, 2002). Beberapa mekanisme proses yang umum atau ada dalam tata kelola TI adalah sebagai berikut: *Tracking of IT Projects and resources consumed, service-level agreements, formally tracking business value of IT, charegerback arrangements* (Weill & Ross, 2004).

Selain dua hal diatas yaitu Struktur dan Proses, ternyata hal yang ketiga yaitu mekanisme hubungan disadari tidak kalah penting mengambil bagian dalam penerapan tata kelola TI. Hal ini mengingat meskipun struktur dan proses baik bukan jaminan akan pencapaian tata kelola TI, namun harus ditunjang dengan saling pengertian antara TI dengan bisnis unit lain atau dengan kata lain

komunikasi. Untuk mencapai tata kelola TI yang efektif diperlukan komunikasi dua arah, partisipasi yang baik dan hubungan kolaborasi antara orang-orang bisnis dan orang-orang TI. Sangat krusial sekali untuk memfasilitasi *sharing, knowledge management, continous education* dan *cross training.* Mekanisme hubungan juga dapat dicapai melalui partisipasi aktif dan kolaborasi antar *stakeholder*, *rewards* dan *incentive*, *business/ IT co-location*, *cross functional business/IT training* dan rotasi.

Komponen utama dari tata kelola TI (Putra, Risma Bayu, Sesuse, Indra Dana, 2009).

1. Apakah keputusan yang perlu dibuat?
2. Siapakah yang memutuskan dan memberi masukan?
3. Bagaimana keputusan tersebut terbentuk dan berperan?

2.8 Tata Kelola TI Pada Institusi Pemerintahan

Suatu tata kelola adalah bagaimana mengubah kebiasaan dalam pengambilan keputusan oleh karena itu pengambilan keputusan harus mengacu kepada prinsip-prinsip dari tata kelola TI diantaranya (Putra, Risma Bayu, Sesuse, Indra Dana, 2009):

1. Citra yang bersih.
    a) Organisasi yang bersih.
    b) Kebijakan yang jelas dan standar.
    c) Komunikasi yang kuat.
    d) Strategi yang jelas.
2. Pemeriksaan secara *independent* dan peningkatan yang berkelanjutan.
3. *Proactive* melakukan perubahan manajemen jika manajemen tidak berjalan dengan baik.
4. Bertanggung jawab dan penanganan bisnis operasi yang bersih.
    a) Organisasi yang terpercaya.

b) Efektif dalam penggunaan TI.
c) Bertanggung jawab terhadap pengelolaan aset.

5. Proses yang akurat.

Tata kelola pemerintahan dengan memanfaatkan teknologi informasi atau yang sering kita sebut sebagai *e-government* yang terus dikembangkan oleh pemerintah perlu melihat ini. Proyek *e-government* di berbagai daerah masih sering terjadi pemborosan dan tidak berguna, hal ini karena belum dipahami tentang pengembangan teknologi informasi dan belum adanya alat kendali baik oleh eksekutif maupun inspektorat jendral.

Menteri Komunikasi dan Informatika Mohammad Nuh dalam sambutan tertulisnya pada Workshop Kode Etik dan Evaluasi Kelompok Kerja Teknologi Informasi dan Komunikasi Nasional, mengatakan bahwa:

Sebagian besar proyek yang berbasis TI dilingkungan pemerintahan tidak dibarengi dengan tingkat pemahaman prinsip TI yang baik. Prinsip-prinsip permasalahan *IT Governance* yang digunakan dalam pengembangan berbagai proyek pembangunan tersebut masih sangat rendah. Selain itu, hal yang lebih memprihatinkan adalah bahwa proses evaluasi sebuah kegiatan berbasis penggunaan TI di lingkungan pemerintahan masih sangat jarang dilakukan, atau bahkan tidak dikenali sama sekali. Oleh karena itu, ditegaskan bahwa pemahaman yang mendalam mengenai tata kelola TI dan evaluasi TIK menjadi hal mendasar yang tidak bisa ditawar lagi dan harus dikuasai di lingkungan pemerintahan.

Manfaat penerapan tata kelola TI pada institusi pemerintahan akan ditunjukkan pada gambar 2.4 berikut ini.

Manfaat Penerapan ICT Governance di Institusi Pemerintah
Nasional a. Koordinasi dan integrasi Rencana TI Nasional b. Mendapatkan standar rujukan kualitas penyelenggaraan TI di seluruh institusi pemerintahan c. Memudahkan monitoring dan evaluasi penyelenggaraan TI di seluruh institusi pemerintahan
Institusional a. Mendapatkan batasan dan panduan sesuai dengan *best practice* dalam penyelenggaraan TI-nya dilingkungan masing-masing b. Mengoptimalkan ketercapaian *value* dari penyelenggaraan TI di lingkungan kerjanya masing-masing: internal manajemen & pelayanan publik
Publik a. Mendapatkan kualitas pelayanan publik yang lebih baik b. Transparansi kriteria batasan penyelenggaraan TI oleh institusi pemerintah, sehingga dapat melakukan fungsi

Gambar 2.4 Manfaat Penerapan ICT Governance Pada Institusi Pemerintahan (Detiknas, 2007)

2.9 Standardisasi Pedoman Tata Kelola Teknologi Informasi

Terdapat berbagai macam *framework* untuk menunjang pembuatan pedoman tata kelola TI. Beberapa diantaranya adalah Cobit, ITIL, dan ISO/IEC 17799. Dalam pembuatan pedoman tata kelola TI pada tugas akhir ini yang akan digunakan adalah berdasarkan ISO/IEC 17799.

Organisasi Internasional untuk Standardisasi (ISO) adalah badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standar nasional setiap negara. ISO menetapkan standar-standar industrial dan komersial dunia. Meski ISO adalah organisasi nonpemerintah, kemampuannya untuk menetapkan standar yang sering menjadi hukum melalui persetujuan atau standar nasional membuatnya lebih berpengaruh daripada kebanyakan organisasi non-pemerintah lainnya. Penerapan ISO di suatu perusahaan berguna untuk:

- Meningkatkan citra perusahaan.

- Meningkatkan kinerja lingkungan perusahaan.
- Meningkatkan efisiensi kegiatan.
- Memperbaiki manajemen organisasi dengan menerapkan perencanaan, pelaksanaan, pengukuran dan tindakan perbaikan (*plan, do, check, act).*
- Mengurangi ancaman risiko.
- Meningkatkan daya saing.
- Meningkatkan komunikasi internal dan hubungan baik dengan berbagai pihak yang berkepentingan.
- Mendapat kepercayaan dari konsumen/mitra kerja/pemodal.

2.10 ISO/IEC 17799

ISO 17799, yaitu sebuah standar untuk sistem manajemen keamanan informasi. Standar kebutuhan ISO 17799 meliputi: dokumen kebijakan keamanan informasi, alokasi keamanan informasi tanggung-jawab, menyediakan semua para pemakai dengan pendidikan dan pelatihan di dalam keamanan informasi, mengembangkan suatu sistem untuk pelaporan peristiwa keamanan, memperkenalkan virus kendali, mengembangkan suatu rencana kesinambungan bisnis, mengendalikan pengkopian perangkat lunak kepemilikan, surat pengantar arsip organisatoris, mengikuti kebutuhan untuk perlindungan data, dan menetapkan prosedur untuk mentaati kebijakan keamanan (ISO, 2005).

ISO/IEC 17799 dikembangkan oleh *The International Organization for Standardization* (ISO) dan *The International Electrotechnical Commission* (IEC). ISO/IEC 17799 bertujuan memperkuat 3 (tiga) element dasar keamanan informasi, yaitu (Carlson, 2001):

1. *Confidentiality:* memastikan bahwa informasi hanya dapat diakses oleh yang berhak.
2. *Integrity:* menjaga akurasi dan selesainya informasi dan metode pemrosesan.

3. *Availability:* memastikan bahwa *user* yang terotorisasi mendapatkan akses kepada informasi dan aset yang terhubung dengannya ketika memerlukannya.

Jaminan kemanan informasi dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang dimaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, dan fungsi-fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruh sasaran keamanan yang dimaksud dapat tercapai.

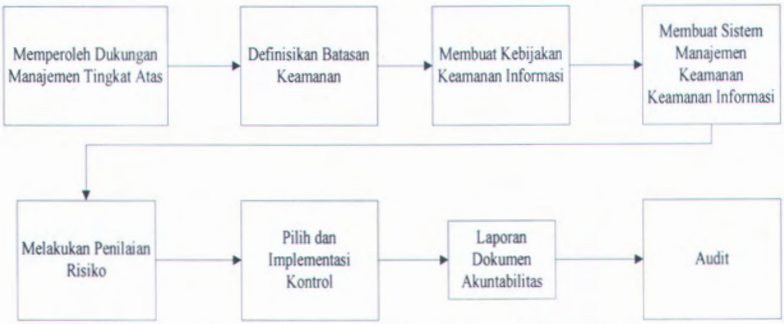
ISO/IEC 17799 terdiri atas 10 pasal pengamatan, 36 objek pengamanan 127 pengawasan keamanan. Dalam tugas akhir ini, penulis mengacu pada klausul 8 yang sesuai dengan proses pengelolaan keamanan sistem informasi yaitu:

Klausul 8: Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi yaitu sebuah klausul untuk memastikan bahwa keamanan dibangun dalam sistem informasi. Persyaratan Keamanan sistem mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna. Disain dan implementasi proses bisnis yang mendukung aplikasi atau layanan sangat menentukan bagi keamanan. Persyaratan keamanan harus diidentifikasi dan disetujui sebelum pengembangan sistem informasi. Semua persyaratan keamanan sisitem informasi, termasuk kebutuhan pengaturan darurat, harus diidentifikasi pada fase persyaratan suatu proyek., dan diputuskan, disetujui serta didokumentasikan sebagai bagian dari keseluruhan kasus bisnis sebuah sistem informasi. Aspek yang terlingkupi, yaitu :

- *Security requirements of information systems.*
- *Correct processing in applications.*
- *Crypthographic controls.*
- *Security of system files.*
- *Security in development and support processes.*

- *Technical vulnerability management*

Tahapan implementasi manajemen keamanan informasi (Carlson, 2001) menggunakan ISO/IEC 17799 dapat dilihat pada gambar 2.5 berikut ini.



Gambar 2.5 Tahapan Implementasi ISO/IEC 17799

Langkah pertama ialah mendapatkan dukungan manajemen atas. Proses pengaturan sebuah infrastruktur yang sesuai dengan organisasi mungkin berat, dan antusiasme serta dedikasi dapat memudar dengan waktu. Sebuah ISO pelaksanaan 17799 berhasil menanamkan keamanan sebagai gaya hidup organisasi didorong dari manajemen tingkat atas. Keamanan informasi bukanlah sebuah program, melainkan adalah sebuah proses.

Selanjutnya langkah kedua adalah menentukan perimeter keamanan, atau domain keamanan, yang, konseptual, harus sesuai sertifikasi ISO 17799. Perimeter keamanan mungkin atau mungkin tidak mencakup organisasi total, namun perimeter keamanan harus berada di bawah kendali organisasi. Jika sebuah organisasi tidak bisa mengendalikan, itu tidak dapat dikelola secara efektif.

Berikutnya langkah ketiga ialah membuat kebijakan keamanan informasi dapat mengambil berbagai bentuk. Mereka mungkin terkandung dalam satu kebijakan dokumen, beberapa dokumen disesuaikan dengan *audience* yang berbeda, atau

pernyataan kebijakan dimasukkan dalam standar. Namun demikian, tujuannya adalah sama. Implementasi pernyataan independen yang menunjukkan dukungan manajemen atas tentang konsep – konsep keamanan informasi dan tujuannya.

Langkah keempat ialah merancang kerangka sistem manajemen keamanan informasi (SMKI) harus dibuat untuk melaksanakan, mengelola, mempertahankan, dan menegakkan proses keamanan informasi. Perjanjian yang diberdayakan oleh dukungan dari manajemen tingkat atas dibuktikan dalam kebijakan keamanan informasi, dengan mendefinisikan perimeter keamanan dan menyediakan rincian *roadmap* strategi informasi keamanan untuk masing-masing dari 10 daerah kontrol ISO 17799.

Langkah kelima ialah mengembangkan manajemen risiko dan strategi mitigasi, dimana aset, ancaman, dan kerentanan diidentifikasi dan risiko sesuai ditentukan besarannya. Kontrol kemudian dapat dipilih untuk menghindari, mengalihkan, atau mengurangi risiko tingkat yang dapat diterima. Penilaian keamanan risiko adalah suatu metode untuk memaksimalkan penggunaan organisasi dengan aset terbatas berbasis risiko yang terukur dan toleransi organisasi terhadap risiko.

Langkah keenam adalah memilih kontrol keamanan yang didasarkan pada ketersediaan aset dan kemampuan manajemen untuk menerima resiko tertentu sebagai ganti menerapkan kontrol. Hal ini dapat diprioritaskan oleh nilai risiko yang diidentifikasi dalam Langkah 5.

Langkah ketujuh adalah membuat sebuah pernyataan implementasi (*document in statement of accountability*) adalah bagian dari SMKI bahwa dokumen yang mengidentifikasi risiko yang ada dalam penilaian risiko dikelola dengan cara pemilihan kontrol. Dokumen ini membahas lokasi kontrol 10 ISO 17799, dan tahapan pemilihan atau tidak adanya kontrol, bersama dengan alasan mengapa itu diperlukan.

Langkah terakhir adalah mengaudit kontrol yang sudah dilakukan untuk melakukan penelaahan atas pelaksanaan

infrastruktur keamanan informasi dengan baik dan bernar. Audit terdiri atas:

- Audit dilakukan oleh organisasi.
- Audit dilakukan oleh seorang pelanggan atau mitra.
- Audit dilakukan oleh auditor independen.

2.11 Panduan Umum Tata Kelola TIK Nasional

Penyelenggaraan pemerintahan dalam rangka pelayanan publik memerlukan *Good Governance*. Implementasi *Good Governance* akan menjamin transparansi, efisiensi, dan efektivitas penyelenggaraan pemerintahan (Detiknas, 2007). Pada sisi lain, penggunaan TIK oleh institusi pemerintahan sudah dilakukan sejak beberapa dekade lalu, dengan intensitas yang semakin meningkat. Untuk memastikan penggunaan TIK tersebut benar-benar mendukung tujuan penyelenggaraan pemerintahan, dengan memperhatikan efisiensi penggunaan sumber daya dan pengelolaan risiko terkait dengannya, diperlukan *Good Governance* terkait dengan TIK, yang dalam dokumen ini disebut sebagai Tata Kelola TIK.

Berikut ini adalah analisis atas kondisi sekarang yang menjadi latar belakang perlunya Tata Kelola TIK Nasional (Detiknas, 2007):

a) Perlunya Rencana TIK nasional yang lebih harmonis. Hampir semua institusi memiliki Rencana TIK, tetapi integrasi dan sinkronisasi di level nasional masih lemah.

b) Perlunya pengelolaan yang lebih baik untuk merealisasikan flagship nasional. *Flagship* nasional yang merupakan inisiatif TIK strategis memerlukan pendekatan yang lebih baik, khususnya dalam hubungan antar lembaga dan hubungan dengan penyedia layanan.

c) Perlunya peningkatan efisiensi dan efektivitas belanja/investasi TIK. Diperlukan mekanisme yang

memungkinkan menghindari kemungkinan terjadinya redundansi inisiatif TIK, sehingga meningkatkan efisiensi dan efektivitas belanja/investasi TIK nasional.

d) Perlunya pendekatan yang meningkatkan pencapaian value dari implementasi TIK nasional. Nilai yang dapat diciptakan dengan implementasi TIK, khususnya yang dapat dirasakan langsung oleh publik.

Panduan Tata Kelola TIK Nasional diperuntukkan bagi seluruh instansi pemerintah di semua level sebagai berikut (Detiknas, 2007):

a) Departemen atau LPND di tingkat pusat.

b) Propinsi.

c) Kabupaten/Kota.

Panduan Tata Kelola TIK Nasional dalam dokumen ini tidak mengatur pengelolaan TIK di badan usaha milik negara seperti BUMN dan BUMD. Panduan Umum Tata Kelola TIK Nasional akan digunakan sebagai prinsip dan panduan bagi setiap institusi pemerintahan dalam penggunaan sumber daya TIK di institusi masing-masing, sehingga memenuhi asas: efektivitas, efisiensi, dan akseptabilitas. Tujuan Panduan Umum Tata Kelola TIK Nasional adalah memberikan batasan dan panduan bagi institusi pemerintahan dan entitas pengambil keputusan di dalamnya dalam pengelolaan sumber daya TIK.

Aspek-aspek berikut ini diharapkan akan mengalami peningkatan secara signifikan dengan implementasi Panduan Umum Tata Kelola TIK Nasional (Detiknas, 2007):

a) Sinkronisasi dan integrasi Rencana TIK Nasional.

b) Efisiensi belanja TIK nasional.

c) Realisasi solusi TIK yang sesuai kebutuhan secara efisien.

d) Operasi sistem TIK yang memberikan nilai tambah secara signifikan kepada publik dan internal manajemen pemerintahan.

Panduan Tata Kelola TIK Nasional terdiri atas lima prinsip dasar yang menjadi pondasi bangunan Tata Kelola TIK Nasional. Prinsip ini mendasari model dan tingkat kedalaman implementasi model.

a) Prinsip 1. Perencanaan TIK yang sinergis dan konvergen di level internal institusi dan nasional. Memastikan bahwa setiap inisiatif selalu didasarkan pada rencana yang telah disusun sebelumnya; dan memastikan bahwa rencana-rencana institusi di semua level pemerintahan, sinergis dan konvergen dengan rencana nasional.

b) Prinsip 2. Penetapan kepemimpinan dan tanggung jawab TIK yang jelas di level internal institusi dan nasional. Memastikan bahwa setiap institusi memahami dan menerima posisi dan tanggung jawabnya dalam peta TIK nasional secara umum, dan memastikan bahwa seluruh entitas fungsional di setiap institusi memahami dan menerima perannya dalam pengelolaan TIK di institusinya masing-masing.

c) Prinsip 3. Pengembangan dan/atau akuisi TIK secara valid. Memastikan bahwa setiap pengembangan dan/atau akuisisi TIK didasarkan pada alasan yang tepat dan dilakukan dengan cara yang tepat; berdasarkan analisis yang tepat dan terus-menerus. Memastikan bahwa dalam setiap pengembangan dan/atau akuisisi TIK selalu ada pertimbangan keseimbangan yang tepat atas manfaat jangka pendek dan jangka panjang, biaya dan risiko-risiko.

d) Prinsip 4. Memastikan operasi TIK berjalan dengan baik, kapan pun dibutuhkan. Memastikan kesesuaian TIK dalam mendukung institusi, responsif atas perubahan kebutuhan

kegiatan institusi, dan memberikan dukungan kepada kegiatan institusi di semua waktu yang dibutuhkan institusi.

e) Prinsip 5. Memastikan terjadinya perbaikan berkesinambungan (*continuous improvement*) dengan memperhatikan faktor manajemen perubahan organisasi dan sumber daya manusia. Memastikan bahwa penetapan: tanggung jawab, perencanaan, pengembangan dan/atau akuisisi, dan operasi TIK selalu dimonitor dan dievaluasi kinerjanya dalam rangka perbaikan berkesinambugan (*continuous improvement*). Memastikan bahwa siklus perbaikan berkesinambungan (*continuous improvement*) dilakukan dengan memperhatikan manajemen perubahan organisasi dan sumber daya manusia.

Model Tata Kelola TIK Nasional difokuskan pada pengelolaan proses-proses TIK melalui mekanime pengarahan dan monitoring & evaluasi yang terdiri atas 5 elemen, yaitu:

- Perencanaan sistemm, proses ini menangani identifikasi kebutuhan organisasi dan formulasi inisiatif-inisiatif TIK apa saja yang dapat memenuhi kebutuhan organisasi tersebut..
- Manajemen belanja/investasi, proses ini menangani pengelolaan investasi/belanja TIK.
- Realisasi sistem, proses ini menangani pemilihan, penetapan, pengembangan/akuisisi sistem TIK, serta manajemen proyek TIK.
- Pengoperasian sistem, proses ini menangani operasi TIK yang memberikan jaminan tingkat layanan dan keamanan sistem TIK yang dioperasikan.
- Pemeliharaan sistem, proses ini menangani pemeliharaan aset-aset TIK untuk mendukung pengoperasian sistem yang optimal.

Model keseluruhan Tata Kelola TIK Nasional ditunjukkan pada gambar 2.6 berikut ini.

Gambar 2.6 Model Tata Kelola Nasional

1. Struktur & Peran Tata Kelola. Yaitu entitas apa saja yang berperan dalam pengelolaan proses-proses TIK dan bagaimana pemetaan perannya dalam pengelolaan proses-proses TIK tersebut. Struktur dan peran tata kelola ini mendasari seluruh proses tata kelola TIK.

2. Proses Tata Kelola. Yaitu proses-proses yang ditujukan untuk memastikan bahwa tujuan-tuuan utama tata kelola dapat tercapai, terkait dengan pencapaian tujuan organisasi, pengelolaan sumber daya, dan manajemen risiko.

a) Lingkup Proses Tata Kelola

i. Perencanaan Sistem. Proses ini menangani identifikasi kebutuhan organisasi dan formulasi inisiatif-inisiatif TIK apa saja yang dapat memenuhi kebutuhan organisasi tersebut.

ii. Manajemen Belanja/Investasi. Proses ini menangani pengelolaan investasi/belanja TIK

iii. Realisasi Sistem. Proses ini menangani pemilihan, penetapan, pengembangan/akuisisi sistem TIK, serta manajemen proyek TIK.

iv. Pengoperasian Sistem. Proses ini menangani operasi TIK yang memberikan jaminan tingkat layanan dan keamanan sistem TIK yang dioperasikan.

v. Pemeliharaan Sistem. Proses ini menangani pemeliharaan aset-aset TIK untuk mendukung pengoperasian sistem yang optimal.

b) Mekanisme Proses Tata Kelola

i. Kebijakan Umum. Ditetapkan untuk memberikan tujuan dan batasan-batasan atas proses TIK bagaimana sebuah proses TIK dilakukan untuk memenuhi kebijakan yang ditetapkan.

ii. Monitoring & Evaluasi. Monitoring & evaluasi ditetapkan untuk memastikan adanya umpan balik atas pengelolaan TIK, yaitu berupa ketercapaian kinerja yang diharapkan. Untuk mendapatkan deskripsi kinerja setiap proses TIK digunakan indikator keberhasilan. Indikator keberhasilan inilah yang akan dapat digunakan oleh manajemen atau auditor, untuk mengetahui apakah proses TIK telah dilakukan dengan baik.

Struktur Tata Kelola. Penetapan entitas struktur tata kelola ini dimaksudkan untuk memastikan kapasitas kepemimpinan yang memadai, dan hubungan antar satuan kerja/institusi pemerintahan yang sinergis dalam perencanaan, penganggaran, realisasi sistem TIK, operasi sistem TIK, dan evaluasi secara umum implementasi TIK di pemerintahan. Berikut ini adalah ketentuan umum terkait dengan Struktur Tata Kelola. Pembentukan CIO dan Komite TIK di tiap institusi pemerintahan merupakan prioritas, disamping entitas-entitas struktur tata kelola TIK yang sudah ada sebelumnya (Detiknas, 2007):

a) Eksekutif Institusi Pemerintahan. Yaitu pimpinan institusi pemerintahan (Kabupaten/Kota, Propinsi, Departemen, LPND)
b) Satuan Kerja Pengelola TIK. Yaitu satuan kerja yang bertugas dalam pengelolaan TIK institusi pemerintahan. Posisi struktural satuan kerja pengelola TIK ini saat ini mempunyai level struktural yang berbeda-beda di institusi-institusi pemerintahan.
c) Satuan Pemilik Proses Bisnis. Yaitu satuan kerja di luar satuan kerja pengelola TIK sebagai pemilik proses bisnis (*Business Process Owner*).

2.12 Pengendalian Dokumen Menurut ISO/IEC 9001:2000

Organisasi harus menetapkan dan memelihara prosedur tertulis untuk pengendalian semua dokumen yang dibutuhkan untuk manajemen dari proses-proses (Gasperz, 2002). Dokumentasi harus dapat dibaca, revisi harus dikendalikan dan dapat diidentifikasi dengan segera, dipelihara dalam susunan yang teratur dan dipertahankan untuk suatu periode waktu yang ditentukan. Prosedur dan tanggungjawab harus ditetapkan dan dipelihara berkaitan dengan pembuatan dan modifikasi dari berbagai jenis dokumen.

Prosedur tertulis untuk pengendalian dokumen harus memperhatikan hal-hal berikut (Gasperz, 2002):

a) Persetujuan kesesuaian dokumen sebelum diterbitkan.
b) Peninjauan-ulang, pembaruan apabila diperlukan, dan persetujuan-ulang dokumen-dokumen.
c) Identifikasi status revisi dari dokumen-dokumen.
d) Menjamin bahwa versi yang relevan dari dokumen yang diterapkan itu tersedia pada tempat-tempat yang diperlukan.
e) Menjamin bahwa dokumen-dokumen itu dapat dibaca, teridentifikasi dan mudah untuk ditemukan kembali.

f) Menjamin bahwa dokumen-dokumen yang berasal dari eksternal adalah teridentifikasi dan pendistribusiannya terkendali.

g) Mencegah penggunaan dokumen-dokumen yang usang atau tidak berlaku lagi, dan menerapkan cara identifikasi yang tepat untuk dokumen-dokumen itu apabila masih dipertahankan untuk suatu maksud tertentu.

2.13 *Standard Operating Prosedures*

2.13.1 Definisi *Standard Operating Procedures* (SOP)

Untuk dapat membuat suatu prosedur operasi yang standar, yang harus dilakukan terlebih dahulu adalah mengetahui definisi, fungsi dan tujuan *Standard Operating Procedure* (SOP), manfaat SOP, bentuk SOP yang dapat dipilih, dan cara implementasi serta pengembangan SOP. Berikut ini adalah uraian mengenai masing-masing bagian tersebut diatas. Berikut ini beberapa definisi tentang *Standard Operating Procedures* (SOP), yaitu (Gasperz, 2002):

- SOP adalah serangkaian instruksi yang menggambarkan pendokumentasian dari yang dilakukan secara berulang pada sebuah organisasi.
- SOP adalah panduan yang menjelaskan secara terperinci bagaimana suatu proses harus dilaksanakan.
- SOP adalah serangkaian instruksi yang digunakan untuk memecahkan suatu masalah.

2.13.2 Fungsi dan Tujuan *Standard Operating Procedures* (SOP)

Fungsi *Standard Operating Procedures* (SOP) adalah untuk mendefinisikan semua konsep dan teknik yang penting serta persyaratan yang dibutuhkan, yang ada dalam setiap kegiatan yang dituangkan ke dalam suatu bentuk yang langsung dapat digunakan oleh karyawan dalam pelaksanaan kegiatan sehari-hari (Gasperz, 2002). Setiap penjelasan yang harus tercantum dalam

SOP merupakan suatu hal yang mungkin sulit dibuat, karena dalam prosedur yang dibuat harus mencantumkan setiap langkah kegiatan yang penting dan harus dijalankan oleh semua karyawan dengan cara yang sama.

2.13.3 Manfaat Standard Operating Procedures (SOP)

Dengan membuat *Standard Operating Procedures*(SOP), ada beberapa manfaat yang dapat diperoleh yaitu :

- Dapat menjelaskan secara detail semua kegiatan dari proses yang dijalankan.
- Dapat menstandarkan semua aktivitas yang dilakukan pihak yang bersangkutan.
- Membantu untuk menyederhanakan semua syarat yang diperlukan dalam proses pengambilan keputusan.
- Dapat meningkatkan komunikasi antara pihak-pihak yang terkait, terutama pekerja dengan pihak manajemen.

2.14 Perbedaan ISO 17799 dan COBIT

2.14.1 ISO 17799

ISO 17799 menjadi ekslusif untuk keamanan informasi dan hanya mencakup masalah tersebut. ISO dibagi menjadi 10 seksi, dengan 36 objektif. Setiap objektif kemudian dibagi kembali menjadi sub-objektif (Solms, 2005). Sisi baik dari penggunaan ISO 17799 untuk tata kelola menyediakan panduan tentang 'bagaimana' harus dilakukan. Ini akan memberi panduan tentang apa kebijakan keamanan informasi dalam hal struktur dan konten.

Karena ini lebih rinci, dan mungkin lebih 'teknis' orientasinya dalam hal ini di banyak kasus merupakan kerangka pilihan manajer TI dan manajer keamanan informasi. Kelemahan dari menggunakan ISO 17799, adalah bahwa kerangka tersebut 'berdiri sendiri', tidak dapat diintegrasikan ke dalam kerangka yang lebih luas untuk tata kelola teknologi informasi (Solms, 2005).

2.14.2 COBIT

COBIT memposisikan dirinya sebagai alat untuk tata kelola teknologi informasi (ITGI, Control Objectives for Information and Related Technologies (COBIT), 2000). Oleh karena itu, Cobit tidak ekslusif untuk keamanan informasi dimana dapat dialamatkan tata kelola teknologi informasi, dan dapat mencakup beberapa masalah yang berkaitan dengan keamanan informasi. COBIT membagi tata kelola teknologi informasi menjadi 34 proses dan menunjang kontrol objektif tingkat tinggi (CO) untuk setiap 34 proses.

Sisi baik menggunakan COBIT sebagai kerangka kerangka tata kelola teknologi informasi pada keamanan informasi adalah 'terintegrasi' menjadi lebih besar atau lebih luas. Kerangka tata kelola teknologi informasi disediakan dalam 33 proses lainnya. Bahkan jika COBIT hanya digunakan untuk keamanan informasi, maka masih menyediakan sisa kerangka lainnya jika perusahaan kemudian memutuskan untuk menjadikannya sebagai dasar tata kelola teknologi informasi pemerintahan juga didefinisikan oleh COBIT (ITGI, Control Objectives for Information and Related Technologies (COBIT), 2000).

Kekurangannya penggunaan COBIT tata kelola teknologi informasi tidak selalu rinci dalam kondisi 'bagaimana' untuk melakukan hal-hal tertentu. The DCO lebih ditujukan kepada 'apa' harus dilakukan. Dalam kebanyakan kasus beberapa pedoman yang lebih rinci untuk merinci tepatnya hal-hal 'bagaimana' harus dilakukan, akan dibutuhkan.

Karena sejarah COBIT yang sering digunakan oleh TI auditor, COBIT dalam banyak kasus juga disukai oleh TI auditor dan manajer risiko TI sebagai kerangka pilihan.

2.14.3 Pemetaan antara ISO 17799 dan COBIT

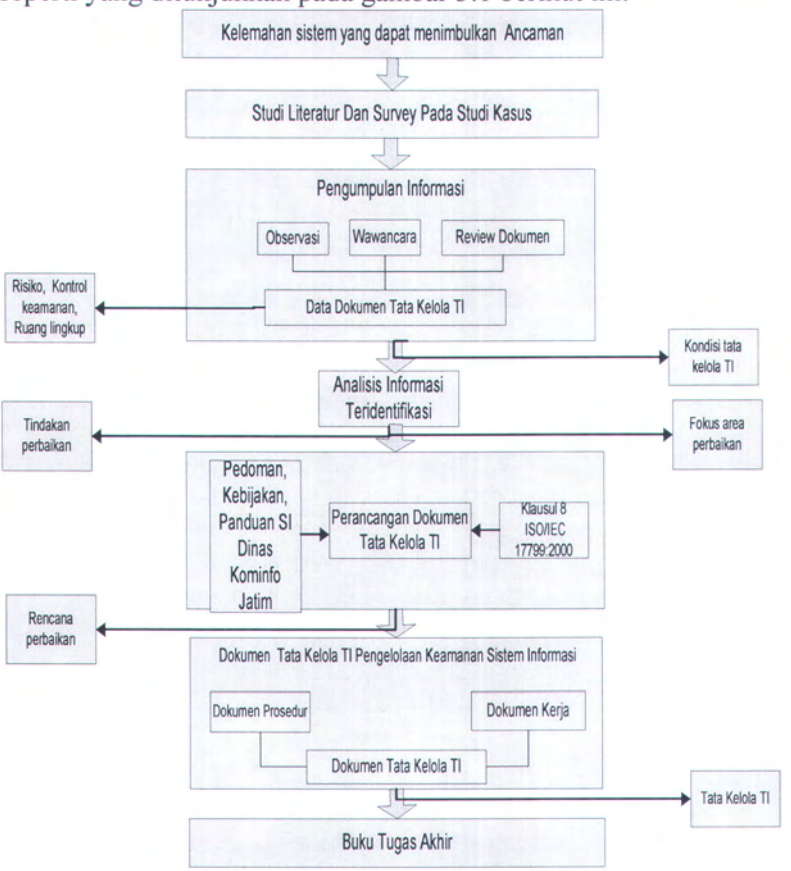
Dalam Pemetaan COBIT antara ISO/IEC 17799, pemetaan rinci antara COBIT dan ISO 17799 disediakan. Setiap DCO COBIT diselidiki, dan disesuaikan, jika ada, ISO 17799 tujuan dan / atau sub-tujuan ditunjukkan kesesuaiannya.

Sayangnya pemetaan hanya satu arah, dari COBIT dengan ISO 17799, dan tidak memberikan pemetaan dari ISO 17799 kembali ke COBIT (ITGI, Control Objectives for Information and Related Technologies (COBIT), 2000). Pemetaan tersebut akan berguna, tetapi dapat cukup mudah untuk menelusuri kembali pemetaan yang disediakan.

Halaman ini sengaja dikosongkan.

BAB III
METODE PENELITIAN

Bab ini menjelaskan urutan langkah-langkah yang dilakukan penulis untuk menyelesaikan tugas akhir ini. Metode penyelesaian tugas akhir ini meliputi lima tahap dan masing-masing tahap dibagi menjadi dua langkah atau lebih. Berikut ini ialah metodologi yang digunakan dalam penelitian tugas akhir seperti yang ditunjukkan pada gambar 3.1 berikut ini.



Gambar 3.1 Metode Penelitian

Metode penelitian ini adalah sebagai berikut:

3.1 Persiapan

Pada tahap ini, penulis melakukan pengamatan terhadap semua kemungkinan kelemahan yang ada pada suatu sistem informasi. Kelemahan yang ditemukan menjadi dasar terhadap penanganan ancaman yang berpotensial bagi TI yang dapat dijadikan acuan perbaikan pengelolaan keamanan sistem informasi ke depannya dalam bentuk sebuah rekomendasi tata kelola TI. Hal tersebut dilakukan untuk mengetahui latar belakang dan tujuan pembuatan dokumen tata kelola teknologi informasi sekaligus memahami kondisi tata kelola TI yang diterapakan di studi kasus. Dalam tahap ini terdapat 2 aktifitas, yaitu:

3.1.1 Studi Literatur

Studi literatur yang dilakukan dalam pembuatan tugas akhir ini adalah pembelajaran literatur yang terkait dengan permasalahan yang ada, seperti pembelajaran mengenai identifikasi komponen, jenis sistem informasi serta arsitektur informasi yang ada pada Dinas Komunikasi Dan Informatika Jawa Timur. Selanjutnya perbedaan *framework* tata kelola TI ISO/IEC 17799 antara COBIT. Selain itu diperlukan kajian yang berdasarkan penelitian yang lain tentang identifikasi ancaman yang muncul di sebuah sistem informasi serta pembelajaran *framework* tata kelola TI yaitu *IT Governance Implementation Guide* dan panduan umum tata kelola TIK nasional yang ada dalam pembuatan dokumen tata kelola TI.

3.1.2 Survey Pada Studi Kasus

Pada tahap ini penulis melakukan identifikasi terhadap sistem informasi yang ada di instansi tersebut disertai dengan proses bisnis yang didukung oleh sistem informasi tersebut. Hal ini merupakan persiapan terpenting karena pada tahap ini penulis merumuskan masalah, tujuan dan manfaat penelitian sehingga akhirnya akan dimengerti hal apa saja yang diharapkan dari hasil penelitian ini.

3.2 Pengumpulan Informasi

Dalam metode penelitian ini terdiri 3 aktivitas yang dilakukan yaitu: observasi, wawancara dan pengamatan dokumen terkait. 3 Aktivitas ini dilakukan setelah pada metode penelitian sebelumnya, penulis menemukan kelemahan dari sistem informasi yang dapat menimbulkan ancaman keamanan di masa mendatang. Hasil dari metodologi penelitian ini, penulis dapat mengidentifikasi risiko, dampak, kontrol keamanan dan sop yang diterapkan. Dengan demikian, penulis dapat mengetahui kondisi *existing* sehingga penulis dapat menyusun tata kelola TI sesuai dengan apa yang diharapkan oleh instansi tersebut meliputi: apa saja komponen tata kelola TI yang ada, siapa yang membuat tata kelola TI tersebut dan sejauh mana peran tata kelola TI yang diterapkan dalam institusi pemerintahan tersebut.

3.2.1 Observasi

Teknik yang digunakan dalam observasi yaitu dengan pengamatan secara langsung mengenai kontrol keamanan yang diimpelementasikan pada sistem informasi yang ada di Bidang Pengembangan TI Dinas Komunikasi Dan Informatika Jawa Timur.

3.2.2 Wawancara

Pada bagian ini, penulis memperoleh keterangan tentang risiko yang sering muncul beserta dampak yang dihasilkan bagi instansi dengan melakukan tanya jawab terhadap pihak yang terlibat langsung dengan pengembangan dan pemeliharaan sistem informasi yang ada pada Dinas Komunikasi Dan Informatika Jawa Timur khususnya Bidang Pengambangan TI. Dengan melakukan wawancara ini, maka penulis dapat memiliki gambaran terhadap rencana perbaikan dalam keamanan sistem informasi.

3.2.3 Pengamatan Dokumen Terkait

Pengamatan dokumen terkait tentang keamanan sistem informasi yang diterapkan di Bidang Pengembangan TI Dinas Komunikasi Dan Informatika Jawa Timur merupakan langkah efektif yang dilakukan oleh penulis dalam mengumpulkan

informasi baik mengenai *sop* yang sudah diterapkan terkait pengembangan dan pemeliharaan sistem informasi maupun dokumen-dokumen pendukung lainnya yang digunakan sebagai acuan tugas dalam instansi tersebut. Dokumen-dokumen tersebut merupakan sumber informasi yang penting dalam mengidentifikasi kondisi keamanan sistem informasi yang ada.

3.3 Analisis Informasi Teridentifikasi

Pada tahap analisis informasi teridentifikasi merupakan tahap untuk melakukan penyusunan dan pengorganisasian risiko yang diperoleh dari kegiatan pengumpulan informasi, dengan melakukan penilaian risiko dan membuat strategi mitigasi sebagai hasil interpretasi pengelolaan keamanan sistem informasi yang ada di Bidang Pengembangan TI.

Penilaian risiko sendiri dilakukan dengan mengalikan besarnya probabilitas frekuensi kemunculan suatu risiko pada institusi dan dampak yang akan dihasilkan (ISO, 2005). Selanjutnya ialah menetapkan strategi mitigasi yang harus dilakukan untuk mengatasi risiko yang ada. Dengan catatan strategi mitigasi tidak semua diimplementasikan kepada pihak institusi, hal ini disebabkan keterbatasan sumberdaya yang dimiliki pihak institusi sehingga hanya beberapa risiko yang mempunyai skala prioritas yang tinggi yang akan ditangani. Lebih lanjut lagi, pada tahap ini penulis dapat menentukan fokus area perbaikan serta tindakan perbaikan bagi risiko yang tidak ditangani dengan tepat sehingga dapat menghasilkan sebuah mekanisme perlindungan yang efektif dan efisien yang sesuai dengan apa diharapkan oleh institusi.

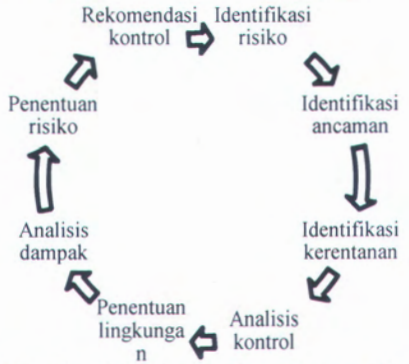
3.3.1 Kerangka Kerja Manajemen Risiko TI

Risiko didefinisikan sebagai kemungkinan yang menonaktifkan pencapaian tujuan. Dalam lingkungan teknologi, risiko umumnya dijelaskan sendiri sebagai ancaman bagi apa yang diperlukan untuk menentukan tingkat kemungkinan terjadinya hal ini dan mengambil tindakan yang diperlukan untuk mengurangi dampaknya. "Risiko merupakan fungsi dari

kemungkinan kemunculan sumber-ancaman yang dihasilkan dari potensi kerentanan tertentu, dan dampak yang dihasilkan dari peristiwa yang merugikan pada organisasi ". Risiko di lingkungan teknologi menggambarkan hubungan langsung antara unsur-unsur berikut:

- **Ancaman**: tindakan yang dapat menimbulkan konsekuensi negatif di operasional proses organisasi.
- **Aset**: aktiva yang terkait dengan sistem informasi atau aplikasi untuk dievaluasi (Data, perangkat keras, perangkat lunak, layanan, dokumen, sumber daya manusia, antara lain-lain).
- **Dampak**: konsekuensi terjadinya berbagai ancaman itu.
- **Kerentanan**: kondisi-kondisi tertentu yang melekat terhadap aset atau yang ada pada lingkungan mereka untuk memfasilitasi perwujudan dari ancaman yang membuat aset menjadi rentan.
- **Kemungkinan**: mengevaluasi semua kegiatan dengan ketidakpastian tentang apa yang dapat diharapkan.

Penilaian risiko adalah alat diagnosis untuk menetapkan dampak nyata risiko dalam organisasi. Hal ini juga dikenal sebagai jantung dari semua kinerja terorganisir untuk mencapai manajemen keamanan global. Penilaian risiko menyiratkan apa yang dibutuhkan untuk dilindungi, dari apa yang harus dilindungi, dan bagaimana melindunginya. Penilaian risiko melibatkan proses manajemen risiko yang diilustrasikan pada gambar 3.2 berikut ini.



Gambar 3.2 Proses Manajemen Risiko

Manajemen risiko mengacu pada evaluasi sumber daya organisasi untuk mencapai tingkat keamanan tertentu. Pentingnya manajemen risiko berada dalam kemampuannya untuk memungkinkan mengidentifikasi dampak masa depan semua proyek dalam organisasi struktur risiko. Ini adalah proses yang berkesinambungan, sejak diperlukan proses yang dilakukan secara berkala untuk mengevaluasi risiko baru yang teridentifikasi dan eksposur risiko tersebut yang dihitung pada tahapan sebelumnya agar tetap efektif. Selain itu, proyeksi risiko (perkiraan resiko) mencoba untuk mengukur risiko masing-masing dengan dua cara yaitu probabilitas bahwa risiko adalah nyata dan konsekuensi yang terkait dengan risiko, jika itu terjadi.

3.4 Pembuatan Dokumen Tata Kelola TI

Tahap ini merupakan tahapan pembuatan dokumen tata kelola teknologi informasi. Untuk membuat sebuah dokumen tata kelola TI, terlebih dahulu pada bab ini diidentifikasi komponen penyusun tata kelola TI sebagai identifikasi kebutuhan tata kelola TI. Aktivitas yang dilakukan ialah dengan menyusun diagram raci chart yang digunakan untuk mengidentifikasi semua stakeholder yang terkati dengan tata kelola TI itu sendiri. Lalu menyusun sebuah rencana perbaikan yang difokuskan ke pemilihan bentuk dokumen tata kelola TI yang tepat, setelah itu menyusun komponen dokumen standar operasional prosedur dan komponen dokumen SOA sebagai hasil validasi komponen dokumen standar operasional prosedur yang telah disetujui oleh pihak institusi.

Lebih lanjut lagi setelah komponen penyusun dokumen tata kelola TI sudah teridentifikasi maka tahap berikutnya ialah menyusun dokumen tata kelola TI berupa

- Dokumen kerja sebagai representasi tugas pokok dan fungsi aparatur negara yang ada di institusi pemerintahan.
- Dokumen prosedur yang didalamnya terdapat struktur tata kelola TI, komponen dokumen prosedur pasca dokumen SOA telah disetujui institusi sebagai

dokumen tata kelola teknologi informasi yang dapat diimplementasikan pada Dinas Komunikasi Dan Informatika Jawa Timur terutama pada Bidang Pengembangan Teknologi Informatika.

3.5 Penyusunan Buku Tugas Akhir

Setiap langkah-langkah pengerjaan tugas akhir ini dari awal hingga akhir terutama dokumen tata kelola TI yang sudah dihasilkan, sekaligus kesimpulan yang didapat dari proses-proses tersebut didokumentasikan dan ditulis dalam sebuah laporan yang sesuai dengan format tugas akhir sehingga menghasilkan laporan tugas akhir.

Halaman ini sengaja dikosongkan.

BAB IV
HASIL PENELITIAN DAN ANALISIS DATA

Bab ini menjabarkan hasil penelitian mengenai tata kelola teknologi informasi pada Dinas Komunikasi Dan Informatika Jawa Timur, khususnya pada Bidang Pengembangan TIK, identifikasi sistem informasi yanga ada di instansi serta proses bisnis yang didukung oleh sistem informasi tersebut. Tidak lupa juga adanya identifikasi risiko yang muncul karena kelemahan sistem, penilaian risiko yang didasarkan pada dampak bagi yang dihasilkan pada instansi, serta pengelolaan mitigasi risiko yang optimal sebagai tujuan perbaikan yang diperlukan agar rancangan tata kelola TI yang disusun dapat mencapai hasil yang diinginkan.

Tahapan penelitian yang dilakukan adalah sebagai berikut:

4.1 Studi Literatur

Hasil yang didapatkan pada tahap ini sudah dicantumkan dalam bab sebelumnya yaitu pada Bab II.

4.2 Survey Pada Studi Kasus

4.2.1 Profil Dinas Komunikasi Dan Informatika

Dinas Komunikasi dan Informatika merupakan unsur pelaksana otonomi daerah, yang dipimpin oleh seorang kepala dinas, yang berada di bawah dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah. Dinas Komunikasi dan Informatika mempunyai tugas melaksanakan urusan pemerintahan daerah berdasarkan asas otonomi dan tugas pembantuan di bidang komunikasi dan informatika. Dinas Komunikasi dan Informatika menyelenggarakan fungsi:

a) Perumusan kebijakan teknis di bidang komunikasi dan informatika.
b) Penyelenggaraan urusan pemerintahan dan pelayanan umum di bidang komunikasi dan informatika.
c) Pembinaan dan pelaksanaan tugas sesuai dengan lingkup tugasnya.
d) Pelaksanaan tugas lain yang diberikan oleh Gubernur.

4.2.2 Visi Dan Misi Dinas Komunikasi Dan Informatika

1. Meningkatkan kapasitas layanan informasi, memberdayakan potensi masyarakat dan kerjasama lembaga komunikasi dan informatika.
2. Meningkatkan profesionalisme aparatur bidang komunikasi dan informatika dan e-*literacy* masyarakat.
3. Mengembangkan infrastruktur TIK melalui pengembangan aplikasi, muatan layanan publik, standarisasi dan pemanfaatan jaringan TIK dalam rangka peningkatan pelayanan publik.
4. Meningkatkan pembinaan, pengawasan dan pengendalian terhadap pengusahaan, penyelenggaraan jasa pos dan telekomunikasi.

4.2.3 Layanan Dinas Komunikasi Dan Informatika

Layanan yang ada dalam Dinas Komunikasi dan Informatika adalah sebagai berikut:

- Kegiatan pelayanan perizinan bidang pos, telekomunikasi dan telekomunikasi khusus diantaranya:
  - Izin Penyelenggaraan Usaha Jasa Titipan.
  - Izin Amatir Radio (IAR).
  - Izin Komunikasi Radio Antar Penduduk (IKRAP).
  - Izin Penguasaan Perangkat Amatir Radio.
  - Izin Penguasaan Perangkat KRAP.
  - Penyelenggaraan Ujian Negara Amatir Radio.
  - Verifikasi Administrasi Dan Data Teknis Ijin Lembaga Penyiaran Televisi.
- Kegiatan pelayanan teknis kepada SKPD – SKPD di lingkungan Pemerintah Provinsi Jawa Timur dengan menempatkan server dan aplikasinya untuk memeperoleh fasilitas akses internet guna mendukung layanan informasi publik.
- Kegiatan layanan yang memfasilitasi keterhubungan dan jaringan antar SKPD untuk mengintegrasikan sistem informasi dan database dalam rangka implementasi e-government dan layanan publik.
- Pusat pengolahan dan produksi informasi yang langsung di upload untuk dipublikasikan dalam website www.jatimprov.go.id. Selain itu juga dihimpun dalam

- Penyelenggaraan pusat informasi bagi masyarakat berbasis TIK dalam rangka memberdayakan masyarakat yang dikelola oleh masyarakat. Selain itu untuk memberikan kemudahan pada masyarakat untuk mengakses informasi secara cepat dan murah, TC juga sebagai tempat pembelajaran TIK dalam rangka meningkatkan pengetahuan dan ketrampilan. Adanya TC juga mendukung kegiatan ekonomi masyarakat dengan dukungan media dan teknologi untuk memudahkan survei pasar, pemasaran dan transaksi.
- Penyelenggaraan kegiatan pembelajaran kelompok informasi masyarakat di pedesaan tentang managemen komunikasi yang efektif, memilih dan memilah informasi secara mandiri termasuk didalamnya kemampuan penguasaan TIK.
- Penyelenggaran pekan informasi yaitu sebuah kegiatan sebagai wahana pemberdayaan lembaga komunikasi masyarakat sebagai agen penyebarluasan informasi sekaligus sebagai publik relation di wilayahnya. Agenda tetap pelaksanaan Pekan Informasi dilaksanakan setahun sekali di kabupaten/kota yang telah mendapat persetujuan lokasi oleh Gubernur Jatim. Pekan informasi juga merupakan ajang bertemunya para anggota KIM dalam tukar menukar informasi dengan berbagai kegiatan:
  - Pameran produk-produk unggulan daerah.
  - Lomba stan.
  - Grand final lomba pertura.
  - Grand final lomba cerdik komunikatif.
  - Lomba animasi dan lomba blogger.
  - Workshop KIM.
  - Sarasehan KIM.
  - Forum Komunikasi Media Tradisional (FK Metra).

bentuk cetak rilis yang didistribusikan ke SKPD, Muspida, masyarakat dan kalangan pers.

- Memfasilitasi akses informasi berbasis TIK untuk mendekatkan pemerintah dengan masyarakat melalui situs www.jatimprov.go.id dan sub domain website Dinas Kominfo.
- Pelayanan informasi berupa "etalase informasi" yang dipergunakan untuk masyarakat berupa layanan:
  - Layanan Langsung (pengunjung).Layanan Melalui Email.
  - Layanan Melalui Telepon.
  - Helpdesk.
  - Layanan Internet.
  - Layanan Dokumentasi.
- Penyelenggaraan radio milik Pemerintah Provinsi Jawa Timur yang memberikan informasi yang aktual, faktual dengan prinsip keseimbangan. JTFM menjadi siaran Radio Publik Lokal di segmen umum menyiarkan musik dan informasi lokal di Jawa Timur. Jangkauan siaran Radio JTFM yang meliputi wilayah Surabaya sekitarnya.
- Kegiatan penyebarluasan informasi melalui media penerbitan Tabloit "Potensi" yang terbit dengan periodesitas terbit setiap bulan sekali didistribusikan pada SKPD lingkungan Provinsi Jatim, ke Kabupaten/Kota, Kecamatan se Jawa Timur dan Kelompok Informasi Masyarakat (KIM) se Jawa Timur.
- Penyelenggaraan program unggulan yang berhubungan langsung dengan masyarakat dan sebagai wadah untuk menyampaikan keluhan masyarakat secara interaktif. Kegiatan Ajang Wadul di laksanakan di stasiun televisi di Jawa Timur dengan jadwal minggu I dan III setiap bulan. Kegiatan ini dinilai tepat sasaran dalam era keterbukaan informasi publik dan mampu berkiparah banyak serta lebih memberi manfaat bagi masyarakat luas.

4.2.4 Struktur Organisasi Bidang Pengembangan TI Dinas Komunikasi Dan Informatika

Struktur organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur dapat dilihat pada lampiran poin A.1, sedangkan struktur organisasi Bidang Pengembangan TI dapat dilihat pada gambar 4.1 berikut ini yang membawahi:

1. Seksi Pengembangan Perangkat Lunak.
2. Seksi Pengembangan Perangkat Keras.
3. Seksi Layanan Teknologi Informasi dan Komunikasi.

Dalam Bidang Pengembangan Teknologi Informatika, masing-masing seksi dipimpin oleh kepala seksi yang berada di bawah dan bertanggung jawab kepada kepala bidang.

Gambar 4.1 Struktur Organisasi Bidang Pengembangan TI Dinas Komunikasi Dan Informatika

4.2.5 Uraian Tugas Bidang Pengembangan TI Dinas Komunikasi Dan Informatika

Uraian tugas Dinas Komunikasi dan Informatika Provinsi Jawa Timur dapat dilihat pada lampiran poin A.2, uraian tugas Bidang Pengembangan Teknologi Informatika terkait pengelolaan keamanan sistem informasi ditunjukkan pada tabel 4.1 berikut ini.

Tabel 4.1 Pemetaan Uraian Tugas Bidang Pengembangan TI

Bidang Pengembangan TI	
Tugas	Melaksanakan pengembangan dan pengendalian serta pemeliharaan sarana prasarana teknologi informatika
Fungsi	a) Pelaksanaan penyusunan pedoman dalam rangka pengembangan teknologi informatika dan komunikasi. b) Pelaksanaan penyusunan kebutuhan dan konfigurasi perangkat keras, perangkat lunak, dan layanan teknologi informasi dan komunikasi. c) Pelaksanaan pemeliharaan perangkat keras dan perangkat lunak. d) Pelaksanaan koordinasi dalam rangka pengembangan teknologi informasi dan komunikasi.
Membawahi:	

Tabel 4.1 Pemetaan Uraian Tugas Bidang Pengembangan TI

Seksi Perangkat Lunak	Seksi Perangkat Keras	Seksi Layanan TIK
a) Menyiapkan bahan pengembangan perangkat lunak. b) Menyiapkan bahan analisis penggunaan dan perkembangan perangkat lunak. c) Menyiapkan bahan kebutuhan perangkat lunak. d) Menyiapkan bahan perekayasaan pengembangan perangkat lunak. e) Menyiapkan bahan pertimbangan penggunaan atau pemilihan perangkat lunak. f) Menyiapkan bahan pelaksanaan kerjasama dalam rangka pengembangan perangkat lunak.	a) Menyiapkan bahan pengembangan perangkat keras. b) Menyiapkan bahan analisis penggunaan dan perkembangan perangkat keras. c) Menyiapkan bahan pertimbangan pernggunaan atau pemilihan perangkat keras. d) Menyiapkan bahan spesifikasi kebutuhan perangkat keras dan sarana pendukung lainnya.	a) Menyiapkan bahan pengumpulan layanan teknologi informasi dan komunikasi. b) Menyiapkan bahan fasilitasi teknologi informasi dan komunikasi. c) Menyiapkan bahan pertimbangan penggunaan atau pemilihan perangkat teknologi informasi dan komunikasi. d) Menyiapkan bahan kerjasama dalam rangka layanan teknologi informasi dan komunikasi.

4.2.6 Proses Bisnis Bidang Pengembangan TI Dinas Komunikasi Dan Informatika

Proses bisnis merupakan representasi dari kegiatan-kegiatan bisnis yang ada di perusahaan atau suatu institusi dalam hal ini sehingga dapat digunakan sebagai acuan dasar dalam proses penelitian lebih lanjut. Gambaran proses bisnis secara umum yang telah didapatkan, kemudian dipetakan ke dalam ISO/IEC 17799 kemudian didapatkan informasi yang relevan dalam pemilihan klausul kontrol keamanan ISO/IEC 17799 terkait dengan pengelolaan keamanan sistem informasi. Adapun proses bisnis pada Dinas KOMINFO Jawa Timur khususnya Bidang Pengembangan TI dapat digambarkan dalam diagram *value chain* gambar 4.2 berikut ini.

	Bidang Pengembangan TI				
	Infrastruktur TI				
Proses Bisnis Dinas KOMINFO	Perencanaann sistem	Pengoperasian sistem	Realisasi sistem	Pelayanan publik	Monitoring
	Perencanaan proyek IT. Penyusunan tata cara pendaftaran E-*Procurement*	Aplikasi BP-LPSE untuk verifikasi E-*Procurement*	Penciptaan aplikasi perangkat lunak dan perangkat keras.	Penyediaan pelatihan bagi para karyawan. Penyediaan layanan TIK.	Mengawasi hasil kinerja tiap-tiap entitas bidang TIK
Proses ISO/IEC 17799 hasil pemetaan prinsip kinerja	*Clause 1 Security Policy*	*Clause 7 Access Control*	*Clause 3 Asset Management*	*Clause 4 Human Resources Security*	*Clause 6 Communications And Operations Management*
	Clause 2 Organization of Information Security	*Clause 8 Informations System Acquisition, Development and Maintenance*	*Clause 5 Physical and Environmental Security*	*Clause 6 Communications And Operations Management*	*Clause 9 Information Security Incident Management*
	Clause 10 Business Continuity Management	-	*Clause 8 Informations System Acquisition, Development and Maintenance*	-	*Clause 11 Compliance*

Gambar 4.2 Diagram *Value Chain* Hasil Pemetaan Proses Bisnis Bidang Pengembangan TI Dinas Kominfo Dengan Klausul Kontrol Keamanan ISO/IEC 17799

Pada gambar 4.2 proses-proses yang ditunjukkan pada diagram *value chain* tersebut masih menggambarkan proses bisnis secara umum sehingga belum dapat merepresentasikan secara khusus terhadap pengelolaan keamanan sistem informasi. Oleh karena itu, perlu adanya pemilahan proses-proses mana yang dirasa tidak dibutuhkan dalam kaitannya dengan pengelolaan keamanan sistem informasi. Hasilnya adalah pada gambar 4.3 berikut ini.

Proses Bisnis Dinas KOMINFO	Bidang Pengembangan TI Infrastruktur TI Perencanaann sistem	Pengoperasian sistem	Realisasi sistem	Pelayanan publik	Monitoring
	Perencanaan proyek IT. Penyusunan tata cara pendaftaran E-*Procurement*	Aplikasi BP-LPSE untuk verifikasi E-*Procurement*	Penciptaan aplikasi perangkat lunak dan perangkat keras.	Penyediaan pelatihan bagi para karyawan. Penyediaan layanan TIK.	Mengawasi hasil kinerja tiap-tiap entitas bidang TIK
Proses ISO/IEC 17799 hasil pemetaan prinsip kinerja	-	-	-	-	-
	-	*Clause 8 Informations System Acquisition, Development and Maintenance*	-	-	-
	-	-	*Clause 8 Informations System Acquisition, Development and Maintenance*	-	-

Gambar 4.3 Diagram *value chain* Hasil Pemilahan Klausul Kontrol Keamanan ISO/IEC 17999 Yang Sesuai Dengan Pengelolaan Keamanan Sistem Informasi Dengan Proses Bisnis Bidang Pengembangan TI Dinas Komunikasi dan Informatika Provinsi Jawa Timur

4.2.7 Sistem Informasi Yang Dikelola Bidang Pengembangan TI Dinas Komunikasi Dan Informatika

Salah satu tugas awal yang paling sulit adalah untuk menentukan perimeter keamanan, atau domain keamanan, yang, konseptual. Perimeter keamanan mungkin atau mungkin tidak mencakup organisasi total, namun perimeter keamanan harus berada di bawah kendali organisasi. Oleh karena itu pada tabel 4.2 penulis akan mengidentifikasikan batasan keamanan dalam pengelolaan keamanan sistem informasi khususnya sistem informasi yang dikelola dan dipelihara oleh Bidang Pengembangan TI yang dapat dilihat pada lampiran poin A.3.

Selain memiliki tugas untuk memelihara dan mengelola beberapa sistem informasi yang disebutkan diatas, Dinas Komunikasi dan Informatika Provinsi Jawa Timur tugas penting lainnya yaitu melakukan pengelolaan dan pemeliharaan website jatimprov.go.id termasuk pembuatan dan pengaturan website tersebut bagi semua SKPD PEMPROV JATIM. Saat ini terdapat 38 nama *website* dibawah naungan domain jatimprov.go.id yang juga ditunjukkan pada tabel 4.2 berikut ini.

Tabel 4.2 Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI Dinas Kominfo Provinsi Jawa Timur

Nama Website	***Domain***	**Fungsi**
Sistem Informasi Pendaftaran Online Penyedia Barang/Jasa LPSE	bplpse.jatimprov.go.id	Pendaftaran dan verifikasi penyedia barang/jasa yang akan mendaftar *e-lelang* yang dilakukan oleh panitia lpse provinsi Jawa Timur

Tabel 4.2 Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI Dinas Kominfo Provinsi Jawa Timur

Sistem Informasi Monitoring Dan Evaluasi Pembangunan Provinsi Jawa Timur	smep.jatimprov.go.id	Melaporkan realisasi penyerapan anggaran apbd/apbn yang telah oleh setiap skpd.
E-lelang	e-lelang.jatimprov.go.id	Pemberitahuan informasi tentang pelelangan dan pendaftaran peserta yang diadakan di Jawa Timur.
Sistem Informasi Evaluasi Perencanaan Pembangunan	sievap.jatimprov.go.id	Mengevaluasi perencanaan pembangunan pemerintah daerah provinsi Jawa Timur.
Sistem Informasi Perencanaan Pembangunan Daerah	sippd-jatim.net	Digunakan untuk merencanakan pembangunan daerah sesuai dengan program yang disusun setiap SKPD Jawa Timur.

Tabel 4.2 Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI Dinas Kominfo Provinsi Jawa Timur

Sistem Informasi Kinerja Pemerintah	bappeda.jatimprov.go.id/ web/sikap	Master perencanaan dan evaluasi seluruh skpd di Jawa Timur sesuai dengan KPI provinsi Jawa Timur
Badan koordinasi wilayah pemerintah dan pembangunan Bojonegoro	bakorwilbojonegoro.jatimprov.go.id	*Website* SKPD
Badan koordinasi wilayah pemerintah dan pembangunan Malang	bakorwilmalang.jatimprov.go.id	*Website* SKPD
Badan kepegawaian daerah provinsi Jawa Timur	bkd.jatimprov.go.id	*Website* SKPD
Badan ketahanan pangan provinsi Jawa Timur	bkp.jatimprov.go.id	*Website* SKPD

Tabel 4.2 Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI Dinas Kominfo Provinsi Jawa Timur

Badan narkotika provinsi Jawa Timur	bnp.jatimprov.go.id	*Website* SKPD
Badan penanaman modal provinsi Jawa Timur	bpm.jatimprov.go.id	*Website* SKPD
Dinas sosial provinsi Jawa Timur	dinsos.jatimprov.go.id	*Website* SKPD
Dinas perikanan dan kelautan provinsi Jawa Timur	diskanlut.jatimprov.go.id	*Website* SKPD
Dinas tenaga kerja, transmigrasi dan kependudukan provinsi Jawa Timur	disnakertransduk.jatimprov.go.id	*Website* SKPD
Dinas kepemudaan dan keolahragaan provinsi Jawa Timur	dispora.jatimrpov.go.id	*Website* SKPD
DPR daerah provinsi Jawa Timur	dprd.jatimprov.go.id	*Website* SKPD

Tabel 4.2 Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI Dinas Kominfo Provinsi Jawa Timur

Dinas pariwisata dan kebudayaan provinsi Jawa Timur	infostrategis.jatimprov.go.id	Info skpd yang strategis di provinsi Jawa Timur
Ikatan pencak silat provinsi Jawa Timur	ipsi.jatimprov.go.id.id	*Website* SKPD
Website pemerintah daerah provinsi Jawa Timur	jatimprov.go.id	*Website* SKPD
Korps pegawai negeri provinsi Jawa Timur	korpri.jatimprov.go.id	*Website* SKPD
Komisi pelayanan publik provinsi Jawa Timur	kpp.jatimprov.go.id	*Website* SKPD
Komisi pemilihan umum provinsi jawa timur	kpujatim.go.id	*Website* SKPD
Pelayanan perizinan terpadu provinsi Jawa Timur	p2t.jatimprov.go.id	Memberikan pelayanan masyarakat dalam satu tempat

Tabel 4.2 Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI Dinas Kominfo Provinsi Jawa Timur

Kantor perwakilan provinsi Jawa Timur di jakarta	perwakilan.jatimprov.go.id	*Website* SKPD
Dinas pekerjaan umum cipta karya dan tata ruang provinsi Jawa Timur	pu-ciptakarya-tataruang.jatimprov.go.id	*Website* SKPD
Biro perekonomian provinsi Jawa Timur	ro-ekonomi.jatimprov.go.id	*Website* SKPD
Sekretariat daerah provinsi Jawa Timur	setda.jatimprov.go.id	*Website* SKPD
Biro organisasi provinsi Jawa Timur	ro-organisasi.jatimprov.go.id	*Website* SKPD
Rumah sakit umum dr.soetomo	rsudrsoetomo.jatimprov.go.id	*Website* SKPD
Rumah sakit umum haji	rsuhaji.jatimprov.go.id	*Website* SKPD
Telecenter provinsi Jawa Timur	tc.jatimprov.go.id	Menyediakan fitur audio dan video conference SKPD lain.

Berdasarkan pengumpulan informasi yang telah dilakukan terkait daftar sistem informasi seperti yang telah ditunjukkan pada tabel 4.2, dapat disimpulkan bahwa:

1. Lebih dari 80% sistem informasi yang berbasis web kurang dikelola dengan baik oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur khususnya Bidang Pengembangan TI. Hal itu terbukti dengan intensitas serangan dari pihak luar yaitu 1x dalam jangka waktu kurang dari 1 bulan yang dapat dikategorikan *High*, sehingga dibutuhkan proses pengelolaan keamanan sistem informasi yang harus ditingkatkan.
2. Dari semua *website* yang sudah dibuat, masih terdapat beberapa *website* jatimprov.go.id yang belum dipergunakan secara optimal karena *website*nya sudah tidak aktif atau *website* sudah aktif menggunakan nama *domain* lain. Itu menyatakan bahwa praktik pengelolaan sistem informasi yang sekarang masih kurang dan jauh memenuhi harapan.
3. Kebanyakan sistem informasi yang dijalankan pada area lokal Dinas Kominfo masih belum dijalankan dan terkendala teknis dalam operasionalnya sehingga area ini tidak menjadi fokus pengelolaan keanaman sistem informasi.
4. Fokus area perbaikan dokumen tata kelola TI yang akan dibuat ditujukan kepada sistem informasi dan *website* SKPD yang sudah teridentifikasi pada tabel 4.2 sebelumnya dikarenakan semua sistem informasi dan website yang sudah teridentifikasi berfungsi dan digunakan sampai sekarang oleh setiap SKPD.
5. Teknik perlindungan keamanan sistem informasi yang akan dibuat disamakan untuk semua sistem informasi walaupun memiliki spesifikasi yang berbeda – beda karena berbasis *web*.

4.3 Observasi

Pengamatan langsung yang dilakukan oleh penulis di institusi ini menghasilkan sebuah rekomendasi kontrol keamanan yang dapat diimplementasikan dan sekaligus memperbaiki proses pengelolaan keamanan sistem informasi yang ada sehingga dapat mengatasi risiko keamanan yang sering terjadi disebabkan kelemahan sistem itu sendiri. Adapun kontrol keamanan yang yang direkomendasikan berdasar dari pengamatan langsung yang dapat dilihat pada lampiran poin A.4 adalah sebagai berikut:

4.3.1 Kontrol Administratif

Kontrol administratif dimaksudkan untuk menjamin bahwa seluruh kerangka kontrol dikontrol sepenuhnya oleh organisasi itu sendiri berdasarkan prosedur-prosedur yang jelas. Pada tabel 4.3 berikut ini penulis menyusun sebuah rekomendasi perbaikan kontrol fisik sebagai rencana perbaikan yang dapat diimplementasikan pada institusi dalam bentuk sebuah dokumen tata kelola TI.

Tabel 4.3 Rekomendasi Perbaikan Kontrol Administratif

Kontrol	Tindakan
Pencegahan	Pelatihan kesadaran keamanan untuk karyawan. Publikasi kebijakan kontrol yang sudah dibuat kepada seluruh karyawan.
Pendeteksian	Mengaudit karyawan yang akan keluar.
Penghindaran	Persetujuan kepemilikan hak data.
Perbaikan	Pengaturan waktu untuk pembersihan data dengan laporan perbaikan sistem.
Pemulihan	Menghubungi pihak berwajib ketika terjadi pelanggaran keamanan.

Tabel 4.3 Rekomendasi Perbaikan Kontrol Administratif

Kontrol administratif di Bidang Pengembangan TI
• Supervisi terhadap para pegawai. • Pembinaan dan pelatihan kepada karyawan. • Pemisahan tugas-tugas setiap karyawan.

4.3.2 Kontrol Operasi

Kontrol operasi dimaksudkan agar sistem beroperasi sesuai dengan yang diharapkan sehingga dapat meningkatkan kualitas pelayanan publik yang diberikan oleh pihak institusi pemerintah ini. Pada tabel 4.4 berikut ini penulis menyusun sebuah rekomendasi perbaikan kontrol operasi sebagai rencana perbaikan yang dapat diimplementasikan pada institusi dalam bentuk sebuah dokumen tata kelola TI.

Tabel 4.4 Rekomendasi Perbaikan Kontrol Operasi

Kontrol	**Tindakan**
Pencegahan	Monitoring sistem dan jaringan. Menghindari pengambilan berkas yang mengandung makro dari sebarang tempat. Menghindari pemakaian perangkat lunak *freeware* atau *shareware* dari sumber yang belum terpercaya.
Pendeteksian	Pemberian pesan *error* ketika terjadi penerobosan keamanan. Secara rutin menjalankan program antivirus untuk mendeteksi infeksi virus. Melakukan pembandingan ukuran-ukuran berkas untuk mendeteksi perubahan ukuran pada berkas.

Tabel 4.4 Rekomendasi Perbaikan Kontrol Operasi

Penghindaran	Akun yang terdaftar akan hilang atau terhapus setelah 3 kali pemasukan *login* salah.
Perbaikan	Pengaturan *firewall* secara berkala dan berganti-ganti setelah ada penerobosan keamanan. Memiliki rencana terdokumentasi tentang pemulihan dari infeksi virus. Memastikan pem-*backup*-an yang bersih. Menjalankan program antivirus untuk menghilangkan virus dari program yang tertular.
Pemulihan	Melakukan restorasi pada data yang sudah disimpan (*backup*) sebelumnya.
Kontrol operasi di Bidang Pengembangan TI	
• Pembatasan akses terhadap pusat data • Pengendalian terhadap virus • Kontrol terhadap peralatan	

4.3.3 Kontrol Fisik

Kontrol yang dilakukan oleh organisasi untuk menjaga hal-hal yang tidak diinginkan baik pada pusat data maupun komponen perangkat keras lain yang digunakan agar dapat mengantisipasi kegagalan sistem komputer. Oleh karena itu peralatan-peralatan yang berhubungan dengan faktor-faktor fisik perlu dipantau dengan baik.

Pada tabel 4.5 berikut ini penulis menyusun sebuah rekomendasi perbaikan kontrol fisik sebagai rencana perbaikan yang dapat diimplementasikan pada institusi dalam bentuk sebuah dokumen tata kelola TI.

Tabel 4.5 Rekomendasi Perbaikan Kontrol Fisik

Kontrol	Tindakan
Pencegahan	Pembatasan akses pada ruangan server.
Pendeteksian	Penggunaan kunci ganda (segel dengan rapat) laci *server*.
Penghindaran	Monitoring ruangan menggunakan kamera CCTV. Menggunakan UPS, untuk mengantisipasi kegagalan sumber daya listrik.
Perbaikan	Mengisolasi ruangan *server*.
Pemulihan	Meninjau kembali catatan elektronik *server*.
Kontrol fisik di Bidang Pengembangan TI	
• Pengontrolan suhu dan kelembaban di ruangan *server*. • Penggunaan komponen cadang (*fault tolerant system*).	

4.4 Wawancara

Wawancara adalah salah satu teknik pengumpulan data secara tatap muka langsung dimana pewawancara (*interviewer*) secara interaktif melakukan tanya jawab dengan orang yang diwawancarai (*interviewee*).

Oleh karena itu, bertanya merupakan cara yang efektif untuk memulai implementasi tata kelola sistem informasi. Setelah jawaban dari pertanyaan yang diajukan diperoleh, selanjutnya diperlukan aksi dan diikuti dengan tindakan selanjutnya. Berikut ini beberapa contoh pertanyaan yang dapat diajukan.

Penjabaran hasil wawancara dengan administrator sistem Bidang Pengembangan TI dapat dilihat pada lampiran A.5.

4.4.1 Untuk mengungkap isu-isu terkait sistem informasi

- Seberapa sering proyek sistem informasi mengalami kegagalan dalam memberikan kontribusi yang seharusnya diterima oleh institusi?

MILIK PERPUSTAKAAN ITS

- Apakah *end-user* merasa puas dengan kualitas dari kinerja sistem informasi yang diberikan?
- Apakah ketersediaan sumber daya, infrastruktur dan kompetensi sistem informasi memenuhi kebutuhan untuk pencapaian tujuan strategi institusi dalam memberikan pelayanan kepada publik?
- Seberapa besar peran yang dilakukan sistem informasi untuk menyelesaikan masalah dibandingkan dengan melakukan perbaikan proses bisnis?
- Bagaimana penerapan kontrol keamanan yang ada di institusi saat ini?
- Serangan apa saja yang sering ditemui dalam sebuah sistem informasi dalam periode tertentu?

4.4.2 Untuk mencari tahu bagaimana cara manajemen menanggapi isu-isu terkait sistem informasi

- Seberapa baikkah tujuan teknologi informasi dan perusahan sejalan?
- Inisiatif strategi apa yang telah diambil oleh manajemen eksekutif untuk mengelola aspek-aspek yang bersifat kritis, terkait dengan pemeliharaan dan pengembangan sistem informasi, dan apakah inisiatif strategi tersebut wajar?
- Apakah penanganan semua risiko yang ada dari penerapan sistem informasi tersebut sudah diterapkan dengan baik?
- Apakah institusi memiliki persediaan yang sudah paling terkini? Apa yang telah dilakukan untuk menangani resiko ini?

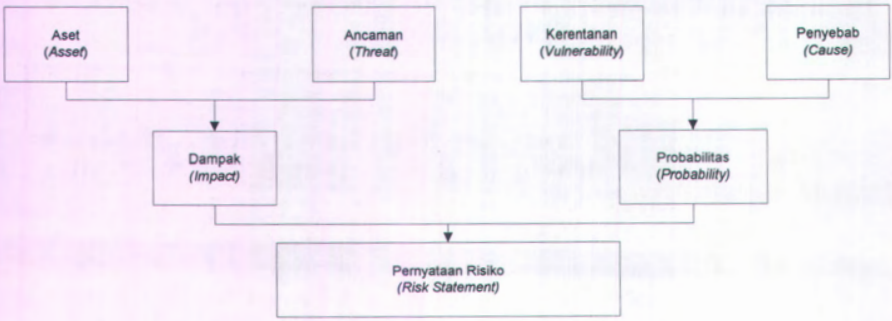
4.4.3 Untuk pengukuran sendiri pelaksanaan Tata Kelola Teknologi Informasi

- Apakah pihak manajemen secara regular melakukan pertemuan untuk membahas risiko-risiko sistem informasi yang muncul pada institusi?
- Bagaimana cara pihak manajemen melakukan artikulasi dan komunikasi tentang bagaimana caranya menyelaraskan antara tujuan bisnis dengan teknologi informasi?
- Bagaimana cara pihak manajemen memperoleh laporan perkembangan dari proyek sistem informasi yang dijalankan?

4.4.4 Identifikasi Risiko

Berkaitan dengan hasil wawancara yang dilakukan oleh penulis, maka selanjutnya dapat dilakukan analisis identifikasi risiko sesuai dengan tahapan proses identifikasi risiko yang terjadi dan ditemukan di Dinas Komunikasi dan Informatika Provinsi Jawa Timur seperti yang ditunjukkan pada gambar 4.6 dengan langkah sebagai berikut:

1. Melakukan identifikasi ancaman (*threat*) terhadap sistem informasi sebagai aset instansi dan dampak bisnis terkait dengan ancaman tersebut.
2. Melakukan identifikasi terhadap kelemahan (*vulnerability*) yang dapat memicu terjadinya ancaman (*threat*).



Gambar 4.4 Proses Identifikasi Risiko

Pada tabel 4.6 berikut ini merupakan aset yang teridentifikasi dalam analisis penelitian ini adalah komponen sistem informasi beserta informasi didalamnya yang sangat berharga bagi institutsi pemerintah tersebut, yang harus dilindungi dan dikelola secara tepat sehingga dapat memenuhi kriteria integritas, ketersediaan dan keandalan.

Tabel 4.6 Identifikasi Aset

No.	Kategori	Sumberdaya
1.	Jaringan	Teknologi *wireless*, jaringan VPN.

Tabel 4.6 Identifikasi Aset

2.	Perangkat lunak	Sistem informasi: BP-LPSE, SMEP, SIEVAP, SIPPD, SIKAP. *website* 38 SKPD, *server hosting*.
3.	Perangkat keras	Komputer *server* dan *client*, printer, scanner, keyboard, mouse, router, switch, colocation server, ruang penyimpanan server, kabel RJ45, dll.
4.	Manusia	administrator, *user* sistem, seluruh karyawan Bidang PTI, staff keamanan *server*, teknis.
5.	Data	Data pendaftar rekanan e-*Procurement*, data KPI SIKAP, data serapan APBD dan APBN, dll.

Selanjutnya ialah mengidentifikasi ancaman (*threat*) yang mengancam keberadaan sistem informasi sebagai aset berharga institusi. Ancaman terhadap sistem informasi muncul karena adanya kelemahan sistem informasi itu sendiri yang harus diwaspadai karena akan berdampak pada gangguan operasional pada proses bisnis yang ada. Terutama jika dampak yang ditimbulkan akibat bencana alam memerlukan waktu, tenaga dan biaya untuk pemulihan yang cukup besar.

Selain ancaman yang telah disebutkan diatas, pada penelitian yang dilakukan di Dinas Komunikasi dan Informatika Provinsi Jawa Timur juga kerap kali ditemukan berbagai variasi tipe serangan (Hisham, M. Haddad, Brunil, D. Romero, 2009) yang muncul disebabkan kelemahan yang ada pada sistem informasi baik berdampak besar maupun kecil pada perusahaan

yang membutuhkan penanganan lebih lanjut agar tidak menganggu kinerja institusi. Semuanya terangkum pada tabel 4.7 berikut ini.

Tabel 4.7 Identifikasi Risiko

No. 01	**Risiko**	Bencana alam	**Aset**	*Hardware*, Jaringan, *Software*, Manusia, Data.
	Penyebab Tidak ada sistem peringatan bencana alam dini.			
	Dampak • Membahayakan proses bisnis. • Proses bisnis dapat terhenti.			
	Kelemahan Pusat data DRC (*Disaster Recovery Center*).			
No. 02	**Risiko**	Gangguan yang disengaja	**Aset**	*Hardware*, Jaringan, *Software*, Data.
	Penyebab Tidak ada kontrol keamanan yang diterapkan.			
	Dampak • Membahayakan proses bisnis.			
	Kelemahan Sistem penanganan keamanan fisik.			
No. 03	**Risiko**	Gangguan utilitas umum	**Aset**	*Hardware*, Jaringan, *Software*,
	Penyebab Tidak ada sistem pemulihan pasca gangguan utilitas.			
	Dampak • Proses bisnis terhenti dan terganggu.			
	Kelemahan • Sumber tenaga listrik, sistem jaringan yang ada.			

Tabel 4.7 Identifikasi Risiko

No. 04	**Risiko**	Kerusakan peralatan.	**Aset**	*Hardware*, Jaringan.
	Penyebab Tidak ada pemeliharaan peralatan secara berkala.			
	Dampak • Proses bisnis terhenti.			
	Kelemahan • Perawatan (*maintenance*) peralatan.			
No. 05	**Risiko**	*Virus* atau *malware*.	**Aset**	*Software*, Jaringan, Data
	Penyebab Tidak ada *software* keamanan yang dipasang dan tidak di*update* untuk menambah *database*.			
	Dampak • Kehilangan data. • Data berubah. • Data tidak dapat diakses.			
	Kelemahan • Software keamanan meliputi: *firewall*, IDS, *antivirus*.			
No. 06	**Risiko**	Moral pegawai	**Aset**	*Software*, Manusia, Data
	Penyebab Tidak ada batasan hak akses masing-masing karyawan dalam sistem informasi.			
	Dampak • Penghapusan data. • Pencurian data. • Proses bisnis terhambat.			
	Kelemahan • Sistem pembatasan hak akses sistem informasi.			

Tabel 4.7 Identifikasi Risiko

No. 07	**Risiko**	*Hacking*	**Aset**	*Software*, Jaringan, Data
	Penyebab Tidak ada enkripsi yang dipasang dalam sistem informasi. Tidak ada sistem perlindungan yang diaktifkan seperti IDS, *firewall*, *antivirus*, internet *filtering*, anti *spam*, dll.			
	Dampak • Kehilangan data. • Data berubah. • Proses bisnis terganggu.			
	Kelemahan • Sistem perlindungan *server*, sistem informasi.			
No. 08	**Risiko**	*Denial of Service (DOS)*	**Aset**	*Software*, Jaringan, Data
	Penyebab Borosnya pemakaian *resource* cpu untuk memampatkan file untuk *client* yang sudah tidak ada. *Server* umumnya mengalokasikan *resource* seperti memori dan waktu untuk melayani semua *request* berupa paket *SYN* melalui koneksi TCP/IP, tanpa bisa membedakan *request* itu benar atau palsu. Tidak ada pembatasan jumlah pengguna pada sistem informasi.			
	Dampak • Mematikan server. • Menyibukkan server. • Proses bisnis terganggu.			
	Kelemahan • Sistem verifikasi *request* SYN oleh *server*.			

Tabel 4.7 Identifikasi Risiko

No. 09	**Risiko**	*Social Engineering*	**Aset**	*Software*, Data
	Penyebab Mekanisme otentikasi *login* sistem informasi tidak dienkripsi atau diberi perlindungan. Tidak ada pembatasan waktu kepada pengguna yang telah masuk ke sistem.			
	Dampak • Pencurian data oleh orang lain. • Hilangnya hak akses karyawan ke dalam sistem. • Hilangnya informasi penting ke orang lain.			
	Kelemahan • Mekanisme enkripsi pada *login* sistem informasi.			
No. 10	**Risiko**	*SQL Injection*	**Aset**	*Software*, Data.
	Penyebab Tidak ada mekanisme validasi data masukan pengguna. Tidak ada batasan hak akses (*priveleges*) setiap pengguna. Tidak ada mekanisme peringatan ketika terjadi kegagalan pada sistem.			
	Dampak • Kehilangan data. • Perubahan data. • Penghapusan data. • Kegagalan sistem sementara. • Proses bisnis terganggu.			
	Kelemahan • Mekanisme validasi data masukan oleh sistem informasi. • Mekanisme pembatasan *priveleges* seorang pengguna.			

Tabel 4.7 Identifikasi Risiko

No. 11	**Risiko**	*Malicious Code*	**Aset**	*Software*, Jaringan, Data.
	Penyebab Tidak ada mekanisme validasi data masukan pengguna. Tidak ada mekanisme enkripsi serta dekripsi pada data masukan dan keluaran. Tidak ada mekanisme pemberian eksepsi ketika terjadi kesalahan dalam program.			
	Dampak • Kelebihan *traffic*. • Konektivitas *website* terputus. • *Server crash* karena terlalu banyak *request* yang harus dilayani.			
	Kelemahan • Mekanisme validasi data masukan oleh sistem informasi. • Mekanisme enkripsi dan dekripsi. • Mekanisme eksepsi.			
No. 12	**Risiko**	*Buffer Overflow*	**Aset**	*Software*, Data.
	Penyebab Beberapa fungsi pada bahasa pemrogramman dapat dikategorikan berbahaya terutama yang berada pada bentuk *library*.			
	Dampak • Kinerja sistem informai menjadi kacau.			
	Kelemahan • Mekanisme validasi fungsi bahasa pemrogramman. • Mekanisme perlindungan *source code* program. • Mekanisme pertimbangan pemilihan bahasa pemrogramman.			

Tabel 4.7 Identifikasi Risiko

No. 13	**Risiko**	*Debugging* dan *Reverse Enggineering*	**Aset**	*Software*, Data.
	Penyebab Tidak ada pencatatan *log* pada *source code* program. Tidak mekanisme perlindungan algoritma pada saat *debugging.* Tidak menerapkan mekanisme *fail-safe-design* pada sistem informasi			
	Dampak • Perubahan struktur sistem informasi. • Pengkopian kode program.			
	Kelemahan • Mekanisme pencatatan *logging.* • Mekanisme perlindungan algoritma.			
No. 14	**Risiko**	*Information Disclosure*	**Aset**	*Software*, Data.
	Penyebab Adanya komentar pada *source code* program. Penampilan informasi yang penting dalam sistem. Ada pengkategorian data sensitif.			
	Dampak • Kebocoran data. • Pengkopian kode program.			
	Kelemahan • Mekanisme pencatatan *logging.* • Mekanisme perlindungan algoritma.			

Berdasarkan data atau informasi yang dikumpulkan sebelumnya dapat diketahui bahwa kondisi tata kelola TI Bidang Pengembangan TI sekarang ini, tidak diterapkan secara optimal, dikarenakan kurangnya perhatian dari pihak manajemen atas terkait pengelolaan keamanan serta ketidakefektifan penanganan semua risiko yang muncul karena kelemahan sistem itu sendiri.

4.5 Pengamatan Dokumen Terkait

Selama tahap pengumpulan informasi terkait dengan dokumen-dokumen yang diberlakukan sebagai acuan dalam pengelolaan keamanan sistem informasi tidak ditemukan sop yang membahas hal tersebut. Hal ini dikarenakan di instansi pemerintah tersebut baru akan dimulai pemetaan seluruh sistem informasi (*roadmap*) dan *sop* terkait dengan pengembangan serta pemeliharaan sistem informasi termasuk pengelolaan keamanan sistem informasi pada tahun 2011.

Namun demikian, ada beberapa dokumen yang dijadikan acuan umum untuk mengimplementasi sebuah sistem informasi seperti berikut ini:

- Keputusan Menteri Dalam Negeri No.45 Tahun 1992 Tentang Pokok-pokok Kebijakan Sistem Informasi Manajemen Departemen Dalam Negeri.
- Instruksi Presiden Republik Indonesia Nomor 6 Tahun 2001 Tentang Pengembangan Dan Pendayagunaan Telematika Di Indonesia.
- Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003 Tentang Kebijakan Dan Strategi Nasional Pengembangan e-Government.
- UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
- Peraturan Daerah Provinsi Jawa Timur Nomor 9 Tahun 2008 Tentang Organisasi Dan Tata Kerja Dinas Daerah Provinsi Jawa Timur.
- Peraturan Daerah Provinsi Jawa Timur Nomor 83 Tahun 2008 Tentang Uraian Tugas Sekretariat, Bidang, Sub bagian dan Seksi Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Berdasarkan informasi yang dikumpulkan pada tahap ini dapat disimpulkan bahwa semua dokumen terkait tidak mempunyai kaitan pada pembahasan pengelolaan keamanan sistem informasi. Dokumen – dokumen itu merupakan cerminan dari sebuah peraturan definitif yang harus dipatuhi sebuah institusi sebagai pedoman tugas yang harus dilakukan setiap hari.

4.6 Analisis Informasi Teridentifikasi

Pada tahap analisis informasi teridentifikasi merupakan tahap untuk melakukan penyusunan dan pengorganisasian risiko yang diperoleh dari kegiatan pengumpulan informasi, dengan melakukan penilaian risiko dan membuat strategi mitigasi sebagai mekanisme perlindungan sistem informasi yang efektif dan efisien disertai tindakan perbaikan yang dapat diimplementasikan institusi.

Aktivitas yang dilakukan dalam penilaian risiko dimulai dengan menilai probabilitas terjadinya ancaman dalam skala periode tertentu disertai frekuensi kejadian serangan seperti yang ditunjukkan tabel 4.8 berikut ini.

Tabel 4.8 Metode Penilaian Probabilitas Risiko (ISO, 2005)

Probabilitas kejadian	**Frekuensi**	**Nilai**
Tidak pernah terjadi	Tidak pernah	0
Sangat rendah	2-3 kali setiap 5 tahun	1
Rendah	<= 1 kali per tahun	2
Sedang	<= 1 kali setiap 6 bulan	3
Tinggi	<= 1 kali setiap bulan	4
Sangat tinggi	>=1 kali setiap bulan	5
Ekstrim	>= 1 kali setiap hari	6

Kemudian penilaian terhadap dampak yang dihasilkan bagi institusi akan ditunjukkan tabel 4.9 berikut ini. Dampak dapat diklasifikan menjadi 6 kategori terdiri atas: tidak mempunyai dampak apapun bagi institusi, dampak minor, sampai dampak yang dihasilkan dapat dikategorikan parah, dimana semuanya telah memiliki derajat pengukuran sendiri seperti yang telah ditentukan oleh framework ISO/IEC 17799.

Tabel 4.9 Metode Penilaian Dampak Risiko (ISO, 2005)

Dampak kejadian	Derajat dampak	Nilai
Tidak berpengaruh	Tidak mempunyai dampak.	0
Minor	Tidak perlu usaha lebih untuk memperbaiki.	1
Signifikan	Dampak dapat diukur, perlu usaha lebih untuk memperbaiki.	2
Merusak	Merusak reputasi dan keyakinan perusahaan. Memerlukan sumber daya lebih untuk memperbaiki	3
Serius	Kehilangan konektivitas. Kehilangan banyak data atau layanan.	4
Parah	Kegagalan sistem permanen.	5

Selanjutnya pada tabel 4.10 berikut ini akan ditunjukkan bagaimana mekanisme penilaian sebuah risiko yang sesuai ISO/IEC 17799. Penilaian risiko dilakukan dengan mengalikan nilai probabilitas yang sudah teridentifikasi sebelumnya dan berapa besar dampak yang dihasilkan bagi institusi. Kategori penialain pun terdiri atas: tidak mempunyai dampak apapun, rendah, sedang, tinggi sampai ekstrim.

Dalam penilaian risiko, penulis mengestimasi bobot dari berbagai ancaman dan serangan yang terjadi di institusi. Skala penilaian ini menentukan seberapa besar prioritas penanganan risiko yang muncul di institusi.

Tabel 4.10 Metode Penilaian Risiko (ISO, 2005)

Perhitungan risiko (Probabilitas x Dampak)	**Nilai**
0	Tidak berpengaruh
1-3	Rendah
4-7	Sedang
8-14	Tinggi
15-19	Kritis
20-30	Ekstrim

Dengan demikian pada tabel 4.11 berikut ini penilaian risiko terhadap sistem informasi yang ada di Bidang Pengembangan TI.

Tabel 4.11 Penilaian Risiko dan Strategi Mitigasi

Risiko	Bencana alam	**Probabilitas kejadian**	1
		Dampak kejadian	5
		Nilai risiko	5
Kategori risiko: SEDANG			
Strategi mitigasi 1) Membuat *disaster recovery plan*. 2) Membangun *Data Center Disaster Recovery Center* yang kuat dan tahan terhadap bencana alam. 3) Melakukan *backup* dan restorasi data.			
Tindakan perbaikan bagi Bidang Pengembangan TI 1) Melakukan pendefinisian dan pendokumentasian prosedur sebagai acuan dalam melakukan aktivitas penting dalam pengelolaan data, terutama dalam prosedur *backup* dan restorasi data. 2) Mulai melaksanakan pelatihan formal bagi karyawan dalam pemahaman pengelolaan data terutama *backup* dan restorasi data serta penerapan prosedur. 3) Menetapkan pelaksana yang bertanggungjawab dalam menjalankan *backup* dan restorasi data.			

Tabel 4.11 Penilaian Risiko dan Strategi Mitigasi

Risiko	Gangguan yang disengaja	**Probabilitas kejadian**	2
		Dampak kejadian	3
		Nilai risiko	6
Kategori risiko: SEDANG			
Strategi mitigasi 1) Memberikan pengamanan terhadap *server*. 2) Melakukan *backup* data. 3) Memberikan perlindungan maksimal terhadap ruang *server* seperti pemasangan CCTV, kunci berlapis.			
Tindakan perbaikan bagi Bidang Pengembangan TI 1) Melakukan pendefinisian dan pendokumentasian prosedur sebagai acuan dalam melakukan aktivitas penting dalam pengelolaan data, terutama dalam prosedur *backup* dan restorasi data. 2) Mulai melaksanakan pelatihan formal bagi karyawan dalam pemahaman pengelolaan data terutama *backup* dan restorasi data serta penerapan prosedur. 3) Menetapkan pelaksana yang bertanggungjawab dalam menjalankan *backup* dan restorasi data. 4) Melakukan pengawasan terkait proses *backup* dan restorasi data. 5) Melakukan komunikasi akan berbagai hal yang berkaitan dengan pengelolaan data dalam lingkup institusi.			
Risiko	Gangguan utilitas umum	**Probabilitas kejadian**	2
		Dampak kejadian	5
		Nilai risiko	10
Kategori risiko: TINGGI			
Strategi mitigasi 1) Menyediakan unit *power supply* (UPS). 2) Merancang struktur jaringan yang efektif, efisien, dan memenuhi standar keamanan. 3) Memilih *domain* dan *hosting* yang terpercaya disertai menyediakan memori maksimum untuk menampung data.			

Tabel 4.11 Penilaian Risiko dan Strategi Mitigasi

<table>
<tr><td rowspan="3">Risiko</td><td rowspan="3">Kerusakan peralatan</td><td>Probabilitas kejadian</td><td>2</td></tr>
<tr><td>Dampak kejadian</td><td>3</td></tr>
<tr><td>Nilai risiko</td><td>6</td></tr>
<tr><td colspan="4">Kategori risiko: SEDANG</td></tr>
<tr><td colspan="4">Strategi mitigasi
1) Maintenance peralatan yang ada secara berkala.</td></tr>
<tr><td colspan="4">Tindakan perbaikan bagi Bidang Pengembangan TI
1) Mengkomunikasikan tanggungjawab perawatan peralatan dalam institusi.
2) Menjalankan pelatihan formal dan knowledge sharing bagi seluruh karyawan terkait perawatan peralatan.
3) Melakukan sosialisasi mengenai berbagai hal yang berkaitan dengan perawatan peralatan.</td></tr>
<tr><td rowspan="3">Risiko</td><td rowspan="3">Virus atau malware</td><td>Probabilitas kejadian</td><td>3</td></tr>
<tr><td>Dampak kejadian</td><td>4</td></tr>
<tr><td>Nilai risiko</td><td>12</td></tr>
<tr><td colspan="4">Kategori risiko: TINGGI</td></tr>
<tr><td colspan="4">Strategi mitigasi
1) Mengelompokkan data berdasarkan kegunaannya secara jelas lalu membuat backupnya.
2) Menggunakan antivirus yang berlisensi.
3) Membuat file log yang mencakup history dari sebuah data.</td></tr>
<tr><td rowspan="3">Risiko</td><td rowspan="3">Moral pegawai</td><td>Probabilitas kejadian</td><td>3</td></tr>
<tr><td>Dampak kejadian</td><td>2</td></tr>
<tr><td>Nilai risiko</td><td>6</td></tr>
<tr><td colspan="4">Kategori risiko: SEDANG</td></tr>
<tr><td colspan="4">Strategi mitigasi
1) Melakukan pelatihan kepada pegawai.
2) Membuat pembatasan hak akses sesuai dengan tingkat kepentingannya.
3) Melalukan pengawasan secara internal terhadap apa yang dikerjakan.</td></tr>
</table>

Tabel 4.11 Penilaian Risiko dan Strategi Mitigasi

<table>
<tr><td colspan="4">Tindakan perbaikan bagi Bidang Pengembangan TI
1) Mengkomunikasikan tanggungjawab perawatan peralatan dalam institusi.
2) Menjalankan pelatihan formal dan knowledge sharing bagi seluruh karyawan terkait perawatan peralatan.
3) Melakukan sosialisasi mengenai berbagai hal yang berkaitan dengan perawatan peralatan.
4) Mendefinisikan tanggungjawab dan tugas masing-masing tiap karyawan secara jelas.
5) Menumbuhkan budaya memberikan penghargaan bagi pengemban peran yang berprestasi sebagai upaya untuk memotivasi.</td></tr>
<tr><td rowspan="3">Risiko</td><td rowspan="3">Hacking</td><td>Probabilitas kejadian</td><td>3</td></tr>
<tr><td>Dampak kejadian</td><td>4</td></tr>
<tr><td>Nilai risiko</td><td>12</td></tr>
<tr><td colspan="4">Kategori risiko: TINGGI</td></tr>
<tr><td colspan="4">Strategi mitigasi
1) Mengaktifkan password pada setiap aktivitas yang membutuhkan kerahasiaan, sehingga kemungkinan terjadinya pencurian data lebih kecil.
2) Mengaktifkan firewall.
3) Menggunakan program utilitas untuk perlindungan software seperti intrusion detection system.</td></tr>
<tr><td rowspan="3">Risiko</td><td rowspan="3">Denial of service (DOS)</td><td>Probabilitas kejadian</td><td>3</td></tr>
<tr><td>Dampak kejadian</td><td>4</td></tr>
<tr><td>Nilai risiko</td><td>12</td></tr>
<tr><td colspan="4">Kategori risiko: TINGGI</td></tr>
<tr><td colspan="4">Strategi mitigasi
1) Terus-menerus memeriksa sumber masukan pengguna.
2) Mendeteksi setiap akses ke perangkat lunak dari sumbernya.
3) Pembatasan jumlah pengguna yang masuk kedalam sistem dalam satu sesi untuk mengurangi penggunaan resource secara besarmaan.</td></tr>
</table>

Tabel 4.11 Penilaian Risiko dan Strategi Mitigasi

Risiko	*Social engineering*	**Probabilitas kejadian**	2
		Dampak kejadian	5
		Nilai risiko	10
Kategori risiko: TINGGI			
Strategi mitigasi 1) Mengintegrasikan biometrik dalam *login* sistem informasi. 2) Metode otentikasi pengguna lain yang lebih ketat. 3) Membatasi hak akses setiap pengguna terutama (*priveleges)* hak istimewanya.			
Risiko	*SQL injection*	**Probabilitas kejadian**	3
		Dampak kejadian	4
		Nilai risiko	12
Kategori risiko: TINGGI			
Strategi mitigasi 1) Memvalidasi masukan pengguna. 2) Menggunakan parameter dan prosedur yang tersimpan dalam *login* sistem. 3) Penggunaan *whitelist* (prinsip kepemilikan hak istimewa). 4) Pemberian eksepsi yang cukup saat terjadi penerobosan sistem.			
Risiko	*Malicious code*	**Probabilitas kejadian**	4
		Dampak kejadian	5
		Nilai risiko	20
Kategori risiko: TINGGI			
Strategi mitigasi 1) Memvalidasi data masukan pengguna. 2) Menerapkan enkripsi dan dekripsi pada data masukan dan keluaran sistem informasi. 3) Pemberian eksepsi ketika sistem informasi berjalan dengan tidak normal. 4) Penggunaan dekripsi "*on the fly*" untuk mendeteksi asal data yang dimasukkan dalam sistem informasi.			

Tabel 4.11 Penilaian Risiko dan Strategi Mitigasi

Risiko	*Buffer overflow*	**Probabilitas kejadian**	3
		Dampak kejadian	4
		Nilai risiko	12
Kategori risiko: TINGGI			
Strategi mitigasi 1) Menggunakan fungsi bahasa pemrogramman yang sudah dikenali dan tidak berbahaya. 2) Penggunaan kelas *string* modern yang tidak bergantung pada karakter dengan pembatas ukuran ialah panjang sebuah *string*.			
Risiko	*Debugging* dan *reverse engineering*	**Probabilitas kejadian**	2
		Dampak kejadian	5
		Nilai risiko	10
Kategori risiko: TINGGI			
Strategi mitigasi 1) Menggunakan teknik enkripsi dan dekripsi yang kuat selama kode dieksekusi pada saat fungsi sistem informasi dijalankan. 2) Mengatur kode sehingga tidak mudah dilakukan *debugging* oleh pihak yang tidak berhak. 3) Menerapkan mekanisme *fail-safe-design* pada pembuatan kode. 4) Mekanisme pencatatan *log* setiap pengembang harus diberlakukan. 5) Mendefinisikan data sensitif yang harus diamankan.			
Risiko	*Information disclosure*	**Probabilitas kejadian**	4
		Dampak kejadian	3
		Nilai risiko	12
Kategori risiko: TINGGI			
Strategi mitigasi 1) Menghilangkan komentar dari *source code* program. 2) Menghindari menampilkan informasi yang tidak perlu. 3) Tidak ada kategori data sensitif dalam sistem informasi. 4) Menangani kesalahan pesan dari lapisan paling rendah.			

Justifikasi terhadap penilaian risiko yang dilakukan sebelumnya adalah sebagai berikut:

1) Berdasarkan hasil penilaian risiko yang dilakukan diatas fokus dari dokumen tata kelola yang akan disusun terdiri atas: *application security*, *encryption*.
2) Diperlukan *disaster recovery planning* dalam dokumen tata kelola yang dibuat untuk menangani risiko yang menghasilkan dampak yang serius bagi institusi pemerintahan tersebut sehingga tidak menggangu proses bisnis yang ada.
3) Penanganan risiko yang akan diimplementasikan di institusi harus mempertimbangkan ketersediaan sumber daya yang ada sehingga penerapan teknik mitigasi risiko yang dapat berjalan secara efektif, efisien dan optimal.
4) Mitigasi risiko sepenuhnya tidak dapat diserahkan kepada pihak ketiga atau rekanan dinas Kominfo, karena dampak yang dihasilkan dari ancaman yang ada masih dapat dirasakan oleh pihak institusi meskipun risiko tersebut meskipun sudah dialihkan dan pihak Kominfo.
5) Dokumen tata kelola yang dibuat juga harus memuat upaya ekstra dari teknik keamanan yang sudah disusun sebagai pelengkap dalam penanganan risiko yang berdampak kritis atau parah bagi keberlangsungan sistem yang ada di institusi.
6) Penanganan risiko dilakukan terhadap ancaman yang mempunyai penilaian **Tinggi – Ekstrim**. Hal ini dikarenakan sumberdaya yang tersedia di Dinas Kominfo tidak mencukupi untuk melakukan penanganan risiko terhadap semua risiko yang muncul. Oleh karena itu untuk risiko yang berkategori **Tidak berpengaruh – Sedang** disusun sebuah tindakan perbaikan yang dapat segera diimplementasikan kepada institusi tersebut dalam rangka untuk menghemat sumberdaya yang ada dan dapat diimplementasikan melalui persetujuan seorang Kepala Bidang Pengembangan TI.

Halaman ini sengaja dikosongkan.

BAB V
PEMBUATAN DOKUMEN TATA KELOLA TEKNOLOGI INFORMASI

Bab ini merupakan tahapan pembuatan dokumen tata kelola teknologi informasi. Tahapan yang dilakukan yaitu menyusun pedoman tata kelola TI yang berupa tugas pokok dan fungsi aparatur negara sebagai representasi dokumen kerja yang ada di institusi pemerintahan, serta dokumen prosedur yang didalamnya terdapat struktur tata kelola, rancangan kebijakan umum dan sebuah pedoman yang memuat instruksi kerja serta prosedur yang harus dilakukan sebagai rancangan tata kelola teknologi informasi pada Dinas Komunikasi Dan Informatika Jawa Timur terutama pada Bidang Pengembangan Teknologi Informatika.

5.1 Dokumen Tata Kelola TI

Dokumen tata kelola TI yang baik dalam institusi pemerintahan diterbitkan melalui: kebijakan umum, dokumen kerja dan standar operasional prosedur yang memiliki elemen seperti berikut ini.

5.1.1 Struktur dan Peran Tata Kelola TI

Yaitu entitas apa saja yang berperan dalam pengelolaan proses-proses TIK dan bagaimana pemetaan perannya dalam pengelolaan proses-proses TIK tersebut. Struktur dan peran tata kelola ini mendasari seluruh proses tata kelola TIK Penetapan entitas struktur tata kelola ini dimaksudkan untuk memastikan kapasitas kepemimpinan yang memadai, dan hubungan antar satuan kerja/institusi pemerintahan yang sinergis dalam perencanaan, penganggaran, realisasi sistem TIK, operasi sistem TIK, dan evaluasi secara umum implementasi TIK di pemerintahan. Berikut ini adalah struktur dan peran yang ada di tata kelola TI Dinas Komunikasi dan Informatika Jawa Timur:

a) Eksekutif Institusi Pemerintahan yaitu Kepala Dinas Kominfo Jatim.

b) CIO Institusi Pemerintahan yaitu Kepala Bidang Pengembangan TI.

c) Satuan Pemilik Proses Bisnis yaitu Kepala Seksi Pengembangan Perangkat Lunak, Kepala Seksi Pengembangan Perangkat Keras, Kepala Seksi Layanan TIK.

Oleh karena itu pengarahan tanggung jawab pada tata kelola ini dinyatakan dalam RACI *Chart* pada tabel 5.1 yang mendefinisikan siapa saja yang terlibat sebagai pihak yang *responsible, accountable, consulted* dan *informed.*

Tabel 5. 1 RACI *Chart*

No	Aktivitas	Fungsi						
		Kepala Bidang PTI	Kasie Pengembangan Perangkat Lunak	Kasie Pengembangan Perangkat Keras	Kasie Layanan TIK	Staff	Teknisi	Administrator
1	Melakukan spesifikasi dan analisis kebutuhan keamanan sistem informasi	A	I	I	I	I	C	R

Tabel 5.1 RACI *Chart*

2	Mengoreksi aplikasi		A			I	C	R
3	Melakukan kontrol kriptografi dalam sistem		A/I				C	R
4	Mengatur keamanan berkas sistem informasi		A/I				C	R
5	Mengontrol keamanan proses pengembangan sistem informasi		A	I	I		C	R
6	Membuat kebijakan dan standar operasional keamanan sistem informasi	A	R	I	I		C	C
7	Memberi perlindungan keamanan *server*	A	I	I	I		C	R
8	Mengatur lingkungan fisik (*maintenance*, monitor, dan laporan keamanan)	A	I	I	I		C	R

Keterangan Diagram RACI Chart:

1. Melakukan spesifikasi dan analisis kebutuhan keamanan sistem informasi dilakukan oleh 2 orang staff seksi pengembangan perangkat lunak bidang pengembangan TI bertindak sebagai *administrator* sistem yang bertanggungjawab kegiatan tersebut. Kemudian berkonsultasi dengan teknisi dari pihak ketiga yaitu rekanan Dinas Komunikasi Dan Informatika Provinsi Jawa Timur. Kegiatan tersebut kemudian dilaporkan dan dipertanggujawabkan kepada Kepala Bidang Pengembangan TI. Selanjutnya diinformasikan kepada pihak-pihak terkait dalam bidang tersebut seperti: kepala seksi pengembangan perangkat lunak, kepala seksi pengembangan perangkat keras, kepala seksi layanan tik serta karyawan yang ada sebagai pengguna dari sistem informasi tersebut.
2. Mengoreksi aplikasi dilakukan oleh 2 orang staff seksi pengembangan perangkat lunak bidang pengembangan TI yang bertindak sebagai *administrator* sistem yang bertanggungjawab dalam kegiatan tersebut. Selain itu pihak ketiga diikutsertakan dalam kegiatan tersebut jika pihak administrator mengalami kesulitan dalam melakukan kegiatan tersebut. Hasil perbaikan aplikasi yang sudah dilakukan dilaporkan kepada kepala seksi pengembangan perangkat lunak.
3. Melakukan kontrol kriptografi dilakukan oleh 2 orang staff seksi pengembangan perangkat lunak bidang pengembangan TI yang bertindak sebagai *administrator* sistem yang bertanggungjawab dalam kegiatan tersebut. Selain itu pihak ketiga yaitu rekanan diikutsertakan dalam kegiatan tersebut jika pihak administrator mengalami kesulitan dalam melakukan kegiatan tersebut. Kemudian kegiatan tersebut diinformasikan dan dipertanggungjawabkan kepada kepala seksi pengembangan perangkat lunak.
4. Melakukan kontrol kriptografi dilakukan oleh 2 orang staff seksi pengembangan perangkat lunak bidang pengembangan TI yang bertindak sebagai *administrator* sistem yang bertanggungjawab dalam kegiatan tersebut. Selain itu pihak ketiga yaitu rekanan diikutsertakan dalam kegiatan tersebut jika pihak administrator mengalami kesulitan. Kemudian kegiatan tersebut diinformasikan dan dipertanggungjawabkan kepada kepala seksi pengembangan perangkat lunak.

5. Mengatur berkas keamanan sistem informasi dilakukan oleh 2 orang staff seksi pengembangan perangkat lunak bidang pengembangan TI yang bertindak sebagai *administrator* sistem yang bertanggungjawab dalam kegiatan tersebut. Selain itu pihak ketiga yaitu rekanan diikutsertakan dalam kegiatan tersebut jika pihak administrator mengalami kesulitan. Kemudian kegiatan tersebut diinformasikan dan dipertanggungjawabkan kepada kepala seksi pengembangan perangkat lunak.
6. Membuat kebijakan dan standar operasional keamanan sistem informasi dilakukan oleh kepala seksi pengembangan perangkat lunak yang dikonsultasikan bersama dengan 2 orang staff pengembangan perangkat lunak sebagai *administrator* sistem serta teknisi dari rekanan yang ada. Kemudian dipertanggungjawabkan kepada kepala bidang pengembangan TI dalam rapat yang secara rutin digelar serta diinformasikan kepada 2 orang kepala seksi yang laiinya sehingga dapat diambil keputusan yang tepat berdasarkan pertimbangan semua seksi yang ada demi kemajuan di masa mendatang.
7. Memberi perlindungan terhadap keamanan *server* dilakukan oleh 2 orang staff seksi pengembangan perangkat lunak bidang pengembangan TI yang bertindak sebagai *administrator* sistem. Bersama dengan teknisi dari rekanan dikonsultasikan *maintenance* apa yang harus dilakukan agar . Setelah itu rangkaian kegiatan tersebut diinformasikan kepada seluruh kepala seksi yang ada dalam bentuk sebuah laporan dalam sebuah rapat yang dipertanggungjawabkan pula kepada kepala bidang pengembangan TI sebagai pimpinan.
8. Mengatur lingkungan fisik (*maintenance*, monitor, dan laporan-laporan keamanan) dilakukan oleh 2 orang staff seksi pengembangan perangkat lunak bidang pengembangan TI yang bertindak sebagai *administrator* sistem. Bersama dengan teknisi dari rekanan dikonsultasikan *maintenance* apa yang harus dilakukan agar . Setelah itu rangkaian kegiatan tersebut diinformasikan kepada seluruh kepala seksi yang ada dalam bentuk sebuah laporan dalam sebuah rapat yang dipertanggungjawabkan pula kepada kepala bidang pengembangan TI sebagai pimpinan.

5.1.2 Rencana Perbaikan Tata Kelola TI

Rencana perbaikan tata kelola TI mengacu pada kondisi tata kelola TI yang sekarang ada dibandingkan dengan kondisi tata kelola TI yang diharapkan oleh pihak institusi seperti yang akan ditunjukkan pada tabel 5.2 berikut ini.

Tabel 5.2 Rencana Perbaikan Tata Kelola TI

Kondisi saat ini	Kondisi yang diharapkan	Rencana perbaikan
Kurangnya perhatian manajemen tingkat atas terkait pengelolaan keamanan sistem informasi.	Diperlukan perhatian yang lebih dari manajemen tingkat atas untuk menangani insiden keamanan sistem informasi.	Menambah sebuah tugas pokok dan fungsi terkait keamanan sistem informasi yang dalam bentuk sebuah dokumen kerja.
Proses pengamanan yang ada tidak efektif menangani insiden keamanan sistem informasi	Diperlukan sebuah mekanisme perlindungan yang efektif untuk mengatasi risiko terhadap sistem informasi.	Membentuk sebuah mekanisme perlindungan sistem informasi yang efektif dan efisien melalui sebuah standar operasional prosedur sebagai pedoman penanganan insiden keamanan sistem informasi.
Terbatas pada pekerjaan teknis untuk mengamankan sistem informasi yang ada.	Dibutuhkan dukungan semua *stakeholders* yang terlibat pengelolaan keamanan sistem informasi.	Membentuk sebuah kebijakan umum terkait keamanan sistem informasi yang dirumuskan oleh Bidang PTI.

5.1.3 Komponen Dokumen Tata Kelola TI

Komponen dokumen tata kelola TI mengacu pada ISO/IEC 17799 klausul 8: akuisisi, pengembangan dan pemeliharaan sistem informasi yang mempunyai beberapa komponen penyusun sebagai berikut ini:

- ***Security requirements of information systems***
  Tujuan: untuk memastikan keamanan yang merupakan bagian yang tak terpisahkan dari sistem informasi, terdiri atas sub kontrol:
  - *Security requirements analysis and specification.*
- ***Correct processing in applications***
  Tujuan: untuk mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi, terdiri atas sub kontrol:
  - *Input data validation.*
  - *Control of internal processing.*
  - *Message integrity.*
  - *Output data validation.*
- ***Cryptographic controls***
  Tujuan: untuk melindungi kerahasiaan, keaslian atau integritas informasi dengan cara kriptografi, terdiri atas sub kontrol:
  - *Policy on the use of crytographic controls.*
  - *Key management.*
- ***Security of system files***
  Tujuan: untuk memastikan keamanan berkas, terdiri atas sub kontrol:
  - *Control of operational software.*
  - *Protection of system test data.*
  - *Access control to program source code.*
- ***Security in development and support processes***
  Tujuan: untuk menjaga keamanan perangkat lunak aplikasi sistem dan informasi, terdiri atas sub kontrol:
  - *Change control procedures.*

- *Technical review of application after operating system changes.*
- *Restrictions on changes to software packages.*
- *Information leakage.*
- *Outsourced software development.*

- ***Technical vulnerability management***
  Tujuan: untuk mengurangi risiko yang timbul dari eksploitasi kerentanan teknis yang dipublikasikan, terdiri atas sub kontrol:
  - *Control of technical vulnerabilities.*

5.1.4 Dokumen SOA (*Statement of Applicability*)

Statement of Applicability (SOA) adalah sebuah dokumen yang berisikan daftar informasi tujuan pengendalian keamanan dan kontrol keamanan yang akan diimplementasikan dalam sebuah organisasi. Dokumen ini dapat digunakan untuk mencari tahu apa yang organisasi inginkan dalam kontrol keamanan informasi dan tujuan pengendaliannya yang seharusnya (disesuaikan dengan sumber daya dan peraturan yang berlaku dalam suatu organisasi). Oleh karena itu sebelum membuat dokumen SOA, diperlukan sebuah penilaian risiko (*risk assesment*) untuk diketahui berbagai ancaman yang dapat muncul, strategi mitigasi risiko serta mengidentifikasi semua hukum dan peraturan yang relevan dan tidak lupa untuk meninjau kembali kebutuhan bisnis organisasi untuk dapat menerapkan sistem manajemen keamanan informasi (SMKI). SOA bisa menjadi bagian dari dokumen penilaian risiko (*risk assesment*), tetapi biasanya ini merupakan dokumen yang berdiri sendiri karena panjang dan terdaftar sebagai dokumen yang diperlukan dalam standar. Elemen yang terdapat dalam SOA adalah sebagai berikut:

- Nama dan nomor kontrol keamanan ISO/IEC 17799.
- Deskripsi kontrol keamanan ISO/IEC 17799.
- Adopsi dari klausul kontrol ISO/IEC 17799 ke organisasi.
- Justifikasi dalam implementasi kontrol keamanan yang ada.
- Referensi yang digunakan dalam dokumen SOA.

Pada tabel 5.3 berikut ini adalah daftar kontrol keamanan dari klausul 8 ISO/IEC 17799 yang akan dibuat dalam dokumen standar operasional prosedur berdasarkan hasil persetujuan pihak institusi yang dituangkan ke dalam dokumen SOA (*statement of applicability*) yang dapat dilihat pada lampiran poin B.1.

Tabel 5.3 Komponen Dokumen Prosedur Dari Pemetaan Dokumen SOA

Kontrol	Deskripsi	Prosedur dan Pedoman
8.1	***Security requirement of information systems***	
8.1.1	*Security requirements analysis and specification*	Pedoman analisis dan spesifikasi kebutuhan keamanan.
8.2	***Correct processing in applications.***	
8.2.1	*Input data validation*	Pedoman validasi data masukan. Prosedur penanganan hak akses.
8.2.2	*Control of internal processing*	Pedoman pengendalian proses internal.
8.2.3	*Message integrity*	*Risk assessment.*
8.2.4	*Output data validation*	Pedoman validasi data keluaran.
8.4	***Security of system files***	
8.4.1	*Control of operational software*	Pedoman pengendalian operasional aplikasi (*software*).

Tabel 5.3 Komponen Dokumen Prosedur Dari Pemetaan Dokumen SOA

8.4.3	*Access control to program source code*	Prosedur *backup* dan restorasi data. Pedoman kontrol akses *source code* program. Prosedur penanganan *virus*.
8.5	***Security in development and support process***	
8.5.1	*Change control procedures*	Pedoman pengendalian perubahan. Prosedur penanganan *update/patch*.
8.5.2	*Technical review of application after operating system changes*	Jadwal pemeliharan dan *log*.
8.5.3	*Restrictions on changes to software packages*	Pedoman pembatasan perubahan paket *software*. Prosedur penanganan *update/patch*.
8.5.4	*Information leakage*	Pedoman kebocoran informasi. Prosedur penanganan serangan dari dalam.

Tabel 5.3 Komponen Dokumen Prosedur Dari Pemetaan Dokumen SOA

8.5.5	*Outsourced software development*	Pedoman pengembangan *software* secara *outsourcing*.
8.6	***Technical vulnerability management***	
8.6.1	*Control of technical vulnerabilities*	*Risk assessment*. Pedoman kontrol kelemahan teknis.

1.2 Kebijakan Keamanan Sistem Informasi

Kebijakan sebuah pernyataan yang akan menjadi arahan dan batasan bagi setiap proses tata kelola. Kebijakan ini ditetapkan untuk memberikan tujuan dan batasan – batasan atas proses TIK bagaimana sebuah proses TIK dilakukan untuk memenuhi kebijakan yang ditetapkan. Kebijakan pengelolaan insiden keamanan informasi ditujukan kepada tiap orang yang memiliki akses yang sah kepada suatu sistem informasi dari organisasi dan lokasi terkait khususnya Bidang Pengembangan TI. Kebijakan ini disusun dalam bentuk sebuah surat keputusan dan bersifat praktis serta dapat diterapkan di lapangan.

RANCANGAN KEBIJAKAN PENGELOLAAN KEAMANAN SISTEM INFORMASI BIDANG PENGEMBANGAN TI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

Latar Belakang

Pengelolaan keamanan sistem informasi di Dinas Komunikasi dan Informatika Jawa Timur khususnya Bidang Pengembangan TI diharapkan dapat membantu instansi ini dapat memberikan keamanan pada sistem informasi secara efektif sekaligus

meningkatkan kinerja pada proses bisnis instansi. Oleh karena itu, perlu adanya sebuah kebijakan pengelolaan keamanan sistem informasi yang selaras dengan tujuan bisnis yang tercantum pada visi dan misi instansi. Dalam proses pengelolaan keamanan sistem informasi, baik meliputi pelaksanaan serta evaluasi, diperlukan kebijakan-kebijakan untuk memberikan panduan agar tujuan-tujuan tersebut dapat tercapai.

Tujuan

Kebijakan tata kelola teknologi informasi dalam pengelolaan keamanan sistem informasi bertujuan untuk:

1) Memenuhi kebutuhan proses bisnis institusi untuk dapat meningkatkan kapasitas layanan informasi dan pengembangan aplikasi dalam rangka peningkatan layanan publik dan meningkatkan profesionalisme aparatur bidang komunikasi dan informatika.
2) Melakukan pengelolaan keamanan sistem informasi secara efektif untuk dapat memastikan integritas, ketersediaan dan kerahasiaan informasi institusi pemerintahan khususnya di provinsi Jawa Timur.
3) Melindungi data sensitif institusi sebagai suatu aset yang berharga.
4) Mendukung secara langsung terselenggaranya layanan teknologi informasi yang berkualitas untuk mendukung aktivitas bisnis institusi pemerintah daerah Jawa Timur dalam rangka peningkatan pelayanan publik.
5) Mengantisipasi perkembangan kebutuhan pengembangan sistem informasi, untuk dapat secara konsisten menyelaraskan dengan perkembangan kebutuhan bisnis.
6) Menjamin proses pengelolaan keamanan sistem informasi sesuai dengan hukum yang berlaku di Indonesia.

Pihak Terkait

Kepala Bidang Pengembangan TI, Kepala Seksi Perangkat Lunak, Kepala Seksi Perangkat Keras, Kepala Seksi Layanan Teknologi Informatika, Staf Seksi Perangkat Lunak, Staf Seksi Perangkat Keras, Staf Seksi Layanan Teknologi Informatika.

Pernyataan Kebijakan

1. **Pedoman Pengelolaan Keamanan Sistem Informasi**
   a) Mendirikan dan memelihara pedoman manajemen pengelolaan keamanan sistem informasi. Hal ini dapat dilakukan dengan melakukan peninjauan spesifikasi dan analisis kebutuhan keamanan pada Dinas KOMINFO terutama bidang PTI.
   b) Memastikan bahwa semua aplikasi yang mendukung seluruh proses bisnis dapat berjalan seoptimal mungkin dengan mengoreksi seluruh fungsi dan fitur yang ada di seluruh aplikasi.
   c) Mengimplementasikan mekanisme penanganan insiden keamanan sistem informasi dengan mengatur keamanan berkas informasi yang disesuaikan dengan alokasi sumber daya TI baik pada proses pengembangan, operasional, pemeliharaan serta pemeliharaan sistem informasi tersebut.
   d) Menganalisis penggunaan metode pengembangan sistem informasi yang disertai teknologi terapan terbaru agar dapat menjamin keamanan sistem informasi tersebut selama tahap pengembangan.
   e) Merencanakan arahan mekanisme pengamanan sistem informasi yang dituangkan dalam sebuah standar operasional prosedur keamanan sistem informasi yang bersifat praktis sesuai dengan visi dan misi organisasi dalam mewujudkan pengelolaan keamanan sistem informasi yang lebih efektif.
   f) Mendirikan sebuah pusat data DRC (*Disaster Recovery Center*) untuk memberikan perlindungan

keamanan kepada *server* agar dapat mendukung proses pemulihan sistem pasca bencana alam yang terjadi.

g) Memonitor dan mengawasi kelangsungan sistem informasi dengan mengatur keamanan lingkungan fisik sehingga dapat mengidentifikasi rencana perbaikan yang dapat diimplementasikan di masa mendatang.

2. Pemrioritasan Pengelolaan Keamanan Sistem Informasi

a) Mengimplementasikan proses pengambilan keputusan dalam memprioritaskan alokasi sumber daya TI yang dapat digunakan baik pada proses operasional, serta proses pemeliharaan sistem informasi sehingga dapat memberikan perlindungan secara efektif dan efisien terhadap risiko yang akan dihadapi.

3. Perencanaan Arahan Teknologi

a) Menginisialisasi arahan teknologi yang sesuai dalam mewujudkan proses pengelolaan keamanan sistem informasi yang lebih baik.

b) Menganalisis rancangan penggunaan teknologi terbaru yang dapat meningkatkan potensi sistem informasi.

c) Mengimplementasikan setiap rencana arahan teknologi, strategi bisnis dan kemungkinan yang ada pada komponen – komponen infrastruktur Bidang Pengembangan TI.

4. Standarisasi Teknologi

a) Menyediakan solusi teknologi yang ter*update* secara konsisten, efektif dan efisien.

b) Mendirikan sebuah media komunikasi internal untuk menyediakan pedoman-pedoman penanganan insiden keamanan sistem informasi yang terbaru, sehingga dapat membantu pemberian petunjuk pada proses

pengelolaan keamanan sistem informasi dalam melakukan pemilihan teknologi.

5. **Peningkatan Mutu Staf**
   a) Menyediakan pelatihan yang berkelanjutan untuk memelihara pengetahuan, ketrampilan, kemampuan serta pengawasan internal disertai peningkatan kesadaran mereka yang diperlukan untuk menerapkan pengelolaan keamanan sistem informasi yang sesuai dengan tujuan organisasi.
   b) Memverifikasi kinerja staf secara teratur terkait kompetensi yang dimiliki untuk memenuhi peran mereka sesuai dasar pelatihan dan pengalaman yang sudah dimiliki pada proses pengelolaan keamanan sistem informasi.
   c) Menentukan kebutuhan inti pengadaan TI dan memverifikasinya sesuai dengan kualifikasi dan program sertifikasi yang ada.

6. **Mengidentifikasi dan Mengelola Permasalahan**
   a) Mengidentifikasi tipe masalah dan memilih prioritas pilihan penanganan masalah yang dapat digunakan dalam melakukan perbaikan proses bisnis Bidang Pengembangan TI.
   b) Menentukan pengelolaan masalah yang tepat sesuai dengan fungsi TI yang ada dan menerapkannya untuk menyelesaikan masalah – masalah yang signifikan dan melakukan tinjauan ulang secara regular terhadap keefektifan dan efisiensi perbaikan yang dilakukan.

Penanggungjawab Aktivitas

Penanggungjawab aktivitas ditentukan sebagaimana tabel 5.1 sebelumny, yang disesuaikan dengan struktur fungsional Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

5.3 Penyusunan Dokumen Kerja

Dokumen kerja disusun sebagai representasi dari tugas pokok dan fungsi yang ada dalam institusi pemerintah. Dengan adanya tugas pokok dan fungsi yang hasilnya dapat dilihat pada lampiran C.1, diharapkan para aparatur negara dapat memenuhi sasaran utama atau pekerjaan yang dibebankan kepada organisasi untuk dicapai dan dilakukan secara optimal. Dalam kaitannya dengan ini, bahwa seorang aparatur negara harus benar-benar melaksanakan tugas pokok yang diamanahkan dengan konsep yang terarah serta konsentrasi yang tinggi dan agar aparatur menghayati tupoksinya, harus melaksanakan prinsip-prinsip organisasi. Prinsip organisasi tersebut adalah sebagai berikut:

- Prinsip perumusan tugas dan fungsi yang jelas.
- Prinsip fungsionalisasi.
- Prinsip koordinasi.
- Prinsip integrasi dan sinkronisasi.
- Prinsip kontinuitas.
- Prinsip lini dan staf.
- Prinsip fleksibilitas.
- Prinsip pendelegasian wewenang.

Dokumen kerja (tugas pokok dan fungsi) yang dibuat memiliki kerangka seperti yang ditunjukkan pada tabel 5.4 berikut ini.

Tabel 5.4 Kerangka Dokumen Kerja

BAB	**Nama Bab**
I	**Ketentuan Umum**
Pasal 1 berisi: Pengertian telekomunikasi, informasi, telematika, perangkat keras, aplikasi, infrastruktur komunikasi yang digunakan, pemerintah provinsi, gubernur, dinas, kepala dinas.	
Tujuan: Agar semua *stakeholder* yang berkepentingan dalam tugas pokok dan fungsi ini memperoleh pemahaman yang sama terhadap pengertian yang ada sehingga tidak mempunyai arti yang ambigu dan membingungkan setiap pihak yang dapat menyebabkan kesalahpahaman tugas masing-masing pihak.	

Tabel 5.4 Kerangka Dokumen Kerja

II	Uraian Tugas (Kelompok Kerja Keamanan Sistem Informasi)
Pasal 2 berisi: Pendefinisian struktur kerja kelompok kerja keamanan sistem informasi disesuaikan struktur organisasi Bidang Pengembangan TI. **Pasal 3 berisi:** Tugas kelompok kerja keamanan sistem informasi. **Pasal 4 berisi:** Prosedur yang dibuat, disusun serta dipatuhi oleh semua orang di dalam kelompok keamanan sistem informasi serta alat bantu yang dapat digunakan untuk menerapkan perlindungan terhadap sistem informasi yang dikelola. **Pasal 5 berisi:** Kompetensi SDM anggota kelompok kerja keamanan sistem informasi, sistem evaluasi dan monitoring serta pelatihan yang dapat dilakukan untuk meningkatkan kompetensi SDM anggota kelompok kerja keamanan sistem informasi. **Pasal 6 berisi:** Peran dan tanggungjawab kelompok kerja keamanan sistem informasi. **Pasal 7 berisi:** Pengukuran kinerja kelompok kerja keamanan sistem informasi dengan menetapkan indikator kerja yang ditetapkan dalam KPI dan KGI.	
Tujuan: Mendefinisikan struktur kerja pihak-pihak yang terlibat dalam proses pengelolaan keamanan sistem informasi sesuai struktur organisasi. Ditambah pula deskripsi tugas, wewenang, prosedur yang harus dipatuhi dan dibuat, bahkan metode penilain kinerja yang harus diterapkan pada kelompok kerja ini.	
III	Ketentuan Penutup
Pasal 8 berisi: Pengaturan teknis pelaksanaan kelompok kerja ini.	

5.4 Penyusunan *Standard Operating Procedures* (SOP)

Dalam pembuatan dokumen SOP yang hasilnya dapat dilihat pada lampiran poin D.1, bahwa perlu diperhatikan cara penulisannya. Karena *Standard Operating Procedures* (SOP) yang baik adalah apabila semua langkah yang ditulis didalamnya dapat dimengerti oleh setiap orang yang menggunakannya. Cara penulisan SOP yang efektif adalah dengan (Gasperz, 2002):

- Menuliskan setiap tahapan proses pada suatu prosedur dalam kalimat yang pendek.
- Menuliskan setiap tahapan proses pada suatu prosedur dalam bentuk kalimat perintah.
- Mengkomunikasikan secara jelas setiap kata yang digunakan dalam suatu prosedur.
- Menggunakan singkatan atau istilah yang memang sudah umum digunakan dalam kehidupan sehari-hari.

5.4.1 Atribut SOP

SOP yang baik memiliki beberapa atribut yang penting sebagai langkah pengendalian dokumen yang terstruktur dari pihak institusi agar menghasilkan kinerja yang optimal seperti sebagai berikut:

- **TUJUAN**
  Prosedur Penulisan Standar Operasi dibuat untuk menstandarisasikan penyusunan komposisi yang tepat dari penulisan semua prosedur operasi standar yang berlaku di lingkungan perusahaan.
- **RUANG LINGKUP**
  Prosedur ini dipergunakan sebagai petunjuk dalam penulisan semua prosedur operasi standar yang berkaitan dengan persyaratan standar yang digunakan yang akan diimplementasikan oleh semua departemen / bagian dalam lingkungan perusahaan. Prosedur ini meliputi semua aktivitas penulisan prosedur operasi standar dalam lingkungan perusahaan.
- **DEFINISI**
  Definisi dari setiap istilah asing yang digunakan dalam sebuah SOP.
- **REFERENSI**
  Referensi yang digunakan dalam menyusun standar operasi, dapat berupa *framework* tata kelola yang digunakan, buku tentang standar operasi sendiri, yang berhubungan dalam penyusunan standar operasional prosedur.

- **INFORMASI UMUM**
  Berisi informasi tentang pemberlakuan dokumen dan/atau catatan pengendalian keamanan sistem informasi yang didistribusikan dan menjadi tanggungjawab Bagian Pengendalian Dokumen serta penanggungjawab dari pelaksanaan prosedur yang ada.
- **PEDOMAN IMPLEMENTASI**
  Berisi tentang pedoman implementasi yang digunakan untuk mengontrol dan mengawasi prosedur yang telah diterapkan dalam institusi.

Beberapa komponen penyusun SOP yang lain dapat dilihat pada lampiran poin B.2.

5.4.2 Kontrol Keamanan

Berdasarkan hasil pemetaan dokumen SOA pada tabel 5.3 (*statement of applicability*) dapat diketahui kebutuhan keamanan yang dibutuhkan oleh pihak institusi. Pada tabel 5.5 berikut ini merupakan daftar prosedur dan pedoman yang akan dibuat disertai kontrol keamanan yang harus diterapkan sesuai ISO/IEC 177999.

Tabel 5.5 Kontrol Keamanan

Daftar prosedur	Kontrol keamanan
Security requirements analysis and specification	Kebutuhan untuk kontrol keamanan hatus ditentukan pada saat laporan kebutuhan bisnis untuk sistem informasi baru, atau penambahan perangkat tambahan pada sistem informasi tersebut.
Input data validation	Data masukan untuk aplikasi harus divalidasi untuk memastikan bahwa data ini benar dan tepat.

Tabel 5.5 Kontrol Keamanan

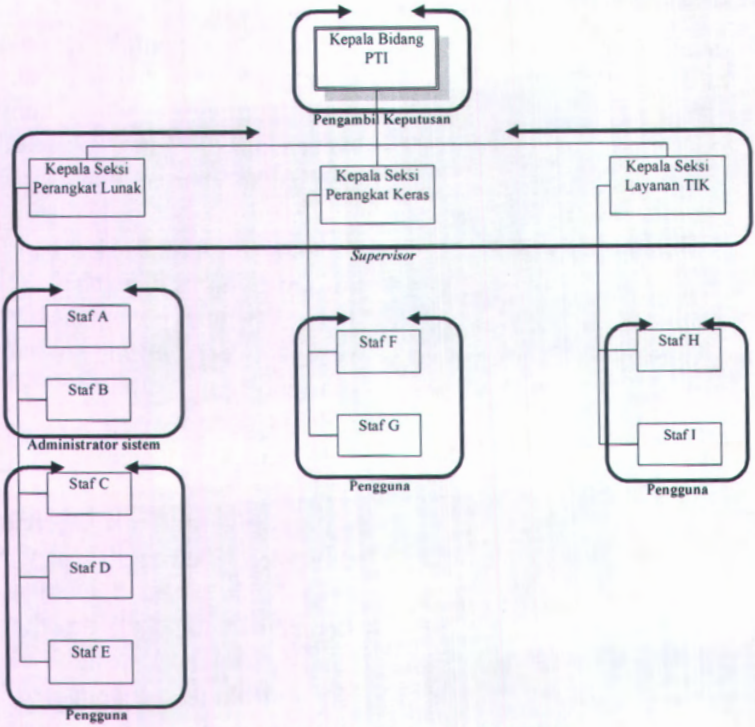
Control of internal processing	Validasi proses internal harus dimasukkan ke dalam aplikasi untuk mendeteksi kesalahan informasi baik melalui kesalahan pemrosesan atau tindakan yang disengaja.
Message integrity	Kebutuhan untuk memastikan keaslian dan melindungi integritas pesan dalam aplikasi harus diidentifikasi, termasuk kontrol yang ada dan diimplementasikan.
Output data validation	Data keluaran dari suatu aplikasi harus divalidasi untuk menjamin bahwa pengolahan informasi yang benar dan sesuai dengan keadaan yang ada.
Control of operational software	Harus ada prosedur untuk mengontrol instalasi perangkat lunak pada sistem operasional.
Access control to program source code	Akses terhadap kode program harus dibatasi.
Change control procedures	Pelaksanaan perubahan harus dikendalikan menggunakan prosedur pengendalian perubahan yang formal.
Technical review of applications after operating system changes	Bila sistem operasi berubah, aplikasi bisnis yang kritis harus ditinjau kembali dan diuji untuk memastikan tidak ada dampak yang merugikan bagi operasional organisasi atau keamanannya.

Tabel 5.5 Kontrol Keamanan

Restrictions on changes to software packages	Modifikasi untuk paket perangkat lunak harus dibatasi pada perubahan yang hanya diperlukan, dan semua perubahan harus benar-benar dikontrol.
Information leakage	Peluang untuk kebocoran informasi harus dicegah.
Outsourced software development	Pengembangan perangkat lunak secara *outsourcing* harus diawasi dan dipantau oleh organisasi.
Control of technical vulnerabilities	Informasi yang tepat waktu tentang kerentanan teknis sistem informasi harus diperoleh, termasuk paparan organisasi untuk mengatasi kerentanan tersebut dievaluasi, dan tindakan yang tepat diambil untuk mengatasi risiko yang terkait.

5.4.3 Struktur Kerja SOP

Pihak manajemen Bidang Pengembangan TI bertanggung jawab untuk memastikan mekanisme operasional TI yang stabil, aman, dan efisien secara keseluruhan, baik yang diselenggarakan sendiri maupun menggunakan jasa pihak lain. Manajemen harus menetapkan standar operasional prosedur TI yang menjamin kesinambungan operasional TI dan memastikan penerapannya baik pada satuan kerja penyelenggara TI atau pihak penyedia jasa maupun pada satuan kerja pengguna TI. Oleh karena itu pada gambar 5.1 berikut ini dijelaskan struktur kerja dari implementasi sebuah standar operasional prosedur yang mencakup semua *stakeholders* yang ada di Bidang PTI.



Gambar 5.1 Struktur Kerja SOP

Berikut ini penjelasan struktur kerja dari standar operasional terkait keamanan sistem informasi di Bidang PTI:

- Kepala Bidang PTI, menjabat sebagai CIO (*Chief Executive Officer*) mempunyai tugas sebagai berikut:
  - Bertindak sebagai pengambil keputusan.
  - Bertanggungjawab atas semua keputusan yang diambil dalam Bidang Pengembangan TI.
  - Menyusun kebijakan yang strategis untuk meningkatkan kinerja Bidang Pengembangan TI sehingga mencapai hasil yang optimal dalam rangka peningkatan pelayanan publik.
  - Memonitor dan mengevaluasi kinerja kepala seksi, staf dan administrator sistem setiap bulan.

- Kepala seksi perangkat lunak, kepala seksi perangkat keras dan kepala seksi layanan TIK, menjabat sebagai *Supervisor* mempunyai tugas sebagai berikut:
  - Memonitor dan mengevaluasi kinerja staf dan *administrator* sistem dalam aktivitas penanganan insiden keamanan sistem informasi.
  - Menyusun tindakan dan rencana perbaikan bersama dengan *administrator* sistem yang dapat digunakan untuk menangani insiden keamanan sistem informasi yang akan terjadi di masa mendatang.
  - Merancang usulan kebijakan bersama Kepala Bidang PTI yang akan diputuskan bersama dalam rapat bidang.
  - Menyediakan perangkat tambahan yang dibutuhkan oleh *administrator* sistem untuk menangani insiden keamanan sistem informasi yang telah terjadi dan untuk meningkatkan kinerja sistem informasi yang ada atas persetujuan Kepala Bidang PTI.
  - Menentukan metode pengembangan perangkat lunak yang digunakan pada proses pengembangan yang dilakukan oleh *administrator* sistem.
- Staf A dan Staf B, menjabat sebagai *administrator* sistem mempunyai tugas sebagai berikut:
  - Bertanggung jawab atas kinerja, integritas dan keamanan *database* sistem informasi yang ada.
  - Pengelola *user access* dan pengelola konfigurasi keamanan sistem informasi.
  - Menerjemahkan *user requirement* yang menjadi rancangan awal sitem, mulai dari *logical database* sampai *user interface.*
  - Pengawasan atau pelatihan sistem informasi yang ada pada pengguna.
  - Merancang sebuah rencana dan tindakan perbaikan bersama dengan kepala seksi.
  - Bertanggung jawab untuk perawatan perangkat keras komputer dan perangkat lunak dengan memelihara, memantau dan mengkonfigurasi jaringan yang masih aktif.

Dalam rangka untuk memenuhi peran dan tanggungjawab semua *stakeholder* yang ada di Bidang Pengembangan TI, maka seyogyanya setiap orang yang sudah teridentifikasi dalam struktur kerja harus mematuhi pedoman dan prosedur yang disusun berdasarkan ISO/IEC 17799 seperti yang ditunjukkan pada tabel 5.6 berikut ini.

Tabel 5.6 Pelaksana SOP

Kepala Seksi	*Administrator* sistem	Pengguna
Pedoman analisis dan spesifikasi kebutuhan keamanan.	Prosedur penanganan serangan dari dalam.	Prosedur penanganan hak akses.
Pedoman validasi data masukan.	Prosedur penanganan *update/patch.*	
Pedoman pengendalian proses internal.	Prosedur penanganan *virus.*	
Pedoman validasi data keluaran.	Jadwal pemeliharaan dan *log.*	
Pedoman pengendalian perubahan.	Prosedur *backup* dan restorasi data.	
Pedoman kontrol akses *source code* program.	*Risk assessment.*	
Pedoman pembatasan perubahan paket *software.*	Prosedur penanganan hak akses.	
Pedoman kebocoran informasi.	Pedoman validasi data masukan.	

Tabel 5.6 Pelaksana SOP

Pedoman pengembangan *software* secara *outsourcing*.	Pedoman pengendalian proses internal.	
Pedoman kontrol kelemahan teknis.	Pedoman validasi data keluaran.	
Risk assessment	Pedoman analisis dan spesifikasi kebutuhan keamanan.	
	Pedoman kontrol akses *source code* program.	
	Pedoman pembatasan perubahan paket *software*.	
	Pedoman kebocoran informasi.	
	Pedoman kontrol kelemahan teknis.	

Halaman ini sengaja dikosongkan.

BAB VI
KESIMPULAN DAN SARAN

Bab ini mengenai kesimpulan yang didapat selama pengerjaan Tugas Akhir ini serta saran perbaikan yang dapat dilakukan untuk penelitian lanjutan.

6.1 Kesimpulan

Kesimpulan yang dapat diambil dari pengerjaan tugas akhir antara lain:

1. Kondisi tata kelola TI yang diterapkan di Bidang Pengembangan TI sekarang ini tidak diterapkan secara optimal, dikarenakan kurangnya perhatian dari pihak manajemen atas terkait pengelolaan keamanan serta ketidakefektifan penanganan semua risiko yang muncul karena kelemahan sistem itu sendiri.
   a) Risiko yang ada dalam proses pengelolaan keamanan sistem informasi adalah sebagai berikut: bencana alam, gangguan yang disengaja, gangguan utilitas umum, kerusakan peralatan, *virus* atau *malware*, moral pegawai, *hacking*, *denial of service* (DOS), *social engineering*, *sql injection*, *malicious code*, *buffer overflow*, *debugging* dan *reverse engineering*, *information disclosure*.
   b) Kontrol keamanan yang dapat diterapkan dalam proses pengelolaan keamanan sistem informasi di Bidang Pengembangan TI ialah kontrol administratif (supervisi terhadap para pegawai, pembinaan dan pelatihan kepada karyawan, pemisahan tugas-tugas setiap karyawan), kontrol operasi (pembatasan akses terhadap pusat data, pengendalian terhadap *virus*, kontrol terhadap peralatan) dan kontrol fisik (pengontrolan suhu dan kelembaban di ruangan *server*, penggunaan komponen cadangan).

c) Dampak yang dihasilkan risiko yang sudah teridentifikasi pada pengelolaan keamanan sistem informasi adalah sebagai berikut:
   - Membahayakan proses bisnis.
   - Proses bisnis dapat terhenti.
   - Proses bisnis terganggu.
   - Kehilangan data.
   - Data berubah.
   - Data tidak dapat diakses.
   - Penghapusan data.
   - Pencurian data.
   - Proses bisnis terhambat.
   - Mematikan *server*.
   - Menyibukkan *server*.
   - Pencurian data oleh orang lain.
   - Hilangnya hak akses karyawan ke dalam sistem.
   - Hilangnya informasi penting ke orang lain.
   - Perubahan data.
   - Kegagalan sistem sementara.
   - Kelebihan *traffic*.
   - Konektivitas *website* terputus.
   - *Server crash*
   - Kinerja sistem informai menjadi kacau.
   - Perubahan struktur sistem informasi.
   - Pengkopian kode program.

d) Metode pengelolaan risiko yang diterapkan di Bidang Pengembangan TI dilakukan pada ancaman yang mempunyai penilaian **Tinggi – Ekstrim**. Hal ini dikarenakan sumberdaya yang tersedia di Dinas Kominfo tidak mencukupi untuk melakukan penanganan risiko terhadap semua risiko yang muncul. Sedangkan untuk risiko yang berkategori **Tidak berpengaruh – Sedang** disusun sebuah tindakan perbaikan yang dapat dengan segera diimplementasikan di institusi tersebut.

2. Kondisi tata kelola TI yang diharapkan oleh Bidang Pengembangan TI ialah sebagai berikut:
   - Poin tambahan di tugas pokok dan fungsi terkait keamanan sistem informasi yang dituangkan ke dalam bentuk sebuah dokumen kerja.
   - Mekanisme perlindungan sistem informasi yang efektif dan efisien melalui sebuah standar operasional prosedur dan pedoman disertai instruksi kerja sebagai panduan penanganan insiden keamanan sistem informasi.
   - Kebijakan umum terkait keamanan sistem informasi agar semua *stakeholders* yang berada di Dinas Komunikasi dan Informatika Jawa Timur terutama Bidang Pengembangan TI terlibat dalam pengelolaan keamanan sistem informasi.

6.2 Saran

Beberapa hal yang diharapkan dapat dilakukan pengembangan penelitian ini antara lain:

1. Agar dokumen tata kelola TI ini mencapai hasil yang diharapkan secara optimal, manajemen tingkat atas harus meninjau dokumen tata kelola TI terkait proses pengelolaan keamanan sistem informasi yang sudah dibuat pada selang waktu terencana. *Review* harus mencakup penilaian kesempatan untuk perbaikan, dan kebutuhan untuk perubahan SMKI, termasuk kebijakan keamanan dan tujuan keamanan, dengan perhatian khusus untuk tindakan korektif atau pencegahan sebelumnya dan efektivitasnya.
2. Dalam pengembangan penelitian yang selanjutnya diharapkan adanya pembuatan rencana perlakuan risiko (*Risk Treatment Plan*) pasca pengimplementasian prosedur oleh pihak instansi. Dalam rangka untuk mengelola risiko yang tidak memiliki strategi mitigasi.

Halaman ini sengaja dikosongkan.

DAFTAR PUSTAKA

Alter, S. (1992). *Information System: A Management Perspective.* The Benjamin/Cummings Publishing Company, Inc.

Alter, S. (2002). *The Information System: The Foundation of E-Business* (4th ed.). New Jersey: Pearson Education, Inc.

Arbiansyah, G., Kristianto, D., Neneng. (2010). Pemetaan Model Tata Kelola Teknologi Informasi Yang Menunjang Strategi Dan Visi Oorganisasi Di Indonesia Pada Bank Swasta XYZ. *Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010)*, (hal. 133-137). Yogyakarta.

Bonar, George H., Hopwood, William S. (1993). *Accounting Information System* (5th ed.). Prentice-Hall, Inc.

Carlson, T. (2001). *Information Security Management: Understanding ISO 17799.* Lucent Technologies Worldwide Services.

Detiknas. (2007). *Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional.* Jakarta: Depkominfo.

Gasperz, V. (2002). *ISO 9001:2000 And Continual Quality Improvement.* Jakarta: PT. Gramedia Pustaka Utama.

Gelinas, Ulric J., Oram, Allan E., Wiggins, William P. (1990). *Accounting Information System.* PWS-KENT Publishing Company.

Guldentops, E., Van Grembergen, W., & De Haes, S. (2002). Control and Governance Maturity Survey: Establishing a reference benchmark and a self assesment tool. *Information System Control Journal, 6.*

Hall, J. A. (2001). *Accounting Information Systems* (3rd ed.). South Western College Publishing.

Hisham, M. Haddad, Brunil, D. Romero. (2009). Asset Identification for Security Risk Assesment in Web Application. *International Journal Of Software Engineering, IJSE, II.*

Industry, M. o. (1999). *Corporate approaches to IT Governance*. Dipetik December 30, 2010, dari www.jipdec.or.jp/chosa/MITIBE/sld001.htm

ISO. (2005). *ISO/IEC 17799.* Switzerland: International Standard for Organization.

ITGI. (2000). *Control Objectives for Information and Related Technologies (COBIT)* (3 ed.). USA.

ITGI. (2001). *Board Briefing on IT Governance*. Dipetik December 28, 2010, dari www.itgi.org

Kadir, A. (2003). *Pengenalan Sistem Informasi.* Yogyakarta: Penerbit ANDI.

Lucas, H. (2000). *Information Technology for Management* (7th ed.). Irwin/McGraw-Hill.

Martin, E. (1999). *Managing Information Technology What Managers Need to Know* (3rd ed.). New Jersey: Pearson Education International.

Peterson, R. (2003). Information strategies and tactics for infomation technology governance. *Proceedings of the 34th HICSS Conference.* PA: Idea Group Publishing.

Putra, Risma Bayu, Sesuse, Indra Dana. (2009). Rancangan Tata Kelola TI Untuk Institusi Pemerintah Studi Kasus BAPPENAS. *Jurnal Sistem Informasi MTI-UI, 4*(1).

Rahmana, A. (2009). Peranan Teknologi Informasi Dalam Peningkatan Daya Saing Usaha Kecil Menengah. *Seminar Nasional Aplikasi Teknologi Informasi 2009 (SNATI 2009)*, (hal. 11-15). Yogyakarta.

Solms, B. v. (2005). Information Security governance: COBIT or ISO 17799 or Both? *Computer & Security*, 99-104.

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

Triantono, H. B. (2007). Kebijakan Keamanan Dengan Standar BS 7799/ ISO 17799. *Seminar Nasional Teknologi Informasi 2007 (SNATI 2007)*, (hal. 75-78). Yogyakarta.

Turban, Efraim., McClesn, Ephraim., Wetherbe, James. (1999). *Information Technology for Management Making Connections for Strategis Advantage* (2nd ed.). John Wiley & Sons, Inc.

Van Grembergen, W. (2002). Introduction to the Minitrack: IT governance and its mechanisms. *Proceedings of the 35th Hawaii International Conference on System Sciences (HICCS).* IEEE.

Wilkinson, J. W. (1992). *Accounting and Information Systems.* John Wiley & Sons, Inc.

Halaman ini sengaja dikosongkan

BIODATA PENULIS

Penulis yang lahir di kota Surabaya 31 Desember 1989 merupakan anak kedua dari dua bersaudara. Pendidikan formal ditamatkan di SDN Gading II Surabaya, SLTPN 1 Surabaya dan SMAN 2 Surabaya. Lulus dari SMAN 2 Surabaya pada tahun 2007, takdir mengantarkan penulis menjadi mahasiswa Jurusan Sistem Informasi ITS Surabaya angkatan 2007 dengan NRP. 5207100027.

Tugas akhir dipilih penulis dengan mengambil bidang minat Perencanaan dan Pengembangan Sistem Informasi (PPSI). Penulis termasuk aktif di beberapa kegiatan seminar, pelatihan ketrampilan mahasiswa yang diselenggarakan oleh jurusan maupun oleh luar jurusan. Penulis juga aktif dalam Himpunan Mahasiswa Sistem Informasi (HMSI), Badan Eksekutif Mahasiswa Fakultas Teknologi Informasi (BEM FTIF), Kajian Islami Sistem Informasi (KISI).

Halaman ini sengaja dikosongkan.

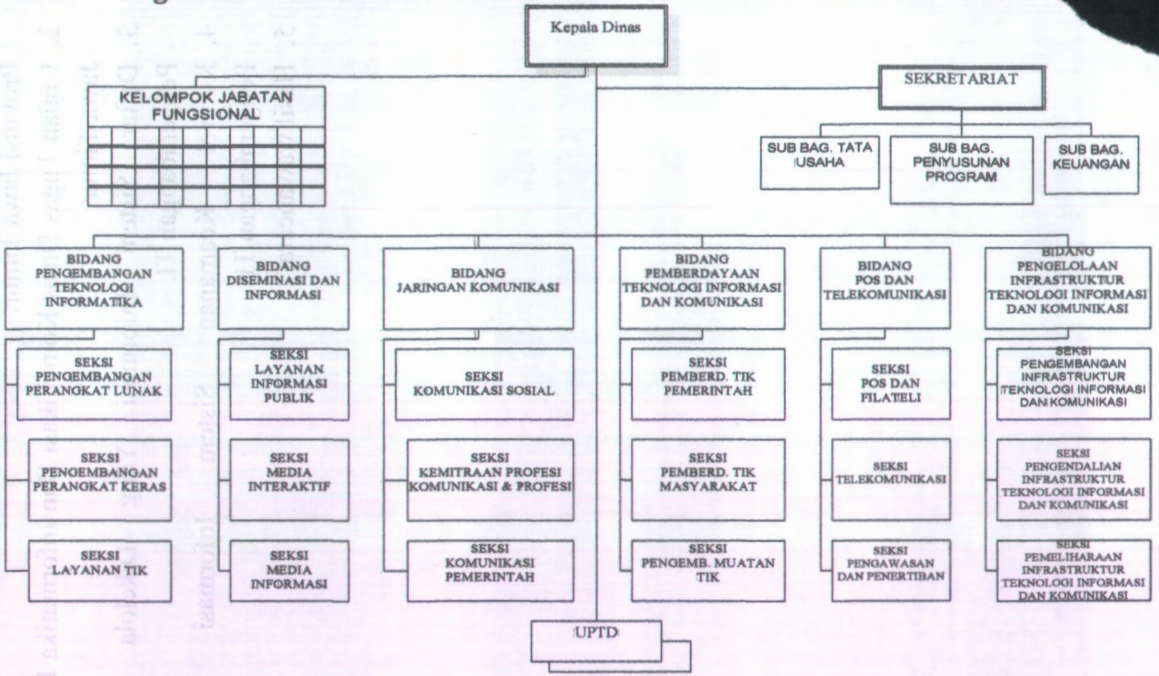
LAMPIRAN A

PENGUMPULAN INFORMASI

A. Pengumpulan Informasi (Information Gathering):

1. Struktur Organisasi Dinas Komunikasi Dan Informatika Provinsi Jawa Timur.
2. Uraian Tugas Dinas Komunikasi Dan Informatika Provinsi Jawa Timur.
3. Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI.
4. Kontrol Keamanan Sistem Informasi Bidang Pengembangan TI.
5. Hasil wawancara.

A.1 Struktur Organisasi Dinas Komunikasi Dan Informatika Provinsi Jawa



Gambar A.1 Struktur Organisasi Dinas Komunikasi dan Informatika Jawa Timur

Struktur organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur, terdiri atas:

a) Kepala Dinas.
b) Sekretariat, membawahi :
    1. Sub Bagian Tata Usaha.
    2. Sub Bagian Penyusunan Program.
    3. Sub Bagian Keuangan.
c) Bidang Pengembangan Teknologi Informatika, membawahi:
    1. Seksi Pengembangan Perangkat Lunak.
    2. Seksi Pengembangan Perangkat Keras.
    3. Seksi Layanan Teknologi Informasi dan Komunikasi.
d) Bidang Diseminasi dan Informasi, membawahi:
    1. Seksi Layanan Informasi Publik.
    2. Seksi Media Interaktif.
    3. Seksi Media Informasi.
e) Bidang Jaringan Komunikasi, membawahi:
    1. Seksi Komunikasi Sosial.
    2. Seksi Kemitraan Profesi Komunikasi dan Informasi.
    3. Seksi Komunikasi Pemerintah.
f) Bidang Pemberdayaan Teknologi Informasi dan Komunikasi, membawahi:
    1. Seksi Pemberdayaan Teknologi Informasi dan Komunikasi Pemerintah.
    2. Seksi Pemberdayaan Teknologi Informatisi dan Komunikasi Masyarakat.
    3. Seksi Pengembangan Muatan Teknologi Informasi dan Komunikasi.
g) Bidang Pos dan Telekomunikasi, membawahi:
    1. Seksi Pos dan Filateli.
    2. Seksi Telekomunikasi.
    3. Seksi Pengawasan dan Penertiban.

h) Bidang Pengelolaan Infrastruktur Teknologi Informasi dan Komunikasi, membawahi:
   1. Seksi Pengembangan Infrastruktur Teknologi Informasi dan Komunikasi.
   2. Seksi Pengendalian Infrastruktur Teknologi Informasi dan Komunikasi.
   3. Seksi Pemeliharaan Infrastruktur Teknologi Informasi dan Komunikasi.

i) Unit Pelaksana Teknis Dinas.

j) Kelompok Jabatan Fungsional.

A.2 Uraian Tugas Dinas Komunikasi Dan Informatika Provinsi Jawa Timur

A.2.1 Sekretariat

Sekretariat mempunyai tugas merencanakan, melaksanakan, mengkoordinasikan, dan mengendalikan kegiatan administrasi umum, kepegawaian, perlengkapan, penyusunan program, keuangan, humas dan protokol. Untuk melaksanakan tugas sebagaimana dimaksud diatas, Sekretaris mempunyai fungsi:

a) Pengelolaan dan pelayanan administrasi umum.
b) Pengelolaan administrasi kepegawaian.
c) Pengelolaan administrasi keuangan.
d) Pengelolaan administrasi perlengkapan.
e) Pengelolaan urusan rumah tangga, humas dan protokol.
f) Pelaksanaan koordinasi penyusunan program, anggaran dan perundang-undangan.
g) Pelaksanaan koordinasi penyelenggaraan tugas-tugas bidang.
h) Pengelolaan kearsipan dan perpustakaan dinas.
i) Pelaksanaan monitoring dan evaluasi organisasi dan tata laksana.
j) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

Susunan Organisasi Sekretariat, terdiri atas:

a) Sub Bagian Tata Usaha.
b) Sub Bagian Penyusunan Program.
c) Sub Bagian Keuangan.

Masing-masing Sub Bagian dipimpin oleh Kepala Sub Bagian yang berada di bawah dan bertanggung jawab kepada Sekretaris.

A.2.1.1 Sub Bagian Tata Usaha

Sub Bagian Tata Usaha, mempunyai tugas:

a) Melaksanakan penerimaan, pendistribusian dan pengiriman surat-surat, penggandaan naskah-naskah dinas, kearsipan dan perpustakaan Dinas.
b) Menyelenggarakan urusan rumah tangga dan keprotokolan.
c) Melaksanakan tugas di bidang hubungan masyarakat.
d) Mempersiapkan seluruh rencana kebutuhan kepegawaian mulai penempatan formasi, pengusulan dalam jabatan, usulan pensiun, peninjauan masa kerja, pemberian penghargaan, kenaikan pangkat, DP-3, DUK, Sumpah / Janji Pegawai, Gaji Berkala, kesejahteraan, mutasi dan pemberhentian pegawai, diklat, ujian dinas, izin belajar, pembinaan kepegawaian dan disiplin pegawai, menyusun standar kompetensi pegawai, tenaga teknis, tenaga fungsional, analisis jabatan, analisi beban kerja, budaya kerja, dan tugas tata usaha kepegawaian lainnya.
e) Melakukan penyusunan kebutuhan perlengkapan, pengadaan dan perawatan peralatan kantor, pengamanan, usulan penghapusan asset dan menyusun laporan pertanggungjawaban atas barang-barang inventaris.
f) Melaksanakan tugas-tugas lain yang diberikan oleh Sekretaris.

A.2.1.2 Sub Bagian Penyusunan Program

Sub Bagian Penyusunan Program, mempunyai tugas:

1. Menghimpun data dan menyiapkan bahan koordinasi penyusunan program.
2. Melaksanakan pengolahan data.
3. Melaksanakan perencanaan program.
4. Menyiapkan bahan penataan kelembagaan, ketatalaksanaan dan perundang-undangan.
5. Menghimpun data dan menyiapkan bahan penyusunan program anggaran.
6. Melaksanakan monitoring dan evaluasi.
7. Melaksanakan penyusunan laporan.
8. Melaksanakan tugas-tugas lain yang diberikan oleh Sekretaris.

A.2.1.3 Sub Bagian Keuangan

Sub Bagian Keuangan, mempunyai tugas:

1. Melaksanakan pengelolaan keuangan termasuk pembayaran gaji pegawai.
2. Melaksanakan pengadministrasian dan pembukuan keuangan.
3. Menyusun laporan pertanggungjawaban atas pelaksanaan pengelolaan keuangan.
4. Melaksanakan tugas-tugas lain yang diberikan oleh Sekretaris.

A.2.2 Bidang Pengembangan Teknologi Informatika

Bidang Pengembangan Tenologi Informatika mempunyai tugas melaksanakan pengembangan dan pengendalian serta pemeliharaan sarana prasarana teknologi informatika. Untuk melaksanakan tugas sebagaimana dimaksud pada diatas Bidang Pengembangan Teknologi Informatika, mempunyai fungsi:

a) Pelaksanaan penyusunan pedoman dalam rangka pengembangan teknologi informatika dan komunikasi.
b) Pelaksanaan penyusunan kebutuhan dan konfigurasi perangkat keras, perangkat lunak, dan layanan teknologi informasi dan komunikasi.

c) Pelaksanaan pemeliharaan perangkat keras dan perangkat lunak.
d) Pelaksanaan koordinasi dalam rangka pengembangan teknologi informasi dan komunikasi.
e) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

Bidang Pengembangan Teknologi Informatika, terdiri atas:
a) Seksi Pengembangan Perangkat Lunak.
b) Seksi Pengembangan Perangkat Keras.
c) Seksi Layanan Teknologi Informasi dan Komunikasi.

Masing-masing seksi dipimpin oleh kepala seksi yang berada di bawah dan bertanggung jawab kepada Kepala Bidang.

A.2.2.1 Seksi Pengembangan Perangkat Lunak

Seksi Pengembangan Perangkat Lunak, mempunyai tugas:
a) Menyiapkan bahan pengembangan perangkat lunak.
b) Menyiapkan bahan analisis penggunaan dan perkembangan perangkat lunak.
c) Menyiapkan bahan kebutuhan perangkat lunak.
d) Menyiapkan bahan perekayasaan pengembangan perangkat lunak.
e) Menyiapkan bahan pertimbangan penggunaan / pemilihan perangkat lunak.
f) Menyiapkan bahan pelaksanaan kerjasama dalam rangka pengembangan perangkat lunak.
g) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.2.2 Seksi Pengembangan Perangkat Keras

Seksi Pengembangan Perangkat Keras, mempunyai tugas:
a) Menyiapkan bahan pengembangan perangkat keras.
b) Menyiapkan bahan analisis penggunaan dan perkembangan perangkat keras.
c) Menyiapkan bahan perencanaan kebutuhan perangkat keras dan sarana pendukung lainnya.
d) Menyiapkan bahan pertimbangan pernggunaan / pemilihan perangkat keras.

e) Menyiapkan bahan spesifikasi kebutuhan perangkat keras dan sarana pendukung lainnya.
f) Menyiapkan bahan pelaksanaan kerjasama pengembangan perangkat keras.
g) Menyiapkan bahan rekayasa pengembangan perangkat keras.
h) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.2.3 Seksi Layanan Teknologi dan Komunikasi

Seksi Layanan Teknologi Informasi dan Komunikasi, mempunyai tugas:

a) Menyiapkan bahan pengumpulan layanan teknologi informasi dan komunikasi.
b) Menyiapkan bahan fasilitasi teknologi informasi dan komunikasi.
c) Menyiapkan bahan pertimbangan penggunaan / pemilihan perangkat teknologi informasi dan komunikasi.
d) Menyiapkan bahan kerjasama dalam rangka layanan teknologi informasi dan komunikasi.
e) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.3 Bidang Diseminasi Dan Informasi

Bidang Diseminasi Dan Informasi mempunyai tugas merumuskan serta melaksanakan kebijakan di bidang diseminasi / penyebarluasan informasi. Untuk melaksanakan tugas sebagaimana maksud diatas Bidang Diseminasi Dan Informasi mempunyai fungsi:

a) Pelaksanaan rumusan dan kebijakan layanan informasi publik.
b) Pelaksanaan penyiapan rumusan dan kebijakan pelaksanaan pemberdayaan media interaktif.
c) Pelaksanaan penyiapan rumusan dan kebijaka pelaksanaan pemberdayaan media informasi.

d) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

Bidang Diseminasi Dan Informasi, membawahi:

1. Seksi Layanan Informasi Publik.
2. Seksi Media Interaktif.
3. Seksi Media Informasi.

Masing-masing seksi dipimpin oleh kepala seksi yang berada di bawah dan bertanggung jawab kepada Kepala Bidang.

A.2.3.1 Seksi Layanan Informasi Publik

Seksi Layanan Informasi Publik, mempunyai tugas:

a) Menyiapkan bahan pelayanan informasi publik.
b) Menyiapkan bahan pelaksanaan identifikasi, pemantauan dan melayani kebutuhan masyarakat terhadap informasi.
c) Menyiapkan bahan pelaksanaan koordinasi kelembagaan layanan publik.
d) Menyiapkan bahan pengelolaan pengaduan masyarakat dibidang layanan publik.
e) Menyiapkan bahan pelaksanaan iklan layanan masyarakat.
f) Menyiapkan bahan koordinasi dengan instansi di lingkungan Pemerintah Provinsi dan Kabupaten/Kota guna mendapatkan bahan sajian pelayanan informasi.
g) Melaksanakan tugas-tugas yang diberikan oleh Kepala Bidang.

A.2.3.2 Seksi Media Interaktif

Seksi Media Interaktif, mempunyai tugas:

a) Menyiapkan bahan pelaksanaan kegiatan penyebarluasan informasi secara langsung (*interpersonal communication*).
b) Menyiapkan bahan sosialisasi kebijakan pembangunan dan pemerintahan.
c) Menyiapkan bahan dialog publik.
d) Menyiapkan bahan fasilitasi komunikasi publik.

e) Menyiapkan bahan koordinasi dengan instansi/lembaga terkait guna mendapatkan bahan sajian pelayanan informasi.
f) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.3.3 Seksi Media Informasi

Seksi Media Informasi, mempunyai tugas:

a) Menyiapkan bahan penyebarluasan informasi melalui media elektronik, cetak dan luar ruang.
b) Menyiapkan bahan diseminasi informasi melalui media radio dan televisi.
c) Menyiapkan bahan pengelolaan radio milik pemerintah daerah.
d) Menyiapkan bahan penerbitan tabloid, majalah dan penerbitan lainnya.
e) Menyiapkan bahan penyertaan pameran/promosi.
f) Menyiapkan bahan pelaksanaan produksi media luar ruang.
g) Menyiapkan bahan pengelolaan news room.
h) Menyiapkan bahan koordinasi dengan instansi/lembaga terkait guna mendapatkan bahan sajian pelayanan informasi.
i) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.4 Bidang Jaringan Komunikasi

Bidang Jaringan Komunikasi mempunyai tugas menyusun dan melaksanakan kebijakan kerjasama jaringan komunikasi antar lembaga komunikasi dan informasi. Untuk melaksanakan tugas sebagaimana yang dimaksud diatas Bidang Jaringan Komunikasi mempunyai fungsi:

a) Pelaksanaan perumusan kebijakan pendayagunaan kelembagaan komunikasi pemerintah dan kelembagaan komunikasi sosial.

b) Pelaksanaan perumusan kebijakan hubungan antar kelembagaan komunikasi dan informasi.
c) Pelaksanaan perumusan kebijakan penguatan lembaga informasi publik.
d) Pelaksanaan perumusan pola pembinaan dan pengembangan jaringan komunikasi.
e) Pelaksanaan koordinasi dibidang pemberdayaan jaringan komunikasi pemerintahan, masyarakat dan pengembangan pelayanan publik.
f) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

Bidang Jaringan Komunikasi, membawahi:
a) Seksi Komunikasi Sosial.
b) Seksi Kemitraan Profesi Komunikasi dan Informasi.
c) Seksi Komunikasi Pemerintah.

Masing-masing seksi dipimpin oleh kepala seksi yang berada di bawah dan bertanggung jawab kepada Kepala Bidang.

A.2.4.1 Seksi Komunikasi Sosial

Seksi Komunikasi Sosial, mempunyai tugas:
a) Menyiapkan bahan perumusan kebijakan pendayagunaan lembaga komunikasi sosial.
b) Menyiapkan bahan pelaksanaan kebijakan di bidang pendayagunaan media tradisional.
c) Menyiapkan bahan pelaksanaan kebijakan pengembangan Kelompok Informasi Masyarakat.
d) Menyiapkan bahan pelaksanaan kebijakan komunitas komunikasi berdasar kesetaraan gender.
e) Menyiapkan bahan koordinasi dibidang pemberdayaan jaringan komunikasi pemerintahan, masyarakat dan pengembangan pelayanan publik.
f) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.4.2 Seksi Kemitraan Profesi Komunikasi dan Informasi

Seksi Kemitraan Profesi Komunikasi dan Informasi, mempunyai tugas:

a) Menyiapkan bahan pelaksanaan kebijakan di bidang kemitraan lembaga.
b) Menyiapkan bahan penyusunan hubungan kemitraan lembaga komunikasi pemerintah.
c) Menyiapkan bahan penyusunan hubungan kemitraan lembaga profesi.
d) Menyiapkan bahan penyusunan hubungan kemitraan lembaga pemanta media/lembaga konsumen media.
e) Menyiapkan bahan koordinasi dan kerjasama dengan lembaga terkait dalam rangka pemberdayaan jaringan komunikasi pemerintahan, masyarakat dan pengembangan pelayanan publik.
f) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.4.3 Seksi Komunikasi Pemerintah

Seksi Komunikasi Pemerintah, mempunyai tugas:

a) Menyiapkan bahan penyusunan kebijakan dan fasilitasi pengembangan pusat informasi publik.
b) Menyiapkan bahan fasilitasi pusat-pusat informasi publik.
c) Menyiapkan bahan fasilitasi pemberdayaan komunitas komunikasi strategis yang berkembang di masyarakat.
d) Menyiapkan bahan koordinasi di bidang pemberdayaan jaringan komunikasi pemerintahan, masyarakat dan pengembangan pelayanan publik.
e) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.5 Bidang Pemberdayaan Teknologi Informasi dan Komunikasi

Bidang Pemberdayaan Teknologi Informasi dan Komunikasi mempunyai tugas melakukan pemberdayaan telematika pemerintahan, masyarakat dan pengembangan muatan telematika. Untuk melaksanakan tugas sebagaimana yang

MILIK PERPUSTAKAAN ITS

dimaksud diatas Bidang Pemberdayaan Teknologi Informasi dan Komunikasi mempunyai fungsi:

a) Pelaksanaan pengumpulan bahan pemberdayaan telematika pemerintahan, masyarakat dan pengembangan muatan telematika.
b) Pelaksanaan penyusunan pedoman dalam rangka pemberdayaan telematika pemerintahan, masyarakat dan pengembangan muatan telematika.
c) Pelaksanaan pembinaan dan bimbingan teknis penerapan dibidang telematika pemerintahan, masyarakat dan pengembangan muatan telematika.
d) Pelaksanaan fasilitasi penerapan telematika pemerintahan, masyarakat dan pengembangan muatan telematika.
e) Pelaksanaan koordinasi dan kerjasama dengan lembaga terkait dalam rangka pemberdayaan telematika pemerintahan, masyarakat dan pengembangan muatan telematika.
f) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

Bidang Pemberdayaan Teknologi Informasi dan Komunikasi, membawahi:

a. Seksi Pemberdayaan Teknologi Informasi dan Komunikasi Pemerintah.
b. Seksi Pemberdayaan Teknologi Informatisi dan Komunikasi Masyarakat.
c. Seksi Pengembangan Muatan Teknologi Informasi dan Komunikasi.

Masing-masing seksi dipimpin oleh kepala seksi yang berada di bawah dan bertanggung jawab kepada Kepala Bidang.

A.2.5.1 Seksi Pemberdayaan Teknologi Informasi dan Komunikasi Pemerintah

Seksi Pemberdayaan Teknologi Informasi dan Komunikasi Pemerintah mempunyai tugas:

a) Menyiapkan pengumpulan bahan pemberdayaan telematika pemerintahan.
b) Menyiapkan bahan penyusunan pedoman dalam rangka pemberdayaan telematika pemerintahan.
c) Menyiapkan bahan fasilitasi penerapan telematika pemerintahan.
d) Menyiapkan bahan koordinasi dibidang pemberdayaan telematika pemerintahan.

A.2.5.2 Seksi Pemberdayaan Teknologi Informasi dan Komunikasi Masyarakat

Seksi Pemberdayaan Teknologi Informasi dan Komunikasi Masyarakat mempunyai tugas:

a) Menyiapkan bahas pengumpulan bahan pemberdayaan telematika bagi masyarakat.
b) Menyiapkan bahan penyusunan pedoman dalam rangka pemberdayaan telematika bagi masyarakat.
c) Menyiapkan bahan fasilitasi penyelenggaraan penerapan telematika di lingkungan masyarakat.
d) Menyiapkan bahan koordinasi dibidang pemberdayaan telematika masyarakat.
e) Menyiapkan bahan sosialisasi pemanfaatan telematika kepada masyarakat.
f) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.5.3 Seksi Pengembangan Muatan Teknologi Informasi dan Komunikasi

Seksi Pengembangan Muatan Teknologi Informasi dan Komunikasi mempunyai tugas:

a) Menyiapkan bahan pengumpulan bahan pengembangan muatan telematika.
b) Menyiapkan bahan penyusunan desain format dan media dalam rangka pengembangan muatan telematika.
c) Menyiapkan bahan perekayasaan pengembangan muatan telematika.

A.2.6 Bidang Pos dan Telekomunikasi

Bidang Pos dan Telekomunikasi mempunyai tugas melaksanakan pembinaan, pengawasan, pengendalian dan penertiban serta evaluasi kegiatan pelayanan usaha jasa pos dan telekomunikasi khusus serta standarisasi alat peralatan pos dan telekomunikasi. Untuk melaksanakan tugas sebagaimana yang dimaksud diatas Bidang Pos dan Telekomunikasi mempunyai fungsi:

a) Pelaksanaan penyusunan analisis pelayanan dan kegiatan usaha jasa pos, filateli, telekomunikasi dan telekomunikasi khusus.
b) Pelaksanaan pemberian pertimbangan standarisasi teknis pos, telekomunikasi dan telekomunikasi khusus di Provinsi.
c) Pelaksanaan penyusunan teknis kegiatan usaha jasa pos, filateli, telekomunikasi dan telekomunikasi khusus.
d) Pelaksanaan pemantauan dan evaluasi kegiatan pelayanan usaha pos, filateli, telekomunikasi dan telekomunikasi khusus.
e) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

Bidang Pos dan Telekomunikasi, membawahi:

a) Seksi Pos dan Filateli.
b) Seksi Telekomunikasi.
c) Seksi Pengawasan dan Penertiban.

Masing-masing seksi dipimpin oleh kepala seksi yang berada di bawah dan bertanggung jawab kepada Kepala Bidang.

A.2.6.1 Seksi Pos dan Filateli

Seksi Pos dan Filateli mempunyai tugas:

a) Menyiapkan bahan ketentuan persyaratan pengusahaan jasa titipan.
b) Menyiapkan bahan pembinaan dan pengendalian jasa titipan.

c) Menyiapkan bahan standarisasi sarana prasarana jasa pos.
d) Menyiapkan bahan pembinaan kegiatan filateli.
e) Menyiapkan bahan analisis data pelayanan jasa titipan dan filateli.
f) Menyiapkan bahan bimbingan dan petunjuk teknis penyelenggaraan jasa pos.
g) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.6.2 Seksi Telekomunikasi

Seksi Telekomunikasi mempunyai tugas:

a) Menyiapkan bahan pertimbangan pengusahaan atau penyelenggaraan jasa telekomunikasi dan telekomunikasi khusus.
b) Menyiapkan bahan pembinaan dan pengendalian penyelenggaraan jaringan dan jasa telekomunikasi serta telekomunikasi khusus.
c) Menyiapkan bahan analisis data pelayanan jasa telekomunikasi dan telekomunikasi khusus.
d) Menyiapkan bahan bimbingan dan petunjuk teknis penyelenggaraan jasa telekomunikasi dan telekomunikasi khusus.
e) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.6.3 Seksi Pengawasan dan Penertiban

Seksi Pengawasan dan Penertiban mempunyai tugas:

a) Menyiapkan bahan pembinaan, pengawasan, pengendalian dan penertiban terhadap pengguna / penyelenggaraan jaringan dan jasa telekomunikasi khusus.
b) Menyiapkan bahan pembinaan, pengawasan, pengendalian, dan penertiban terhadap pengusahaan / penyelenggaraan jasa titipan telekomunikasi khusus.
c) Menyiapkan bahan pembinaan dan pengawasan penggunaan / pemanfaatan menara telekomunikasi.

d) Menyiapkan bahan monitoring dan evaluasi pengusahaan, penyelenggaraan usaha jasa titipan, telekomunikasi dan telekomunikasi khusus.
e) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.7 Bidang Pengelolaan Infrastruktur Teknologi Informasi dan Telekomunikasi

Bidang Pengelolaan Infrastruktur Teknologi Informasi dan Komunikasi mempunyai tugas melaksanakan pengembangan, pengendalian dan pemeliharaan infrastruktur jaringan Teknologi Informasi dan Komunikasi. Untuk melaksanakan tugas sebagaimana yang dimaksud diatas Bidang Pengelolaan Infrastruktur Jaringan Teknologi Informasi dan Komunikasi, mempunyai fungsi:

a) Pelaksanaan penyusunan pedoman pengembangan, pengendalian dan pemeliharaan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
b) Pelaksanaan penyusunan kebutuhan dan konfigurasi pengendalian dan pemeliharaan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
c) Pelaksanaan, pengembangan, pengendalian, dan pemeliharaan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
d) Pelaksanaan koordinasi dalam rangka pengembangan pengendalian dan pemeliharaan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
e) Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

Bidang Pengelolaan Infrastruktur Teknologi Informasi dan Komunikasi, membawahi:

a) Seksi Pengembangan Infrastruktur Teknologi Informasi dan Komunikasi.
b) Seksi Pengendalian Infrastruktur Teknologi Informasi dan Komunikasi.

c) Seksi Pemeliharaan Infrastruktur Teknologi Informasi dan Komunikasi.

Masing-masing seksi dipimpin oleh kepala seksi yang berada di bawah dan bertanggung jawab kepada Kepala Bidang.

A.2.7.1 Seksi Pengembangan Infrastruktur Teknologi Informasi dan Komunikasi

Seksi Pengembangan Infrastruktur Teknologi Informasi dan Komunikasi mempunyai tugas:

a) Menyiapkan bahan pengembangan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
b) Menyiapkan bahan perekayasaan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
c) Menyiapkan bahan penerapan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
d) Menyiapkan bahan pelaksanaan uji coba hasil pengembangan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
e) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.7.2 Seksi Pengendalian Infrastruktur Teknologi Inormasi dan Komunikasi

Seksi Pengendalian Infrastruktur Teknologi Informasi dan Komunikasi mempunyai tugas:

a) Menyiapkan bahan pengendalian infrastruktur jaringan Teknologi Informasi dan Komunikasi.
b) Menyiapkan bahan petunjuk operasional infrastruktur jaringan Teknologi Informasi dan Komunikasi.
c) Menyiapkan bahan pertimbangan penggunaan / pemilihan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
d) Menyiapkan bahan kerjasama pengendalian infrastruktur jaringan Teknologi Informasi dan Komunikasi.

LAMPIRAN B

KOMPONEN DOKUMEN TATA KELOLA TI

e) Menyiapkan bahan pelaksanaan operasionalisasi infrastruktur jaringan Teknologi Informasi dan Komunikasi.
f) Menyiapkan bahan monitoring, evaluasi dan pelaporan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
g) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.2.7.3 Seksi Pemeliharaan Infrastruktur Teknologi Informasi dan Komunikasi

Seksi Pemeliharaan Infrastruktur Teknologi Informasi dan Komunikasi mempunyai tugas:

a) Menyiapkan bahan pemeliharaan infrastruktur jaringan Teknolog Informasi dan Komunikasi.
b) Menyiapkan bahan pelaksanaan penilaian dan pengkajian kelayakan infrastruktur jaringan Teknologi Informasi dan Komunikasi.
c) Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.

A.3 Daftar Sistem Informasi Yang Dikelola Bidang Pengembangan TI

Tabel A.1 Daftar Sistem Informasi Yang Dikelola Bidang PTI

Nama Website	Domain
Sistem Informasi Pendaftaran Online Penyedia Barang/Jasa LPSE	bplpse.jatimprov.go.id
Sistem Informasi Monitoring Dan Evaluasi Pembangunan Provinsi Jawa Timur	smep.jatimprov.go.id
E-lelang	e-lelang.jatimprov.go.id

Tabel A.1 Daftar Sistem Informasi Yang Dikelola Bidang PTI

Sistem Informasi Evaluasi Perencanaan Pembangunan	sievap.jatimprov.go.id
Sistem Informasi Perencanaan Pembangunan Daerah	sippd-jatim.net
Sistem Informasi Kinerja Pemerintah	bappeda.jatimprov.go.id/ web/sikap
Asosiasi telecenter provinsi Jawa Timur	astel.jatimprov.go.id
Badan koordinasi wilayah pemerintah dan pembangunan Bojonegoro	bakorwilbojonegoro.jatimprov.go.id
Badan koordinasi wilayah pemerintah dan pembangunan Malang	bakorwilmalang.jatimprov.go.id
Badan penelitian dan pengembangan provinsi Jawa Timur	balitbang.jatimprov.go.id
Badan kepegawaian daerah provinsi Jawa Timur	bkd.jatimprov.go.id
Badan ketahanan pangan provinsi Jawa Timur	bkp.jatimprov.go.id
Badan lingkungan hidup provinsi Jawa Timur	blh.jatimprov.go.id
Badan narkotika provinsi Jawa Timur	bnp.jatimprov.go.id
Badan penanggulangan bencana daerah pronvinsi Jawa Timur	bpbd.jatimprov.go.id
Badan penanaman modal provinsi Jawa Timur	bpm.jatimprov.go.id

Tabel A.1 Daftar Sistem Informasi Yang Dikelola Bidang PTI

Dinas sosial provinsi Jawa Timur	dinsos.jatimprov.go.id
Dinas perikanan dan kelautan provinsi Jawa Timur	diskanlut.jatimprov.go.id
Dinas tenaga kerja, transmigrasi dan kependudukan provinsi Jawa Timur	disnakertransduk.jatimprov.go.id
Dinas kepemudaan dan keolahragaan provinsi Jawa Timur	dispora.jatimrpov.go.id
Dinas lalu lintas dan angkutan jalan provinsi Jawa Timur	dllaj.jatimprov.go.id
DPR daerah provinsi Jawa Timur	dprd.jatimprov.go.id
Dinas pariwisata dan kebudayaan provinsi Jawa Timur	infostrategis.jatimprov.go.id
Ikatan pencak silat provinsi Jawa Timur	ipsi.jatimprov.go.id.id
Badan koordinasi keluarga berencana nasional provinsi Jawa Timur	jatim.bkkbn.go.id
Pemerintah daerah provinsi Jawa Timur	jatimprov.go.id
Kelompok informasi masyarakat Jawa Timur	kim.jatimprov.go.id
Keterbukaan informasi publik provinsi Jawa Timur	kip.jatimprov.go.id
Korps pegawai negeri provinsi Jawa Timur	korpri.jatimprov.go.id

Tabel A.1 Daftar Sistem Informasi Yang Dikelola Bidang PTI

Komisi penyiaran daerah provinsi Jawa Timur	kpid.jatimprov.go.id
Komisi pelayanan publik provinsi Jawa Timur	kpp.jatimprov.go.id
Komisi pemilihan umum provinsi jawa timur	kpujatim.go.id
Pemerintah kabupaten Nganjuk	nganjukkab.go.id
Pelayanan perizinan terpadu provinsi Jawa Timur	p2t.jatimprov.go.id
Kantor perwakilan provinsi Jawa Timur di jakarta	perwakilan.jatimprov.go.id
Plasa Jawaa Timur	plasa.jatimprov.go.id
Plasa Jawa Timur	plaza.jatimprov.go.id
Dinas pekerjaan umum cipta karya dan tata ruang provinsi Jawa Timur	pu-ciptakarya-tataruang.jatimprov.go.id
Biro perekonomian provinsi Jawa Timur	ro-ekonomi.jatimprov.go.id
Sekretariat daerah provinsi Jawa Timur	setda.jatimprov.go.id
Biro organisasi provinsi Jawa Timur	ro-organisasi.jatimprov.go.id
Rumah sakit umum dr.soetomo	rsudrsoetomo.jatimprov.go.id
Rumah sakit umum haji	rsuhaji.jatimprov.go.id
Telecenter provinsi Jawa Timur	tc.jatimprov.go.id

A.4 Kontrol Keamanan Sistem Informasi Bidang Pengembangan TI

Kontrol Administratif

- Supervisi terhadap para pegawai. Termasuk pula cara melakukan kontrol terhadap pegawai yang ada agar tidak melakukan penyimpangan yang dapat mengancam keamanan sebuah sistem informasi. Dalam prakteknya ialah adanya larangan untuk memberikan informasi penting seperti username dan password sebuah sistem informasi pada pihak luar, adanya pengecekan ulang terhadap apa yang dikerjakan tiap staff/karyawan oleh seorang kepala seksi.
- Adanya pembinaan dan pelatihan yang diperlukan sebelum mengimplementasi sebuah sistem informasi agar setiap karyawan yang ditugaskan agar dapat mengerti bagaimana cara mengoperasikannya.
- Pemisahan tugas-tugas dalam pekerjaan dengan tujuan agar tidak seorang pun yang dapat menguasai suatu proses yang lengkap. Pada prakteknya, telah ada pemisahan tugas pada setiap bidang yang ada sehingga tidak dimungkinkan adanya kesempatan untuk melakukan kecurangan.
- Laporan perbaikan sistem yang ditujukan kepada kepala seksi pengembangan perangkat lunak ketika mengalami kegagalan sistem karena adanya serangan dari pihak luar sehingga mempengaruhi proses bisnis yang ada seperti pada gambar dibawah ini.

Kontrol operasi

- Kontrol terhadap peralatan

  Kontrol terhadap peralatan dilakukan secara berkala (1 hari sekali) dengan tujuan meminimalisir kegagalan sistem sehingga tidak menganggu keberlanjutan proses bisnis yang ada. Namun demikian, masih muncul beberapa kegagalan sistem yang disebabkan layanan

DNS dan proxy yang mati sehingga akses internet di dalam jaringan akan terganggu.

- Pembatasan akses terhadap pusat data
  Akses terhadap ruang yang menjadi pusat data (server) dibatasi sesuai dengan wewenang yang dilakukan. Pada praktenya di instansi hal tersebut telah dilakukan dengan cara memberikan kunci terhadap lapisan perlindungan pada 2 orang yang berbeda, misalnya pintu terhadap ruang server diberikan kepada salah satu staff seksi pengembangan perangkat lunak sedangkan kunci terhadap loker server dipegang oleh kepala seksi pengembangan perangkat lunak. Kemudian dalam ruang server dipasang CCTV untuk merekam siapa saja yang pernah memasukinya.
- Pengendalian terhadap virus
  Menyadarkan pada setiap pemakai akhir sebuah sistem informasi untuk waspada terhadap virus. Biasanya penularan virus terjadi karena adanya interaksi pengkopian data dari flashdisk ke komputer secara langsung. Secara rutin menjalankan program antivirus yang berlisensi selama 1 tahun untuk mendeteksi infeksi virus. Menjalankan program antivirus untuk menghilangkan virus dari file yang tertular.
- Perlindungan fisik terhadap pusat data
  Untuk menjaga hal-hal yang tidak diinginkan terhadap pusat data, faktor lingkungan yang menyangkut suhu, kelembaban udara, kebersihan, bahaya banjir ruangan sangat diperhatikan dengan benar. Pada prakteknya suhu di ruangan yang berisi peralatan komputer berada pada tingkat 70 dan 74 derajat Fahrenheit. Sedangkan pada ruangan server berada pada tingkat 80 dan 90 Farenheit.

Kontrol perangkat keras

- Untuk mengantisipasi kegagalan sistem komponen, instansi menerapkan sistem komputer yang berbasis

fault-tolerant. Dengan adanya sistem ini, diharapkan komponen dalam sistem yang mengalami kegagalan maka komponen cadangan mengambil alih peran komponen yang rusak dan sistem dapat melanjutkan operasinya tanpa interupsi. Sistem fault-tolerant yang diterapkan ada 1 level, yaitu hanya ada pada transaksi. Toleransi kegagalan pada level transaksi ditangani melalui mekanisme basis data yang disebut rollback, yang akan mengembalikan ke keadaan semula yaitu keadaan sebelum terjadi kegagalan transaksi.

Kontrol akses terhadap sistem komputer

- Pada instansi untuk melakukan pembatasan akses terhadap sebuah sistem informasi, setiap pemakai diberi otorisasi yang berbeda-beda. Setiap pemakai dilengkapi dengan hak akses, NIP dan password. Password terdiri dari beberapa kombinasi numerik yang dibuat berasal dari NIP setiap karyawan yang terdiri dari 18 karakter. Sebelum pemakai berhasil masuk ke dalam sistem (*login*), mulai dari hak akses sampai nama pemakai akan diperiksa sehingga pemakai akan mendapatkan hak akses sesuai dengan otoritas yang telah ditentukan. Ketika salah satu komponen dari pengenal tiap pegawai yang telah disebutkan sebelumnya tidak dikenali maka pegawai tersebut tidak dapat memasuki sistem (*login*).

A.5 Hasil Wawancara

Survei dengan metode wawancara ini merupakan bagian dari penelitian Tugas Akhir mahasiswa Jurusan Sistem Informasi, Institut Teknologi Sepuluh November, yang bertujuan untuk memperoleh informasi dari karyawan Bidang Pengembangan TI sebagai pihak yang terkait dalam pengelolaan TI khususnya pada proses keamanan sistem informasi.

Daftar pertanyaan ini dikembangkan sesuai dengan tugas pokok dan fungsi yang dilakukan oleh Bidang Pengembangan TI khususnya pada proses pengembangan perangkat lunak yang menunjang proses bisnis Dinas Komunikasi dan Informatika Jawa Timur.

Untuk kebutuhan di atas mohon kiranya Bapak/Ibu sebagai responden dapat memberikan opininya sebagai jawaban atas pertanyaan-pertanyaan yang diberikan dalam wawancara ini untuk kemudian dapat kami olah dalam penelitian Tugas Akhir ini.

Jabatan Responden	Staff	NIP:
Nama Responden	Harsanto	
Unit/Bidang/Subbid	PTI	
Tanda Tangan		

Gambar A.2 Informasi Penelitian Wawancara Orang Pertama

Survei dengan metode wawancara ini merupakan bagian dari penelitian Tugas Akhir mahasiswa Jurusan Sistem Informasi, Institut Teknologi Sepuluh November, yang bertujuan untuk memperoleh informasi dari karyawan Bidang Pengembangan TI sebagai pihak yang terkait dalam pengelolaan TI khususnya pada proses keamanan sistem informasi.

Daftar pertanyaan ini dikembangkan sesuai dengan tugas pokok dan fungsi yang dilakukan oleh Bidang Pengembangan TI khususnya pada proses pengembangan perangkat lunak yang menunjang proses bisnis Dinas Komunikasi dan Informatika Jawa Timur.

Untuk kebutuhan di atas mohon kiranya Bapak/Ibu sebagai responden dapat memberikan opininya sebagai jawaban atas pertanyaan-pertanyaan yang diberikan dalam wawancara ini untuk kemudian dapat kami olah dalam penelitian Tugas Akhir ini.

Jabatan Responden	Staf PTI.	NIP: 19776917 200701 1 005
Nama Responden	Ivy Ruby Artha	
Unit/Bidang/Subbid	Pengembangan Teknologi Informasi	
Tanda Tangan		

Gambar A.3 Informasi Penelitian Wawancara Orang Kedua

Hasil Wawancara Orang Pertama

Gambar A.4 Hasil Wawancara Orang Pertama

No	Pertanyaan	Komentar
1.	Seberapa sering proyek sistem informasi mengalami kegagalan dalam memberikan kontribusi yang seharusnya diterima oleh institusi?	Probabilitas kegagalan dalam sistem informasi yang dibuat hanya 10% dari total sistem informasi yang dibuat.
2.	Apakah end-user merasa puas dengan kualitas dari kinerja sistem informasi yang diberikan?	Ya, hampir seluruh end-user yang notabene sebagai karyawan merasa puas dengan kinerja sistem informasi.
3.	Apakah ketersediaan sumber daya, infrastruktur dan kompetensi sistem informasi memenuhi kebutuhan untuk pencapaian tujuan strategi institusi dalam memberikan pelayanan kepada publik?	Ketersediaan sumber daya, infrastruktur dan kompetensi sistem informasi telah memenuhi kebutuhan untuk pencapaian tujuan strategi institusi dalam pemberian layanan publik. Kecuali ada permintaan khusus dalam penerapan sistem informasi yang ada seperti: tes CPNS.

Gambar A.4 Hasil Wawancara Orang Pertama

4.	Seberapa besar peran yang dilakukan sistem informasi untuk menyelesaikan masalah dibandingkan dengan melakukan perbaikan proses bisnis?	Peran sistem informasi yang ada lebih cenderung menyelesaikan masalah yang ada daripada melakukan perbaikan terhadap proses bisnis yang ada.
5.	Bagaimana penerapan kontrol keamanan yang ada di institusi saat ini?	Kontrol keamanan yang diterapkan dalam institusi saat ini berupa pengecekan *domain website* dengan melihat statusnya pada *server hosting* 1x sehari.
6.	Serangan apa yang ada di instansi ini?	*SQL injection, social engineering, denial of service, virus, malicious code, buffer overflow, debugging, reverse engineering, information disclosure.*
7.	Seberapa baikkah tujuan sistem informasi dan perusahaan sejalan?	Dalam memenuhi pelayanan publik sistem informasi yang ada telah memberikan kontribusi yang sangat berarti.

Gambar A.4 Hasil Wawancara Orang Pertama

8.	Inisiatif strategi apa yang telah diambil oleh pihak manajemen untuk mengelola aspek-aspek yang bersifat kritis, terkait dengan pemeliharaan dan pengembangan sistem informasi?	Strategi yang diberikan ialah memberikan fasilitas yang lebih dan teknisi untuk menangani serangan yang terjadi. Selain itu dalam rangka menerapkan teknik keamanan sistem, pihak manajemen membuat keputusan yang strategis untuk memberikan keamanan terhadap aset yang ada.
9.	Apakah penanganan semua risiko yang ada dari penerapan sistem informasi tersebut sudah diterapkan dengan baik?	Penanganan semua risiko yang ada dari penerapan sistem informasi sudah diterapkan dengan baik tetapi kurang efektif untuk mengatasi serangan yang ada.
10.	Apakah institusi memiliki persediaan yang sudah paling terkini?	Persediaan peralatan yang ada di Dinas Kominfo sudah memenuhi tetapi belum ada regenerasi terhadap peralatan yanga ada.

Gambar A.4 Hasil Wawancara Orang Pertama

11.	Apakah pihak manajemen secara regular melakukan pertemuan untuk membahas risiko-risiko sistem informasi yang muncul pada instansi?	Pertemuan dilakukan untuk membahas risiko-risiko pada sistem informasi serta cara penanganannya tetapi tidak secara regular.
12.	Bagaimana cara pihak manajemen melakukan artikulasi dan komunikasi tentang bagaimana caranya menyelaraskan antara tujuan bisnis dengan teknologi informasi?	Pihak manajemen sering kali melakukan pertemuan (rapat) sebulan sekali untuk membahas penyelerasan tujuan bisnis dengan teknologi informasi yang ada.
13.	Bagaimana cara pihak manajemen memperoleh laporan perkembangan dari proyek sistem informasi yang dijalankan?	Pihak manajemen mendapatkan laporan secara regular tentang perkembangan proyek sistem informasi yang dijalankan.

Hasil Wawancara Orang Pertama

Tabel A.2 Hasil Wawancara Orang Kedua

No	Pertanyaan	Komentar
1.	Seberapa sering proyek sistem informasi mengalami kegagalan dalam memberikan kontribusi yang seharusnya diterima oleh institusi?	Tidak ada kegagalan dalam sistem informasi yang dibuat.
2.	Apakah end-user merasa puas dengan kualitas dari kinerja sistem informasi yang diberikan?	Ya, hampir seluruh end-user yang notabene sebagai karyawan merasa puas dengan kinerja sistem informasi.
3.	Apakah ketersediaan sumber daya, infrastruktur dan kompetensi sistem informasi memenuhi kebutuhan untuk pencapaian tujuan strategi institusi dalam memberikan pelayanan kepada publik?	Ketersediaan sumber daya, infrastruktur dan kompetensi sistem informasi telah memenuhi kebutuhan untuk pencapaian tujuan strategi institusi dalam pemberian layanan publik. Kecuali ada permintaan khusus dalam penerapan sistem informasi yang ada seperti: tes CPNS.

Tabel A.3 Hasil Wawancara Orang Kedua

4.	Seberapa besar peran yang dilakukan sistem informasi untuk menyelesaikan masalah dibandingkan dengan melakukan perbaikan proses bisnis?	Peran sistem informasi yang ada lebih cenderung menyelesaikan masalah yang ada daripada melakukan perbaikan terhadap proses bisnis yang ada.
5.	Bagaimana penerapan kontrol keamanan yang ada di institusi saat ini?	Kontrol keamanan yang diterapkan dalam institusi saat ini berupa pengecekan *domain website* dengan melihat statusnya pada *server hosting* 1x sehari.
6.	Serangan apa yang ada di instansi ini?	*SQL injection, denial of service, virus, malicious code, debugging, reverse engineering, information disclosure.*
7.	Seberapa baikkah tujuan sistem informasi dan perusahaan sejalan?	Dalam memenuhi pelayanan publik sistem informasi yang ada telah memberikan kontribusi yang sangat berarti.

Tabel A.4 Hasil Wawancara Orang Kedua

8.	Inisiatif strategi apa yang telah diambil oleh pihak manajemen untuk mengelola aspek-aspek yang bersifat kritis, terkait dengan pemeliharaan dan pengembangan sistem informasi?	Strategi yang diberikan ialah memberikan fasilitas yang lebih dan teknisi untuk menangani serangan yang terjadi. Selain itu dalam rangka menerapkan teknik keamanan sistem, pihak manajemen membuat keputusan yang strategis untuk memberikan keamanan terhadap aset yang ada.
9.	Apakah penanganan semua risiko yang ada dari penerapan sistem informasi tersebut sudah diterapkan dengan baik?	Penanganan semua risiko yang ada dari penerapan sistem informasi sudah diterapkan dengan baik tetapi kurang efektif untuk mengatasi serangan yang ada.
10.	Apakah institusi memiliki persediaan yang sudah paling terkini?	Persediaan peralatan yang ada di Dinas Kominfo sudah memenuhi tetapi belum ada regenerasi terhadap peralatan yanga ada.

Tabel A.5 Hasil Wawancara Orang Kedua

11.	Apakah pihak manajemen secara regular melakukan pertemuan untuk membahas risiko-risiko sistem informasi yang muncul pada instansi?	Pertemuan dilakukan untuk membahas risiko-risiko pada sistem informasi serta cara penanganannya tetapi tidak secara regular.
12.	Bagaimana cara pihak manajemen melakukan artikulasi dan komunikasi tentang bagaimana caranya menyelaraskan antara tujuan bisnis dengan teknologi informasi?	Pihak manajemen sering kali melakukan pertemuan (rapat) sebulan sekali untuk membahas penyelerasan tujuan bisnis dengan teknologi informasi yang ada.
13.	Bagaimana cara pihak manajemen memperoleh laporan perkembangan dari proyek sistem informasi yang dijalankan?	Pihak manajemen mendapatkan laporan secara regular tentang perkembangan proyek sistem informasi yang dijalankan dari pihak rekanan.

Halaman ini sengaja dikosongkan.

LAMPIRAN C

DOKUMEN KERJA

B. Komponen Dokumen Tata Kelola TI (IT Governance Component)

1. Dokumen SOA (*Statement of Applicability Document*)
2. Format dokumen standar operasional prosedur (*Standard operating procedure document format*)

B.1 Dokumen SOA (*Statement of Applicability Document*)

Kontrol	Deskripsi	Persetujuan	Justifikasi	Referensi
8.1	***Security requirement of information systems***			
8.1.1	*Security requirements analysis and specification.*	Ya	Bidang PTI melakukan dukungan pengembangan dan pemeliharaan perangkat lunak pada beberapa sistem informasi yang ada. Namun perangkat tambahan untuk perangkat keras memerlukan permintaan perubahan.	Pedoman analisis dan spesifikasi kebutuhan keamanan.

8.2	***Correct processing in applications.***			
8.2.1	*Input data validation*	Ya	Bidang PTI melakukan dukungan pengembangan perangkat lunak untuk semua sistem informasi yang ada.	Pedoman validasi data masukan. Prosedur penanganan hak akses.
8.2.2	*Control of internal processing*	Ya	Bidang PTI melakukan pemeliharaan perangkat lunak untuk semua sistem informasi yang ada	Pedoman pengendalian proses internal.
8.2.3	*Message integrity*	Ya	Bidang PTI melakukan dukungan pengembangan perangkat lunak untuk	*Risk assessment.*

			semua sistem informasi yang ada.	
8.2.4	*Output data validation*	Ya	Bidang PTI melakukan dukungan pengembangan perangkat lunak untuk semua sistem informasi yang ada.	Pedoman validasi data keluaran.
8.3	***Crytographic controls***			
8.3.1	*Policy on the use of crytographic controls*	Tidak	Bidang PTI tidak mempunyai sumber daya manusia yang berkompeten dalam penanganan kriptografi.	a/n
8.3.2	*Key management*	Tidak	Bidang PTI tidak	n/a

			mempunyai sumber daya manusia yang berkompeten dalam penanganan kriptografi.	
8.4	***Security of system files***			
8.4.1	*Control of operational software.*	Ya	Untuk mencegah perubahan kontrol akses yang tidak sah.	Pedoman pengendalian perubahan. Prosedur penanganan *update/patch.*
8.4.2	*Protection of system test data*	Tidak	Bidang PTI tidak melakukan dukungan pengembangan perangkat lunak untuk	n/a

			semua sistem informasi yang ada.	
8.4.3	*Access control to program source code*	Ya	*Source code* aplikasi harus disimpan sebagai cadangan.	Prosedur *backup* dan restorasi data. Pedoman kontrol akses *source code* program. Prosedur penanganan *virus*.
8.5	***Security in development and support process***			
8.5.1	*Change control procedures*	Ya	Setiap perubahan yang dilakukan memerlukan permintaan	Pedoman pengendalian perubahan.

			perubahan.	Prosedur penanganan *update/patch.*
8.5.2	*Technical review of application after operating system changes*	Ya	Menginformasikan ke pemilik aplikasi ketika sistem operasi yang digunakan telah dirubah.	Jadwal pemeliharaan dan *log.* Prosedur penanganan *virus.*
8.5.3	*Restrictions on changes to software packages*	Ya	Beberapa paket perangkat lunak harus mempunyai pembatas hak akses	Pedoman pembatasan perubahan paket *software.* Prosedur penanganan *update/patch.*

8.5.4	*Information leakage*	Ya	Peluang untuk kebocoran informasi harus dicegah.	Pedoman kebocoran informasi. Prosedur penanganan serangan dari dalam.
8.5.5	*Outsourced software development*	Ya	Pengembangan perangkat lunak dilakukan oleh bidang PTI.	Pedoman pengembangan *software* secara *outsourcing*.
8.6	***Technical vulnerability management***			
8.6.1	*Control of technical vulnerabilities*	Ya	Kerentanan teknis sistem informasi harus dikelola.	*Risk assessment.* Pedoman kontrol kelemahan teknis.

B.2 Format dokumen prosedur (*Standard Operating Procedure Document Format*)

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

PROSEDUR PENULISAN PROSEDUR OPERASI STANDAR

Dibuat Oleh	**Nama**	**Jabatan**	**Tanda Tangan**	**Tanggal**
Disahkan Oleh	**Nama**	**Jabatan**	**Tanda Tangan**	**Tanggal**

DAFTAR DISTRIBUSI

No.	**Departemen/Bagian**	**Personel**	**Tanda Tangan**	**Tanggal**

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

CATATAN PERUBAHAN PROSEDUR PENULISAN PROSEDUR OPERASI STANDAR

Revisi ke	Tanggal	Halaman	Paragraf	Alasan	Disahkan Oleh	Fungsi / Jabatan	Tanda Tangan

Logo Perusahaan	Nama Perusahaan

Prosedur: Penulisan Prosedur Operasi Standar		
	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

1. **TUJUAN**
   Prosedur Penulisan Standar Operasi dibuat untuk menstandarisasikan penyusunan komposisi yang tepat dari penulisan semua prosedur operasi standar yang berlaku di lingkungan perusahaan.
2. **RUANG LINGKUP**
   Prosedur ini dipergunakan sebagai petunjuk dalam penulisan semua prosedur operasi standar yang berkaitan dengan persyaratan standar yang digunakan yang akan diimplementasikan oleh semua departemen / bagian dalam lingkungan perusahaan. Prosedur ini meliputi semua aktivitas penulisan prosedur operasi standar dalam lingkungan perusahaan.
3. **DEFINISI**
   3.1 DCC : *Document Control Centre*
   3.2 QMS : *Quality Management System*
   3.3 SOP : *Standard Operating Procedure*
4. **REFERENSI**
   Referensi yang digunakan dalam menyusun standar operasi, dapat berupa *framework* tata kelola yang digunakan, buku tentang standar operasi sendiri, dll.

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

5. INFORMASI UMUM

5.1 Prosedur ini diberlakukan untuk dokumen dan/atau catatan pengendalian keamanan sistem informasi yang didistribusikan dan menjadi tanggungjawab Bagian Pengendalian Dokumen.

5.2 Penanggung jawab pelaksanaan prosedur ini dilakukan oleh manajemen tingkat menengah yang memimpin suatu departemen atau bidang dalam sebuah instansi.

6. PEDOMAN IMPLEMENTASI

6.1 DOKUMEN YANG DIKENDALIKAN

6.1.1. Pedoman keamanan

6.1.2. Prosedur Sistem Kualitas

6.1.3. Instruksi Kerja (*Work Instructions*)

6.1.4. Formulir, Master List Dokumen dan Catatan Kualitas (Data Tercetak)

6.1.5. Dokumen Umum

6.2 METODE PENYUSUNAN DOKUMEN

6.2.1. Penyusunan Dokumen Pedoman Kualitas dan Prosedur (berikut penjelasan) sebagai berikut:

6.2.1.1. Lembar Pengendalian dan Pengesahan

Header: Nama Perusahaan, nama prosedur, nomor dokumen, nomor edisi, no revisi, tanggal efektif dokumen berlaku, halaman dan jumlah, serta persetujuan penerbitan dokumen yang bersangkutan.

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

Jumlah Penggandaan: sesuai dengan jumlah *copy* pada daftar distribusi.
Departemen/Bagian dan Personel: menunjukkan pejabat yang memegang dokumen.
Tanggal Distribusi: tanggal dokumen tersebut didistribusikan oleh Bagian Pengendalian Dokumen.

6.2.1.2. Catatan Revisi

Bila dokumen direvisi, maka harus dicatat dalam lembar perubahan (halaman 2 setiap dokumen) dan harus disahkan oleh Kepala Bidang Pengembangan TI.

6.2.1.3. Daftar Isi

Berisi nomor bab, judul bab dan nomor halaman dalam dokumen.

1. Tujuan
   Berisi tujuan dibuatnya dokumen yang bersangkutan.
2. Ruang Lingkup
   Menunjukkan dimana (ruang lingkup) penerapan dokumen yang bersangkutan.
3. Definisi
   Berisi definisi-definisi atau istilah-istilah khusus yang perlu diketahui.

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

4. Referensi
Acuan/rujukan yang digunakan untuk terlaksananya penerapan dokumen yang bersangkutan..
5. Informasi Umum
Berisi informasi umum yang berkaitan dengan pengendalian dokumen dan data.

1. Prosedur dan Tanggung Jawab
Berisi rincian tugas yang harus dilaksanakan dan personel terkait yang harus bertanggung jawab terhadap implementasi prosedur itu.
2. Keadaan Khusus
Berisi informasi mengenai keadaan-keadaan khusus yang berkaitan dengan pengendalian dokumen dan catatan kualitas.
3. Dokumentasi
Keterangan yang menyangkut bentuk keberadaan dokumen yang bersangkutan.
4. Lampiran
Berisi lampiran-lampiran yang berkaitan dengan pengendalian dokumen dan catatan kualitas.

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

6.2.2. Penyusunan Instruksi Kerja (berikut penjelasan) sebagai berikut:

6.2.2.1. Informasi Pengesahan

Header: Nama Perusahaan, nama prosedur, nomor dokumen, nomor edisi, nomor revisi, tanggal efektif dokumen berlaku, halaman dan jumlah, serta persetujuan penerbitan dokumen yang bersangkutan.

Jumlah Penggandaan: sesuai dengan jumlah *copy* pada daftar distribusi.

Departemen/Bagian dan Personel: menunjukkan pejabat yang memegang dokumen.

Tanggal Distribusi: tanggal dokumen tersebut didistribusikan oleh Bagian Pengendalian Dokumen.

6.2.2.2. Instruksi

Berisi urutan kerja.

6.2.3. Penyusunan Formulir (berikut penjelasan) sebagai berikut:

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

6.2.3.1. Informasi Pengesahan

Header/Footer: Nama Perusahaan, nama prosedur, nomor dokumen, nomor edisi, nomor revisi, tanggal efektif dokumen berlaku, halaman dan jumlah, serta persetujuan penerbitan formulir yang bersangkutan.

Jumlah Tembusan: sesuai dengan jumlah formulir.

Departemen/Bagian dan Personel: menunjukkan pejabat yang memegang formulir.

Tanggal Distribusi: tanggal formulir tersebut didistribusikan oleh Bagian Pengendalian Dokumen.

6.2.3.2. Format Formulir

Format formulir disusun sesuai kebutuhan informasi data yang akan dikumpulkan.

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur *Operasi Standar*	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

6.2.4. Penyusunan Dokumen Umum

6.2.4.1. Informasi Pengesahan

Header: Nama Perusahaan, nama prosedur, nomor dokumen, nomor edisi, nomor revisi, tanggal efektif dokumen berlaku, halaman dan jumlah, serta persetujuan penerbitan dokumen yang bersangkutan.

Jumlah Penggandaan: sesuai dengan jumlah *copy* pada daftar distribusi.

Departemen/Bagian dan Personel: menunjukkan pejabat yang memegang dokumen.

Tanggal Distribusi: tanggal dokumen tersebut didistribusikan oleh Bagian Pengendalian Dokumen.

6.2.4.2. Isi Dokumen

Berisi informasi selain prosedur, instruksi kerja dan formulir.

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

6.3 METODE PENYUSUNAN DOKUMEN

Setiap pembuatan dokumen pengelolaan keamanan sistem informasi harus mendapat bukti pinjaman dan persetujuan dan kecukupannya oleh personel yang berwenang, sebagai berikut:

a. Pedoman pengelolaan keamanan sistem informasi ditinjau berulang-ulang dan ditandatangani oleh Wakil Manajemen, disetujui oleh Pimpinan tertinggi institusi pemerintahan.
b. Prosedur-prosedur pengelolaan keamanan sistem informasi ditinjau berulang-ulang dan ditandatangani oleh Kepala Bidang dan disetujui oleh Wakil Manajemen.
c. Instruksi kerja (*Work Instructions*) ditinjau berulang-ulang dan ditandatangani oleh Kepala Bidang dan disetujui oleh Wakil Manajemen.
d. Formulir ditinjau berulang-ulang dan ditandatangani oleh Kepala Bidang dan disetujui oleh Wakil Manajemen.
e. Dokumen umum ditinjau berulang-ulang dan ditandangani oleh Penerbit dokumen dan disetujui oleh Pejabat yang berwenang terhadap dokumen tersebut.
f. Untuk pengesahan hasil penggandaan digunakan stempel basah.

6.4 PENOMORAN DOKUMEN

Identifikasi tiap-tiap dokumen selain judul adalah dengan penomoran sebagai berikut:

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

1. **Pedoman Kualitas**

DCC/QMB/000/000 → No urut

→ Kode Departemen / Bagian

→ Kode Pedoman Pengelolaan Kualitas (*Quality Manual Book*)

→ Kode Badan Pengendalian Dokumen (*Document Control Centre*)

2. **Prosedur**

DCC/SOP/000/000 → No urut

DCB → Kode Departemen / Bagian

DCF → Kode Prosedur (*Standard Operating Procedure*)

→ Kode Badan Pengendalian Dokumen (*Document Control Centre*)

Logo Perusahaan	Nama Perusahaan

Prosedur: Penulisan Prosedur Operasi Standar		
	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

6.5 METODE PENERBITAN DOKUMEN

6.5.1. Metode Pendistribusian Penerbitan dan Penarikan Dokumen

Ada 2 (dua) metode pendistribusian penerbitan dokumen, yaitu:

6.5.1.1. Langsung

Untuk penerbitan di lokasi pengembangan perangkat lunak, langsung diserahkan kepada penanggung jawab terkait dengan tanda bukti penerimaan sesuai formulir nomor: DCC/FML/ADP/001. Dan untuk penarikan dengan tanda bukti penarikan sesuai formulir nomor: DCC/FML/ADP/002.

6.5.1.1. Tidak Langsung

Untuk penerbitan di lokasi pengembangan perangkat lunak dengan surat pengantar dan tanda bukti penerimaan sesuai formulir nomor: DCC/FML/ADP/001. Dan untuk penarikan dengan tanda bukti penarikan sesuai formulir nomor: DCC/FML/ADP/002.

<table>
<tr><td>Logo Perusahaan</td><td colspan="2">Nama Perusahaan</td></tr>
<tr><td rowspan="5">Prosedur: Penulisan Prosedur Operasi Standar</td><td>No. Dokumen</td><td>No.dokumen</td></tr>
<tr><td>Edisi</td><td>Edisi dokumen</td></tr>
<tr><td>Revisi</td><td>Banyak revisi</td></tr>
<tr><td>Berlaku Efektif</td><td>Tanggal berlaku</td></tr>
<tr><td>Halaman</td><td>Halaman keberapa dari total halaman</td></tr>
</table>

6.5.2. Metode Penerbitan Ulang Dokumen

Wakil Manajemen dapat menerbitkan ulang suatu dokumen, termasuk Pedoman Kualitas (Quality manual) dan/atau prosedur, jika:

6.5.2.1. Mengalami revisi sebanyak 5 kali.
6.5.2.2. Terjadi perbaikan sistem kualitas.
6.5.2.3. Ada perubahan struktur organisasi yang Mempengaruhi isi dokumen.
6.5.2.4. Ada perubahan teknologi.
6.5.2.5. Instruksi kerja (*work instructions)* sudah tidak sesuai dengan urutan pelaksanaan tugas.

Bila terjadi penerbitan ulang, dokumen usang yang bersangkutan, dengan surat perintah Wakil Manajemen akan ditarik kembali (formulir nomor: DCC/FML/ADP/002).

6.6 METODE PEREVISIAN DOKUMEN

Sesuai level dokumen, dapat diajukan permohonan oleh peninjau dokumen terkait dengan formulir nomor: DCC/FML/ADP/003. Setelah disetujui, kemudian oleh Kepala Dinas atau Wakil Manajemen dicatat dalam catatan revisi (halaman 2 di setiap dokumen), Untuk lebih jelasnya, perhatikan diagram di bawah ini:

Logo Perusahaan	Nama Perusahaan

Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

Jenis Dokumen / Level Dokumen	Peninjau / Pemohon	Pengesahan
Pedoman Kualitas / Manual	Wakil Manajemen	Pimpinan institusi
Prosedur	*Kepala Bidang*	*Wakil Manajemen*
Prosedur	Kepala Bidang	Wakil Manajemen
Instruksi Kerja	Kepala Bidang	Wakil Manajemen
Formulir	Kepala Bidang	Wakil Manajemen
Dokumen Umum	Penerbit Dokumen	Pejabat yang berwenang

6.7 METODE PEMUSNAHAN DOKUMEN USANG

6.7.1. Untuk dokumen-dokumen yang didistibusikan dan diarsip oleh Badan Pengendalian Dokumen (dokumen sistem kualitas), disimpan oleh Badan Pengendalian Dokumen dan diberi tanda stempel.

6.7.2. Untuk dokumen lainnya dimusnahkan dan dibuat berita acara pemusnahan dokumen dengan formulir nomor: DCC/FML/ADP/004.

6.8 PERANGKAT PENGENDALIAN DOKUMEN

Daftar induk dokumen:

a. Untuk Pedoman Kualitas dan Prosedur
   Formulir nomor: DCC/FML/ADP/005
b. Instruksi Kerja
   Formulir nomor: DCC/FML/ADP/006
c. Formulir
   Formulir nomor: DCC/FML/ADP/007
d. *Dokumen Umum*
   Formulir nomor: DCC/FML/ADP/008

Logo Perusahaan	Nama Perusahaan	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	No.dokumen
	Edisi	Edisi dokumen
	Revisi	Banyak revisi
	Berlaku Efektif	Tanggal berlaku
	Halaman	Halaman keberapa dari total halaman

7. **KEADAAN KHUSUS**
   Tidak Ada.
8. **DOKUMENTASI**
   Prosedur ini didokumentasikan dalam bentuk *hard copy* (kertas) dan file: DCC.SOP.ADP.002.DOC, serta pengendalian lainnya yang diatur dalam prosedur pengendalian dokumen.

Halaman ini sengaja dikosongkan.

C. Dokumen Kerja *(Work Instructions)*

USULAN PERATURAN GUBERNUR JAWA TIMUR
NOMOR: XX TAHUN 2011
TENTANG
URAIAN TUGAS BIDANG PENGEMBANGAN TEKNOLOGI INFORMATIKA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

Diperbanyak oleh:
BIRO ORGANISASI
SEKRETARIAT DAERAH PROVINSI JAWA TIMUR

GUBERNUR PROVINSI JAWA TIMUR

USULAN PERATURAN GUBERNUR JAWA TIMUR
NOMOR XX TAHUN 2011

TENTANG
URAIAN TUGAS BIDANG PENGEMBANGAN TEKNOLOGI INFORMATIKA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

GUBERNUR JAWA TIMUR

Menimbang : bahwa sebagai pelaksanaan ketentuan Pasal 51 Peraturan Daerah Provinsi Jawa Timur Nomor 9 Tahun 2008 tentang Organisasi dan Tatakerja Dinas Daerah Provinsi Jawa Timur yang diundangkan dalam Lembaran Daerah Provinsi Jawa Timur Tanggal 22 Agustus 2008 Nomor 2 Tahun 2008 Seri D, perlu mengatur Uraian Tugas Bidang, Sub Bagian dan Seksi Dinas Komunikasi Dan Informatika Provinsi Jawa Timur dalam Peraturan Gubernur.

Mengingat : 1. Undang-undang Nomor 2 Tahun 1950 tentang Pembentukan Provinsi Jawa Timur juncto Undang-undang Nomor 18 Tahun 1950 tentang Mengadakan Perubahan Undang-undang Tahun 1950 Nomor 2 dari hal Pembentukan Provinsi

Jawa Timur (Lembaran Negara Republik Indonesia Tahun 1950 Nomor 32);

2. Undang-undang Nomor 8 Tahun 1974 tentang Pokok-pokok Kepegawaian (Lembaran Negara Republik Indonesia Tahun 1974 Nomor 55, Tambahan Lembaran Negara Republik Indonesia Nomor 3041) sebagaimana telah diubah dengan Undang-undang Nomor 43 tahun 1999 (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 169, Tambahan Lembaran Negara Republik Indonesia Nomor 3890);
3. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881);
4. Undang-undang Nomor 32 Tahun 2002 tentang Penyiaran (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 139, Tambahan Lembaran Negara Republik Indonesia Nomor 4252);
5. Undang-undang Nomor 10 Tahun 2004 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 53, Tambahan Lembaran Negara Republik Indonesia Nomor 4389);
6. Undang-undang Nomor 32 Tahun 2004 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 125, Tambahan Lembaran Negara Republik Indonesia Nomor 4437), sebagaimana telah diubah dengan Undang-undang Nomor 12 Tahun 2008 (Lembaran Negara Republik Indonesia Tahun 2008 nomor 59, Tambahan Lembaran Negara Republik Indonesia Nomor 4844);

7. Peraturan Pemerintah Nomor 6 Tahun 1988 tentang Koordinasi Kegiatan Instansi Vertikal di Daerah (Lembaran Negara Republik Indonesia Tahun 1988 Nomor 10, Tambahan Lembaran Negara Republik Indonesia Nomor 3373);
8. Peraturan Pemerintah Nomor 79 Tahun 2005 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2005 Nomor 165, Tambahan Lembaran Negara Republik Indonesia Nomor 4593);
9. Peraturan Pemerintah Nomor 38 Tahun 2007 tentang Pembagian Urusan Pemerintahan Antara Pemerintah, Pemerintah Daerah Provinsi dan Pemerintahan Daerah Kabupaten/Kota (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 82);
10. Peraturan Pemerintah Nomor 41 Tahun 2007 tentang Organisasi Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 89, Tambahan Lembaran Negara Republik Indonesia Nomor 4741);
11. Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2007 tentang Petunjuk Teknis Penataan Organisasi Perangkat Daerah;
12. Peraturan Daerah Provinsi Jawa Timur Nomor 5 Tahun 2006 tentang Pembentukan Peraturan Daerah (Lembaran Daerah Provinsi Jawa Timur Tahun 2006 Nomor 4 Seri E);
13. Peraturan Daerah Provinsi Jawa Timur Nomor 7 Tahun 2008 tentang Urusan Pemerintahan Daerah Provinsi Jawa Timur (Lembaran Daerah Provinsi Jawa Timur Tahun 2008 Nomor 4 Seri E);

14. Peraturan Daerah Provinsi Jawa Timur Nomor 9 Tahun 2008 tentang Organisasi Dan Tata Kerja Dinas Daerah (Lembaran Daerah Provinsi Jawa Timur Tahun 2008 Nomor 2 Seri D).

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG URAIAN TUGAS BIDANG PENGEMBANGAN TEKNOLOGI INFORMATIKA DINAS INFORMASI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Pemerintah Provinsi adalah Pemerintah Provinsi Jawa Timur;
2. Gubernur adalah Gubernur Jawa Timur;
3. Dinas adalah Dinas Komunikasi Dan Informatika Provinsi Jawa Timur;
4. Kepala Dinas adalah Kepala Dinas Komunikasi Dan Informatika Provinsi Jawa Timur;
5. Telematika (telekomunikasi, media dan informatika) adalah merupakan sinergi antara teknologi informasi dan teknologi komunikasi yang diarahkan pada ketersediaan jaringan informasi dan data yang menghubungkan instansi pemerintah provinsi dalam rangka otomatisasi pelayanan umum;
6. Telekomunikasi adalah setiap pemancaran, pengiriman dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio atau sistem elektromagnetik lainnya;

7. Informasi adalah hasil pengolahan data berupa yang mempunyai bentuk, nilai dan arti bagi pemakainya;
8. Perangkat keras adalah komponen fisik dari suatu sistem komputer;
9. Program Aplikasi adalah program komputer yang dirancang untuk menjalankan suatu aplikasi tertentu.
10. Infrastruktur komunikasi: jaringan komputer/komunikasi, koneksi internet;
11. Administrator adalah pihak yang mempunyai hak dan kewenangan serta bertanggung jawab mengurusi kelancaran penyelenggaraan sistem elektronik.
12. Sistem Informasi adalah penerapan teknologi informasi sesuai dengan karakteristik organisasi dan manajemen tertentu yang berfungsi untuk memperoleh, memasukkan, mengolah, menyimpan, mengirimkan, menyampaikan, atau mengkomunikasikan data dan/atau informasi, dan meliputi keterpaduan komponen-komponen; perangkat keras komputer, program komputer, data komputer, data komunikasi, prosedur-prosedur, sumber daya manusia, dan peralatan-peralatan pelengkap lain yang digunakan.
13. Sistem Informasi Pemerintah Provinsi adalah sistem informasi yang digunakan untuk mendukung sistem administrasi pemerintahan provinsi Jawa Timur.
14. *Web server* adalah suatu program aplikasi yang ditujukan agar suatu *server* yang menerima dan menangani permintaan *web browser* dari pengguna dalam protokol HTTP dan HTTPS yang memberikan respon berupa pengiriman informasi kepada *web browser*.
15. *Web browser* adalah program komputer yang digunakan sebagai penelusur informasi yang digunakan oleh pengguna internet untuk memperoleh informasi dari suatu Situs Web yang disediakan oleh *Web server*.
16. Penyelenggara Negara adalah adalah pejabat negara yang menjalankan fungsi eksekutif, legislatif, atau yudikatif, dan pejabat lain yang fungsi dan tugas pokoknya berkaitan dengan

penyelenggaraan negara sesuai dengan ketentuan peraturan perundangundangan yang berlaku.

BAB II
URAIAN TUGAS

Bagian Kesatu
Bidang Pengembangan Teknologi Informatika

Pasal 2

(1) Bidang pengembangan TI mempunyai tugas melindungi sistem informasi pemerintah provinsi dalam rangka melindungi HAM dan melayani publik. Khususnya terhadap otentisitas, keutuhan, dan ketersediaan informasi demi kepentingan publik itu sendiri.
(2) Bidang Pengembangan TI menyusun mekanisme perlindungan atas situs pemerintah provinsi demi akuntabilitas dan kepercayaan publik terhadap substansi informasi yang disediakan. Insiden keamanan sistem informasi dapat menimbulkan permasalahan yang serius jika tampilan situs dirusak, layanan publik terhenti dan informasi yang bersifat sensitif jatuh ketangan pihak yang salah.
(3) Untuk melaksanakan tugas sebagaimana dimaksud pada ayat (1) dan ayat (2) Bidang Pengembangan Teknologi Informatika, mempunyai fungsi:
    a) Pelaksanaan penyusunan mekanisme keamanan yang baik pada sistem informasi pemerintah provinsi. Yaitu sebuah sistem yang dapat memberikan kejelasan informasi bagi penyelenggara dan pengguna, tidak membuat ketertantungan terhadap penggunaan jenis teknologi tertentu, serta dapat memberikan kemandirian bagi penyelenggara negara untuk mengembangkan sendiri lebih lanjut sistem tersebut sesuai dengan perkembangan

organisasi penyelenggaraan pemerintah provinsi dari waktu ke waktu.

b) Pelaksanaan perumusan kebijakan internal dalam memuat kejelasan proses pengembangan dan pengimplementasian sistem informasi yang mencakup kejelasan rancangan dan penerapan serta pengoperasiannya serta telah memperhitungkan insiden ataupun kejadian-kejadian tak tentu yang tidak dikehendaki.

c) Pelaksanaan keterbukaan informasi publik mempunyai kewajiban kehatian-hatian (*duty of care*) terhadap penyediaan atau penyajian informasi kepada publik.

Pasal 3

(1) Bidang Pengembangan Teknologi Informatika, mempunyai tugas:

a) Memberikan pertimbangan kepada Kepala Bidang Pengembangan TI, sebagai pimpinan dalam suatu bidang, sehubungan dengan penetapan kebijakan, standar dan prosedur yang diperlukan pada tata kelola teknologi informasi dalam pengelolaan keamanan sistem informasi.

b) Membantu dalam melakukan pengelolaan keamanan sistem informasi secara efektif untuk dapat memastikan integritas, ketersediaan dan kerahasiaan data institusi.

c) Membantu memastikan dukungan layanan sistem informasi pada terselenggaranya operasional layanan teknologi informasi pada proses bisnis baik utama maupun pendukung institusi.

d) Memperoleh solusi bersama atas berbagai permasalahan dan melakukan evaluasi terhadap pelaksanaan pengelolaan keamanan sistem informasi selama ini.

e) Melakukan komunikasi dan sosialisasi secara efektif dan intensif tentang kebutuhan pengelolaan keamanan sistem informasi untuk memenuhi kebutuhan layanan publik.

f) Melakukan komunikasi dan sosialisasi secara efektif dan intensif sehingga mendapatkan komitmen manajemen untuk membenahi sistem pengelolaan keamanan sistem informasi secara menyeluruh terkait dengan peningkatan layanan publik, dapat dipahami secara luas di seluruh jajaran internal organisasi.

g) Menumbuhkan kesadaran dan kepedulian kepada seluruh jajaran internal organisasi bahwa tata kelola TI dalam proses pengelolaan keamanan sistem informasi merupakan hal yang penting dan perlu untuk dilakukan secara tepat.

h) Melakukan evaluasi secara periodik terhadap pelaksanaan tata kelola teknologi informasi dalam proses pengelolaan sistem informasi, untuk selanjutnya dapat ditentukan tindakan perbaikan.

i) Melakukan pendefinisian, implementasi, dan pemelihaaan atas beberapa kebijakan pada tata kelola teknologi informasi dalam pengelolaan keamanan sistem informasi.

(2) Bidang Pengembangan Teknologi Informatika menyelengarakan pertemuan sekurangnya sekali dalam kurun waktu 2 bulan untuk membahas pengelolaan keamanan sistem informasi pemerintah provinsi.

Pasal 4

(1) Bidang Pengembangan Teknologi Informatika mempunyai prosedur sebagai berikut:

Pendefinisian dan penyempurnaan prosedur dan pedoman utama yang diperlukan dalam pengelolaan keamanan sistem informasi, dengan mempertimbangkan objektif dalam proses pengelolaan keamanan sistem informasi, yang meliputi:

a) Prosedur *backup* data.

b) Prosedur restorasi data.

c) Prosedur penanganan virus.
d) Prosedur penanganan spam.
e) Prosedur penanganan update/patch.
f) Prosedur penanganan serangan dari dalam.
g) Prosedur penanganan hak akses.
h) Pedoman analisis dan spesifikasi kebutuhan keamanan.
i) Pedoman validasi data masukan.
j) Pedoman kontrol proses internal.
k) Pedoman validasi data keluaran.
l) Pedoman kontrol operasional software.
m) Pedoman kontrol akses *source code* program.
n) Pedoman kontrol perubahan.
o) Pedoman pembatasan perubahan paket *software*.
p) Pedoman kebocoran informasi.
q) Pedoman pengembangan *software* secara *outsourcing*.
r) Pedoman kontrol kelemahan teknis.

(3) Pendefinisian dan penyempurnaan prosedur dan pedoman tersebut dilakukan dengan mempertimbangkan hasil kajian konsep *best-practice* dalam pengelolaan keamanan sistem informasi, kebutuhan kedepan untuk meningkatkan kualitas layanan teknologi informasi dan kemampuan SDM teknologi organisasi.

(4) Prosedur dan pedoman yang telah ditetapkan dipantau pelaksanaannya dan ditinjau secara berkala untuk disesuaikan dengan kondisi dan kebutuhan institusi yang senantiasa berkembang.

(5) Menggunakan alat bantu terkini untuk melakukan otomasi langkah yang telah didefinisikan dalam prosedur dan pedoman pengelolaan keamanan sistem informasi, sesuai dengan rencana standarisasi penggunaan perangkat bantu yang telah ditetapkan dalam rencana strategis teknologi informasi organisasi.

Pasal 5

(1) Bidang Pengembangan Teknologi Informatika mempunyai kompetensi sebagai berikut:
   a) Melakukan penilaian terhadap SDM teknologi informasi yang terkait dengan peran dalam proses pengelolaan keamanan sistem informasi untuk mengetahui tingkat kompetensi yang telah dimiliki dan yang diharapkan sesuai dengan kebutuhan, unuk selanjutnya dilakukan analisis untuk dapat menentukan perencanaan pelatihan.
   b) Mendefinisikan secara rinci kebutuhan kompetensi yang diperlukan untuk dapat melakukan peran dalam proses pengelolaan keamanan sistem informasi secara efektif.
   c) Melakukan perencanaan kebutuhan kompetensi SDM teknologi informasi, diterapkan pembinaan karir (*carrer-path*) yang jelas terkait prasyarat kompetensi yang diperlukan secara konsisten mengikuti program pelatihan formal sesuai dengan *roadmap* kompetensi yang ditetapkan.
   d) Menyelenggarakan pelatihan formal dan *knowledge sharing* bagi para pelaksana peran dalam pengelolaan keamanan sistem informasi yang dilakukan sesuai dengan rencana pelatihan, dengan materi sebagai berikut:
      a) Pemahaman pada hal-hal yang berkaitan dengan pengelolaan keamanan sistem informasi, untuk menambah wawasan yang sangat menunjang peningkatan kompetensinya.
      b) Penerapan prosedur dalam pengelolaan keamanan sistem informasi.
      c) Penggunaan perangkat bantu yang dimanfaatkan dalam pengelolaan keamanan sistem informasi.

(6) Melakukan evaluasi dan monitoring terhadap efektivitas terhadap pelaksanaan pelatihan secara keseluruhan, sebagai upaya perbaikan kualitas pelatihan secara berkelanjutan.

(7) Dalam rangka pemenuhan kebutuhan kompetensi terutama untuk dapat menangani peran-peran dalam proses pengelolaan keamanan sistem informasi, dengan mempertimbangkan keterbatasan secara kuantitas staff teknologi informasi dan hasil analisis biaya dan manfaat (*cost and benefit analysis*) yang diperlukan, maka dapat dilakukan rekrutmen ataupun *outsourcing*.

Pasal 6

(1) Bidang Pengembangan Teknologi Informatika memiliki peran dan tanggungjawab sebagai berikut:
   a) Pemilahan secara jelas peran-peran dalam proses pengelolaan keamanan sistem informasi yang didefinisikan dalam tugas pokok dan fungsi aparatur negara, disertai pulan dengan pendefinisian deskripsi tugas yang jelas (*job description*).
   b) Tanggungjawab dan kepemilikan yang melekat pada peran-peran dalam manajemen keamanan sistem informasi sudah didefinisikan secara formal, untuk penunjukkan terhadap perorangan ditetapkan melalui Peraturan Gubernur provinsi Jawa Timur.
   c) Mengembangkan budaya untuk memberikan penghargaan kepada staff bidang pengembangan teknologi informasi yang telah menjalankan peran dalam pengelolaan keamanan sistem informasi dengan baik sebagai suatu cara pendekatan dalam memotivasi kerja.
   d) Bila peran-peran dalam manajemen keamanan sistem informasi dilakukan secara *outsourcing*, maka harus ada kejelasan tentang tugas, tanggungjawab dan tingkat kinerja yang harus dipenuhi oleh pihak *outsourcing*, yang harus dinyatakan secara jelas dalam perjanjian kerjasama.

Pasal 7

(1) Kinerja Bidang Pengembangan Teknologi Informatka dapat diukur dengan:

a) Mendefinisikan indikator pencapaian kinerja (KPI) dan pencapaian tujuan (KGI) yang diperlukan untuk dapat memberikan indikasi keberhasilan pada pencapaian tujuan dalam rangkaian proses pengelolaan keamanan sistem informasi.

b) Melakukan kesepakatan dengan menetapkan target tingkat kinerja secara kuantitatif dari beberapa indikator yang telah didefinisikan dalam KPI dan KGI.

c) Melakukan pengawasan terhadap proses pengelolaan keamanan sistem informasi dengan melakukan pengukuran secara berkelanjutan terhadap indikator yang telah ditetapkan dalam KPI dan KGI, dan membandingkan realisasi hasil pengukuran dengan target tingkat kinerja.

d) Terkait dengan realisasi hasil pengukuran yang tidak memenuhi target tingkat kinerja, akan segera dilakukan langkah-langkah perbaikan dan penyempurnaan yang dilakukan.

BAB III
KETENTUAN PENUTUP

Pasal 8

Hal-hal yang belum diatur dalam Peraturan Gubernur ini sepanjang mengenai teknis pelaksanaannya akan diatur lebih lanjut oleh Kepala Dinas.

Pasal 9

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.
Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Jawa Timur.

Ditetapkan di Surabaya
pada tanggal

Gubernur Jawa Timur

ttd

Gubernur Jawa Timur

Halaman ini sengaja dikosongkan.

LAMPIRAN D

DOKUMEN STANDAR OPERASIONAL PROSEDUR

D. Dokumen Standar Operasional Prosedur *(Standard Operating Procedures Document)*

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	1 dari 41

PROSEDUR PENULISAN PROSEDUR OPERASI STANDAR

	Nama	Jabatan	Tanda Tangan	Tanggal
Dibuat Oleh				
Disahkan Oleh	**Nama**	**Jabatan**	**Tanda Tangan**	**Tanggal**

DAFTAR DISTRIBUSI

No.	Departemen/Bagian	Personel	Tanda Tangan	Tanggal

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	2 dari 41

CATATAN PERUBAHAN PROSEDUR PENULISAN PROSEDUR OPERASI STANDAR

Revisi ke	Tanggal	Halaman	Paragraf	Alasan	Disahkan Oleh	Fungsi / Jabatan	Tanda Tangan

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	3 dari 41

1. **TUJUAN**

   Untuk memastikan bahwa Dinas Komunikasi dan Informatika Provinsi Jawa Timur terutama Bidang Pengembangan TI mempunyai mekanisme perlindungan dalam proses pengelolaan keamanan sistem informasi secara keseluruhan, yang memadai, efektif dan efisien untuk dapat digunakan dalam aktivitas sehari-hari secara lengkap baik dalam kondisi darurat ataupun normal, atas permintaan dari pemiliki sistem yang ada.

2. **RUANG LINGKUP**

   (1) Pedoman analisis dan spesifikasi kebutuhan keamanan.
   (2) Pedoman validasi data masukan.
   (3) Pedoman pengendalian proses internal.
   (4) Pedoman validasi data keluaran.
   (5) Pedoman pengendalian operasional software.
   (6) Pedoman kontrol akses *source code* program.
   (7) Pedoman pengendalian perubahan.
   (8) Pedoman pembatasan perubahan paket *software*.
   (9) Pedoman kebocoran informasi.
   (10) Pedoman pengembangan *software* secara *outsourcing*.

(11) Pedoman kontrol kelemahan teknis.
(12) Prosedur *backup* data.
(13) Prosedur restorasi data.
(14) Prosedur penanganan *virus*.
(15) Prosedur penanganan *spam*.
(16) Prosedur penanganan *update/patch*.
(17) Prosedur penanganan serangan dari dalam.
(18) Prosedur penanganan hak akses.

3. DEFINISI

3.1 DCC : *Document Control Centre*
3.2 QMB : *Security Manual Book*
3.3 SOP : *Standard Operating Procedure*
3.4 WIS : *Working instruction*
3.5 FML : Formulir
3.6 PTI : Pengembangan Teknologi Informatika

4. REFERENSI

Gasperz, V. (2002). *ISO 9001:2000 And Continual Quality Improvement.* Jakarta: PT. Gramedia Pustaka Utama.

Buku "Training-Led-Consultancy (TLC): Quality Improvement Program", Citra Serayu Mas, Banyumas,

September 1999, Oleh Dr. Vincent Gaspersz, CFPIM, CIQA.
ISO. (2005). *ISO/IEC 17799.* Switzerland: International Standard for Organization.

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/SMB/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	5 dari 41

5. INFORMASI UMUM

5.1 Prosedur dan pedoman ini diberlakukan untuk dokumen dan/atau catatan pengendalian keamanan sistem informasi yang didistribusikan dan menjadi tanggungjawab Bagian Pengendalian Dokumen.

5.2 Penanggung jawab pelaksanaan prosedur ini adalah Kepala Bidang Pengembangan TI.

6. PEDOMAN IMPLEMENTASI

6.1 PEDOMAN ANALISIS DAN SPESIFIKASI KEBUTUHAN KEAMANAN

(1) Pertimbangan akan kontrol keamanan harus diterapkan ketika paket perangkat lunak sedang dikembangkan atau dibeli.

(2) Kebutuhan keamanan dan kontrolnya harus mencerminkan nilai bisnis dari aset informasi yang ada, disertai kerusakan proses bisnis potensial yang dihasilkan. Sebagai hasil kegagalan atau ketiadaan keamanan.

(3) Kebutuhan sistem untuk keamanan sistem informasi dan proses penerapannya harus terintegrasi dan teridentifikasi dengan rinci pada tahap awal proyek.

(4) Kontrol keamanan harus diperkenalkan pada tahap desain secara signifikan karena lebih murah daripada

menerapkannya pada saat pemeliharaan sistem atau setelah implementasi.

(5) Jika paket perangkat lunak itu dibeli, maka pengujian formal dan proses akuisisi harus diikuti.

(6) Kontrak dengan pihak pengembang harus memenuhi kebutuhan keamanan yang teridentifikasi.

(7) Jika fungsi keamanan di produk yang diusulkan tidak memenuhi kebutuhan keamanan (terkait risiko dan kontrol keamanan) yang sudah ditetapkan sebelumnya maka produk tersebut perlu dipertimbangkan terlebih dahulu sebelum dibeli.

(8) Jika ada fungsi tambahan pada sistem yang akan diberikan dan menyebabkan risiko keamanan, maka struktur pengendalian keamanan yang sudah dibuat harus ditinjau ulang untuk menentukan seberapa besar manfaat yang dihasilkan dari peningkatan fungsi tersebut.

6.2 PEDOMAN VALIDASI DATA MASUKAN

(1) Proses pengecekan atau validasi data masukan terutama pemeriksaan batasan ukuran *field* harus diterapkan pada saat transaksi *login* terjadi untuk mendeteksi kesalahan yang terjadi sebagai berikut:

a. Data yang mempunyai nilai *out-of-range*.
b. Karakter yang tidak valid dalam data.

a. Data yang hilang atau tidak lengkap.
b. Data yang melebihi batas atas dan bawah data.
c. Kontrol data yang tidak sah atau tidak konsisten.

(2) *Field* yang harus dibatasi ialah *field* yang memiliki batasan pada kisaran data yang akan dimasukkan.
(3) Peninjauan ulang secara periodik pada field kunci yang ada pada sistem informasi tersebut atau berkas data untuk mengkonfirmasi validitas dan integritas data.
(4) Memeriksa dokumen masukan yang berupa hard copy untuk mencegah perubahan yang tidak sah oleh pihak ketiga.
(5) Membuat prosedur untuk menanggapi kesalahan validasi data masukan.
(6) Mendefinisikan tanggungjawab semua karyawan yang berperan menjadi pengguna sistem terkait proses pemasukan data.
(7) Membuat catatan (*log*) aktivitas, pengguna yang terlibat dalam proses pemasukan data.
(8) Membuat mekanisme pemeriksaan atau validasi data masukan secara otomatis oleh sistem itu sendiri untuk mengurangi risiko kesalahan dan mencegah serangan *buffer overflow*, *sql injection* serta *malicious code*.

6.3 PEDOMAN PENGENDALIAN PROSES INTERNAL

(1) Pada saat tahap mendesain dan mengimplementasikan sebuah sistem informasi, pengembang harus memastikan bahwa risiko kegagalan proses pengolahan informasi yang mengarah pada hilangnya integritas data harus diminimalkan. Daerah yang harus dipertimbangkan adalah sebagai berikut:

a. Menggunakan fungsi menambah (*add*), menghapus (*delete*) dan mengupdate (*modify*) saat akan mengubah data.
b. Membuat sebuah prosedur pencegahan pada sistem informasi yang berjalan agar berjalan sesuai fungsi yang ada atau berjalan setelah mengalami kegagalan pengolahan data sebelumnya.
c. Menggunakan program utilitas yang sesuai untuk proses pemulihan (*recover*) dari kegagalan sistem.
d. Membuat sebuah mekanisme perlindungan terhadap serangan yang menggunakan teknik *buffer overflow*.

(2) Membuat sebuah mekanisme validasi pemeriksaan dampak yang dihasilkan terutama bagi proses bisnis ketika terjadi kerusakan data yang bergantung dari sifat sistem informasi itu sendiri.

(3) Membuat sebuah *checklist* yang tepat, dan semua kegiatan didokumentasikan serta hasilnya harus disimpan aman yang meliputi kegiatan sebagai berikut:
   a. Kontrol session (*session or batch control*), untuk memeriksa validasi data setelah proses update dilakukan.
   b. Kontrol keseimbangan (*balancing control*), untuk memeriksan keseimbangan jumlah data setelah proses modifikasi dilakukan meliputi: total file yang ter*update*, kontrol program ke program (*program to program controls*), dan kontrol *run-to run*.

(4) Memvalidasi mekanisme sistem data masukkan yang dihasilkan.

(5) Memeriksa integritas, keaslian atau fitur keamanan terhadap data dan sistem informasi yang digunakan meliputi fitur *upload* atau *download* berkas.

(6) Menghitung total kecacatan dari semua catatan dan berkas yang ada.

(7) Memeriksa kapabilitas sistem informasi yang digunakan untuk memastikan sistem informasi tersebut dapat dijalankan pada waktu yang tepat.

(8) Memeriksa sistem informaasi yang ada untuk memastikan bahwa sistem informasi yang dijalankan berfungsi dalam urutan yang benar.
(9) Membuat sebuah catatan (*log*) kegiatan atau aktivitas yang dilakukan oleh sistem informasi tersebut selama proses pengolahan data.

6.4 PEDOMAN VALIDASI DATA KELUARAN

(1) Menguji kewajaran data yang dihasilkan (*output*) sebuah sistem informasi.
(2) Merekonsiliasi jumlah kontrol dalam sistem informasi untuk memastikan semua data diproses dan diolah dengan benar.
(3) Memberikan informasi yang cukup bagi pengguna atau pada sistem informasi tersebut terkait pengolahan data terkait keakuratan, kelengkapan, ketepatan dan klasifikasi informasi atau data yang dihasilkan.
(4) Membuat sebuah prosedur untuk merespon pengujian validasi data keluaran.
(5) Mendefinisikan tanggung jawab semua personel yang terlibat dalam proses keluaran data.
(6) Menciptakan suatu catatan kegiatan dalam proses validasi data keluaran.

6.5 PEDOMAN PENGENDALIAN OPERASIONAL APLIKASI

(1) Proses *upgrade* sistem operasi harus dilakukan bila ada kebutuhan yang mendesak untuk melakukannya, misalnya sistem operasi yang digunakan saat ini sudah tidak mendukung kebutuhan bisnis yang ada.

(2) Perbaruan perangkat lunak, aplikasi dan perpustakaan program hanya boleh dilakukan oleh *administrator* sistem yang terlatih.

(3) Persetujuan fungsi operasional sebuah aplikasi hanya boleh dilakukan saat kode yang bersangkutan dieksekusi, bukan dikembangkan oleh kode program itu sendiri.

(4) Pengimplementasian perangkat lunak dan sistem operasi hanya boleh dilaksanakan setelah lolos dari tahap pengujian. Pengujian itu sendiri harus mencakup uji pada kegunaan, keamanan dan kemudahan sistem bagi pengguna (*user friendly*).

(5) Sistem kontrol konfigurasi harus digunakan untuk tetap mengawasi dan memonitor semua aplikasi yang sudah diimplementasikan disertai dokumentasi sistem itu sendiri.

(6) Menetapkan strategi *rollback* sebelum sebuah perubahan pada operasional aplikasi dilakukan.

(7) Mengaudit catatan (*log*) secara berkala terkait semua pembaruan perpustakaan program operasional.

(8) Mempertahankan versi perangkat lunak sebelumnya sebagai tolak ukur kontigensi.

(9) Proses *upgrade* sistem operasi harus dilakukan bila ada kebutuhan yang mendesak untuk melakukannya, misalnya sistem operasi yang digunakan saat ini sudah tidak mendukung kebutuhan bisnis yang ada.

(10) Perbaruan perangkat lunak, aplikasi dan perpustakaan program hanya boleh dilakukan oleh *administrator* sistem yang terlatih.

(11) Persetujuan fungsi operasional sebuah aplikasi hanya boleh dilakukan saat kode yang bersangkutan dieksekusi, bukan dikembangkan oleh kode program itu sendiri.

(12) Pengimplementasian perangkat lunak dan sistem operasi hanya boleh dilaksanakan setelah lolos dari tahap pengujian. Pengujian itu sendiri harus mencakup uji pada kegunaan, keamanan dan kemudahan sistem bagi pengguna (*user friendly*).

(13) Sistem kontrol konfigurasi harus digunakan untuk tetap mengawasi dan memonitor semua aplikasi yang sudah diimplementasikan disertai dokumentasi sistem itu sendiri.

(14) Menetapkan strategi *rollback* sebelum sebuah perubahan pada operasional aplikasi dilakukan.

(15) Mengaudit catatan (*log*) secara berkala terkait semua pembaruan perpustakaan program operasional.

(16) Mempertahankan versi perangkat lunak sebelumnya sebagai tolak ukur kontigensi.

(17) Menyimpan versi awal atau versi lama dari perangkat lunak, bersama dengan semua informasi yang diperlukan termasuk: parameter, prosedur, rincian konfigurasi dan perangkat lunak pendukung.

(18) Pemeliharaan perangkat lunak harus dilakukan secara berkala dan periodik yang dilakukan oleh pengembang. Dengan catatan bila institusi membeli perangkat lunak tersebut.

(19) Mempertimbangkan risiko yang akan dihadapi jika institusi tetap mengandalkan pemakaian perangkat lunak yang sudah tidak didukung dan dimaintenance oleh pihak pengembang.

(20) Mempertimbangkan keputusan untuk meng*upgrade* perangkat lunak ke versi baru yang disesuaikan kebutuhan bisnis yang dihasilkan dan struktur keamanan yang dibuat.

(21) Menggunakan software patch yang harus diterapkan untuk mengurangi kelemahan keamanan sistem.

(22) Membatasi akses fisik dan logis yang hanya diberikan kepada pengembang untuk tujuan perbaikan ketika diperlukan sesuai dengan persetujuan manajemen. Kegiatan tersebut juga harus dimonitor dan diawasi.

(23) Perangkat lunak komputer dapat mengandalkan perangkat lunak eksternal, yang harus dipantau dan dikendalikan untuk menghindari perubahan yang tidak sah dan dapat mengeksploitasi kelemahan sistem.

6.6 PEDOMAN KONTROL AKSES *SOURCE CODE* PROGRAM

(1) Mencegah akses kontrol *source code* program dapat dilakukan dengan tidak memasukkan perpustakaan (*library*) *source code* ke dalam sistem.

(2) *Source code* program dan perpustakaannya harus dikelola sesuai dengan prosedur yang diterapkan sebelumnya.

(3) Membatasi akses karyawan yang tidak memiliki kepentingan dalam pengembangan sebuah perangkat lunak.

(4) Menaruh program pada lingkungan yang aman.
(5) Memperbarui perpustakaan *source code* program dan item terkait yang dilakukan yang hanya boleh dilakukan setelah otorisasi oleh pihak manajemen.
(6) Membuat catatan audit yang harus dikelola secara berkala untuk semua akses yang menuju perpustakaan (*library*) *source code*.
(7) Melakukan pemeliharaan dan menyalin serta menyimpan perpustakaan source code program yang harus patuh pada prosedur pengendalian perubahan yang ketat.

6.7 PEDOMAN KONTROL PERUBAHAN

(1) Memelihara dan menyimpan catatan persetujuan perubahan yang telah disepakati baik oleh pengembang dan institusi.
(2) Memastikan perubahan diajukan oleh pihak yang berwenang.
(3) Meninjau kontrol dan prosedur integritas untuk memastikan bahwa mereka tidak akan berubah oleh perubahan yang dilakukan.
(4) Mengidentifikasi semua perangkat lunak, informasi, entitas *database* dan perangkat keras yang membutuhkan perubahan.

(5) Memperoleh persetujuan formal untuk proposal perubahan yang diajukan secara rinci sebelum melakukan kegiatan tersebut.

(6) Memastikan pengguna menerima dokumen perubahan secara resmi sebelum melakukan aktivitas tersebut.

(7) Memastikan dokumentasi sistem untuk diperbarui sesuai spesifikasi yang sudah ditentukan selama kegiatan perubahan dilakukan.

(8) Membuat kontrol versi dokumen untuk semua pembaruan perangkat lunak.

(9) Mempertahankan jejak audit dari semua permintaan perubahan.

(10) Memastikan bahwa dokumentasi operasional perangkat lunak dan prosedur pemakaian oleh pengguna juga diubah agar sesuai antara satu dengan yang lain.

(11) Memastikan bahwa pelaksanaan perubahan terjadi pada saat yang tepat dan tidak menganggu proses bisnis yang terlibat.

6.8 PEDOMAN PEMBATASAN PERUBAHAN PAKET *SOFTWARE*

(1) Mengidentifikasi dan menilai seluruh risiko yang muncul selama pengembangan *software*.

(2) Perangkat lunak yang dikembangkan harus memperoleh persetujuan dari pihak manajemen.
(3) Menghitung dampak yang akan dihasilkan saat institusi melakukan pemeliharaan di masa mendatang.
(4) Pengujian dan pendokumentasian harus dilakukan ketika proses pengembangan *software* sedang dilaksanakan. Sehingga dapat digunakan kembali jika diperlukan pembaruan di masa depan.
(5) Perubahan *software* hendaknya dilakukan pada software yang sudah disalin, bukan menggunakan software yang asli.
(6) Perubahan akan dapat dilakukan pada perangkat lunak setelah mendapat persetujuan dari pihak manajemen terkait penggunaan versi yang terbaru.
(7) Diperlukan pengujian dan validasi hasil pengujian terkait dengan modifikasi yang dilakukan oleh suatu badan independen (auditor eksternal).

6.9 PEDOMAN KEBOCORAN INFORMASI

(1) Pemindaian terhadap media penyimpanan yang digunakan dan komunikasi yang ada harus dilakukan untuk menemukan data atau informasi yang tersembunyi.

(2) Menggunakan teknik masking dan modulasi sistem informasi yang ada untuk mengurangi kemungkinan pihak ketiga dapat memperoleh informasi atau data yang *ada pada sistem informasi tersebut.*

(3) Melakukan pemantauan terhadap semua karyawan yang ada dan kegiatan sistem dibawah peraturan dan perundang – undangan yang berlaku.

6.10 PEDOMAN PENGEMBANGAN *SOFTWARE* SECARA *OUTSOURCING*

(1) Pihak pengembang harus mempunyai sertifikasi kualitas, kode etik yang dipatuhi, dan hak kekayaan intelektual yang terdaftar secara resmi.

(2) Memberikan hak akses kepada institusi untuk melakukan audit kualitas dan menilai keakuratan pekerjaan yang dilakukan oleh pihak pengembang.

(3) Membuat sebuah kontrak perjanjian yang mensyaratkan akan kualitas fungsional dari sistem informasi yang akan dibuat dan keamanan dalam setiap kode sistem informasi yang dikembangkan.

(4) Melakukan pengujian sebelum mengimplementasikan sistem informasi yang sudah selesai dikembangkan.

(5) Mendokumentasikan hasil pengujian dan memberikannya kepada pihak institusi agar dapat divalidasi.

6.11 PEDOMAN KONTROL KELEMAHAN TEKNIS

(1) Institusi harus mendefinisikan dan menetapkan peran serta tanggung jawab yang terkait dengan manajemen penanganan kelemahan teknis termasuk di dalamnya kegiatan pemantauan kelemahan, penilaian risiko keamanan, pelacakan aset dan penggunaan *patch* disertai koordinasi setiap orang di dalam institusi.

(2) Informasi sumber daya yang akan digunakan untuk mengidentifikasi kelemahan teknis terkait sistem informasi yang ada.

(3) Mendefinisikan kerangka waktu terhadap reaksi yang dilakukan untuk menangani kelemahan teknis yang berpotensi menghasilkan dampak yang besar.

(4) Mengidentifikasi risiko yang muncul setelah identifikasi kelemahan sistem informasi sudah dilakukan dan tindakan yang dapat diambil untuk menangani risiko tersebut.

(5) Mematikan layanan atau kemampuan sistem informasi yang terkait dengan kelemahan sistem itu sendiri.

(6) Mengadaptasi atau menambahkan kontrol akses seperti *firewall*, pembatasan jaringan, dll.

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/SOP/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	20 dari 41

(7) Menggunakan program utilitas lain untuk mendeteksi atau mencegah serangan yang akan muncul (*intrusion detection system*).

(8) Membuat sebuah catatan terhadap semua prosedur yang sudah dilakukan.

(9) Proses penanganan manajemen kelemahan teknis harus dipantau secara teratur dan dievaluasi oleh pihak manajemen untuk memastikan efektivitas dan efisiensi.

(10) Penanganan terhadap sistem yang memiliki risiko yang tinggi harus dilakukan terlebih dahulu.

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/SOP/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	21 dari 41

7. PROSEDUR

7.1 PROSEDUR *BACKUP* DATA

(1) Bidang Pengembangan Teknologi Informatika perlu menetapkan strategi *backup* data yang dilakukan dengan mempertimbangkan kebutuhan bisnis dan *continuity plan*, yang terdiri atas *full backup* dan *incremental backup*.

(2) Penjadwalan kegiatan *backup* data dilakukan secara mingguan, yang ditetapkan dengan mempertimbangkan kebutuhan bisnis yang tertuang dalam tingkat mutu layanan yang telah ditetapkan oleh Kepala Dinas terkait dengan layanan masyarakat, tingkat kompleksitas data, tingkat perubahan data, jumlah data, dan kapabilitas *administrator* sistem.

(3) Melakukan kegiatan *backup* data yang dilakukan secara periodik sesuai dengan penjadwalan yang telah ditetapkan sesuai dengan strategi yang telah ditetapkan maupun atas permintaan tertentu dari pemilik data.

(4) Aktivitas *backup* dilakukan dengan menggunakan alat bantu berupa program utilitas yang merupakan standar yang telah ditetapkan institusi, dalam rangka khusus menangani *backup data*.

(5) Media backup yang digunakan mempertimbangkan kapasitas penyimpanan, metode akses, daya tahan media penyimpanan, dan kepraktisan dalam penyimpanan.

(6) Pengaturan lokasi penyimpanan terhadap media *backup* ditentukan dengan mempertimbangkan kebutuhan penarikan data (*data retrieval*), efektifitas biaya, integritas data yang berkelanjutan dan kebutuhan keamanan terhadap berbagai bentuk ancaman baik akibat bencana alam maupun gangguan lainnya.

(7) Untuk mengurangi tingkat risiko maka lokasi penyimpanan *backup* dilakukan secara *dual location*, yaitu di lokasi *onsite* dan *offsite*.

(8) Pengaturan periode penyimpanan ditentukan sedemikian rupa dengan mempertimbangkan beberap hal, meliputi nilai data, masa manfaat data, dan kebutuhan legal.

(9) Memelihara secara sistematis inventori terhadap media dan menjamin penggunaan serta integritas dari media penyimpanan yang digunakan.

(10) Melakukan evaluasi secara periodik dengan melakukan rekonsiliasi antara kejadian aktual dan yang tercatat pada dokumentasi untuk ditindaklanjuti bila ditemui kejanggalan.

(11) Identifikasi eksternal sesuai standar yang ada, terhadap semua media penyimpanan dan melakukan pengendalian pergerakan fisik media untuk mendukung akuntabilitas.

(12) Memastikan perlindungan yang memadai terhadap objek data yang sedang dalam proses pengiriman (*transmission and transport*) dari akses pihak yang tidak berhak (*unauthorized access*), modifikasi dan salah alamat.

(13) Permasalahan teknis yang timbul selama proses backup data dilaporkan oleh *administrator* sistem kepada setiap kepala seksi.

7.2 PROSEDUR RESTORASI DATA

(1) Restorasi data dapat dilakukan sesuai dengan permintaan dari pemilik data.

(2) *Administrator* sistem melakukan pencatatan waktu yang diperlukan pada setiap kegiatan restorasi data secara lengkap, untuk dilakukan perhitungan rata-rata waktu restorasi.

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/SOP/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	24 dari 41

(3) Melakukan pengujian aktivitas restorasi yang dilakukan terhadap media penyimpanan secara periodik disesuaikan dengan kebutuhan bisnis dan tingkat risiko terhadap keberadaan objek data, untuk dapat memastikan bahwa media penyimpanan tersebut masih dapat dibaca dan data yang tersimpan memenuhi kriteria integritas.

(4) Melakukan evaluasi secara periodik dengan melakukan rekonsiliasi antara kejadian yang terjadi di lapangan dan yang ada pada catatan untuk ditindaklanjuti bila ditemui kejanggalan.

(5) Memastikan perlindungan yang memadai terhadap objek data yang sedang dalam proses pengiriman (*transmission and transport*) dari akses pihak yang tidak berhak (*unauthorized access*), modifikasi dan salah alamat.

7.3 PROSEDUR PENANGANAN *VIRUS*

(1) Mengisolasi dan memutus koneksi jaringan

a. Hal pertama yang dapat dilakukan apabila Anda merasa atau mengetahui telah terinfeksi virus adalah dengan memutus koneksi fisik komputer Anda dari jaringan.

MILIK PERPUSTAKAAN ITS

b. Dengan asumsi bahwa komputer Anda yang membawa virus dan menyebarkan ke jaringan atau sebaliknya komputer Anda terkena virus dari jaringan.

c. Tetaplah memutus koneksi dari jaringan sampai dilakukan penghapusan virus tersebut dari komputer Anda atau sebaliknya dari jaringan.

(2) Menghapus virus

a. Setelah komputer diisolasi dan diputuskan dari jaringan, maka lakukan penghapusan program virus tersebut dengan menggunakan program antivirus yang spesifik dapat menangani virus tersebut.

b. Menghapus program virus tersebut hanya pada berkas yang terinfeksi tidaklah cukup. Karena banyak virus yang mengkopi dirinya menjadi banyak rupa dan bersembunyi di berbagai tempat, dan menginfeksi program dan dokumen lain. Maka cara untuk memperbaikinya adalah dengan menjalankan program utilitas penghapus yang dikhususkan untuk virus tersebut.

(3) Mengembalikan data

Banyak akibat yang ditimbulkan dari serangan virus mulai dari penamaan ulang sampai penghapusan berkas - berkas yang penting. Setelah virus dihapus maka dapat dilakukan:

a. Instal ulang program

Beberapa virus dapat menghancurkan sistem operasi, untuk itu gunakanlah CD instalasi ulang cepat sistem operasi berdasarkan kondisi sistem sebelum terkena virus. Untuk menginstal kembali aplikasi-aplikasi yang ada maka diperlukan lisensi aplikasi untuk registrasi ulang.

b. Periksa infeksi virus

Setelah sistem berjalan seperti semula, maka lakukanlah pemeriksaan akan virus secara menyeluruh terhadap semua berkas dan dokumen yang ada pada komputer tersebut. Begitupula dengan yang ada pada semua komputer di jaringan termasuk *server*.

c. Kembalikan berkas-berkas

Kehilangan berkas – berkas data tergantung pada jenis serangan dari virus tersebut. Apabila virus tersebut menyerang program aplikasi maka file-file data dapat tidak terserang. Namun seringkali juga virus menyebabkan kehilangan berkas data, dan kehilangan tidak dapat dihindari.

d. Dokumentasikan proses
Dokumentasikan langkah-langkah yang Anda lakukan dalam memperbaiki sistem, mencakup file dan aplikasi mana yang Anda kembalikan dan metode yang digunakan. Apabila ada hal-hal tidak diinginkan dapat dilacak ulang, atau dapat juga digunakan untuk referensi apabila terjadi serangan serupa.

(4) Cegah infeksi

a. Penting untuk memakai perangkat lunak *antivirus* dan selalu *update* definisi *virus*nya. Apabila belum memakai anti-virus, mulailah dari sekarang. Apabila sudah, segeralah update definisi *virus*nya. Kemudian *instal update/patch* yang dibutuhkan oleh sistem operasi dan seluruh aplikasi yang ada untuk menutup semua kemungkinan lubang keamanan.

b. Kemudian, ubahlah semua *password*, termasuk *password* akses ke ISP, FTP, *e-mail*, dan situs *web*. Beberapa program *virus* dapat menangkap *password* Anda atau membongkarnya, sehingga dapat disalahgunakan penciptanya. Mengganti password adalah penting.

Semua data berharga yang ada di komputer sebaiknya diberi *password*, dan sebaiknya dibuat atau diganti saat ini. *Password* setidaknya 8 karakter, kombinasi dari huruf besar atau kecil, angka, simbol, dan tanda-tanda huruf lain. Hindari menggunakan kata-kata yang mudah dikenali, frase dan juga nama.

(5) Belajar dari kesalahan

a. Walaupun serangan virus dapat disembuhkan, serangan yang telah terjadi dapat digunakan untuk mengevaluasi penerapan keamanan saat ini. Jika saat ini *virus* masuk, kemungkinan akan datang juga bisa. Penting untuk evaluasi ukuran-ukuran keamanan Anda, bila ada, dan mengapa tidak efektif.

7.4 PROSEDUR PENANGANAN *SPAM*

(1) Gunakan perangkat lunak pemfilter atau pemblokir *e-mail spam*.

(2) Jangan membalas *e-mail* yang tidak dikenal atau yang seperti ciri-ciri spam. Dengan dibalas maka pengirim *spam* akan yakin akan keberadaan *e-mail* Anda, dan mengakibatkan semakin banyak lagi *e-mail spam* ke *inbox* Anda.

(3) Jangan sekalipun mengirimkan informasi - informasi pribadi ke suatu situs *web* yang tidak aman (situs yang aman akan ditandai dengan tanda gembok biasanya berwarna kuning di kanan bawah/atas *browser*).

(4) Jangan sekalipun mengirim alamat *e-mail* melalui ruang *chat*, *instant message*, atau forum *internet* dan *newsgroup*.

(5) Canangkanlah secara tertulis aturan institusi mengenai *email* dan pastikan semua pegawai membacanya. Beri petunjuk mengenai bagaimana mengatasi *e-mail* yang tidak wajar. Aturan tersebut harus mencantumkan apakah dibolehkan untuk mendaftar ke *newsletter* atau situs *web* yang membutuhkan *e-mail*. Pastikan semua pegawai menandatangani aturan tersebut.

(6) Jangan menampilkan link langsung dari alamat e-mail pada situs *web*. Melainkan tampilkan dalam bentuk yang program tidak dapat membacanya. Program yang dikenal namanya "*spambots*" selalu mencari situs-situs *web* untuk apa saja yang memiliki tanda "@". Salah satu cara untuk menampilkannya adalah dengan menggunakan tanda "[at]" sebagai pengganti "@".

(7) Pastikan firewall dikonfigurasi untuk memblokir semua lalu lintas data yang tidak diinginkan.

(8) Doronglah karyawan yang lain untuk tidak menggunakan *mailing list*, terutama yang tidak dikenal kredibilitasnya, karena seringkali digunakan *spammers* untuk memastikan kebenaran suatu alamat *e-mail*.

(9) Laporlah ke ISP terkait alamat-alamat *e-mail* yang digunakan *spammers* untuk menyebarkan *spam*. Dengan melaporkan ke ISP, secara tidak langsung dapat membantu meringankan *bandwidth* jaringan yang habis digunakan *spam* untuk menyebarkan diri.

7.5 PROSEDUR PENANGANAN *UPDATE/PATCH*

(1) Selalu berhubungan dengan pengembang perangkat lunak. Banyak pengembang perangkat lunak menyediakan fasilitas notifikasi ke pelanggan mereka, disamping mereka juga menampilkan informasi mengenai *update* dan *patch* di situs *web* mereka. Lakukanlah pengecekan ini secara rutin.

(2) Tentukan tingkat kedaruratan dari kelemahan tersebut. Kebijakan manajemen *patch* yang baik sebaiknya menjelaskan proses yang diambil untuk dapat mengidentifikasi dan menerapkan *patch*, dan yang bertanggungjawab pada setiap langkah ini dalam alur kerja. Langkah pertama pada proses ini adalah menetapkan profil dari masing-masing aplikasi yang Anda gunakan, biasanya menggambarkan sensitivitas aplikasi tersebut.

(3) Apabila memungkinkan, sebaiknya dipisahkan antara pemeriksa dan pelaksana. Tujuannya agar saling cek satu sama lain, dan juga meminimalkan bias yang mungkin ditimbulkan dari masing-masing pihak.

(4) Masukkan semua prosedur manajemen *patch* dalam tulisan. Tetapkan secara jelas semua tanggunjawab manajemen *patch*, misalnya identifikasi kerawanan, evaluasi dan uji *patch*, serta implementasi *patch*. Dokumentasikan semua keputusan untuk menginstal atau tidak *patch* yang ada.

(5) Uji, uji, dan uji lagi. Kadangkala *patch* juga dapat mengakibatkan masalah keamanan baru. Sebelum Anda menerapkan *patch* ke sistem utama yang berjalan, terapkanlah terlebih dahulu pada lingkungan pengujian untuk memastikan *patch* tersebut tidak membuka kerawanan yang telah ditutup sebelumnya atau malah membuka kerawanan baru. Banyak kejadian buruk yang menceritakan bahwa sistem tidak berfungsi lagi setelah menerapkan *patch*.

(6) Urutan pertama diinstal pertama. Pada kerawanan yang membutuhkan beberapa *patch*, penting untuk menginstal *patch* sesuai urutan instalnya.

(7) Pertimbangkan layanan pihak ketiga. Apabila manajemen *patch* terasa terlalu membebani sumberdaya institusi maka pertimbangkanlah untuk mencari layanan identifikasi dan manajemen *patch* yang dapat mengurangi biaya dan *overhead* yang disebabkan oleh manajemen *patch*.

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/SOP/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	33 dari 41

7.6 PROSEDUR PENANGANAN *SERANGAN DARI DALAM*

(1) Susunlah aturan keamanan yang efektif. Gunakanlah untuk mendaftarkan aset informasi institusi dan semua akses ke informasi tersebut. Pastikan semua anggota mengerti akan aturan tersebut. Beri pembelajaran pada mereka mengenai risiko yang dapat terjadi apabila membolehkan akses ke akun dan *password* mereka. Peringatkan akan bahayanya *social engineering*, dimana penyusup mencari akses yang tidak berhak ke informasi dengan meningkatkan kewaspadaan mereka. *E-mail* yang terlihat seperti berasal dari teman, namun di dalamnya *terdapat executable attachment* yang berisi *virus*, adalah merupakan contoh *social engineering* yang umum. Untuk itu harus dapat ditingkatkan kewaspadaan akan serangan seperti ini.

(2) Pastikan pegawai mendapat akses hanya ke data dan sistem yang mereka butuhkan. Hal ini terdengar sederhana, adalah tidak wajar apabila seorang pegawai membutuhkan akses berkali-kali lebih besar dari yang ia butuhkan. Apabila diperlukan, dapat diterapkan pembatasan akses dengan menggunakan perangkat lunak kontrol akses.

(3) Apabila dibutuhkan kerjasama dengan pihak luar seperti rekanan yang memerlukan akses ke jaringan, pastikan akses tersebut dibatasi hanya pada kegiatan yang dibutuhkan. Ketika menetapkan tingkat akses, pastikan bahwa tiap tingkat tersebut tidak memberikan kebocoran pada aset yang lebih berharga.

Salah satu caranya adalah dengan memberikan rekanan tersebut akun yang dapat kadaluarsa secara otomatis pada tanggal yang sama dengan saat kontrak selesai, kecuali apabila diperpanjang.

7.7 PROSEDUR PENANGANAN HAK AKSES

(1) Mengatur akses ke sistem informasi melalui mekanisme *authentication* dan *access control.*

(2) Pemakai harus melalui proses *authentication* dengan menuliskan userid (*user identification*) dan *password.*

(3) Apabila keduanya valid, maka pemakai diperbolehkan untuk masuk dan menggunakan sistem, tetapi apabila di antara keduanya atau salah satunya tidak valid, maka akses akan ditolak.

(4) Penolakan ini tercatat dalam berkas log berupa waktu dan tanggal akses, asal hubungan (*connection*) dan berapa kali koneksi yang gagal itu.

(5) Pemakai diberikan akses sesuai dengan *level* yang dimilikinya melalui sebuah *access control*.

8.1 JADWAL PEMELIHARAAN (MAINTENANCE)

(1) Pekerjaan *Maintenance Support and Service* dilaksanakan berdasarkan jadwal pemeliharaan yang sudah ditetapkan dengan Kepala Bidang Pengembangan TI memiliki kriteria sebagai berikut:
   a. Minimal 1 bulan atau 2 bulan.
   b. Minimal 6 bulan atau 1 tahun.

(2) Setelah tercipta adanya kesepakatan terkait masa kerja yang dituangkan di dalam perjanjian nota kesepahaman, barulah terwujud akan adanya pekerjaan *maintenance support*.

(3) Dalam pelaksanaan *maintenance support* di lapangan, yang akan melakukan pekerjaan tersebut adalah *administrator* sistem. Pekerjaan *maintenance support* disesuaikan dengan waktu jam kerja .

(4) Apabila dalam jadwal pelaksanaan *maintenance support* terdapat hari libur nasional, maka pekerjaan tersebut akan diliburkan pula kecuali untuk kasus – kasus tertentu yang bersifat mendesak.

(5) Pekerjaan *maintenance support* yang terjadwal berlangsung selama sekali/beberapa kali dalam satu minggu dan setiap pekerjaan memakan waktu selama ± 1-5 jam.

(6) **Dalam melaksanakan setiap pekerjaan *maintenance support*, *administrator* sistem wajib mendokumentasikan hasil perkerjaannya tersebut ke supervisor agar memiliki arsip yang sewaktu-waktu akan diperlukan, dan** untuk memastikan media penyimpanan dapat dibaca kembali dan memenuhi kriteria integritas data.

8.2 PENGAWASAN KINERJA DAN INSPEKSI

Aktivitas pengelolaan keamanan sistem informasi akan dimonitor dan diinspeksi oleh supervisor yang juga bertanggungjawab untuk penugasan pekerjaan. Apabila ditemukan ketidaksesuaian baik disengaja maupun yang tidak disengaja sehingga menyebabkan kegagalan sistem, maka diambil langkah – langkah perbaikan selanjutnya sesuai dengan kebutuhan.

8.3 PENGUKURAN, ANALISIS DAN PENINGKATAN

(1) Mengidentifikasi proses – proses pengukuran yang penting yang ditetapkan oleh pihak manajemen.

(2) Menggunakan data guna meyakinkan suatu jaminan terhadap kesesuaian produk dan sistem manajemen keamanan, serta meningkatkan terus – menerus efektivitas dari sistem.

(3) Menentukan apakah memerlukan penggunaan teknik – teknik atau alat – alat statistikal.

(4) Memelihara kepuasaan pelanggan dalam hal ini masyarakat.

(5) Melakukan audit keamanan sistem informasi internal oleh administrator sistem.

(6) Melaporkan hasil – hasil audit kepada Kepala Bidang Pengembangan TI sebagai orang yang berwenang atau bertanggung jawab.

(7) Memantau proses audit guna menjamin bahwa proses itu tetap memiliki kapabilitas.

(8) Memantau proses audit guna menjamin bahwa proses itu tetap memiliki kapabilitas.

(9) Memisahkan sistem informasi yang cacat agar tidak tercampur dengan sistem informasi yang memiliki kondisi baik.

(10) Memetakan kebutuhan perbaikan baik dalam tindakan maupun strategi penanganan sistem informasi yang cacat.
(11) Mengumpulkan data, melakukan analisis data dan memetakan serta menginterpretasikan tentang hal – hal yang penting terkait dengan kecacatan sistem informasi tersebut.
(12) Melakukan peningkatan terus – menerus.
(13) Mengidentifikasi masalah aktual dan masalah potensial yang ada.
(14) Mengidentifikasi penyebab masalah tersebut terjadi.
(15) Menguji dan memvalidasi kebutuhan peningkatan terus – menerus agar tetap berlangsung.

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR	
Prosedur: Penulisan Prosedur Operasi Standar	No. Dokumen	DCC/FML/PTI/001
	Edisi	01
	Revisi	00
	Berlaku Efektif	
	Halaman	40 dari 41

FORMULIR RENCANA TINDAKAN PERBAIKAN 5W-2H

Nama karyawan:
Topik program:
Lama program (Minggu):
Waktu awal program (Tanggal-Bulan-Tahun):
Waktu akhir program (Tanggal-Bulan-Tahun):

Apa (What)	Dimana (Where)	Bilamana (When)	Mengapa (Whom)	Siapa (Who)	Bagaimana (How)	Biaya (How much)

	DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR		
Prosedur: Penulisan Prosedur Operasi Standar		No. Dokumen	DCC/FML/PTI/001
		Edisi	01
		Revisi	00
		Berlaku Efektif	
		Halaman	41 dari 41

FORMULIR PEMERIKSAAN HASIL – HASIL PENINGKATAN KEAMANAN

Nama karyawan:
Topik program:
Lama program (Minggu):
Waktu awal program (Tanggal-Bulan-Tahun):
Waktu akhir program (Tanggal-Bulan-Tahun):

No.	Karakteristik Keamanan	Performansi Awal Program	Tindakan Perbaikan yang Dilakukan	Performansi Akhir Program	Dampak Positif dari Program

Halaman ini sengaja dikosongkan.

LAMPIRAN E

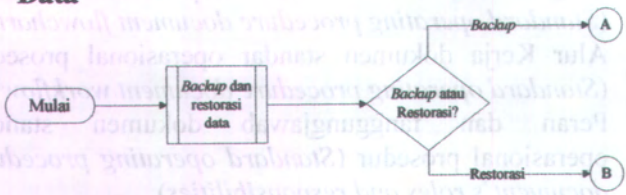
ALUR KERJA STANDAR OPERASIONAL PROSEDUR

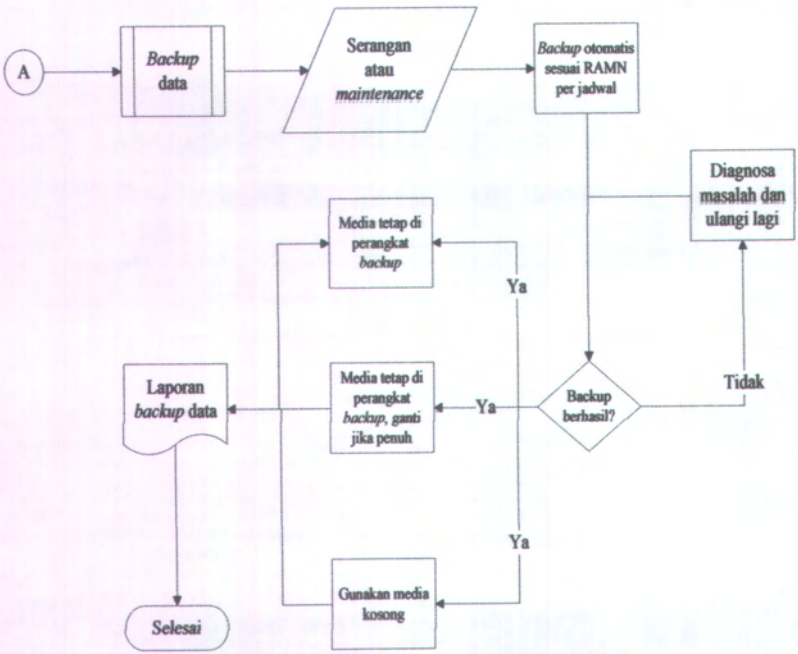
E. Alur Kerja Standar Operasional Prosedur *(Standard Operating Procedures Document Workflow)*

1. Diagram kerja dokumen standar operasional prosedur (*Standard operating procedure document flowchart*)
2. Alur Kerja dokumen standar operasional prosedur (*Standard operating procedure document workflow*)
3. Peran dan tanggungjawab dokumen standar operasional prosedur (*Standard operating procedure document's roles and responsibilities*)

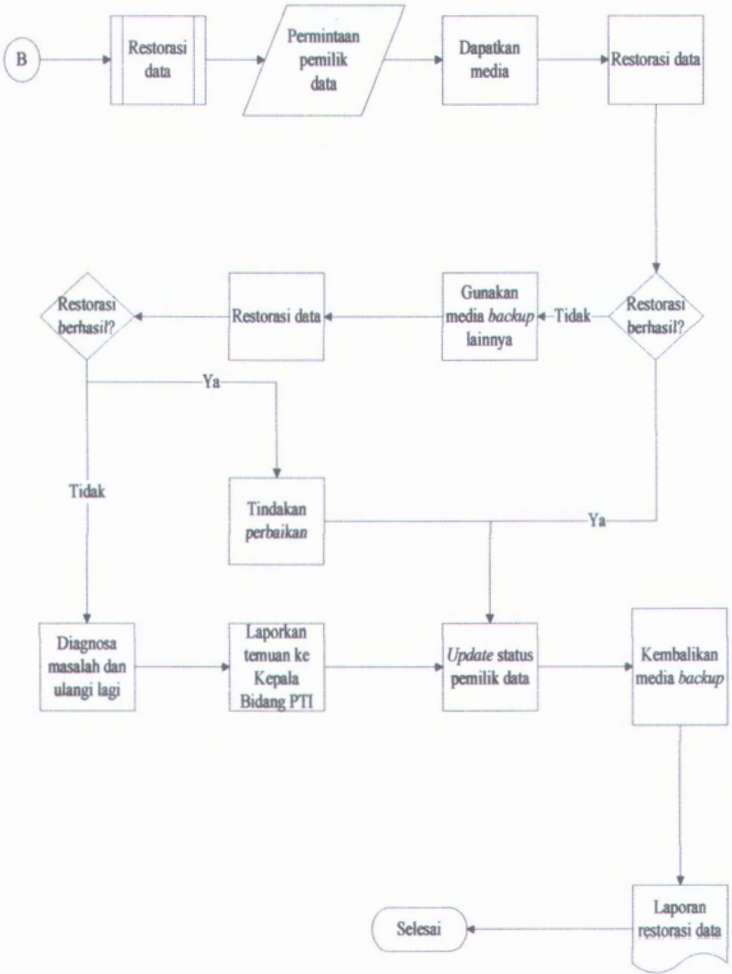
E.1 Diagram Kerja Standar Operasional Prosedur

E.1.1 Diagram Kerja Prosedur Backup dan Restorasi Data



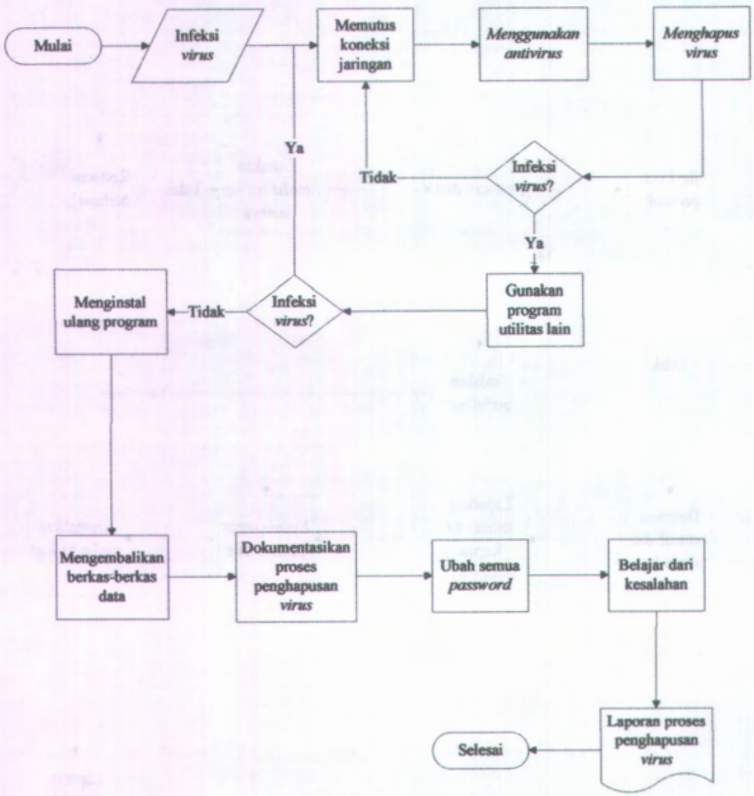


Gambar E.1 *Flowchart* Prosedur *Backup* Data



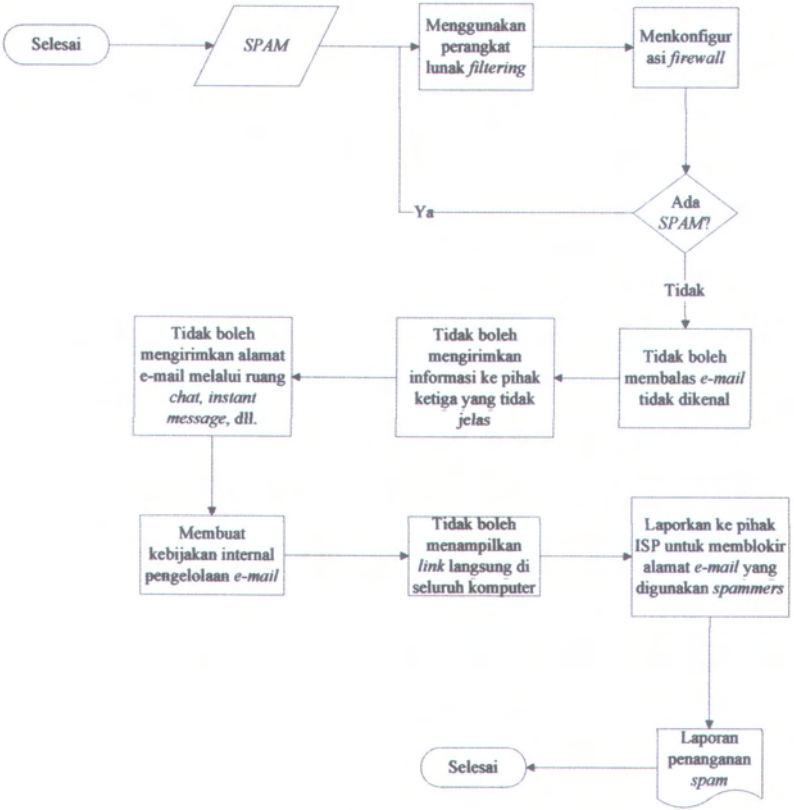
Gambar E.2 *Flowchart* Prosedur Restorasi Data

E.1.2 Diagram Kerja Prosedur Penanganan *Virus*



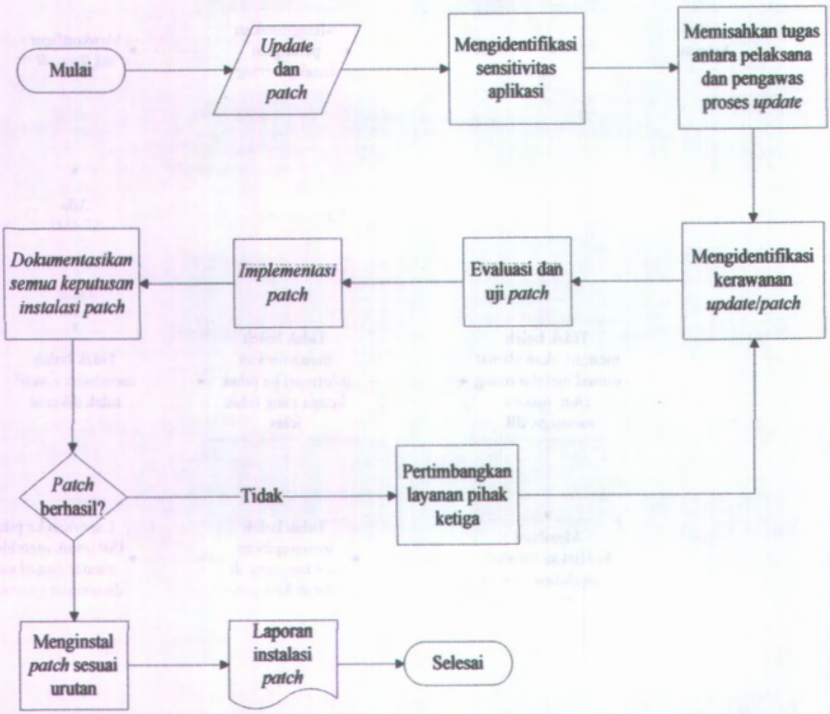
Gambar E.3 *Flowchart* Prosedur Penanganan *Virus*

E.1.3 Diagram Kerja Prosedur Penanganan *Spam*



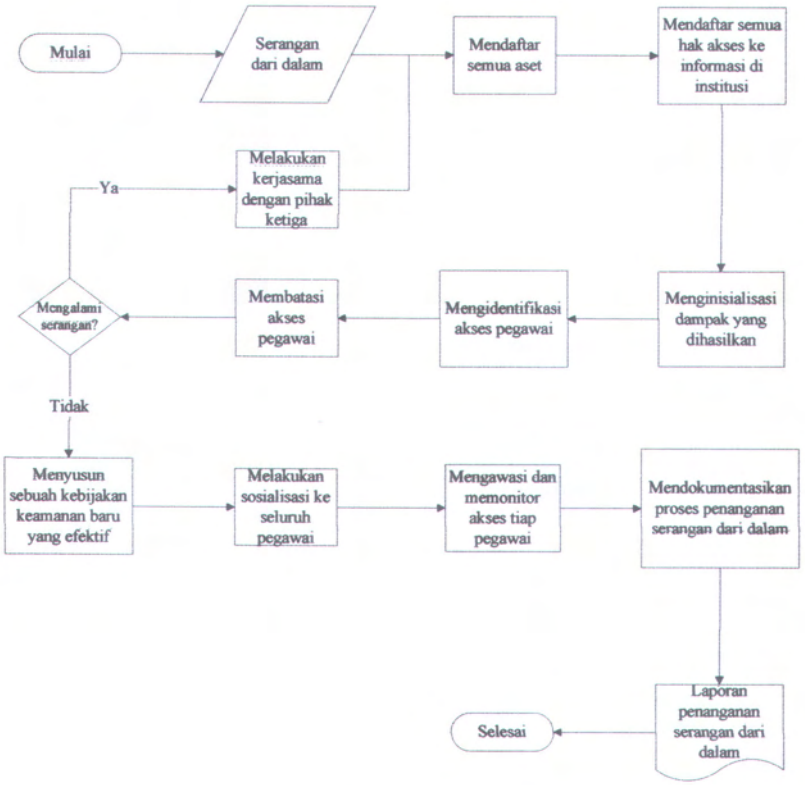
Gambar E.4 *Flowchart* Prosedur Penanganan *Spam*

E.1.4 Diagram Kerja Prosedur Penanganan *Update/patch*



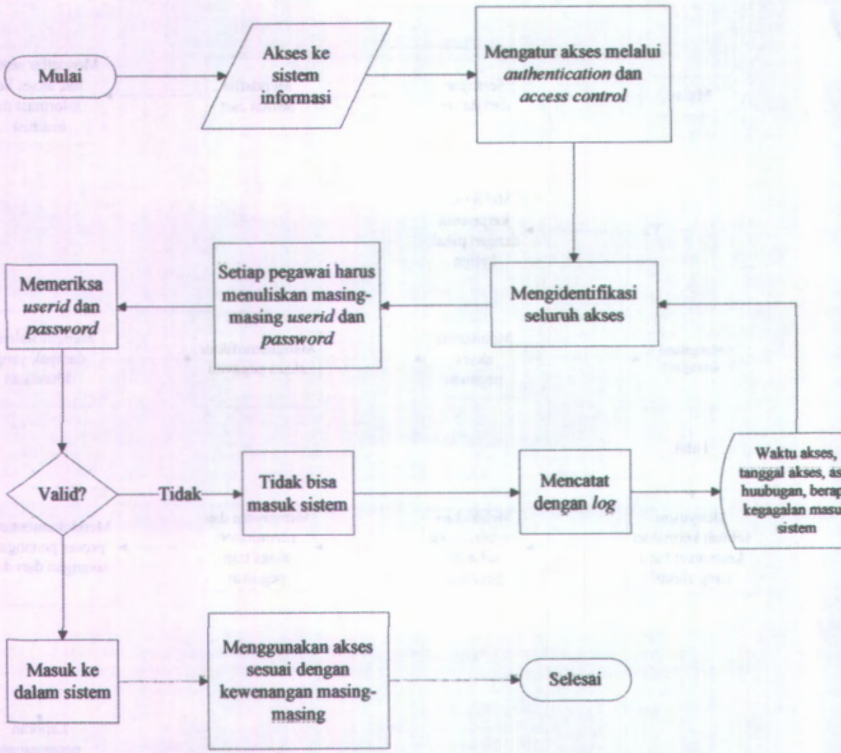
Gambar E.5 *Flowchart* Prosedur Penanganan *Update/Patch*

E.1.5 Diagram Kerja Prosedur Penanganan Serangan Dari Dalam



Gambar E.6 *Flowchart* Prosedur Penanganan Serangan Dari Dalam

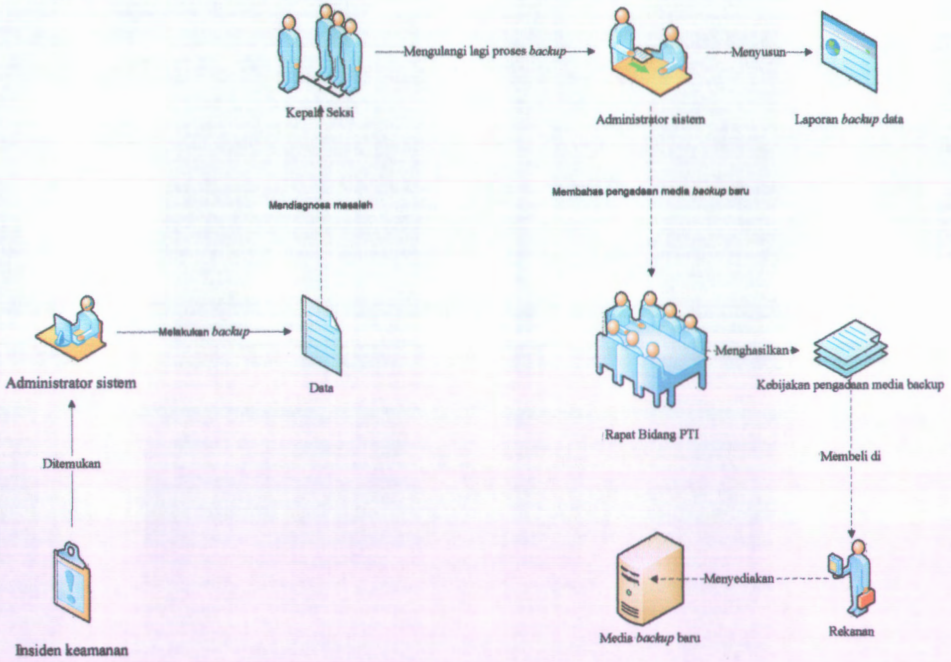
E.1.6 Diagram Kerja Prosedur Penanganan Hak Akses



Gambar E.7 *Flowchart* Prosedur Penanganan Hak Akses

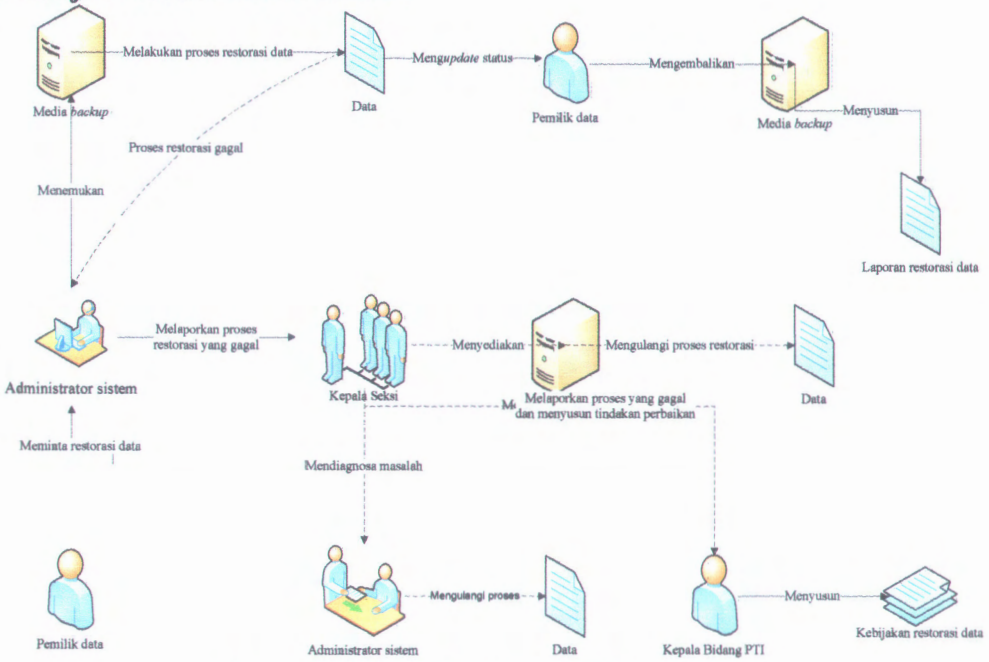
E.2 Alur Kerja Dokumen Standar Operasional Prosedur

E.2.1 Alur Kerja Prosedur *Backup* Data



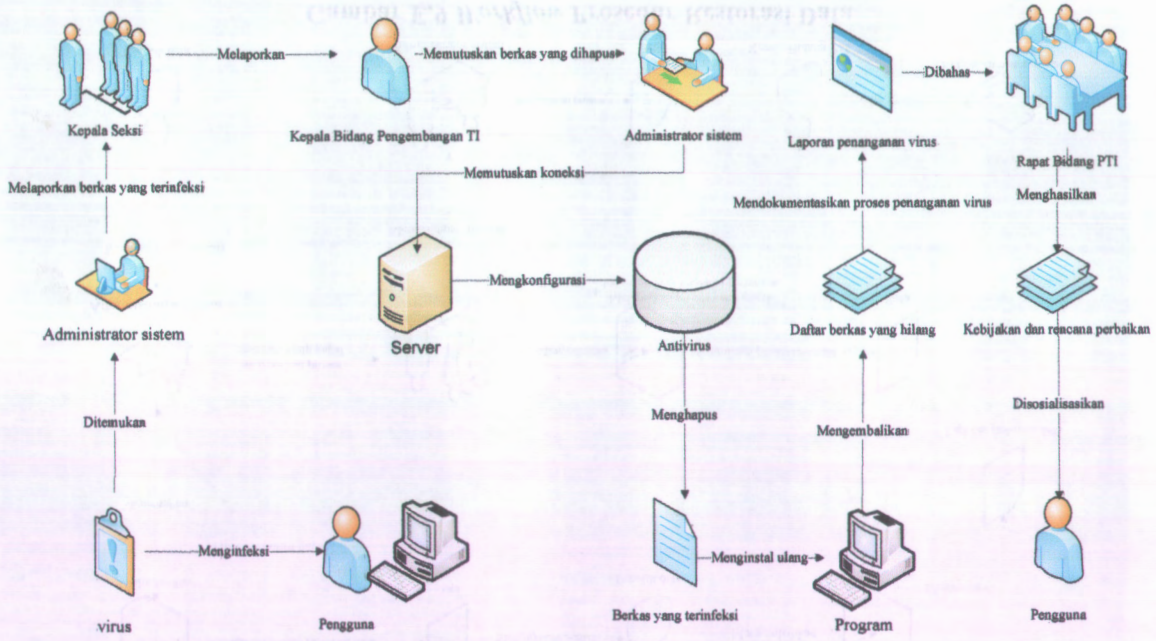
Gambar E.8 *Workflow* Prosedur *Backup* Data

E.2.2 Alur Kerja Prosedur Restorasi Data



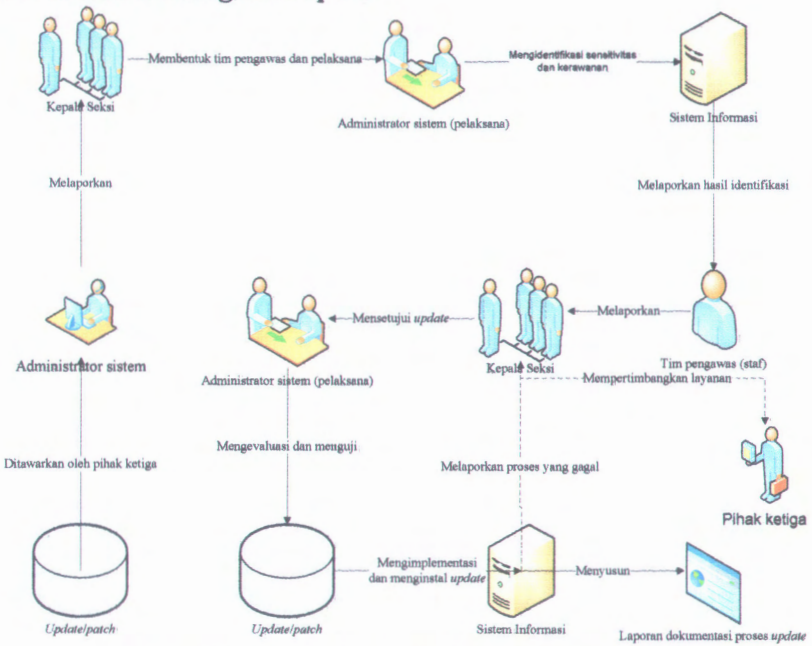
Gambar E.9 *Workflow* Prosedur Restorasi Data

E.2.3 Alur Kerja Prosedur Penanganan *Virus*



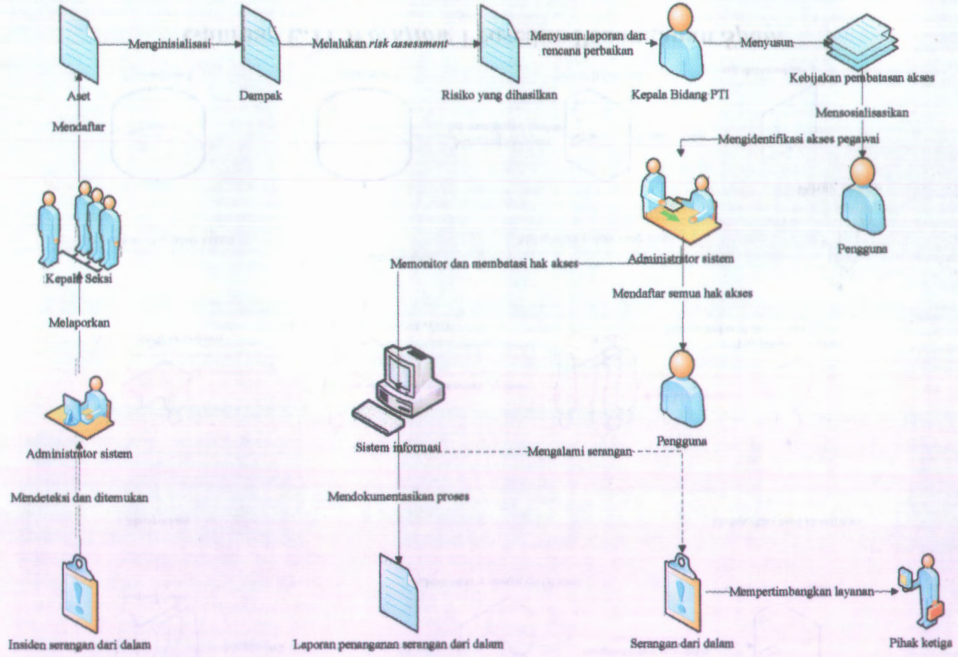
Gambar E.10 *Worflow* Prosedur Penanganan *Virus*

E.2.4 Alur Kerja Prosedur Penanganan *Spam*



Gambar E.11 *Workflow* Prosedur Penanganan *Spam*

E.2.5 Alur Kerja Prosedur Penanganan Serangan Dari Dalam



Gambar E.11 *Workflow* Prosedur Penanganan Serangan Dari Dalam