ANALISIS KEPATUHAN KARYAWAN TERHADAP KEBIJAKAN PENGAMANAN DATA PADA PT XYZ DENGAN STANDAR COBIT 5

TUGAS AKHIR

DIMAS ARYO ANGGORO

1102001019

PROGRAM SARJANA STRATA 1

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN ILMU KOMPUTER

UNIVERSITAS BAKRIE

JAKARTA

2014

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri,
Dan semua sumber baik yang dikutip maupun dirujuk
Telah saya nyatakan dengan benar

Nama	**: DIMAS ARYO ANGGORO**
NIM	**: 1102001019**
Tanda Tangan	**:**
Tanggal	**: 21 Juli 2014**

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh

Nama : Dimas Aryo Anggoro

NIM : 1102001019

Program Studi : Teknik Informatika

Fakultas : Teknik dan Ilmu Komputer

Judul Skripsi : Analisis Kepatuhan Karyawan terhadap Kebijakan Pengamanan Data pada PT XYZ dengan Standar COBIT 5

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer Universitas Bakrie.

DEWAN PENGUJI

Pembimbing : Refyul Rey Fatri, M.Sc., Ph.D. (……)

Penguji I : Berkah I. Santoso, S.T., M.T.I. (……)

Penguji II : Yudhiansyah Ahmadin, S.T., M.T.I. (……)

Ditetapkan di : Jakarta

Tanggal : 21 Juli 2014

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik dan tepat waktu. Dalam penyusunan Tugas Akhir ini tentunya tidak lepas dari bantuan dan dorongan dari berbagai pihak. Tanpa bantuan dan dorongan dari berbagai pihak, Tugas Akhir ini tidak dapat terselesaikan dengan baik dan tepat waktu. Ucapan terima kasih penulis haturkan kepada :

1. Mama dan Papa yang telah memelihara, mendidik, dan memberikan kasih sayang kepada penulis dari kecil hingga saat ini.
2. Adik Sareh Prasetyo Aji yang telah menjadi teman bagi penulis dari kecil hingga saat ini.
3. Keluarga besar penulis yang selalu memberikan dukungan dan kasih sayang kepada penulis.
4. Bapak Refyul Rey Fatri, M.Sc., Ph.D. selaku dosen pembimbing yang telah memberikan arahan dan bimbingan kepada penulis selama penyusunan Tugas Akhir.
5. Bapak Berkah I. Santoso, S.T., M.T.I. selaku dosen pembahas dan penguji yang telah memberikan bimbingan kepada penulis dalam penyusunan Tugas Akhir.
6. Bapak Yudhiansyah Ahmadin, S.T., M.T.I. selaku dosen penguji yang telah memberikan revisi kepada penulis dalam penyusunan Tugas Akhir.
7. Para dosen Program Studi Teknik Informatika dan Sistem Informasi Universitas Bakrie atas ilmu yang diberikan selama penulis menuntut ilmu di bangku perkuliahan dan pemberian saran kepada penulis dalam penyusunan Tugas Akhir.
8. Bapak Hartarto selaku pihak departemen IT PT XYZ atas informasi yang diberikan pada saat pelaksanaan wawancara.
9. Karyawan PT XYZ yang telah bersedia menjadi responden dalam pengisian kuesioner.
10. Rasyid, Eryk, Zia, dan Dinda yang telah berpartisipasi dalam penyusunan tugas akhir.

11. Rekan-rekan Program Studi Teknik Informatika 2010 yang telah memberikan informasi dan menemani penulis dalam penyusunan Tugas Akhir.
12. Seluruh rekan Universitas Bakrie yang turut mendukung penulis dalam penyusunan Tugas Akhir.

Tidak ada kesempurnaan pada setiap penyusunan laporan. Oleh karena itu, penulis mengharapkan kritik dan saran dari pembaca demi kesempurnaan laporan tugas akhir. Penulis berharap tugas akhir ini dapat memberikan manfaat untuk pembaca pada umumnya dan keluarga Universitas Bakrie pada khususnya.

Jakarta, 21 Juli 2014

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama : Dimas Aryo Anggoro
NIM : 1102001019
Program Studi : Teknik Informatika
Fakultas : Teknik dan Ilmu Komputer
Jenis Tugas Akhir : Audit / Evaluatif

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

Analisis Kepatuhan Karyawan terhadap Kebijakan Pengamanan Data pada PT XYZ dengan Standar COBIT 5

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

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 21 Juli 2014

Yang Menyatakan

(Dimas Aryo Anggoro)

ANALISIS KEPATUHAN KARYAWAN TERHADAP KEBIJAKAN PENGAMANAN DATA PADA PT XYZ DENGAN STANDAR COBIT 5

Dimas Aryo Anggoro

ABSTRAK

Penelitian ini dilakukan untuk mengukur tingkat kepatuhan karyawan terhadap kebijakan pengamanan data pada perusahaan. Penulis meneliti dampak yang terjadi pada perusahaan terkait tingkat kepatuhan karyawan. Fokus penelitian ini adalah tentang sistem dan kebijakan pengamanan data yang telah diterapkan, tingkat kepatuhan karyawan terhadap kebijakan pengamanan data, dan faktor yang mempengaruhi tingkat kepatuhan karyawan. Penulis melakukan survei untuk mendapatkan nilai aktual dari tingkat kepatuhan karyawan terhadap sistem pengamanan data dan faktor yang mempengaruhinya. Penulis melakukan pengolahan data statistik berupa uji validitas dan uji reliabilitas. Penulis menggunakan *framework* COBIT 5 untuk melakukan penelitian tentang kebijakan pengamanan data. Hasil dari penelitian berupa indeks tingkat kepatuhan karyawan terhadap sistem pengamanan data pada perusahaan dan faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan. Penulis mencoba menarik hubungan antara tingkat kepatuhan dan faktor yang mempengaruhi tingkat kepatuhan tersebut dengan penerapan sistem dan kebijakan pengamanan data. Selain itu, penulis melakukan analisis kesenjangan dari hasil keterkaitan hubungan tingkat kepatuhan karyawan dengan penerapan sistem dan kebijakan pengamanan data. Dari hasil nilai aktual dan nilai ekspektasi yang ditentukan, penulis mendapatkan *margin* dari analisis kesenjangan di atas. Penulis memberikan rekomendasi untuk pertimbangan dalam pembuatan kebijakan pengamanan data pada masa yang akan datang berdasarkan hasil analisis kesenjangan yang telah penulis lakukan.

Kata kunci : Sistem dan Kebijakan Pengamanan Data, Tingkat Kepatuhan Karyawan, Faktor yang Mempengaruhi Tingkat Kepatuhan Karyawan, Analisis Kesenjangan, COBIT 5

ANALISIS KEPATUHAN KARYAWAN TERHADAP KEBIJAKAN PENGAMANAN DATA PADA PT XYZ DENGAN STANDAR COBIT 5

Dimas Aryo Anggoro

ABSTRACT

This research was conducted to measure the level of employee compliance to corporate policies on data security. The author examines the impact that occurs to the company related to compliance level of employee. The focus of this research is about the system and policies of data security that have been applied, the level of employee compliance to data protection policies, and factors that affect the level of employee compliance. The author conducted a survey to get the actual value of the level of employee compliance to data security systems and factors that influence it. The author performs statistical data processing in the form of validity test and reliability test. The author uses the COBIT 5 framework for conducting research about data security policy. The results of the research is in the form of indices level of employee compliance with the security system data on the company and the factors that affect the level of employee compliance. The author tries to draw a relationship between the level of compliance and factors affecting the level of compliance with the implementation of the system and policies of data security. Moreover, the authors conduct a gap analysis of the results of inter-relationship of employee compliance level with the implementation of the system and policies of data security. From the actual value and the expected value that have been determined, the author obtains the margin of the gap analysis above. The author provides recommendations for consideration in making data security policy in the future based on the results of the gap analysis that has been done.

Keywords : Data Security System and Policies, Employee Compliance Level Factors that Influence Employee Compliance level, Gap Analysis, COBIT 5

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS

DAFTAR LAMPIRAN

DAFTAR SINGKATAN

APO	: *Align, Plan, Organise*
BAI	: *Build, Acquire, Implement*
BCP	: *Business Continuity Plan*
CD	: *Compact Disc*
COBIT	: *Control Objectives for Information and Related Technology*
DSS	: *Deliver, Service, Support*
DWDM	: *Dense Wavelength Division Multiplexing*
EDM	: *Evaluate, Direct, Monitor*
FIF	: *Federal International Finance*
ISACA	: *Information Systems Audit and Control Association*
IT	: *Information Technology*
LAN	: *Local Area Network*
LTO	: *Linear Tape Open*
MEA	: *Monitor, Evaluate, Assess*
MPLS	: *Multiprotocol Label Switching*
OCTAVE	: *Operationally Critical Threat, Asset, And Vulnerability Evaluation*
PC	: *Personal Computer*
PT	: Perseroan Terbatas
RAID	: *Redundant Array of Independent Disks*
SPSS	: *Statistical Package for the Social Sciences*
TB	: *Tera Byte*
TI	: Teknologi Informasi
WAN	: *Wide Area Network*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini teknologi sudah tidak dapat dipisahkan dari kehidupan manusia, mulai dari kegiatan sehari-hari yang sederhana sampai dengan yang sangat penting. Dalam menjalankan bisnis, perusahaan tidak dapat lepas dari penggunaan teknologi. Apabila tidak *up-to-date*, perusahaan akan kalah bersaing dalam bidang teknologi informasi.

Teknologi informasi merupakan segala sesuatu yang dapat digunakan orang dalam melakukan pekerjaan berupa pemrosesan informasi untuk mendukung dan mengolah informasi tersebut sesuai dengan kebutuhan perusahaan (Valacich, 2010). Penerapan teknologi informasi juga harus dilakukan pada perusahaan untuk dapat memberikan solusi bagi perusahaan demi kepentingan bisnisnya. Mayoritas perusahaan telah menerapkan teknologi informasi sehingga kelangsungan proses bisnis dapat berjalan dengan baik.

PT. XYZ telah menerapkan teknologi informasi sebagai sarana dalam mengerjakan tugas kantor. Tiap karyawan diberikan hak akses untuk menggunakan sumber daya teknologi informasi. Dalam pertukaran dan pengamanan data, perusahaan memerlukan *Local Area Network* (LAN). Setiap karyawan dalam melakukan tugas kantor harus terhubung dengan LAN supaya dapat berkomunikasi dengan pihak lain dalam satu perusahaan.

Karyawan dapat melakukan penyimpanan data di *local* dan *network storage*. *Network storage* perusahaan disediakan untuk menyimpan dokumen karyawan di *server*. Hal ini bertujuan untuk mengamankan data karyawan dan mencegah kehilangan data yang terjadi karena adanya masalah pada *local storage*.

Robocopy adalah *tools* berupa baris perintah yang digunakan untuk replikasi dokumen. *Tools* ini membantu menjaga salinan identik dari struktur direktori pada satu komputer atau antar komputer di lokasi terpisah yang terhubung dengan jaringan komputer (Hicks, 2012). *Remote backup* merupakan proses *backup* yang dilakukan dengan menggunakan LAN sehingga mengharuskan kedua situs saling

terhubung (King, 1991). Proses *backup* data karyawan pada *local storage* dilakukan oleh Sub Departemen *IT Computing and Infrastructure* PT XYZ secara manual menggunakan *robocopy* melalui *remote backup*. Proses *backup* data dengan menggunakan *robocopy* dilakukan secara terjadwal oleh departemen IT perusahaan. *Backup robocopy* tidak menjamin keamanan data pada *local storage* karyawan. Kegagalan pada proses *backup robocopy* dapat disebabkan karena *file* yang akan di-*backup* sedang digunakan karyawan pada saat proses *backup* sedang berlangsung. Akibatnya, tidak semua data yang ada pada *local storage* mereka aman karena tidak ter-*backup* seluruhnya di *storage*.

Hal yang menjadi perhatian disini adalah masalah perilaku karyawan terhadap kepedulian pada keamanan data. Kepedulian karyawan mempengaruhi tingkat kepatuhan terhadap kebijakan pengamanan data. Karyawan dalam melakukan pekerjaan lebih banyak yang menyimpan di *local storage* daripada di *network storage*. Penyimpanan di *local storage* rawan terhadap kerusakan fisik sehingga dapat mengakibatkan kehilangan data. Selain itu ketidaksengajaan penghapusan data dan proses instalasi ulang sistem operasi juga dapat mengakibatkan hilangnya data pada *local storage*.

Dalam kebijakan IT perusahaan, tiap karyawan diharuskan untuk menyimpan data mereka di *network storage* untuk melindungi data mereka. Perusahaan menerapkan peraturan pada tiap karyawan untuk dapat menjaga kerahasiaan dan tidak menyalahgunakan data perusahaan. Oleh karena itu, perlu adanya pengukuran tingkat kepatuhan karyawan terhadap kebijakan pengamanan data yang mana dapat mempengaruhi kinerja perusahaan. Selain itu perlu diteliti tentang faktor penyebab yang mempengaruhi kepatuhan karyawan terhadap kebijakan pengamanan data.

Diperlukan kebijakan pengamanan data pada masa yang akan datang untuk mengatasi masalah tentang sistem dan kebijakan pengamanan data. Kebijakan tersebut bertujuan untuk mencegah masalah yang dapat terjadi terhadap keamanan data selanjutnya. Kebijakan yang perlu diterapkan adalah tentang apa saja cara yang harus dilakukan oleh perusahaan supaya karyawan peduli tentang keamanan data. Dengan demikian, dampak yang didapatkan adalah keamanan data yang terjamin sehingga karyawan dapat melakukan pekerjaan dengan baik.

1.2 Perumusan Masalah

Masalah yang didapat dirumuskan dengan pokok bahasan di bawah ini.

- Bagaimanakah sistem dan kebijakan pengamanan data yang diterapkan pada perusahaan berdasarkan domain COBIT 5?
- Seberapa besar tingkat kepatuhan karyawan terhadap kebijakan pengamanan data?
- Seberapa besar tingkat faktor-faktor yang mempengaruhi kepatuhan karyawan terhadap peraturan tentang pengamanan data?
- Apa sajakah strategi yang dapat dilakukan perusahaan untuk meningkatkan tingkat kepatuhan terhadap kebijakan pengamanan data pada masa yang akan datang?

1.3 Batasan Masalah

Masalah yang diteliti dibatasi oleh hal-hal berikut ini:

- Sistem dan kebijakan pengamanan data PT XYZ.
- Tingkat kepatuhan karyawan terhadap kebijakan pengamanan data pada PT XYZ.
- Faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data pada PT XYZ.
- Kesenjangan/*gap* antara nilai ekspektasi dan nilai aktual dari tingkat kepatuhan karyawan terhadap kebijakan pengamanan data beserta faktor-faktor yang mempengaruhinya.

1.4 Tujuan Penelitian

Tugas akhir yang penulis susun ini bertujuan untuk:

- Mengetahui seberapa besar kepatuhan karyawan terhadap kebijakan pengamanan data yang telah ditetapkan oleh perusahaan.
- Mengetahui faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap sistem dan kebijakan pengamanan data.

1.5 Manfaat Penelitian

Penelitian yang ditulis memiliki manfaat sebagai berikut:

1.5.1 Bagi Pihak PT. XYZ

- Menjelaskan pentingnya kepedulian karyawan terhadap sistem dan kebijakan pengamanan data yang berdampak pada kinerja PT XYZ.
- Mengetahui tingkat kepatuhan karyawan terhadap kebijakan pengamanan data yang diterbitkan oleh Departemen IT PT XYZ supaya dapat dilakukan perbaikan kebijakan apabila terdapat kekurangan dari hasil evaluasi yang dilakukan oleh penulis.
- Mengetahui faktor yang mempengaruhi kepatuhan karyawan terhadap peraturan tentang pengamanan data.
- Memberikan rekomendasi kepada PT XYZ sebagai pertimbangan dalam pembuatan kebijakan pengamanan data pada masa yang akan datang berdasarkan hasil analisis kesenjangan yang telah penulis lakukan.

1.5.2 Bagi Peneliti Lain

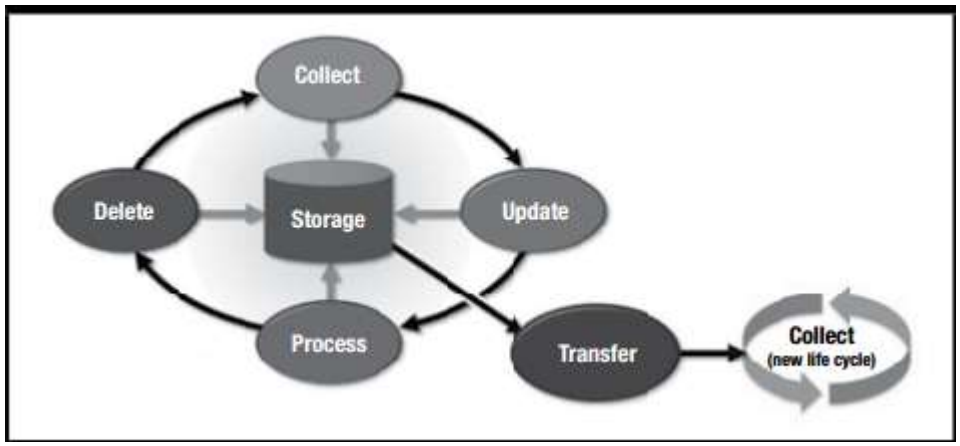
- Memberikan gambaran tentang bagaimana cara mengukur tingkat kepatuhan karyawan terhadap kebijakan pengamanan data dan faktor yang mempengaruhinya.
- Memberikan gambaran tentang sistem dan kebijakan pengamanan data perusahaan.
- Memberikan gambaran tentang implementasi sistem dan kebijakan pengamanan data pada perusahaan berdasarkan *framework* COBIT 5.

BAB II
TINJAUAN PUSTAKA

2.1 Siklus Hidup Informasi (*Information Life Cycle*)

Berdasarkan (Salido, 2010), berikut adalah penjelasan tentang siklus hidup informasi:

Dalam mengidentifikasi risiko yang kemungkinan dapat terjadi, langkah-langkah teknis yang tepat dan pemilihan kegiatan untuk melindungi data rahasia mestinya dilakukan oleh perusahaan. Sebuah organisasi harus terlebih dahulu memahami bagaimana informasi mengalir melalui sistem informasi dari waktu ke waktu dan bagaimana informasi tersebut diakses dan diproses pada tahap yang berbeda oleh beberapa aplikasi dan pengguna dalam berbagai tujuan. Memahami risiko dalam setiap tahap siklus informasi dapat membantu menjelaskan tentang perlindungan apa saja yang diperlukan untuk meminimalisasi risiko tersebut. Gambar 2.1 di bawah ini adalah contoh aliran informasi pada perusahaan. Informasi yang mengalir mengalami proses pengumpulan (*collect*), pembaharuan (*update*), pengolahan (*process*), dan penghapusan (*delete*). Informasi juga berpindah (*transfer*) ke sistem lain selain mengalir pada suatu sistem informasi perusahaan.



Gambar 2.1 Siklus Hidup Informasi
(Sumber: Salido, 2010. Data Governance for Privacy, Confidentiality and Compliance: A Holistic Approach, ISACA Journal, halaman 3)

2.2 Manajemen Risiko Teknologi Informasi (*IT Risk Management*)

Berdasarkan pedoman dari (An Australian Government Initiative, 2013), berikut adalah penjelasan mengenai manajemen risiko pada teknologi informasi:

Setiap adanya perencanaan sesuatu biasanya menimbulkan risiko yang baru, sama halnya dengan proses implementasi sistem IT pada perusahaan. Sebelum proses implementasi sistem yang baru tersebut, perlu dipertimbangkan risiko-risiko yang kemungkinan dapat terjadi. Dalam mencegah dan mengatasi kemungkinan risiko, maka diterapkanlah prinsip-prinsip manajemen risiko.

Manajemen risiko adalah berupa perencanaan yang bertujuan untuk mengatur peningkatan kinerja perusahaan, inovasi, produktivitas, analisis, dan mitigasi yang dapat diterima apabila ada sesuatu yang menyalahi kebijakan yang telah ditetapkan atau terdapat hal yang terjadi di luar dugaan. Dengan mengidentifikasi potensi risiko sebelum melakukan implementasi sistem, hal buruk yang mungkin terjadi dapat diantisipasi dengan strategi yang diterapkan sehingga dapat menghindari atau meminimalisasi ancaman risiko tersebut dan berdampak pada kesuksesan tujuan bisnis dengan lebih mudah dicapai.

Berdasarkan majalah bisnis ”Vibiznews” edisi 24 November 2007 tentang manajemen risiko, berikut adalah penjelasan mengenai strategi dalam manajemen risiko:

> “Strategi dalam implementasi manajemen risiko yang dapat digunakan antara lain menyerahkan risiko pada pihak lain, menghindari risiko, dan mengurangi kemungkinan terjadinya risiko. Berikut adalah penjelasan mengenai proses dalam manajemen risiko:
>
> a. Identifikasi Risiko
>
> Proses ini meliputi identifikasi risiko yang mungkin terjadi dalam suatu aktivitas usaha. Identifikasi risiko secara akurat dan lengkap sangatlah vital dalam manajemen risiko. Salah satu aspek penting dalam identifikasi risiko adalah mendaftar risiko yang mungkin terjadi sebanyak mungkin.
>
> b. Analisis Risiko
>
> Setelah melakukan identifikasi risiko, maka tahap berikutnya adalah pengukuran risiko dengan cara melihat potensial terjadinya

seberapa besar kerusakan/*severity* dan probabilitas terjadinya risiko tersebut. Penentuan probabilitas terjadinya suatu *event* sangatlah subyektif dan lebih berdasarkan nalar dan pengalaman. Beberapa risiko memang mudah untuk diukur, namun sangatlah sulit untuk memastikan probabilitas suatu kejadian yang sangat jarang terjadi. Sehingga, pada tahap ini sangat penting untuk menentukan dugaan yang terbaik supaya nantinya kita dapat memprioritaskan dengan baik dalam implementasi perencanaan manajemen risiko. Kesulitan dalam pengukuran risiko adalah menentukan kemungkinan terjadi suatu risiko karena informasi statistik tidak selalu tersedia untuk beberapa risiko tertentu. Selain itu, mengevaluasi dampak kerusakan seringkali cukup sulit untuk asset immateriil.

c. Pengelolaan Risiko

Jenis-jenis cara mengelola risiko:

1. *Risk avoidance*

   Yaitu memutuskan untuk tidak melakukan aktivitas yang mengandung risiko sama sekali. Dalam memutuskan untuk melakukannya, maka harus dipertimbangkan potensial keuntungan dan potensial kerugian yang dihasilkan oleh suatu aktivitas.

2. *Risk reduction*

   Risk reduction atau disebut juga *risk mitigation* yaitu merupakan metode yang mengurangi kemungkinan terjadinya suatu risiko ataupun mengurangi dampak kerusakan yang dihasilkan oleh suatu risiko.

3. *Risk transfer*

   Yaitu memindahkan risiko kepada pihak lain, umumnya melalui suatu kontrak (asuransi) maupun *hedging*.

d. Implementasi Manajemen Risiko

Setelah memilih respon yang akan digunakan untuk menangani risiko, maka pengimplementasikan metode yang telah direncanakan tersebut dapat dilakukan.

e. Pemantauan Risiko

Mengidentifikasi, menganalisis dan merencanakan suatu risiko merupakan bagian penting dalam perencanaan suatu proyek. Namun, manajemen risiko tidaklah berhenti sampai disana saja. Praktek, pengalaman dan terjadinya kerugian akan membutuhkan suatu perubahan dalam rencana dan keputusan mengenai penanganan suatu risiko. Sangatlah penting untuk selalu memonitor proses dari awal mulai dari identifikasi risiko danpengukuran risiko untuk mengetahui keefektifan respon yang telah dipilih dan untuk mengidentifikasi adanya risiko yang baru maupun berubah. Sehingga, ketika suatu risiko terjadi maka respon yang dipilih akan sesuai dan diimplementasikan secara efektif."

2.3 Kebijakan IT (*IT Policy*)

Berdasarkan pedoman dari Chevron *Corporation* tahun 2011 dalam hal kebijakan IT, berikut adalah penjelasan tentang kebijakan keamanan IT:

Penerapan manajemen risiko sangat perlu diterapkan pada implementasi sistem. Oleh karena suatu sistem yang digunakan oleh karyawan, perlu adanya sesuatu yang mengatur agar manajemen risiko dalam implementasi sistem berjalan dengan baik. Sesuatu yang mengatur dan mengikat tersebut adalah kebijakan. Kebijakan/*policy* perlu dirancang apabila akan mengimplementasi sistem yang digunakan oleh banyak orang. *Policy* berguna untuk mengatur perilaku karyawan supaya manajemen risiko yang telah ditetapkan berjalan dengan baik dalam penanggulangan risiko yang disebabkan oleh implementasi sistem.

2.4 Keamanan Informasi (*Information Security*)

Berdasarkan (Rainer & Charles A. Snyder, 1991), berikut adalah penjelasan tentang masalah yang sering terjadi dalam manajemen risiko:

"Tidak ada keamanan sistem informasi yang memiliki jaminan 100%. Sistem tersebut jelas membutuhkan biaya yang terlalu besar dan tidak nyaman dalam pemakaian sistem. Masalah yang sering terjadi pada manajemen risiko adalah

kurangnya kepedulian dari *user*, *attention, concern*, dan komitmen terhadap manajemen yang telah ditetapkan."

Berdasarkan (Supradono, 2009), berikut adalah penjelasan tentang keamanan informasi:

"Aset informasi: *hardware, software,* sistem, informasi dan manusia, merupakan aset yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Keamanan informasi tidak bisa hanya disandarkan pada alat/*tools* atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi. Untuk itu butuh pengelolaan keamanan informasi yang sistemik dan komprehensif. Aspek kebutuhan keamanan informasi harus memuat 3 unsur penting yakni:

1. Kerahasiaan/*Confidentiality*

   Merupakan aspek yang menjamin kerahasiaan data atau informasi. Memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.

2. Integritas/*Integrity*

   Merupakan aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang / *authorized*. Keakuratan dan keutuhan informasi harus terjaga.

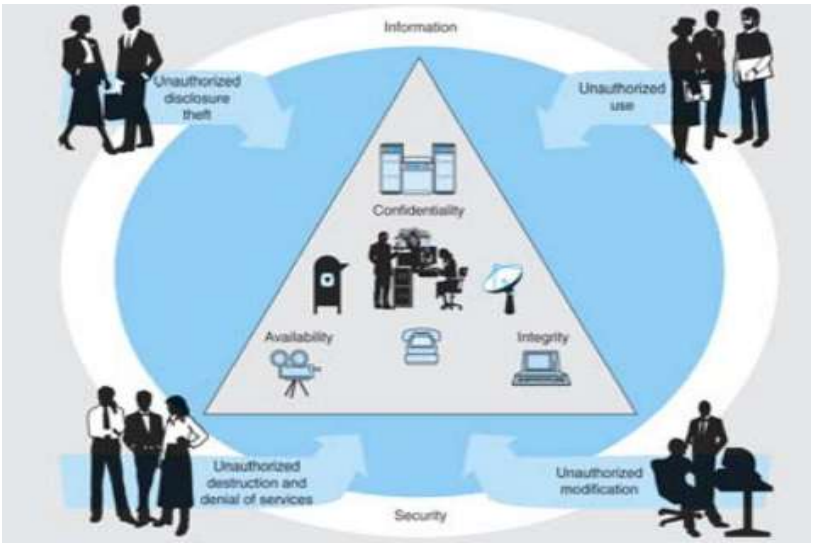
3. Ketersediaan/*Availability*

   Merupakan aspek yang menjamin bahwa data akan tersedia saat dibutuhkan. Memastikan *user* yang berhak dapat menggunakan informasi dan perangkat terkait bilamana diperlukan.

Tiga aspek keamanan rawan terhadap ancaman serangan-serangan yang mengancam keberadaanya baik serangan terhadap sumber-sumber informasi baik secara fisik dan melalui akses secara jaringan.

Untuk mengatasi risiko keamanan butuh kemampuan dalam pengelolaan/manajemen risiko keamanan informasi untuk itu dibutuhkan pendekatan ilmu manajemen"

Gambar 2.2 di bawah ini menjelaskan bahwa suatu sistem harus menerapkan tiga unsur keamanan informasi (*confidentiality*, *integrity*, *availability*) untuk melindungi informasi yang ada di dalam sistem tersebut. Informasi yang berada dalam suatu sistem rawan oleh ancaman baik dari dalam maupun dari luar.



Gambar 2.2 Tiga Unsur Aspek Keamanan Informasi
(Sumber: Supradono, Bambang, Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation), Media Elektrika, Vol.2, No.1, 2009, halaman 4)

2.5 Keamanan Informasi Perusahaan (*Corporate Information Security*)

Berdasarkan pedoman dari Chevron *Corporation* tahun 2011 dalam hal keamanan informasi, berikut adalah penjelasan tentang kebijakan keamanan IT:

Pada penerapan manajemen risiko teknologi informasi dengan menerapkan kebijakan pengamanan IT pada perusahaan, keamanan data sangat dijunjung tinggi dan dilakukan *authentication login/access* untuk dapat memasuki suatu sistem atau mengakses data. Perusahaan kini telah menerapkan kebijakan *"Data Privacy"* dengan mengadakan pelatihan kepada karyawan secara *online* melalui intranet perusahaan. Salah satu *concern* dalam masalah *data privacy* adalah masalah "*Data Loss"* yang berarti data yang dimiliki oleh seorang karyawan dapat diakses secara ilegal oleh orang lain dan kemudian dicuri atau kehilangan data akibat dari *human error*.

Selain itu, perusahaan memberikan hak akses kepada pihak IT yang bertugas untuk *monitoring*, *maintenance*, *backup*, dan *recovery* data karyawan dengan tujuan melindungi data supaya tidak hilang atau dicuri. Pihak IT tersebut diberikan akses *administrator* dengan memasukkan admin ID dan *password*. Jaminan bahwa pihak IT tidak menyalahgunakan data karyawan adalah adanya kontrak kerja tentang hak, kewajiban, dan tanggung jawab pihak IT terhadap keamanan data perusahaan beserta risiko-risiko yang akan diterima apabila menyalahgunakan data perusahaan.

2.6 Kepatuhan (*Compliance*)

Berdasarkan (Creech & Alderman, 2010), berikut adalah penjelasan tentang kepatuhan terhadap kebijakan teknologi informasi:

Kepatuhan kebijakan teknologi informasi (*IT policy compliance*) merupakan sebuah implementasi dan manajemen teknologi informasi yang memenuhi standar yang disetujui dan ditetapkan. Beberapa bidang pada *IT policy compliance* adalah *user awareness and training* dan *procedures and standards*. Penerapan kontrol kepatuhan terhadap kebijakan teknologi informasi merupakan suatu topik yang penting karena sebagian besar dari tata kelola dan bisnis saat ini dilakukan dengan menggunakan teknologi informasi. Pada suatu organisasi yang berjalan dengan menggunakan teknologi informasi, terdapat beberapa risiko yang dapat terjadi. Risiko tersebut akan menimbulkan akibat negatif bagi organisasi. Penerapan kebijakan sangat penting diterapkan untuk menghindari risiko-risiko yang berdampak buruk bagi perusahaan. Keuntungan bagi perusahaan juga akan tercapai apabila patuh terhadap kebijakan yang telah diterapkan.

Dalam pengamanan data perusahaan yang tersimpan pada *local drive*, perusahaan melakukan upaya untuk *backup* data karyawan dengan metode *remote backup* secara terjadwal. Selain itu, karyawan juga dihimbau untuk melakukan *backup* data pekerjaan mereka dengan media penyimpanan portabel pribadi.

2.7 Proses Pengamanan Data (*Backup*)

Berdasarkan (Pakpahan, 2013), berikut adalah penjelasan mengenai proses *backup* data:

Backup data adalah memindahkan atau menyalin kumpulan informasi (data) yang tersimpan di dalam *harddisk* komputer yang biasanya dilakukan dari satu lokasi/perangkat ke lokasi/perangkat lain. Data atau kumpulan informasi tersebut bisa berupa file dokumen, gambar, video, audio, *system windows*, *driver*, atau *software*/program tertentu.

Pada teknologi informasi, *backup* mengacu pada penyalinan data. Suatu data yang merupakan data salinan yang dapat di-*restore* kembali apabila ada data yang hilang. Data salinan tersebut biasa disebut dengan *backup*. *Backup* berguna untuk dua tujuan utama.

a. Mengembalikan/*restore* data yang mengalami kerusakan akibat bencana alam (misal: banjir, gempa bumi).
b. Mengembalikan file setelah mengalami kesalahan menghapus atau kerusakan data. Para pemakai memahami bahwa kerusakan akan terjadi, *hard drives* akan gagal, *motherboards* rusak, dan kekeliruan dalam menghapus data.

Untuk mencegah hal tersebut, diperlukan *backup* data *file* yang merupakan salinan dari *file-file* yang masih aktif dalam *network storage* sebagai pelindung/cadangan bila *file* rusak/hilang.

2.7.1 *Local Backup*

Local backup merupakan metode backup dimana tempat salinan data ditempatkan pada *harddisk* eksternal, *flashdisk*, atau CD yang terpasang pada komputer secara langsung dan dilakukan tanpa melalui jaringan komputer (Handy Backup, 2014).

2.7.2 *Remote Backup*

Berdasarkan (King, 1991), berikut adalah penjelasan mengenai *remote backup*:

Sistem *remote backup* melacak kondisi situs utama. Tujuan dari *remote backup* adalah mengamankan data apabila terjadi kerusakan pada situs utama yang berakibat hilangnya data. Proses *remote backup* dilakukan dengan menggunakan LAN sehingga mengharuskan kedua situs tersebut saling terhubung. Situs utama dan situs *backup* secara fisik harus terpisah sehingga apabila terjadi kerusakan pada salah satu situs, situs yang lain tidak terkena dampak kerusakannya.

2.8 Prinsip Dasar COBIT 5

Berdasarkan penjelasan pada jurnal ISACA tahun 2012, *Control Objectives for Information and Related Technology* (COBIT 5) secara umum memiliki 5 prinsip dasar yaitu:

1. *Meeting Stakeholder Needs*

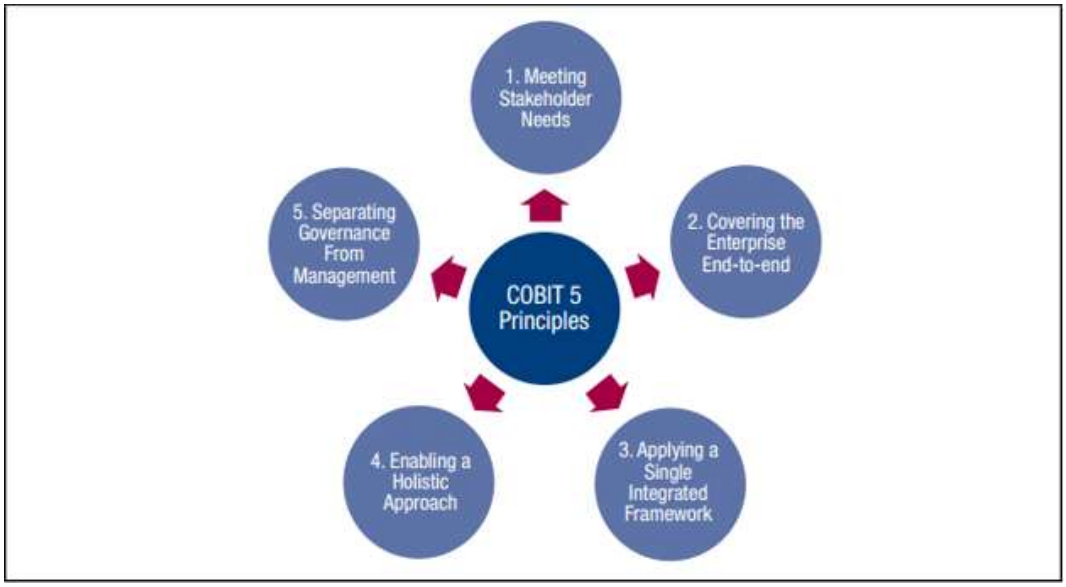
   Terdapat usaha dari perusahaan untuk menciptakan nilai bagi para *stakeholder* dengan menjaga keseimbangan antara realisasi manfaat, optimalisasi risiko, dan penggunaan sumber daya.
2. *Covering the Enterprise End-to-end*

   COBIT 5 memadukan tata kelola IT dan tata kelola perusahaan.
3. *Applying a Single Integrated Framework*

   Terdapat banyak standar yang berkaitan dengan IT, masing-masing memberikan panduan pada subset dari kegiatan IT. COBIT 5 sejalan dengan standar lain yang relevan dan kerangka kerja pada tingkat tinggi. Dengan demikian, COBIT 5 dapat menjadi kerangka menyeluruh untuk tata kelola dan manajemen perusahaan.
4. *Enabling a Holistic Approach*

   Tata kelola dan manajemen perusahaan yang efektif dan efisien membutuhan pendekatan holistik, dengan mempertimbangkan beberapa komponen yang saling berinteraksi.
5. *Separating Governance From Management*

   COBIT 5 membuat perbedaan yang jelas antara tata kelola dan manajemen.



Gambar 2.3 Prinsip Dasar COBIT 5
(Sumber: ISACA. 2012. COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows: ISACA, halaman 13)

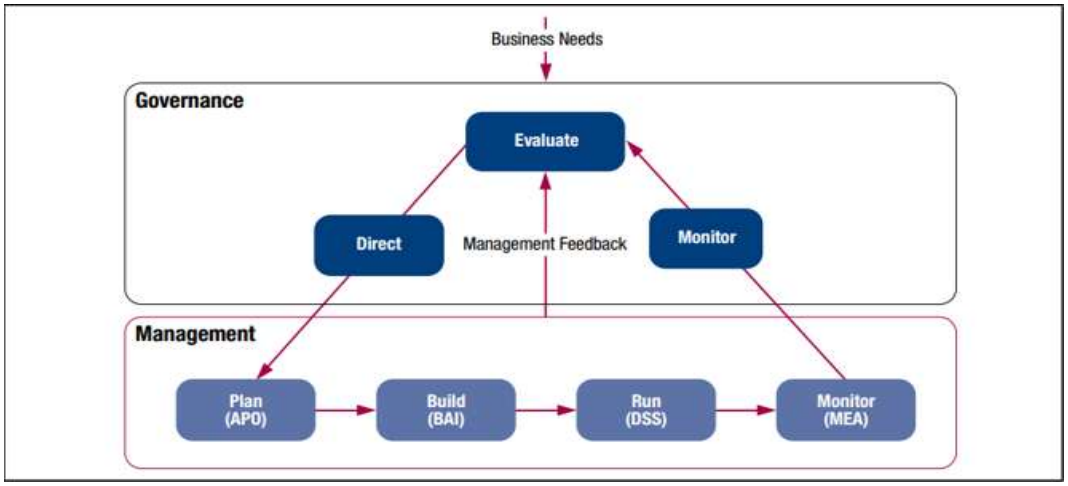
2.9 Domain COBIT 5

Berdasarkan penjelasan pada jurnal ISACA tahun 2012, COBIT 5 *framework* dirancang dengan 5 domain yang masing-masing mencakup penjelasan rinci dan termasuk panduan secara luas dan bertujuan sebagai tata kelola dan manajemen IT perusahaan.

Lima domain yang ada pada COBIT 5 adalah:

1. Evaluate, Direct, and Monitor (EDM)
2. Align, Plan, and Organise (APO)
3. Build, Acquire, and Implement (BAI)
4. Deliver, Service, and Support (DSS)
5. Monitor, Evaluate, and Assess (MEA)

Gambar 2.4 di bawah ini memberi gambaran tentang pemisahan tata kelola dan manajemen pada COBIT 5. Tata kelola meliputi EDM sedangkan manajemen meliputi APO, BAI, DSS, dan MEA.



Gambar 2.4 Domain Tata Kelola dan Manajemen pada COBIT 5
(Sumber: ISACA, 2012. COBIT® 5: Enabling Processes. Rolling Meadows: ISACA, halaman 23)

2.9.1 Implementasi APO

Berdasarkan penjelasan pada jurnal ISACA tahun 2012, berikut adalah penjelasan mengenai APO01.08 dan APO09.03

a. APO01.08 : Memelihara Kepatuhan dengan Kebijakan dan Prosedur
   Menempatkan prosedur untuk memelihara kepatuhan dengan pengukuran kinerja kebijakan dan *enabler* lain dari kerangka kontrol, dan menegakkan konsekuensi dari ketidakpatuhan ataupun kinerja yang tidak memadai. Melacak perkembangan kinerja dan mempertimbangkan hal tersebut dalam perancangan ke depan untuk perbaikan *control framework*.
   Penulis mengambil domain APO01.08 karena terdapat beberapa aktivitas pada domain APO01.08 yang terkait dengan penelitian ini:
   - Melacak kepatuhan terhadap kebijakan dan prosedur.
   - Menganalisis ketidakpatuhan dan mengambil tindakan yang tepat.
   - Menganalisis kecenderungan dalam kinerja dan mengambil tindakan yang tepat.

b. APO09.03 : Menetapkan dan Mempersiapkan Kesepakatan Layanan
   Menetapkan dan mempersiapkan kesepakatan layanan berdasarkan pilihan pada katalog servis, termasuk kesepakatan operasional internal.

Penulis mengambil domain APO09.03 karena terdapat beberapa aktivitas pada domain APO09.03 yang terkait dengan penelitian ini.

- Menganalisis persyaratan untuk perjanjian layanan baru yang diterima dari manajemen relasi bisnis untuk memastikan bahwa persyaratan dapat disesuaian. Mempertimbangkan aspek-aspek seperti waktu layanan, ketersediaan, kinerja, kapasitas, keamanan, kontinuitas, kepatuhan dan peraturan masalah, kegunaan, dan kendala permintaan.
- Perjanjian rancangan *customer service* berdasarkan layanan, paket layanan, dan pilihan tingkat pelayanan dalam katalog layanan yang relevan.

2.9.2 Implementasi DSS

Berdasarkan penjelasan pada jurnal ISACA tahun 2012, berikut adalah penjelasan mengenai DSS04.07, DSS05.06, dan DSS06.03.

a. DSS04.07 : Mengelola Peraturan *Backup*
   Mengelola ketersediaan dari informasi bisnis yang *critical*
   Penulis mengambil domain DSS04.07 karena terdapat beberapa aktivitas pada domain DSS04.07 yang terkait dengan penelitian ini:
   - Manajemen *backup* data.
   - Penjelasan tentang *on-site* dan *off-site storage* pada *backup* data.
   - Pengadaan *Business Continuity Plan* (*BCP*) *awareness* dan *training*.

b. DSS05.06 : Mengelola Dokumen dan *Output Devices* yang Sensitif
   Membangun pengamanan fisik yang memadai, praktik pelaporan, dan manajemen inventaris yang sensitif melalui aset IT.
   Penulis mengambil domain DSS05.06 karena terdapat beberapa aktivitas pada domain DSS05.06 yang terkait dengan penelitian ini:
   - Pemberian hak akses pada dokumen yang bersifat sensitif.

- Menetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan dan pembuangan data dalam bentuk khusus dan perangkat *output* ke dalam, di dalam, dan keluar dari perusahaan.

c. DSS06.03 : Mengelola Peraturan, Tanggung Jawab, Hak Akses, dan Tingkat Otoritas

Mengelola peraturan bisnis, tanggung jawab, tingkat otoritas, dan pemisahan tugas yang diperlukan untuk mendukung tujuan proses bisnis. Mengizinkan akses untuk setiap aset informasi yang berkaitan dengan informasi dan proses bisnis, termasuk yang berada di bawah pengawasan bisnis, IT, dan pihak ketiga. Hal ini menjamin bahwa bisnis mengetahui dimana data tersebut dan siapa yang menangani data perusahaan.

Penulis mengambil domain DSS06.03 karena terdapat beberapa aktivitas pada domain DSS06.03 yang terkait dengan penelitian ini:

- Mengalokasikan peran dan tanggung jawab berdasarkan deskripsi kerja yang disetujui dan dialokasikan untuk proses bisnis.
- Memberikan kesadaran dan pelatihan tentang peran dan tanggung jawab secara teratur sehingga setiap orang memahami tanggung jawab mereka.
- Pentingnya kontrol, integritas, dan kerahasiaan informasi perusahaan dalam bentuk apapun.
- Melakukan peninjauan secara periodik terhadap ketentuan akses kontrol untuk memastikan bahwa semua hak akses yang valid dan selaras dengan peran para staf yang telah dialokasikan.

2.9.3 Implementasi MEA

Berdasarkan penjelasan pada jurnal ISACA tahun 2012, berikut adalah penjelasan mengenai MEA01.01 dan MEA03.03

a. MEA01.01 : Menetapkan Pendekatan Pengawasan

Terlibat dengan para pemangku kepentingan untuk membangun dan memelihara pendekatan pengawasan untuk menentukan tujuan, ruang lingkup, serta metode untuk mengukur solusi bisnis, penyampaian layanan, dan kontribusi terhadap tujuan perusahaan. Mengintegrasikan pendekatan ini dengan sistem manajemen kinerja perusahaan.

Penulis mengambil domain MEA01.01 karena terdapat beberapa aktivitas pada domain MEA01.01 yang terkait dengan penelitian ini:

- Menyelaraskan dan secara berkelanjutan memelihara *monitoring* evaluasi dengan pendekatan bisnis dan *tools* yang digunakan untuk pengumpulan data dan pelaporan ke perusahaan.
- Mengajukan permohonan, memprioritaskan dan mengalokasikan sumber daya untuk pemantauan (mempertimbangkan kesesuaian, efisiensi, efektivitas dan kerahasiaan).

b. MEA03.03 : Mengkonfirmasi Kepatuhan Eksternal

Memastikan dipatuhinya kebijakan, prinsip, standar, prosedur dan metodologi dengan persyaratan hukum, peraturan dan kontrak.

Penulis mengambil domain MEA03.03 karena terdapat beberapa aktivitas pada domain MEA03.03 yang terkait dengan penelitian ini:

- Secara teratur mengevaluasi kebijakan organisasi, standar, prosedur dan metodologi dalam semua fungsi perusahaan untuk memastikan kepatuhan dengan persyaratan hukum dan peraturan yang relevan dalam kaitannya dengan pengolahan informasi.
- Mengatasi kesenjangan kepatuhan dalam kebijakan, standar, dan prosedur secara tepat waktu.
- Mengevaluasi secara periodik proses serta kegiatan bisnis dan TI, mengevaluasi kegiatan untuk memastikan kepatuhan terhadap hukum, peraturan, dan kontrak persyaratan yang diterapkan.
- Secara teratur meninjau pola kegagalan kepatuhan berulang. Apabila diperlukan, perusahaan dapat memperbaiki kebijakan, standar, prosedur, metodologi, serta proses dan kegiatan terkait.

2.10 Tinjauan Penelitian Terdahulu

Terdapat beberapa penelitian terdahulu yang menjadi tinjauan dalam pengukuran tingkat kepatuhan karyawan dalam kebijakan pengamanan data perusahaan. Sebagai bahan tinjauan dalam penelitian ini akan dicantumkan beberapa hasil penelitian terdahulu yang dilakukan oleh beberapa peneliti.

a. Penelitian yang dilakukan oleh Alvin, Wongso Soekamto, dan Riny Harsono pada tahun 2013 dengan judul penelitian "Analisis dan Evaluasi Tata Kelola IT Pada PT FIF dengan Standar COBIT 5". Penelitian tersebut membahas tentang pengukuran 28 proses yang terdapat dalam COBIT 5 yang termasuk di dalam perspektif internal berdasarkan pemetaan COBIT 5 proses terhadap IT-*related goal* pada Departemen IT PT FIF ditambah dengan 1 proses yang termasuk dalam perspektif finansial pada perusahaan. Hasil dari penelitian terdahulu adalah perhitungan antara *capability level* terkini PT FIF. Terdapat *gap* antara *capability level* terkini PT FIF dengan target *capability level* PT FIF.

   Hubungan dengan penelitian ini adalah bahwa terfokus pada pengambilan aspek domain COBIT 5 yang berkaitan dengan sistem dan kebijakan pengamanan data yang telah diterapkan oleh perusahaan. Pelaksanaan pengukuran dilakukan dari perspektif karyawan terhadap tingkat kepatuhan karyawan terhadap kebijakan pengamanan data serta faktor-faktor yang mempengaruhi tingkat kepatuhan. Domain COBIT yang digunakan adalah penelitian ini APO01.08, APO09.03, DSS04.07, DSS05.06, DSS06.03, MEA01.01, dan MEA03.03.

b. Penelitian yang dilakukan oleh Bambang Supradono pada tahun 2009 dengan judul penelitian "Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE (*Operationally Critical Threat, Asset, And Vulnerability Evaluation*)". Penelitian tersebut membahas tentang tiga aspek dalam keamanan informasi yaitu *confidentiality, integrity,* dan *availability*. Penelitian dilakukan dengan sebuah pendekatan dengan metode OCTAVE terhadap evaluasi risiko keamanan informasi yang

komprehensif, sistematik, terarah, dan dilakukan sendiri. Pendekatan yang dilakukan disusun dalam satu set kriteria yang mendefinisikan elemen esensial dari evaluasi risiko keamanan informasi.

Hasil dari penelitian terdahulu adalah berupa pengukuran praktek keamanan dalam organisasi, analisis ancaman, dan pembangunan strategi proteksi dan katalog yang menjadikan sumber koleksi pengetahuan. Koleksi tersebut meliputi koleksi strategi dan praktek keamanan informasi, koleksi sumber ancaman secara umum, koleksi dari kelemahan berdasarkan platform dan aplikasi

Hubungan dengan penelitian ini adalah, dalam implementasi sistem keamanan pada kebijakan pengamanan data dalam perusahaan perlu menerapkan aspek *confidentiality*, *integrity*, dan *availability*. Data harus bersifat rahasia dimana tidak dapat diakses oleh pihak yang tidak berwenang, data yang dikirim harus sama dengan yang diterima, dan data harus selalu ketersediaan kapanpun data diperlukan.

c. Penelitian lain juga dilakukan oleh Suyono pada tahun 2008 dengan judul penelitian "Penerapan Tata Kelola Pelaksanaan Proyek-Proyek/Kegiatan TI Sekretariat Jenderal Departemen Energi dan Sumber Daya Mineral". Penelitian yang dilakukan bertujuan untuk mencoba mengetahui apakah pengelolaan proyek-proyek/kegiatan TI sudah sesuai dengan Standar Tata Kelola TI dan rencana Strategis Sistem Informasi yang sudah dibuat.

Hasil dari penelitian terdahulu adalah berupa pemetaan pelaksanaan proyek-proyek IT yang ada pada organisasi dan tingkat *maturity level* organisasi berdasarkan *maturity model* COBIT 4.1 PO10.

Hubungan dengan penelitian ini adalah menggunakan pengukuran tata kelola IT dengan menggunakan *framework* COBIT. Penelitian sebelumnya juga melakukan pengukuran dengan cara wawancara terhadap pihak IT dan *user* dalam pengumpulan data.

Berikut adalah tabel korespondensi penelitian terdahulu yang memberikan informasi mengenai nama peneliti, tahun penelitian, dan judul penelitian.

Nama Peneliti	**Tahun Penelitian**	**Judul Penelitian**
Alvin, Wongso Soekamto, dan Riny Harsono	2013	Analisis dan Evaluasi Tata Kelola IT pada PT FIF dengan Standar COBIT 5
Bambang Supradono	2009	Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE (*Operationally Critical Threat, Asset, And Vulnerability Evaluation*)
Suyono	2008	Penerapan Tata Kelola Pelaksanaan Proyek-Proyek/Kegiatan TI Sekretariat Jenderal Departemen Energi dan Sumber Daya Mineral

Tabel 2.1 Tabel Penelitian Terdahulu

BAB III
METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Dalam penelitian ini, jenis penelitian yang digunakan adalah metode kuantitatif dan kualitatif.

a. Kuantitatif

   Metode kuantitatif dipilih dengan tujuan analisis penelitian terhadap tingkat kepatuhan karyawan tentang keamanan data serta penilaian terhadap faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data. Langkah ini dilakukan dengan melakukan perhitungan dan analisis kepatuhan serta faktor yang mempengaruhi kepatuhan karyawan dalam kebijakan pengamanan data. Hal yang menjadi luaran adalah indeks tingkat kepatuhan karyawan terhadap kebijakan pengamanan data serta indeks tingkat tiap faktor yang mempengaruhinya. Hasil perhitungan dan analisis juga digunakan sebagai pertimbangan dalam perbaikan kebijakan pengamanan data pada perusahaan.

b. Kualitatif

   Metode kualitatif dilakukan dengan cara melakukan penelitian terhadap kebijakan pengamanan data serta prosedur keamanan data perusahaan dengan standar COBIT 5. Selain itu juga dilakukan penelitian tentang faktor apa saja yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamaman data. Hal yang menjadi luaran adalah berupa sistem dan kebijakan pengamanan data pada perusahaan serta faktor yang mempengaruhi kepatuhan karyawan terhadap sistem pengamanan data.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan adalah dengan menggunakan metode survei dan wawancara.

3.2.1 Survei

Metode survei akan dilaksanakan dengan cara menyebarkan kuesioner dengan objek sebanyak 36 sampel yang mewakili jumlah populasi karyawan pada perusahaan. Kuesioner yang disebarkan terdapat 25 *item* pertanyaan untuk setiap responden dari departemen dan jabatan yang beragam. Pengukuran pada setiap pertanyaan menggunakan skala likert 5. Survei dilaksanakan di kantor regional Jakarta. Kuesioner bertujuan untuk mengumpulkan data tentang penilaian terhadap karyawan terhadap hal-hal sebagai berikut:

- Tingkat kepatuhan terhadap kebijakan pengamanan data
- Penilaian terhadap faktor yang mempengaruhi kepatuhan karyawan terhadap kebijakan pengamanan data

3.2.2 Wawancara

Penulis melakukan wawancara kepada beberapa karyawan dari departemen dan jenjang karir yang berbeda mengenai penilaian sistem dan kebijakan IT perusahaan untuk mengetahui faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data.

Penulis juga melakukan wawancara kepada Departemen IT yang memiliki peran penting dalam manajemen risiko pada perusahaan yang juga berperan dalam hal kebijakan pengamanan data. Informasi yang diharapkan setelah dilakukannya proses wawancara kepada Departemen IT perusahaan adalah:

- Sistem pengamanan data perusahaan
- Kebijakan pengamanan data perusahaan
- Masalah dalam sistem pengamanan data

Dalam pengumpulan data, variabel yang akan diteliti adalah tingkat kepatuhan karyawan terhadap kebijakan pengamanan data pada perusahaan dengan menghitung faktor-faktor yang berpengaruh terhadap tingkat kepatuhan karyawan. Tingkat kepatuhan yang diperoleh kemudian analisis kesenjangannya dengan kebijakan pengamanan data perusahaan yang dijelaskan oleh departemen IT dalam wawancara.

Faktor-faktor yang mempengaruhi tingkat kepatuhan terhadap kebijakan pengamanan karyawan terbagi ke dalam 4 aspek berikut ini:

- Keamanan
- Regulasi
- Pengaksesan
- Utilisasi

Kemudian diukur tingkat kepatuhan karyawan terhadap kebijakan pengamanan data serta dilakukan analisis terhadap faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data.

3.3 Pemilihan Sampel Data

Pengambilan data dalam penelitian ini dilakukan dengan menggunakan metode survei dan wawancara. Instrumen berupa kuesioner pada metode survei dilakukan dengan sejumlah sampel yang mewakili populasi perusahaan. Pemilihan sampel data dilakukan dengan cara *random sampling* dari populasi yang homogen. Sedangkan dalam wawancara, narasumber yang akan memberikan keterangan adalah:

1. Departemen IT *Planning and Technology*

   Memberikan penjelasan mengenai sistem dan kebijakan pengamanan data perusahaan. Memberikan ekspektasi penilaian tentang faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data perusahaan berdasarkan hasil *monitoring* sebelumnya. Merupakan salah satu departemen yang berwenang dalam *maintenance* sistem IT dan mengatur kebijakan IT pada perusahaan.
2. Karyawan perusahaan

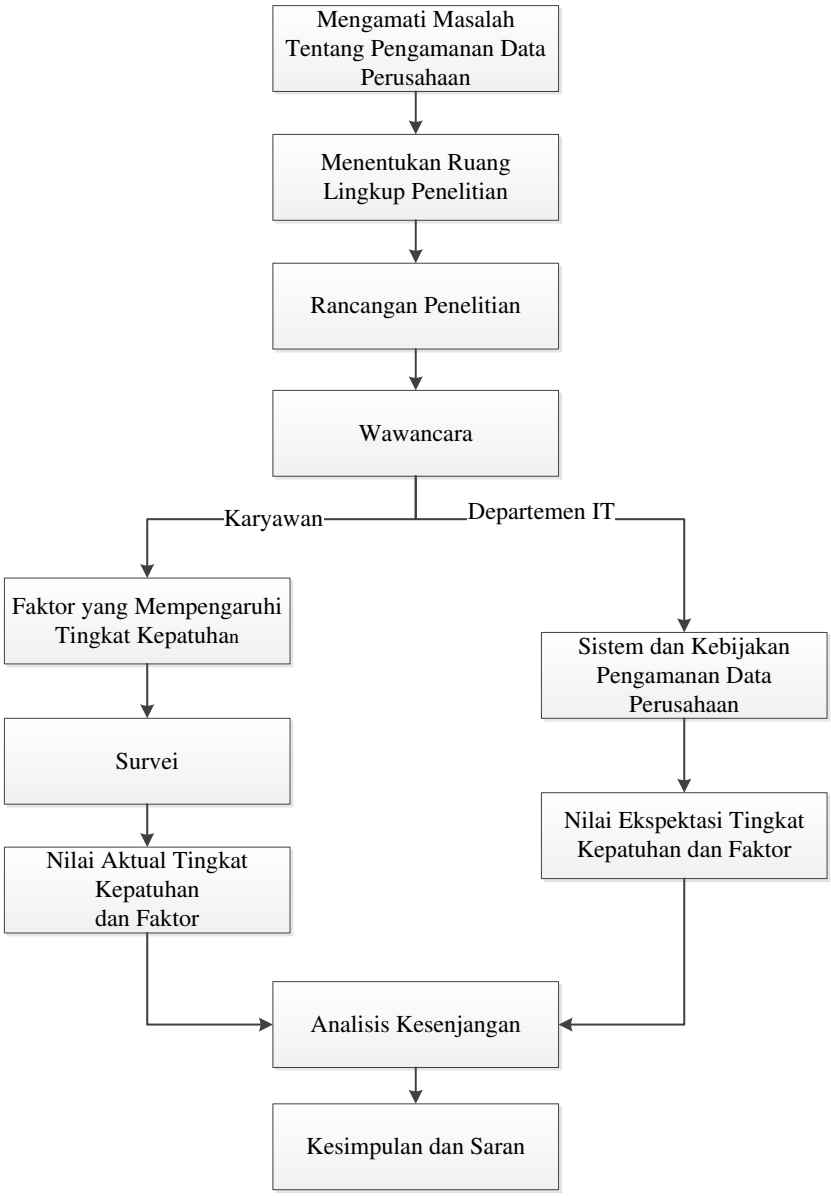
   Memberikan penjelasan tentang faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data perusahaan. Jumlah karyawan yang dipilih sebanyak 3 orang dari departemen yang berbeda.

3.4 Rencana Penelitian

Penelitian ini dilaksanakan bertujuan untuk mendapatkan informasi sebagai berikut:

1. Tingkat kepatuhan terhadap kebijakan pengamanan data
2. Faktor-faktor yang mempengaruhi tingkat kepatuhan terhadap kebijakan pengamanan data
3. Peninjauan tentang sistem dan kebijakan pengamanan data pada perusahaan

Berikut adalah *flowchart* dari penelitian yang akan dilaksanakan



Gambar 3.1 Diagram Alur Penelitian

Penulis melakukan penelitian di PT. XYZ karena data yang diperoleh dari survei dan wawancara dapat dilakukan dengan mudah karena mendapatkan izin untuk melakukan pengumpulan data. Berikut adalah penjelasan langkah-langkah dalam pelaksanaan penelitian:

1. Menemukan tingkat kepedulian dari beberapa karyawan terhadap keamanan data mereka yang kurang sehingga melakukan hal yang menyalahi kebijakan pengamanan data yang telah diterapkan.
2. Melakukan wawancara kepada departemen IT *Planning and Technology* untuk melakukan konfirmasi mengenai adanya tindakan dari beberapa karyawan yang kurang patuh terhadap kabijakan pengamanan data.
3. Melakukan wawancara terhadap karyawan mengenai faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data perusahaan.
4. Melakukan wawancara kembali kepada departemen IT untuk mendapatkan:
    a. Informasi mengenai nilai ekspektasi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data serta faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data perusahaan berdasarkan hasil audit sebelumnya yang telah didokumentasikan.
    b. Informasi mengenai sistem dan kebijakan pengamanan data yang telah diterapkan berdasarkan faktor-faktor yang telah diberikan oleh karyawan dari hasil wawancara.
5. Melakukan survei kepada karyawan untuk mendapatkan nilai aktual mengenai tingkat kepatuhan karyawan terhadap kebijakan pengamanan data beserta faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data.
6. Membandingkan hasil analisis yang berupa tingkat kepatuhan karyawan dengan kebijakan pengamanan data dan faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan yang diperoleh dari survei dengan nilai ekspektasi yang telah ditentukan.

7. Menganalisis tingkat kepatuhan karyawan dan faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan dari data kuantitatif yang didapatkan dari survei.
8. Memberi kesimpulan tentang hasil penelitian dan memberikan saran kepada perusahaan sebagai pertimbangan dalam pembuatan kebijakan baru tentang pengamanan data.

3.5 Teknik Analisis Data

Penelitian yang diteliti menggunakan sejumlah sampel yang mewakili populasi perusahaan. Pada pengukuran data, penulis menentukan *confidence of interval* pada penelitian sebesar 95%. Dipilihlah 95% karena memiliki nilai $\alpha = 0.05$ dan bernilai 2σ sehingga memiliki nilai yang representatif terhadap populasi.

3.5.1 Skala Pengukuran Kuesioner

Dalam penilaian tingkat kepatuhan karyawan terhadap kebijakan pengamanan data dan faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data, dibuatlah skala pengukuran sebagai berikut.

Skala	Keterangan
1	Sangat Rendah
2	Rendah
3	Cukup
4	Tinggi
5	Sangat Tinggi

Tabel 3.1 Tabel Penilaian Skala Likert

3.5.2 Uji Statistik

Berdasarkan hasil kuesioner, penulis menggunakan beberapa metode statistik dalam pengolahan data. Dalam penghitungan data kuantitatif, *tools* yang digunakan adalah berupa program SPSS. SPSS dipilih karena memiliki fitur untuk melakukan uji validitas dan reliabilitas.

a. Uji Validitas

Uji validitas pada penelitian dilakukan dengan tujuan untuk melihat apakah uji statistik yang telah diterapkan benar-benar mengukur semua data yang seharusnya diukur. Apabila uji statistik pada penelitian dilakukan, hasil dari perhitungan dapat bersifat representatif atau mewakili populasi. Uji validitas data dilakukan dengan menggunakan korelasi *Bivariate Pearson* (*Product Moment Pearson*).

$$r = \frac{n\Sigma XY - \Sigma X\Sigma Y}{\sqrt{\left((n\Sigma X^2 - (\Sigma X)^2)(n\Sigma Y^2 - (\Sigma Y)^2)\right)}} \quad \text{..... (Rumus 3.1)}$$

Keterangan:

r = koefisien korelasi

n = jumlah sampel data

X = skor tiap item

Y = skor total item

Uji validitas yang digunakan adalah dengan metode uji dua sisi (*two-tailed test*) dengan *level of significance* ($\alpha = 0.05$).

- Apabila r hitung $\geq$ r tabel maka item pertanyaan pada kuesioner yang diajukan berkorelasi signifikan terhadap skor total (data valid).
- Apabila r hitung $\leq$ r tabel maka item pertanyaan pada kuesioner yang diajukan tidak berkorelasi signifikan terhadap skor total (data tidak valid).

b. Uji Reliabilitas

Uji reliabilitas pada penelitian dilakukan dengan tujuan untuk mengetahui adanya konsistensi alat ukur yang berupa kuesioner dalam penggunaannya, atau dengan kata lain alat ukur tersebut mempunyai hasil yang konsisten apabila digunakan berkali-kali pada waktu yang berbeda. Dalam

penelitian ini uji reliabilitas yang digunakan adalah dengan metode *cronbach's alpha.*

$$\alpha = \left(\frac{K}{K-1}\right)\left(1 - \frac{\Sigma S_i^2}{S^2}\right)$$ ..... (Rumus 3.2)

Keterangan:

α = koefisien reliabilitas c*ronbach's alpha*

K = jumlah *item* pertanyaan

S_i^2 = nilai varians jawaban tiap *item*

S^2 = nilai varians skor total

c. Analisis Kesenjangan

Analisis kesenjangan digunakan untuk mengetahui kesenjangan (*gap*) antara hasil survei berupa nilai aktual dengan nilai ekspektasi yang telah ditentukan. Kemudian akan dianalisis penyebab terjadinya kesenjangan tersebut.

Gap = Nilai Aktual – Nilai Ekspektasi ..... (Rumus 3.3)

3.6 Manajemen Data Perusahaan

Dalam sistem penyimpanan data, perusahaan memberikan fasilitas kepada karyawan berupa *local storage* yang terdapat pada setiap unit komputer dan *network storage* yang berupa *cloud* dimana penyimpanan data dilakukan pada *server storage*. Berikut merupakan pembagian *storage* dan masing-masing fungsinya.

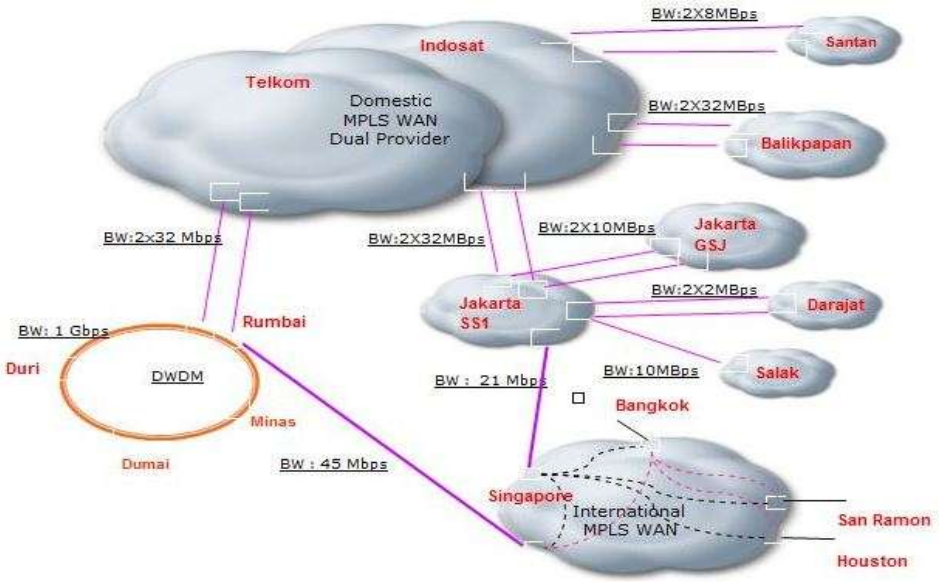
Local Storage	Fungsi
C	Menyimpan *file email* dan *file pribadi*
Network Storage	Fungsi
L	Menyimpan *file-based application*

O	Menyimpan *shared file* pada perusahaan yang dapat dibuka oleh seluruh karyawan, dan dihapus seminggu sekali
P	Menyimpan dokumen pekerjaan karyawan secara personal
S	Menyimpan dokumen yang tidak terstruktur

Tabel 3.2 Tabel Fungsi Storage Perusahaan

3.7 Topologi Jaringan Perusahaan

Dalam sistem jaringan, perusahaan menerapkan metode *cloud computing* dimana memiliki topologi sebagai berikut.



Gambar 3.2 Topologi Jaringan Perusahaan
(Sumber: Dokumen Perusahaan)

Perusahaan memiliki beberapa wilayah dalam pertukaran data secara lokal. Wilayah tersebut adalah Sumatera, Jakarta, Balikpapan dan Santan. Selain bertukar data secara regional, pertukaran data secara nasional dan internasional juga diterapkan oleh perusahaan. Berikut adalah penjelasan tentang sistem jaringan yang diterapkan PT XYZ.

- Region Sumatera menggunakan *Dense Wavelength Division Multiplexing* (DWDM) memiliki *bandwidth* 1 Gbps dalam *flow* pertukaran data dalam region Sumatera.
- Region Jakarta GSJ, Darajat, dan Salak pada *storage* masing-masing wilayah menggunakan *cloud*, dan masing-masing terhubung ke *cloud* Jakarta SS1
- Region Sumatera, Jakarta SS1, Balikpapan, dan Santan saling terhubung dengan *Cloud Domestic Multiprotocol Label Switching* (MPLS) WAN *Dual Provider* yang merupakan *cloud* nasional perusahaan.
- Region Sumatera dan Jakarta SS1 masing-masing terhubung ke international MPLS WAN yang merupakan *cloud* internasional perusahaan. Bertujuan supaya kantor yang berada di dalam negeri dan luar negeri dapat saling mengakses dan bertukar data.

3.8 *Gantt Chart*

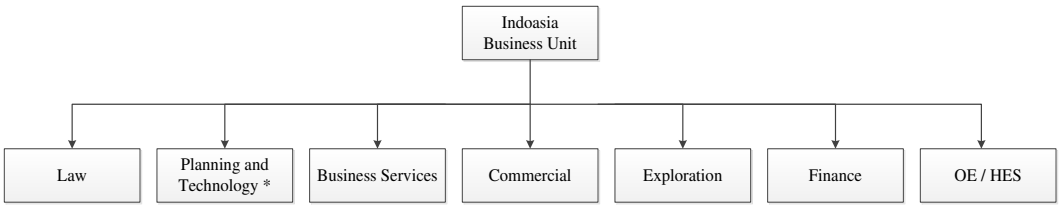
Rencana penyusunan tugas akhir ini dilakukan dari minggu ke-3 bulan Februari sampai minggu ke-4 bulan Juli. Berikut adalah *timeline* rincian kegiatan penyusunan tugas akhir.

Deskripsi	Periode																							
	Februari 2014				Maret 2014				April 2014				Mei 2014				Juni 2014				Juli 2014			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Pemilihan topik																								
Menemukan masalah																								
Penyusunan pendahuluan																								
Pencarian referensi																								
Penyusunan metodologi dan kerangka pemikiran																								
Revisi proposal skripsi																								
Persiapan seminar proposal																								
Seminar proposal skripsi																								
Revisi proposal skripsi																								
Penyusunan pertanyaan																								
Pelaksanaan wawancara																								
Penyusunan kuesioner																								
Pelaksanaan survei																								
Analisis data																								
Revisi																								
Persiapan sidang skripsi																								
Sidang skripsi																								
Revisi hasil sidang skripsi																								

Tabel 3.3 Gantt Chart Penyusunan Tugas Akhir

3.9 Struktur Organisasi Perusahaan

Berikut ini adalah gambaran struktur organisasi yang diterapkan dalam perusahaan.



Gambar 3.3 Struktur Organisasi Perusahaan

BAB IV
ANALISIS DAN PEMBAHASAN

4.1 Hasil Wawancara

4.1.1 Departemen IT

Setelah dilakukan wawancara kepada departemen IT, penulis mendapatkan informasi tentang sistem dan kebijakan pengamanan data dalam perusahaan dengan menggunakan standar COBIT 5.

Berdasarkan domain COBIT 5 pada domain APO01.08, APO09.03, DSS04.07, DSS05.06, DSS06.03, MEA01.01, dan MEA03.03, penulis mendapatkan bahwa sistem dan kebijakan perusahaan adalah sebagai berikut.

a. APO01.08
   - Pengadaan penghitungan mengenai tingkat kepatuhan karyawan terhadap kebijakan pengamanan data yang telah diterapkan
   - Terdapat kebiasaan beberapa karyawan melakukan penyimpanan data bukan di P *drive* melainkan di *local drive*. Hal tersebut menjadi permasalahan bagi IT untuk dapat tetap menjaga keamanan data karyawan. Beberapa cara yang digunakan untuk mengamankan data adalah dengan melakukan *backup* secara terjadwal terhadap data karyawan yang tersimpan di *local drive*.
   - Apabila terjadi kehilangan data karyawan yang tersimpan di *local drive*, perusahaan berusaha untuk membantu *recovery* data karyawan dengan menggunakan *software recovery tools*. Sedangkan apabila terjadi kehilangan data di P *drive* yang disebabkan oleh kelalaian karyawan, karyawan diwajibkan segera menghubungi pihak IT untuk *recovery* data.

- *Output*:

Deskripsi	Tindakan
Perbaikan dari tindakan ketidakpatuhan	• Perusahaan melakukan *backup* secara terjadwal terhadap data karyawan di *local drive*. • Perusahaan melakukan *recovery* data karyawan yang tersimpan di *local drive.*

Tabel 4.1 Tabel Output APO01.08

b. APO09.03

- Perusahaan menerapkan keamanan untuk melindungi data yang tersimpan pada P *drive*.
- Perusahaan memberikan jaminan kepada karyawan terhadap kerahasiaan, integritas, dan ketersediaan data yang tersimpan pada P *drive*.
- Jaminan keamanan dalam bentuk enkripsi data dalam pertukaran data serta pemberian perlindungan pada *network drive* dengan menggunakan aplikasi *drive encryption*.
- *Output*:

Deskripsi	Tindakan
Service level agreements	• Perusahaan memberikan jaminan keamanan (kerahasiaan, integritas, ketersediaan) data karyawan. • Data yang mengalir melalui sistem jaringan perusahaan diberikan pengamanan berupa enkripsi. • PC *server* dan *client* yang ada di perusahaan diberikan *software* antivirus untuk mencegah kerusakan data.

Tabel 4.2 Tabel Output APO09.03

c. DSS04.07

- Dalam pengamanan data, perusahaan melakukan metode penyimpanan data karyawan pada P *drive*. *Folder* "*My Documents*" secara *default* tersimpan di P *drive.* Kapasitas P *drive* yang diterapkan adalah sebesar 9 TB.
- Dalam penyimpanan data, *storage* yang digunakan untuk penyimpanan P *drive* adalah menggunakan teknologi RAID-5.
- Metode *archiving* untuk data yang tersimpan di P *drive* adalah menggunakan *Tape Backup* dengan media LTO-5 dan dilakukan secara 24 jam *nonstop*.
- Perusahaaan memberikan sosialisasi terkait kebijakan pengamanan data dengan menggunakan penjelasan yang mudah dipahami oleh seluruh karyawan dari berbagai departemen.
- Sosialisasi yang diadakan dikaitkan dengan tujuan bisnis, dilakukan penjelasan terhadap keuntungan dalam penyimpanan data di P *drive* dan dampak-dampak yang dapat terjadi apabila tidak patuh terhadap kebijakan pengamanan data.
- Karyawan dihimbau untuk melakukan *backup* data pekerjaan mereka menggunakan media portabel pribadi yang telah diproteksi dengan menggunakan enkripsi. Aktivitas *backup* dilakukan supaya apabila kinerja *server* dan jaringan sedang buruk, karyawan tetap dapat mengerjakan pekerjaan kantor dengan data yang telah disimpan dalam media portabel pribadi yang telah dienkripsi tersebut.
- Pelaksanaan *backup* data yang dilakukan secara terjadwal oleh pihak IT menggunakan perintah *robocopy* dengan metode *remote backup*. Data yang telah di-*backup* kemudian disimpan di *storage*.
- Proses *remote backup* dengan *robocopy* memiliki kekurangan sebagai berikut:
    - Apabila data yang akan di-*copy* sedang terbuka, data tersebut tidak bisa ter-*copy* sehingga proses *remote backup* dengan *robocopy* tidak dapat menjamin keamanan 100% data pekerjaan

karyawan. Kemudian dua minggu setelah *backup* dilaksanakan, data karyawan akan dihapus dari *storage*.

- Tidak menjamin keamanan data secara *real time*. Apabila saat data hilang berbeda dengan saat data di-*backup* oleh IT, data yang disimpan pada rentang waktu antara *backup* dan data pada *local drive* hilang tidak ter-*backup* sehingga data tidak terselamatkan.

- *Output*:

Deskripsi	Tindakan
Pengecekan hasil dari *backup* data	• Data yang tersimpan di *folder* "*My Documents*" secara *default* tersimpan di P *drive* • Pelaksanaan *backup* terhadap data di *local drive.* • Pengadaan sosialisasi tentang pengamanan data. • Pelaksanaan *backup* data secara *offsite* (*remote desktop*) hanya dapat dilakukan oleh IT *Computing and Infrastrusture.* • Karyawan melakukan *backup onsite* dengan menggunakan media penyimpanan portabel pribadi.

Tabel 4.3 Tabel Output DSS04.07

d. DSS05.06

- Perusahaan telah menerapkan sistem keamanan dalam pengamanan data karyawan. Penerapan sistem keamanan tersebut adalah berupa pemberian *smartbadge*, *user ID*, dan *password* apabila akan mengakses PC.
- Pengamanan data selain menjadi tanggung jawab pihak IT, juga merupakan tanggung jawab karyawan. Karyawan diwajibkan

memantau data mereka supaya tidak diakses oleh pihak yang tidak berkepentingan untuk mencegah penyalahgunaan data.

- Karyawan tidak boleh menyebarkan data perusahaan keluar dari lingkup perusahaan.
- *Output*:

Deskripsi	Tindakan
Inventaris dari dokumen dan *devices* yang sensitif	• Perusahaan menyediakan *local drive* dan *network drive* untuk menyimpan data. • Tiap inventaris penyimpanan data yang disediakan diberikan perlindungan berupa enkripsi.
Hak akses	• *Smartbadge*, *user ID*, dan *password* diperlukan untuk melakukan pengaksesan sistem PC.

Tabel 4.4 Tabel Output DSS05.06

e. DSS06.03

- Peraturan yang diterapkan dalam perusahaan adalah tiap karyawan diwajibkan melindungi data perusahaan. Penjagaan data berlaku untuk semua data baik data pekerjaan personal karyawan maupun data *confidential* perusahaan. Karyawan tidak boleh menyebarkan data kepada pihak yang tidak berkepentingan untuk mencegah tindakan penyalahgunaan data.
- Pencegahan yang dilakukan perusahaan dalam hal pelanggaran terhadap kebijakan pengamanan data adalah dengan mengembangkan budaya sadar risiko informasi (*information risk awareness*). Perusahaan juga menerapkan peraturan yang ditujukan kepada para *supervisor* untuk menghimbau *subvisor* untuk mematuhi kebijakan pengamanan data.
- Perusahaan memberikan hak akses kepada karyawan sesuai kewajiban dan tanggung jawab. Sebagai contoh: Departemen IT berhak

mengakses data karyawan demi pengamanan data karyawan. Jaminan bahwa pihak IT tidak menyalahgunakan data karyawan adalah adanya kontrak kerja tentang hak, kewajiban, dan tanggung jawab pihak IT terhadap keamanan data perusahaan beserta risiko-risiko yang akan diterima apabila menyalahgunakan data perusahaan.

- Output:

Deskripsi	Tindakan
Pengalokasian peran dan tanggung jawab	• Tanggung jawab karyawan untuk menjaga keamanan data mereka. • Tanggung jawab pihak IT untuk menjaga data karyawan di P *drive.* • Karyawan berperan untuk menegakkan *security awareness.* • *Supervisor* berperan untuk menghimbau *subvisor* untuk peduli terhadap keamanan data.
Pengalokasian hak akses	• Hak akses data hanya untuk karyawan tersebut secara personal. • Hak akses IT *administrator* dapat mengakses dengan tujuan untuk mengamankan data karyawan tetapi tidak boleh menyalahgunakan data tersebut.

Tabel 4.5 Tabel Output DSS06.03

f. MEA01.01

- Pengadaan *monitoring* kepada karyawan mengenai penilaian terhadap P *drive*. Apabila terjadi masalah, dapat dilaporkan dan dilakukan pembuatan penanganan ataupun kebijakan baru untuk kedepannya.
- Perusahaan menerapkan sistem penyimpanan dan pengaksesan data pada P *drive* dengan mempertimbangkan segi kemudahan,

kenyamanan, dan efisiensi waktu supaya proses tersebut tidak mengganggu pekerjaan karyawan.

- Perusahaan melakukan evaluasi terhadap sistem pengamanan data setiap tahunnya.
- *Output*:

Deskripsi	Tindakan
Pemantauan kebutuhan	• Menganalisis sumber daya yang berkaitan dengan sistem pengamanan data.
Pemantauan tujuan dan metrik yang disetujui	• Menganalisis kemudahan, kenyamanan, dan efisiensi dalam penyimpanan maupun pengaksesan data pada P *drive*.

Tabel 4.6 Tabel Output MEA01.01

g. MEA03.03

- Perusahaan mengadakan penilaian kepada karyawan mengenai kebijakan pengamanan data. Penilaian dilakukan dengan tujuan untuk mengetahui apakah kebijakan yang diterapkan dapat dipatuhi oleh karyawan atau tidak.
- Penilaian dari karyawan terhadap kebijakan pengamanan data digunakan sebagai acuan dalam pembuatan kebijakan yang akan datang.
- *Output*:

Deskripsi	Tindakan
Mengidentifikasi kesenjangan kepatuhan	• Melakukan evaluasi terhadap kesenjangan kepatuhan terhadap kebijakan pengamanan data.
Mengkonfirmasi kepatuhan	• Mengukur tingkat kepatuhan karyawan. • Melakukan penilaian terhadap penerapan kebijakan.

Tabel 4.7 Tabel Output MEA03.03

4.1.2 Karyawan

Setelah dilakukannya wawancara kepada karyawan, penulis mendapatkan informasi mengenai faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data. Selain itu hipotesis yang ditentukan terhadap tingkat kepatuhan karyawan terhadap kebijakan pengamanan data adalah pada indeks 4.00.

Faktor yang diutarakan oleh responden dikelompokkan menjadi empat aspek yaitu aspek keamanan, regulasi, pengaksesan, dan utilisasi. Berikut adalah faktor-faktor yang diutarakan oleh karyawan beserta domain COBIT 5 yang digunakan.

FAKTOR		
NO.	**DESKRIPSI**	**DOMAIN COBIT 5**
A	**KEAMANAN**	
1	Jaminan kerahasian data yang disimpan di P *drive*	APO09.03
2	Jaminan konsistensi informasi dalam tiap data yang disimpan di P *drive*	APO09.03
3	Jaminan ketersediaan data yang disimpan di P *drive*	APO09.03
4	Kejelasan mengenai adanya peraturan tentang tanggung jawab karyawan untuk melindungi data perusahaan	DSS05.06
5	Keamanan pada penerapan kontrol akses yang telah dilakukan untuk melindungi data dari pengaksesan yang tidak sah	DSS05.06
6	Tanggung jawab yang dimiliki karyawan untuk memantau akses data dari pihak yang tidak berkepentingan	DSS05.06
B	**REGULASI**	
1	Pemahaman terhadap sistem dan kebijakan pengamanan data	DSS06.03

2	Tingkat keyakinan karyawan terhadap aturan yang diterapkan dapat melindungi keamanan data	MEA03.03
3	Tingkat keyakinan karyawan terhadap aturan yang diterapkan dapat dipatuhi semua karyawan	MEA03.03
4	Adanya pengaruh dari teman untuk patuh terhadap kebijakan pengamanan data	DSS06.03
5	Adanya pengaruh dari atasan untuk patuh terhadap kebijakan pengamanan data	DSS06.03
6	Intensitas perusahaan dalam memberikan sosialisasi terhadap kebijakan penyimpanan data	DSS04.07
7	Kejelasan mengenai kebijakan pengamanan data di perusahaan	DSS04.07
8	Kejelasan prosedur penyimpanan data di P *drive*	DSS04.07
9	Kesediaan dalam penanggungan risiko apabila melanggar prosedur pengamanan data	APO01.08
C	**PENGAKSESAN**	
1	Kemudahan dalam penyimpanan data di P *drive*	MEA01.01
2	Efisiensi waktu dalam penyimpanan data di P *drive*	MEA01.01
3	Kenyamanan dalam penyimpanan data di P *drive*	MEA01.01
4	Kemudahan dalam pengaksesan data di P *drive*	MEA01.01
5	Efisiensi waktu dalam pengaksesan data di P *drive*	MEA01.01
6	Kenyamanan dalam pengaksesan data di P *drive*	MEA01.01
D	**UTILISASI**	
1	Besar kapasitas P *drive*	MEA01.01
2	Tingkat kecepatan LAN perusahaan	MEA01.01
3	Kinerja server dan jaringan perusahaan	MEA01.01

Tabel 4.8 Tabel Faktor

4.2 Hasil Survei

Setelah dilaksanakan survei terhadap sejumlah 36 responden mengenai tingkat kepatuhan terhadap kebijakan pengamanan data dan faktor yang mempengaruhi tingkat kepatuhan terhadap kebijakan pengamanan data, akan dilakukan analisis kesenjangan terhadap hasil survei terhadap ekspektasi. Uji validitas dan uji reliabilitas dilakukan sebelum melakukan analisis kesenjangan.

4.2.1 Uji Validitas

Uji validitas akan menguji tiap variabel yang digunakan pada kuesioner, dimana keseluruhan variabel penelitian berjumlah 4 variabel dengan 25 *item* pertanyaan. Uji validitas dilakukan dengan menggunakan metode *bivariate pearson*. Hasil dari uji validitas yang akan didapatkan adalah apakah data yang diperoleh valid atau tidak. Jika *r* hitung untuk tiap *item* pertanyaan lebih besar dari *r* tabel dan nilai *r* positif, maka item pernyataan dikatakan valid (Lihat Lampiran 1).

Berdasarkan analisis yang telah dilakukan, diperoleh bahwa indikator yang digunakan untuk mengukur variabel-variabel yang digunakan dalam penelitian ini mempunyai koefisien korelasi hitung (*r* hitung) yang lebih besar dari *r* tabel = 0.329 (Lihat Lampiran 2) untuk nilai *r* tabel dengan $n = 36$ dan $\alpha = 0.05$, sehingga semua indikator tersebut adalah valid.

4.2.2 Uji Reliabilitas

Uji reliabilitas data pada perusahaan dilakukan dengan tujuan untuk mengetahui adanya konsistensi alat ukur yang berupa kuesioner dalam penggunaannya, atau dengan kata lain alat ukur tersebut mempunyai hasil yang konsisten apabila digunakan berkali-kali pada waktu yang berbeda. Uji reliabilitas data dilakukan dengan menggunakan uji *cronbach-alpha*. Hasil dari uji reliabilitas yang akan didapatkan adalah nilai α. Berikut adalah hasil dari uji reliabilitas.

Reliability Statistics

Cronbach's Alpha	N of Items
.921	25

Tabel 4.9 Tabel Hasil Uji Reliabilitas

Hasil tersebut menunjukkan bahwa alat ukur mempunyai nilai *cronbach's alpha* yang besar yaitu 0.921 sehingga dapat dikatakan bahwa semua konsep pengukur masing-masing variabel dari kuesioner adalah sangat baik dan reliabel (Lihat Lampiran 3). Oleh karena itu, *item-item* pertanyaan pada setiap *item* pertanyaan tersebut layak digunakan sebagai alat ukur.

4.3 Analisis Kesenjangan

Setelah dilakukan analisis, didapatkan kesenjangan pada tingkat kepatuhan karyawan terhadap sistem dan kebijakan pengamanan data. Berikut adalah tabel kesenjangan tingkat kepatuhan.

Penilaian	Nilai Ekspektasi	Nilai Aktual	Kesenjangan
Kepatuhan	**4.00**	**3.83**	**-0.17**

Tabel 4.10 Tabel Kesenjangan Tingkat Kepatuhan

Selain didapatkan hasil yang berupa indeks tingkat kepatuhan, didapatkan juga indeks tingkat faktor-faktor yang mempengaruhinya. Berikut adalah tabel kesenjangan faktor-faktor yang mampengaruhi yang telah dikelompokkan ke dalam aspek keamanan, regulasi, pengaksesan, dan utilisasi.

No.	Faktor	Nilai Ekspektasi	Nilai Aktual	Kesenjangan
A	**Keamanan**	**4.67**	**4.11**	**-0.56**
1	Kerahasiaan Data	4.00	4.03	0.03
2	Integritas Data	5.00	4.00	-1.00
3	Ketersediaan Data	4.00	4.00	0.00
4	Kejelasan Peraturan Tanggung Jawab Karyawan Terhadap Data Perusahaan	5.00	4.28	-0.72
5	Keamanan Kontrol Akses	5.00	4.39	-0.61

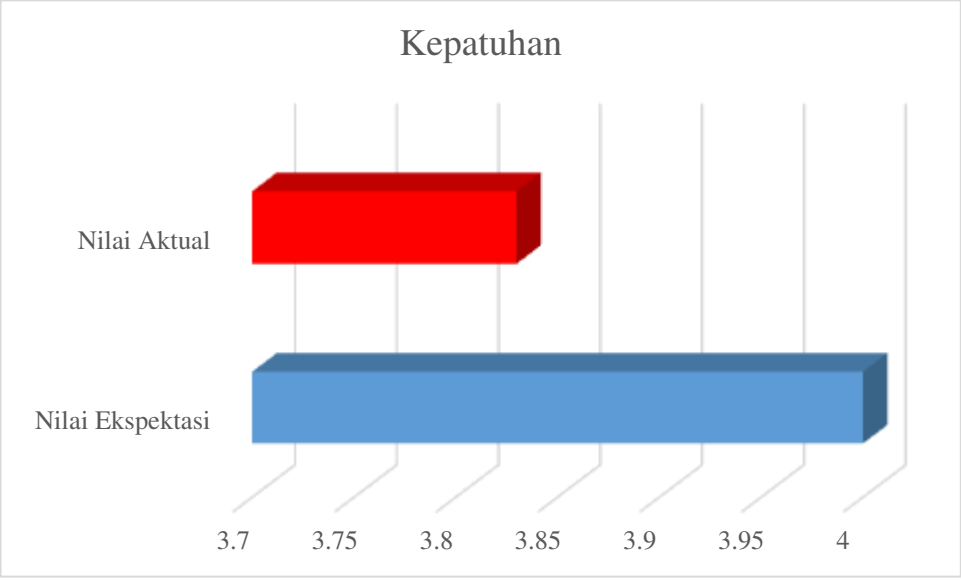
6	Tanggung Jawab Memantau Akses Data	5.00	3.97	-1.03
B	**Regulasi**	**4.22**	**3.93**	**-0.29**
1	Pemahaman Sistem dan Kebijakan	4.00	3.86	-0.14
2	Keyakinan Aturan Dapat Melindungi Data	5.00	4.22	-0.78
3	Keyakinan Aturan Dapat Dipatuhi	4.00	3.83	-0.17
4	Pengaruh Teman	4.00	3.69	-0.31
5	Pengaruh Atasan	5.00	4.06	-0.94
6	Intensitas Sosialisasi	4.00	4.08	0.08
7	Kejelasan Kebijakan	4.00	4.14	0.14
8	Kejelasan Prosedur	4.00	3.86	-0.14
9	Kesediaan Menanggung Risiko	4.00	3.67	-0.33
C	**Pengaksesan**	**3.83**	**3.99**	**0.16**
1	Kemudahan Penyimpanan	4.00	4.19	0.19
2	Efisiensi Waktu Penyimpanan	4.00	3.97	-0.03
3	Kenyamanan Penyimpanan	3.00	3.92	0.92
4	Kemudahan Pengaksesan	4.00	3.97	-0.03
5	Efisiensi Waktu Pengaksesan	4.00	3.92	-0.08
6	Kenyamanan Pengaksesan	4.00	4.00	0.00

D	**Utilisasi**	**3.33**	**3.82**	**0.49**
1	Kapasitas P *drive*	2.00	3.47	1.47
2	Kecepatan LAN	4.00	4.00	0.00
3	Kinerja *Server* dan Jaringan	4.00	4.00	0.00

Tabel 4.11 Tabel Kesenjangan Faktor

Kesenjangan dapat terjadi akibat adanya perbedaan dari apa yang diharapkan oleh perusahaan dengan realita penilaian terhadap karyawan. Tingkat kesenjangan merupakan selisih antara nilai aktual dan nilai ekspektasi. Nilai kesenjangan yang diukur adalah kesenjangan tingkat kepatuhan karyawan terhadap kebijakan pengamanan data serta kesenjangan faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan pengamanan data. Analisis dilakukan setelah didapatkan nilai kesenjangan untuk memberikan penilaian terhadap sistem dan kebijakan pengamanan data yang telah diterapkan oleh perusahaan. Berikut adalah nilai beserta analisis kesenjangan yang diperoleh.

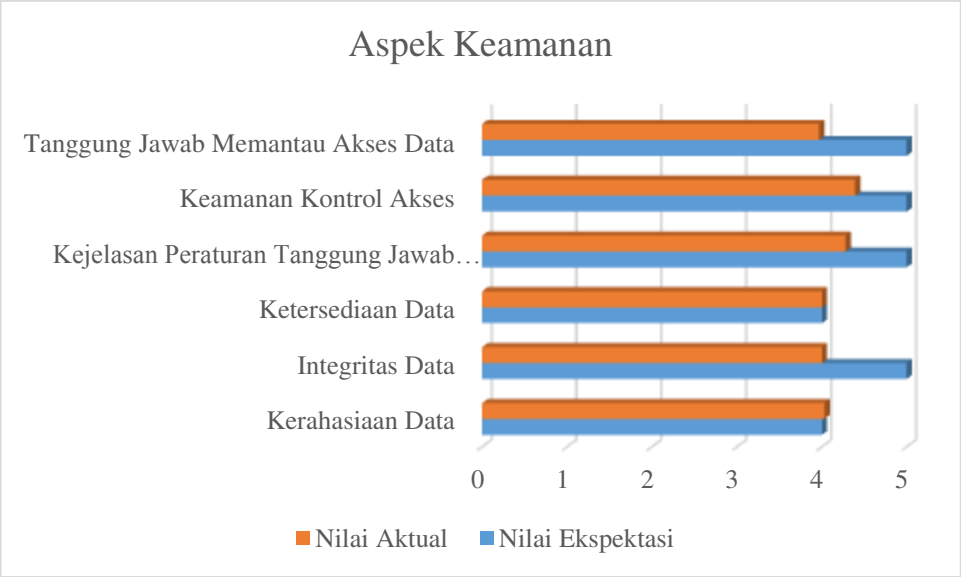
a. Kepatuhan



Gambar 4.1 Grafik Tingkat Kepatuhan

Tingkat kepatuhan karyawan terhadap sistem dan kebijakan pengamanan data yang didapatkan adalah sebesar 3.83 dengan nilai ekspektasi 4.00. Terdapat kesenjangan sebesar -0.17. Penilaian tingkat kepatuhan terhadap sistem dan kebijakan pengamanan data yang dilakukan terhadap karyawan lebih rendah dibandingkan dengan nilai ekspektasi. Perlu adanya peningkatan terhadap faktor-faktor yang mempengaruhi supaya nilai kepatuhan dapat meningkat menjadi lebih besar dari nilai ekspektasi.

b. Aspek Keamanan



Gambar 4.2 Grafik Faktor Aspek Keamanan

Pada aspek keamanan didapatkan nilai rata-rata aktual adalah sebesar 4.11, sedangkan nilai ekspektasi adalah sebesar 4.67. Terdapat kesenjangan sebesar -0.56. Dapat dikatakan bahwa nilai aktual pada aspek keamanan dalam sistem dan kebijakan pengamanan data masih di bawah nilai ekspektasi. Hal ini menunjukkan bahwa penerapan keamanan data pada perusahaan sudah berjalan dengan cukup baik, tetapi masih terdapat beberapa poin yang perlu ditingkatkan karena terdapat nilai kesenjangan negatif yang rendah. Akan tetapi perlu adanya peningkatan pada aspek keamanan pada kebijakan pengamanan data yang akan datang untuk meningkatkan nilai aktual supaya berada sama dengan atau di atas nilai

ekspektasi. Peningkatan pada aspek keamanan dilakukan supaya sistem dan kebijakan pengamanan data yang diterapkan dapat berjalan lebih optimal sehingga diharapkan dapat meningkatkan tingkat kepatuhan karyawan terhadap kebijakan pengamanan data.

Perusahaan perlu meningkatkan jaminan konsistensi informasi di dalam data yang tersimpan pada P *drive* dan memastikan bahwa data karyawan ketika disimpan sama dengan data ketika diakses. Data yang disimpan harus mendapat jaminan bahwa data tidak rusak. Penerapan sistem enkripsi data, keamanan jaringan, dan penerapan *antivirus* perlu diperbaiki supaya sistem keamanan yang ada dapat menjadi lebih baik.

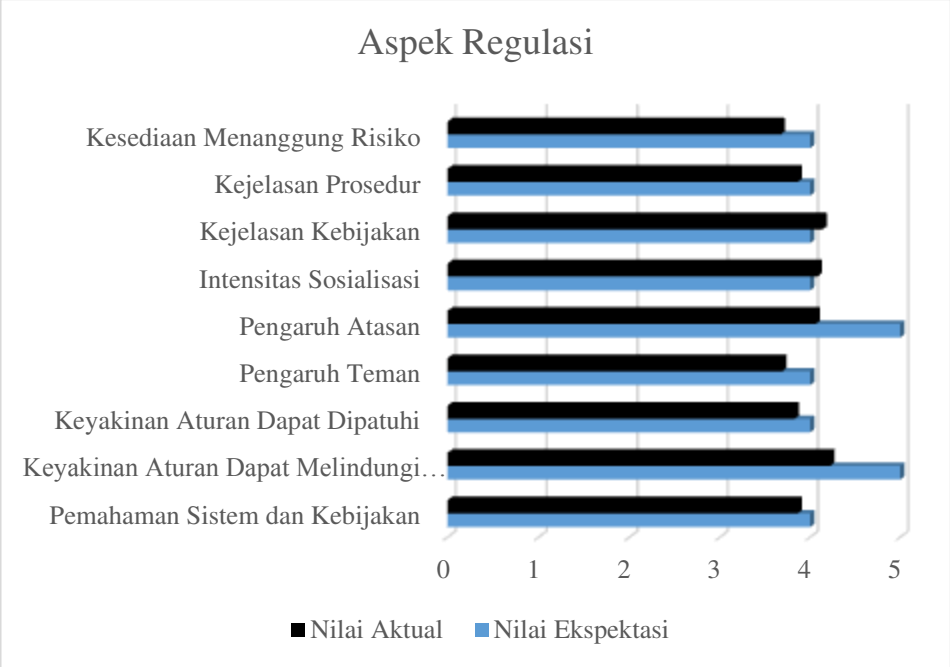
Penerapan kontrol akses yang ada pada perusahaan sudah dinilai cukup baik tetapi perlu adanya peningkatan karena terdapat kesenjangan yang bernilai negatif. Peningkatan kontrol akses pada perusahaan dapat dilakukan dengan cara pemberian akses kontrol pada setiap pengaksesan data sehingga dapat lebih memperkecil kemungkinan data diakses oleh pihak yang tidak berwenang.

Tanggung jawab yang dimiliki oleh karyawan untuk melindungi data mereka terhadap akses tidak sah memiliki nilai di bawah ekspektasi. Kebiasaan sebagian karyawan yang kurang peduli terhadap pengamanan data menyebabkan karyawan ragu terhadap kualitas kepedulian depertemen IT terhadap keamanan data. Akibatnya karyawan tidak yakin atas keamanan data mereka apabila disimpan di P *drive*. Dalam mengatasi hal ini, perlu ditingkatkan budaya kepedulian terhadap keamanan data kepada seluruh karyawan. Hal ini dilakukan supaya karyawan peduli dan tingkat tanggung jawab karyawan diharapkan menjadi lebih tinggi dari nilai ekspektasi. Apabila tingkat tanggung jawab karyawan meningkat, diharapkan tingkat kepercayaan karyawan kepada Departemen IT menjadi lebih meningkat sehingga tingkat kepatuhan karyawan terhadap kebijakan pengamanan data menjadi lebih baik dari nilai ekspektasi.

Tingkat kejelasan peraturan tentang tanggung jawab yang dinilai karyawan berada di bawah nilai ekspektasi. Perusahaan perlu menerapkan peraturan-peraturan yang bertujuan untuk mengontrol penyebaran data di dalam

perusahaan maupun keluar perusahaan. Apabila peraturan diterapkan lebih jelas dan mudah dimengerti, diharapkan nilai aktual akan menjadi lebih besar dari nilai ekspektasi sehingga dapat meningkatkan tingkat kepatuhan karyawan terhadap kebijakan pengamanan data.

c. Aspek Regulasi



Gambar 4.3 Grafik Faktor Aspek Regulasi

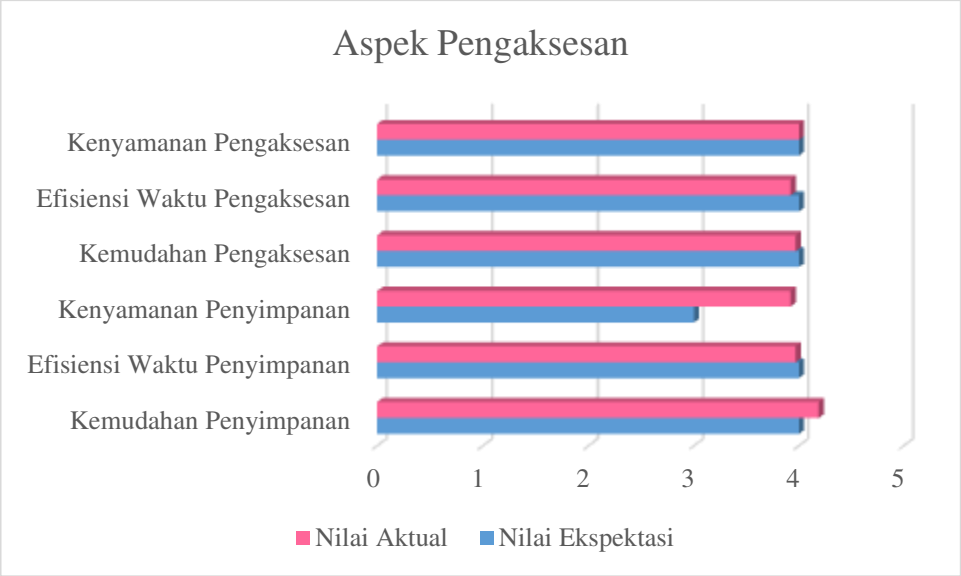
Pada aspek regulasi didapatkan nilai rata-rata aktual adalah sebesar 3.93, sedangkan nilai ekspektasi adalah sebesar 4.22. Terdapat kesenjangan sebesar -0.29. Dapat dikatakan bahwa nilai aktual pada aspek regulasi dalam sistem dan kebijakan pengamanan data masih di bawah nilai ekspektasi. Hal ini menunjukkan bahwa penerapan regulasi terhadap kebijakan keamanan data pada perusahaan sudah berjalan dengan cukup baik, tetapi masih terdapat beberapa poin yang perlu ditingkatkan karena terdapat nilai kesenjangan negatif. Oleh karena itu, perlu adanya perbaikan pada kebijakan yang akan datang terhadap penerapan regulasi yang berkaitan dengan kebijakan pengamanan data untuk meningkatkan nilai aktual supaya berada di atas nilai ekspektasi.

Perusahaan perlu menjelaskan kepada seluruh karyawan mengenai sistem dan kebijakan pengamanan data dengan mengkaitkan dengan tujuan dari tiap departemen. Penggunaan bahasa dalam penjelasan sebaiknya menggunakan bahasa yang lebih sederhana sehingga mudah dimengerti oleh berbagai pihak. Perlu adanya penjelasan mengenai keuntungan dalam penyimpanan data di P *drive* serta dampak-dampak yang dapat terjadi apabila tidak patuh terhadap kebijakan pengamanan data. Perusahaan juga perlu memberikan kejelasan berupa prosedur yang bertujuan untuk memperjelas kebijakan pengamanan data supaya kebijakan yang diterapkan lebih mudah untuk dilakukan sehingga dapat lebih dipatuhi oleh karyawan.

Peran dan tanggung jawab setiap karyawan dalam penegakan kebijakan pengamanan data telah ditentukan oleh perusahaan. Karyawan pada jenjang karir berbeda memiliki peran dan tanggung jawab yang berbeda. Seorang *supervisor* diwajibkan untuk memberikan himbauan kepada *subvisor* untuk patuh terhadap kebijakan pengamanan data. Seorang karyawan diharapkan untuk menegakkan kepatuhan terhadap kebijakan pengamanan data dengan cara mengajak karyawan lain terdekat untuk patuh terhadap kebijakan pengamanan data demi terciptanya budaya sadar risiko informasi.

Penanggungan risiko atas ketidakpatuhan terhadap kebijakan pengamanan data berada di bawah nilai ekspektasi. Perilaku sebagian karyawan yang tidak bersedia menanggung risiko apabila tidak patuh terhadap kebijakan menyebabkan tingkat kepatuhan yang rendah. Hal ini menyebabkan terjadinya kekhawatiran karyawan apabila departemen IT tidak bersedia menanggung risiko apabila terjadi kehilangan atau kerusakan pada data karyawan yang tersimpan di P *drive*. Perlu adanya penegasan mengenai risiko-risiko yang ditanggung karyawan apabila tidak patuh terhadap kebijakan pengamanan data.

d. Aspek Pengaksesan



Gambar 4.4 Grafik Faktor Aspek Pengaksesan

Pada aspek pengaksesan didapatkan nilai rata-rata aktual adalah sebesar 3.99, sedangkan nilai ekspektasi adalah sebesar 3.83. Terdapat kesenjangan sebesar 0.16. Dapat dikatakan bahwa nilai aktual pada aspek pengaksesan data di P *drive* dalam sistem dan kebijakan pengamanan data sudah di atas nilai ekspektasi. Hal ini menunjukkan bahwa penerapan sistem pengaksesan data di P *drive* sudah berjalan dengan baik dikarenakan tingkat kesenjangan yang bernilai positif. Dengan kata lain sistem pengaksesan data pada perusahaan sudah cukup baik untuk diterapkan dan perlu untuk dipertahankan.

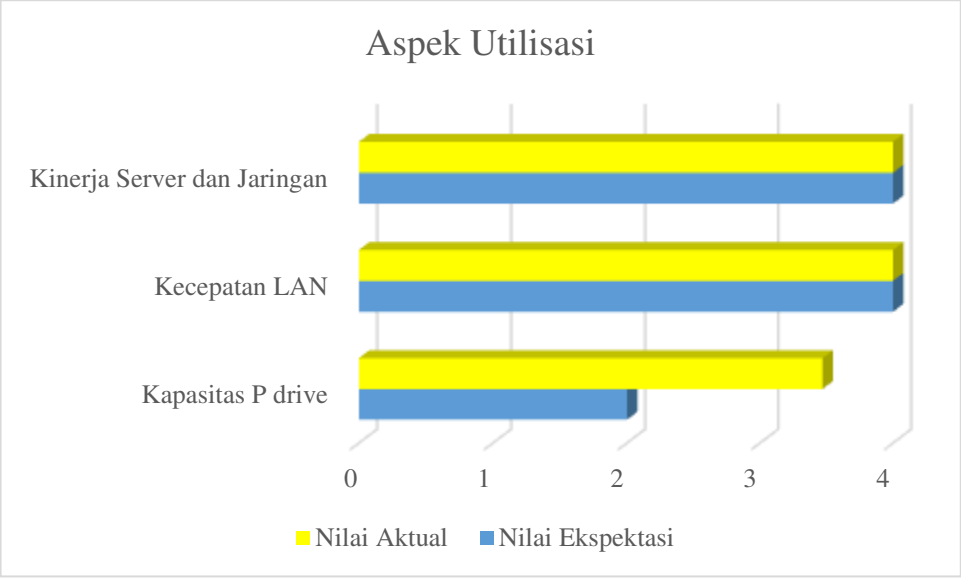
Penyimpanan dan pengaksesan data di P *drive* memiliki tingkat efisiensi waktu di bawah nilai ekspektasi. Perlu adanya metode penyimpanan dan pengaksesan data di P *drive* yang memerlukan waktu lebih singkat. Apabila terdapat metode penyimpanan yang lebih singkat dari implementasi saat ini diharapkan tingkat kepatuhan karyawan dapat meningkat karena tidak memerlukan waktu yang lama sehingga tidak menggangu waktu kerja karyawan. Efisiensi waktu penyimpanan dapat berupa pemangkasan cara untuk menjangkau P *drive*. Dalam penyimpanan, akan lebih efisien apabila *default* penyimpanan untuk

seluruh pekerjaan yang telah dikerjakan tertuju pada *folder* "*My Documents*" dimana tersimpan pada P *drive*, bukan pada *Recent Save Location*. Sedangkan dalam pengaksesan, akan lebih efisien apabila ketika membuka *software* yang menunjang pekerjaan kantor karyawan seperti *Microsoft Office* dengan *default open file* tertuju pada *folder "My Documents*", bukan pada *Recent Save Location*.

Faktor kenyamanan dalam pengaksesan data di P *drive* masih berada di bawah nilai ekspektasi. Hal ini perlu dijadikan budaya bagi karyawan supaya menjadi kebiasaan untuk mengakses data di P *drive* sehingga tingkat kenyamanan akan meningkat seiring berjalannya waktu.

Faktor kemudahaan dalam penyimpanan dan pengaksesan data perlu dipertahankan karena sudah berada di atas nilai ekspektasi. Faktor kemudahan yang bernilai tinggi adalah karyawan tidak harus menghubungi pihak IT apabila hendak membuka dokumen yang tersimpan pada P *drive*, dengan kata lain karyawan dapat membuka data mereka sendiri. Selain itu, kemudahan pengaksesan dengan cara dokumen yang tersimpan pada *folder* "*My Documents*" secara *default* tersimpan pada P *drive*.

e. Aspek Utilisasi



Gambar 4.5 Grafik Faktor Aspek Utilisasi

Pada aspek utilisasi didapatkan nilai rata-rata nilai aktual adalah sebesar 3.82, sedangkan nilai ekspektasi adalah sebesar 3.33. Terdapat kesenjangan positif sebesar 0.49. Dapat dikatakan bahwa nilai aktual pada aspek utilisasi dalam sistem pengamanan data sudah di atas nilai ekspektasi. Hal ini menunjukkan bahwa penerapan utilisasi dalam sistem pengamaan data sudah berjalan dengan baik dikarenakan tingkat kesenjangan yang bernilai positif. Dengan kata lain, utilisasi yang ada pada perusahaan sudah cukup baik untuk diterapkan dan perlu untuk dipertahankan

Fasilitas P *drive* yang disediakan perusahaan sudah baik karena nilai aktual sudah melebihi nilai ekspektasi. Kapasitas P *drive* yang diterapkan saat ini adalah sebesar 9 TB dan dinilai dari prespektif karyawan sudah cukup untuk menyimpan dokumen pekerjaan karyawan. Untuk poin kecepatan LAN serta kinerja *server* dan jaringan perlu dipertahankan sehingga diharapkan nilai aktual dapat bernilai sama atau bahkan melebihi nilai ekspektasi untuk kedepannya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis yang dilakukan terhadap tingkat kepatuhan, faktor-faktor pada aspek keamanan, regulasi, pengaksesan, dan utilisasi, berikut adalah kesimpulan dari penelitian ini yang penulis dapatkan:

- Tingkat kepatuhan karyawan terhadap kebijakan pengamanan data adalah sebesar **3.83** dengan nilai ekspektasi **4.00**. Hasil dari penilaian terhadap karyawan tersebut di bawah nilai ekspektasi. Untuk meningkatkan indeks kepatuhan karyawan menjadi di atas nilai ekspektasi, perlu adanya peningkatan dari aspek keamanan, regulasi, pengaksesan, atau utilisasi.
- Faktor-faktor pada aspek keamanan yang diterapkan masih di bawah nilai ekspektasi. Hasil dari penelitian pada aspek keamanan adalah sebesar **4.11** dengan nilai ekspektasi **4.67**. Faktor pada aspek keamanan yang perlu ditingkatkan adalah:
    - Jaminan integritas data yang tersimpan pada P *drive*.
        - Ekspektasi : 5.00
        - Aktual : 4.00
        - Kesenjangan : -1.00
    - Kejelasan peraturan tentang tanggung jawab karyawan terhadap data perusahaan.
        - Ekspektasi : 5.00
        - Aktual : 4.28
        - Kesenjangan : -0.72
    - Keamanan kontrol akses
        - Ekspektasi : 5.00
        - Aktual : 4.39
        - Kesenjangan : -0.41
    - Tanggung jawab karyawan dalam memantau akses data.
        - Ekspektasi : 5.00

        - Aktual : 3.97
        - Kesenjangan : -1.03

    Peningkatan dilakukan supaya didapatkan nilai indeks faktor-faktor aspek keamanan meningkat sehingga didapatkan tingkat kepatuhan di atas nilai ekspektasi. Sedangkan faktor-faktor yang perlu dipertahankan adalah:

    - Jaminan kerahasiaan data yang tersimpan pada P *drive*
        - Ekspektasi : 4.00
        - Aktual : 4.03
        - Kesenjangan : 0.03
    - Jaminan ketersediaan data yang tersimpan pada P *drive*
        - Ekspektasi : 4.00
        - Aktual : 4.00
        - Kesenjangan : 0.00

- Faktor-faktor pada aspek regulasi yang diterapkan masih di bawah nilai ekspektasi. Hasil dari penelitian pada aspek regulasi adalah sebesar **3.93** dengan nilai ekspektasi **4.22**. Faktor pada aspek regulasi yang perlu ditingkatkan adalah:
    - Pemahaman terhadap sistem dan kebijakan pengamanan data.
        - Ekspektasi : 4.00
        - Aktual : 3.86
        - Kesenjangan : -0.14
    - Keyakinan bahwa aturan yang diterapkan dapat melindungi data
        - Ekspektasi : 5.00
        - Aktual : 4.22
        - Kesenjangan : -0.78
    - Keyakinan bahwa aturan dapat dipatuhi oleh karyawan
        - Ekspektasi : 4.00
        - Aktual : 3.83
        - Kesenjangan : -0.17
    - Pengaruh teman dalam kepatuhan terhadap kebijakan pengamanan data

        - Ekspektasi : 4.00
        - Aktual : 3.69
        - Kesenjangan : -0.31
    - Pengaruh atasan dalam kepatuhan terhadap kebijakan pengamanan data
        - Ekspektasi : 5.00
        - Aktual : 4.06
        - Kesenjangan : -0.94
    - Kejelasan prosedur dalam penyimpanan data di P *drive*
        - Ekspektasi : 4.00
        - Aktual : 3.86
        - Kesenjangan : -0.14
    - Kesediaan menanggung risiko atas pelanggaran terhadap kebijakan pengamanan data
        - Ekspektasi : 4.00
        - Aktual : 3.67
        - Kesenjangan : -0.33

  Peningkatan dilakukan supaya didapatkan nilai indeks faktor-faktor aspek regulasi meningkat sehingga didapatkan tingkat kepatuhan di atas nilai ekspektasi. Sedangkan faktor-faktor yang perlu dipertahankan adalah:

    - Intensitas perusahaan dalam memberikan sosialisasi terhadap kebijakan penyimpanan data
        - Ekspektasi : 4.00
        - Aktual : 4.08
        - Kesenjangan : 0.08
    - Kejelasan mengenai kebijakan pengamanan data di perusahaan
        - Ekspektasi : 4.00
        - Aktual : 4.17
        - Kesenjangan : 0.17

- Secara keseluruhan faktor-faktor pada aspek pengaksesan yang diterapkan sudah di atas nilai ekspektasi. Akan tetapi, perlu adanya peningkatan pada

beberapa faktor yang berada di bawah nilai ekspektasi. Hasil dari penelitian pada aspek pengaksesan adalah sebesar **3.99** dengan nilai ekspektasi **3.83**. Faktor pada aspek pengaksesan yang perlu ditingkatkan adalah:

- Efisiensi waktu penyimpanan data
  - Ekspektasi : 4.00
  - Aktual : 3.97
  - Kesenjangan : -0.03
- Efisiensi waktu pengaksesan data
  - Ekspektasi : 4.00
  - Aktual : 3.92
  - Kesenjangan : -0.08
- Kemudahan pada pengaksesan data
  - Ekspektasi : 4.00
  - Aktual : 3.97
  - Kesenjangan : -0.03

Peningkatan dilakukan supaya didapatkan nilai indeks faktor-faktor aspek pengaksesan meningkat sehingga didapatkan tingkat kepatuhan di atas nilai ekspektasi. Sedangkan faktor-faktor yang perlu dipertahankan adalah:

- Kemudahan dalam penyimpanan data di P drive
  - Ekspektasi : 4.00
  - Aktual : 4.19
  - Kesenjangan : 0.19
- Kenyamanan dalam penyimpanan data di P drive
  - Ekspektasi : 3.00
  - Aktual : 3.92
  - Kesenjangan : 0.92
- Kenyamanan dalam pengaksesan data di P drive
  - Ekspektasi : 4.00
  - Aktual : 4.00
  - Kesenjangan : 0.00

- Faktor-faktor pada aspek utilisasi yang diterapkan sudah di atas nilai ekspektasi. Hasil dari penelitian pada aspek pengaksesan adalah sebesar **3.82** dengan nilai ekspektasi **3.33**. Oleh karena itu, nilai indeks faktor-faktor pada aspek utilisasi perlu dipertahankan. Berikut adalah faktor-faktor pada aspek utilisasi yang perlu dipertahankan:
    - Besar kapasitas P drive
        - Ekspektasi : 2.00
        - Aktual : 3.47
        - Kesenjangan : 1.47
    - Tingkat kecepatan LAN perusahaan
        - Ekspektasi : 4.00
        - Aktual : 4.00
        - Kesenjangan : 0.00
    - Kinerja *server* dan jaringan perusahaan
        - Ekspektasi : 4.00
        - Aktual : 4.00
        - Kesenjangan : 0.00

5.2 Saran

Setelah dilakukan analisis kesenjangan mengenai tingkat kepatuhan terhadap kebijakan pengamanan data dan faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan, perlu adanya peningkatan kedepannya untuk nilai faktor yang berada di bawah nilai ekspektasi.

Adapun saran-saran yang perlu dipertimbangkan untuk dapat meningkatkan performa dari faktor-faktor tersebut adalah sebagai berikut.

- PT XYZ sebaiknya melakukan peningkatan pada sisi keamanan dengan cara memperketat kontrol akses, menegakkan tanggung jawab karyawan terhadap pengamanan data, dan memperbaiki sistem yang bertujuan untuk memelihara konsistensi data di dalam P *drive*.
- PT XYZ sebaiknya menggunakan cara sosialisasi yang lebih jelas, menarik, bahasa yang lebih sederhana, penjelasan mengenai keuntungan dalam kepatuhan kebijakan, dampak akibat pelanggaran kebijakan, dan

mengkaitkan dengan tujuan tiap departemen agar dapat dimengerti oleh semua karyawan di seluruh departemen.

- PT XYZ sebaiknya lebih intensif menghimbau para *supervisor* untuk mengajak *subvisor* supaya lebih patuh terhadap kebijakan pengamanan data.
- PT XYZ perlu melakukan proses *backup* data di luar jam kerja untuk menghindari kegagalan penyalinan data yang disebabkan karena data yang sedang terbuka.
- PT XYZ perlu melakukan sistem penjadwalan secara jelas mengenai tanggal *backup* dan data karyawan mana saja yang akan di-*backup* pada tanggal tersebut.
- PT XYZ perlu mempertimbangkan metode penyimpanan dan pengaksesan data pada P *drive*. Metode yang digunakan sebaiknya menggunakan cara yang lebih sederhana dan tidak memerlukan waktu banyak untuk menyimpan data di P *drive*. Dengan menerapkan semua *default* penyimpanan dokumen pekerjaan pada *folder "My Documents"*, data akan selalu tersimpan ke P *drive*.
- PT XYZ perlu membudayakan karyawan untuk menjadikan P *drive* sebagai *default* penyimpanan dokumen pekerjaan. Perlu pembiasaan dalam pengaksesan data di P *drive* untuk karyawan untuk meningkatkan kenyamanan dalam penyimpanan maupun pengaksesan data pada P *drive*.

DAFTAR PUSTAKA

Alvin, Soekamto, W., & Harsono, R. (2013). *Analisis dan Evaluasi Tata Kelola IT Pada PT FIF dengan Standar COBIT 5.* Tesis. Jakarta: Bina Nusantara University.

An Australian Government Initiative. (2013). *Managing ICT Risk for SMEs.* Enterprise Connect.

Chevron Corp. (2011). *IT Induction Session.* IndoAsia.

Creech, J., & Alderman, M. (2010). *IT Policy Compliance for Dummies.* West Sussex: Wiley.

Handy Backup. (2014, March 27). *Local Backup*. Retrieved from Handy Backup: http://www.handybackup.net/backup_terms/local_backup.shtml

Hicks, J. (2012). *Tips & Tricks for Protecting User Data on Windows 7.* ScriptLogic Corporation.

ISACA. (2012). *COBIT® 5: Enabling Processes.* Rolling Meadows: ISACA.

King, R. P.-M. (1991). Management of a Remote Backup Copy for Disaster Recovery. *ACM Transactions on Database Systems, Vol.16, No.2*, 338.

Pakpahan, C. E. (2013). Desain dan Implementasi Backup dan Restore Data Menggunakan Aplikasi RSYNC dan FTP Server Pada PT. Panca Agro Niaga Lestari Palembang. *Jurnal Jenius Politeknik PalComTech Vol.3 No.1*, 2.

Rainer, R. K., & Charles A. Snyder, H. H. (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems Vol.8 No.1*, 143.

Salido, J. (2010). Data Governance for Privacy, Confidentiality and Compliance: A Holistic Approach. *ISACA Journal Vol. 6*, 2-3.

Supradono, B. (2009). Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation). *Media Elektrika, Vol. 2, No. 1*, 4.

Suyono. (2008). *Penerapan Tata Kelola Pelaksanaan Proyek-Proyek/Kegiatan TI Sekretariat Jenderal Departemen Energi dan Sumber Daya Mineral.* Tesis. Jakarta: Universitas Indonesia.

Valacich, J., & Schneider, C. (2010). *Information Systems Today 4e.* Upper Saddle River: Pearson.

Vibiznews. (2007, November 24). *Manajemen Resiko.* Retrieved from Software Project Management: http://s2informatics.files.wordpress.com/2007/11/proses_manajemen_risiko.pdf

LAMPIRAN

Lampiran 1. Hasil Uji Validitas

		Nilai Total
Tingkat Kepatuhan	Pearson Correlation	**.499(**)**
Kerahasiaan Data	Pearson Correlation	**.619(**)**
Integritas Data	Pearson Correlation	**.451(**)**
Ketersediaan Data	Pearson Correlation	**.397(*)**
Kejelasan Peraturan Tanggung Jawab Data Perusahaan	Pearson Correlation	**.475(**)**
Keamanan Kontrol Akses	Pearson Correlation	**.498(**)**
Tanggung Jawab Karyawan Memantau Akses Data	Pearson Correlation	**.601(**)**
Pemahaman Sistem dan Kebijakan	Pearson Correlation	**.570(**)**
Keyakinan Aturan Dapat Melindungi Data	Pearson Correlation	**.672(**)**
Keyakinan Aturan Dapat Dipatuhi	Pearson Correlation	**.686(**)**
Pengaruh Teman	Pearson Correlation	**.484(**)**
Pengaruh Atasan	Pearson Correlation	**.707(**)**
Intensitas Sosialisasi	Pearson Correlation	**.575(**)**

		Nilai Total
Kejelasan Kebijakan	Pearson Correlation	**.777(**)**
Kejelasan Prosedur	Pearson Correlation	**.706(**)**
Kesediaan Menanggung Risiko	Pearson Correlation	**.686(**)**
Kemudahan Penyimpanan	Pearson Correlation	**.507(**)**
Efisiensi Waktu Penyimpanan	Pearson Correlation	**.652(**)**
Kenyamanan Penyimpanan	Pearson Correlation	**.738(**)**
Kemudahan Penyimpanan	Pearson Correlation	**.674(**)**
Efisiensi Waktu Penyimpanan	Pearson Correlation	**.666(**)**
Kenyamanan Penyimpanan	Pearson Correlation	**.780(**)**
Kapasitas P *drive*	Pearson Correlation	**.358(*)**
Kecepatan LAN	Pearson Correlation	**.526(**)**
Kinerja *Server* dan Jaringan	Pearson Correlation	**.445(**)**
Nilai Total	Pearson Correlation	**1**

(**) Korelasi signifikan pada $\alpha = 0.01$ (*two-tailed*)

(*) Korelasi signifikan pada $\alpha = 0.05$ (*two-tailed*)

Lampiran 2. Tabel Koefisien Korelasi (*r*)

(Sumber : http://junaidichaniago.wordpress.com)

df = (N-2)	Tingkat signifikansi untuk uji satu arah				
	0.05	0.025	0.01	0.005	0.0005
	Tingkat signifikansi untuk uji dua arah				
	0.1	0.05	0.02	0.01	0.001
1	0.9877	0.9969	0.9995	0.9999	1.0000
2	0.9000	0.9500	0.9800	0.9900	0.9990
3	0.8054	0.8783	0.9343	0.9587	0.9911
4	0.7293	0.8114	0.8822	0.9172	0.9741
5	0.6694	0.7545	0.8329	0.8745	0.9509
6	0.6215	0.7067	0.7887	0.8343	0.9249
7	0.5822	0.6664	0.7498	0.7977	0.8983
8	0.5494	0.6319	0.7155	0.7646	0.8721
9	0.5214	0.6021	0.6851	0.7348	0.8470
10	0.4973	0.5760	0.6581	0.7079	0.8233
11	0.4762	0.5529	0.6339	0.6835	0.8010
12	0.4575	0.5324	0.6120	0.6614	0.7800
13	0.4409	0.5140	0.5923	0.6411	0.7604
14	0.4259	0.4973	0.5742	0.6226	0.7419
15	0.4124	0.4821	0.5577	0.6055	0.7247
16	0.4000	0.4683	0.5425	0.5897	0.7084
17	0.3887	0.4555	0.5285	0.5751	0.6932
18	0.3783	0.4438	0.5155	0.5614	0.6788
19	0.3687	0.4329	0.5034	0.5487	0.6652
20	0.3598	0.4227	0.4921	0.5368	0.6524
21	0.3515	0.4132	0.4815	0.5256	0.6402
22	0.3438	0.4044	0.4716	0.5151	0.6287
23	0.3365	0.3961	0.4622	0.5052	0.6178
24	0.3297	0.3882	0.4534	0.4958	0.6074
25	0.3233	0.3809	0.4451	0.4869	0.5974

26	0.3172	0.3739	0.4372	0.4785	0.5880
27	0.3115	0.3673	0.4297	0.4705	0.5790
28	0.3061	0.3610	0.4226	0.4629	0.5703
29	0.3009	0.3550	0.4158	0.4556	0.5620
30	0.2960	0.3494	0.4093	0.4487	0.5541
31	0.2913	0.3440	0.4032	0.4421	0.5465
32	0.2869	0.3388	0.3972	0.4357	0.5392
33	0.2826	0.3338	0.3916	0.4296	0.5322
34	0.2785	0.3291	0.3862	0.4238	0.5254
35	0.2746	0.3246	0.3810	0.4182	0.5189
36	0.2709	0.3202	0.3760	0.4128	0.5126
37	0.2673	0.3160	0.3712	0.4076	0.5066
38	0.2638	0.3120	0.3665	0.4026	0.5007
39	0.2605	0.3081	0.3621	0.3978	0.4950
40	0.2573	0.3044	0.3578	0.3932	0.4896
41	0.2542	0.3008	0.3536	0.3887	0.4843
42	0.2512	0.2973	0.3496	0.3843	0.4791
43	0.2483	0.2940	0.3457	0.3801	0.4742
44	0.2455	0.2907	0.3420	0.3761	0.4694
45	0.2429	0.2876	0.3384	0.3721	0.4647
46	0.2403	0.2845	0.3348	0.3683	0.4601
47	0.2377	0.2816	0.3314	0.3646	0.4557
48	0.2353	0.2787	0.3281	0.3610	0.4514
49	0.2329	0.2759	0.3249	0.3575	0.4473
50	0.2306	0.2732	0.3218	0.3542	0.4432

Lampiran 3. Tabel Koefisien Cronbach's Alpha (α)

(*Sumber : http://en.wikipedia.org/wiki/Cronbach's_alpha*)

Cronbach's alpha	Konsistensi
$\alpha \geq 0.9$	Sangat baik
$0.7 \leq \alpha < 0.9$	Baik
$0.6 \leq \alpha < 0.7$	Dapat diterima
$0.5 \leq \alpha < 0.6$	Buruk
$\alpha < 0.5$	Tidak dapat diterima

Lampiran 4. Tabel Olahan Rata-rata Nilai Aktual Tingkat Kepatuhan dan Faktor

Responden	Kepatuhan	Faktor			
		Keamanan	Regulasi	Pengaksesan	Utilisasi
1	3	4.67	3.33	3.33	4.33
2	5	3.67	4.56	4.5	4.67
3	3	3.67	3.67	4.33	4.33
4	4	4	4	5	4
5	4	4.67	3.67	3.17	2.67
6	2	2.83	3	3.5	3.67
7	5	5	4.89	4	3
8	4	4.5	3.44	2.5	4
9	3	3.5	3.56	4	4
10	4	4.5	4.11	4.33	4
11	4	4.5	4.22	4	3.67
12	5	5	4.33	4.67	5
13	4	4.33	3.89	4.67	3.33
14	4	4.17	4.11	4	4
15	4	4.17	4.11	3.5	4.67
16	4	3.83	3.22	3.67	4
17	4	4	3	3.67	3.33
18	3	5	5	5	5
19	2	3.33	3	3.17	2.33
20	4	4.5	4.33	3.67	3.33
21	4	3.5	4.44	5	4
22	5	4.67	4.89	5	3.67
23	5	3.5	3.67	3.83	4
24	4	4	4.22	4.17	3.67
25	5	3.67	4.44	3.67	4.33
26	4	3.67	2.89	4	3.67
27	4	3.17	3.67	3.5	3.67
28	5	4.83	4.67	4.67	4.67
29	3	4.33	3.89	4	3.33
30	4	4.83	4.11	5	3.67
31	3	3	3	3	3.67
32	4	3.5	3.33	3.33	2.67
33	3	4.67	4.33	4.83	4.67
34	3	4.17	4.33	3.83	3.67
35	3	4.17	3.67	3.5	3.67
36	4	4.5	4.67	3.83	3.33

Lampiran 5. Kuesioner Penelitian

KUESIONER PENELITIAN

Saya Dimas Aryo Anggoro, mahasiswa Program Sarjana Universitas Bakrie, Fakultas Teknik dan Ilmu Komputer, Program Studi Teknik Informatika, bermaksud untuk melakukan penelitian dalam rangka penyusunan Tugas Akhir yang berjudul:

" ANALISIS KEPATUHAN KARYAWAN TERHADAP KEBIJAKAN PENGAMANAN DATA PADA PT XYZ DENGAN STANDAR COBIT 5"

Sehubungan dengan hal tersebut, saya mengharapkan bantuan Bapak/Ibu untuk bersedia mengisi kuisioner yang telah disusun sesuai dengan kondisi nyata yang dirasakan oleh Bapak/Ibu. Jawaban Bapak/Ibu akan sangat bermanfaat bagi penelitian ini. Atas kesediaan dan kerjasama Bapak/Ibu, saya ucapkan terima kasih.

IDENTITAS RESPONDEN

Jenis kelamin : Laki-laki / Perempuan
Umur : ..... tahun

PETUNJUK PENGISIAN

Kuesioner ini ditujukan untuk mengukur:

- Tingkat kepatuhan karyawan terhadap kebijakan pengamanan data
- Sistem dan kebijakan pengamanan data perusahaan pada PT XYZ dari perspektif karyawan sebagai faktor yang mempengaruhi tingkat kepatuhan terhadap kebijakan pengamanan data.

Pada bagian ini, Bapak/Ibu diminta untuk **melingkari** atau **memberikan tanda silang (x)** pada salah satu kolom nilai pemenuhan. Adapun penjelasan mengenai penilaian tiap item pertanyaan adalah sebagai berikut:

Nilai 1 = Sangat Rendah
Nilai 2 = Rendah
Nilai 3 = Cukup
Nilai 4 = Tinggi
Nilai 5 = Sangat Tinggi

NO.	PERTANYAAN	TINGKAT				
		RENDAH				TINGGI
	KEPATUHAN					
1	Seberapa besar tingkat kepatuhan anda untuk menyimpan data pekerjaan di P *drive*?	1	2	3	4	5
A	**KEAMANAN**					
1	Seberapa besar jaminan kerahasiaan data yang disimpan pada P *drive*?	1	2	3	4	5
2	Seberapa besar jaminan konsistensi informasi dalam tiap data yang disimpan pada P *drive*?	1	2	3	4	5
3	Seberapa besar jaminan ketersediaan data yang disimpan pada P *drive*?	1	2	3	4	5
4	Seberapa jelas peraturan tentang tanggung jawab karyawan untuk melindungi data perusahaan disampaikan?	1	2	3	4	5
5	Seberapa aman penerapan kontrol akses yang telah dilakukan untuk melindungi data dari pengaksesan yang tidak sah?	1	2	3	4	5
6	Seberapa besar tanggung jawab yang dimiliki karyawan untuk memantau akses data dari pihak yang tidak berkepentingan?	1	2	3	4	5

B	**REGULASI**					
1	Seberapa besar pemahaman anda terhadap sistem dan kebijakan pengamanan data?	1	2	3	4	5
2	Seberapa besar keyakinan anda bahwa apabila aturan yang diterapkan dapat melindungi keamanan data?	1	2	3	4	5
3	Seberapa besar keyakinan anda bahwa apabila aturan yang diterapkan dapat dipatuhi semua karyawan?	1	2	3	4	5
4	Seberapa besar pengaruh dari teman untuk patuh terhadap kebijakan pengamanan data?	1	2	3	4	5
5	Seberapa besar pengaruh dari atasan untuk patuh terhadap kebijakan pengamanan data?	1	2	3	4	5
6	Seberapa besar tingkat intensitas perusahaan memberikan sosialisasi terhadap kebijakan pengamanan data?	1	2	3	4	5
7	Seberapa jelas kebijakan pengamanan data di perusahaan disampaikan?	1	2	3	4	5
8	Seberapa jelas prosedur penyimpanan data di P *drive* disampaikan?	1	2	3	4	5
9	Seberapa besar kesediaan anda untuk menanggung risiko apabila melanggar prosedur pengamanan data?	1	2	3	4	5
C	**PENGAKSESAN**					
1	Seberapa besar tingkat kemudahan dalam penyimpanan data di P *drive*?	1	2	3	4	5
2	Seberapa besar tingkat efisiensi waktu dalam penyimpanan data di P *drive*?	1	2	3	4	5
3	Seberapa besar tingkat kenyamanan dalam penyimpanan data di P *drive*?	1	2	3	4	5

4	Seberapa besar tingkat kemudahan dalam pengaksesan data di P *drive*?	1	2	3	4	5
5	Seberapa besar tingkat efisiensi waktu dalam pengaksesan data di P *drive*?	1	2	3	4	5
6	Seberapa besar tingkat kenyamanan dalam pengaksesan data di P *drive*?	1	2	3	4	5
D	**UTILISASI**					
1	Seberapa besar kapasitas P *drive* yang disediakan oleh perusahaan untuk tiap karyawan?	1	2	3	4	5
2	Seberapa cepat LAN yang diterapkan di perusahaan?	1	2	3	4	5
3	Seberapa baik kinerja *server* dan jaringan yang diterapkan di perusahaan?	1	2	3	4	5

Lampiran 6. Hasil Wawancara kepada Departemen IT

a. Pertanyaan:

   Bagaimanakah perusahaan memberikan jaminan keamanan terhadap data yang tersimpan di P *drive* dengan mempertimbangkan segi kerahasiaan, integritas, dan ketersediaan data?

   Jawaban:

   Departemen IT menerapkan keamanan untuk melindungi data yang tersimpan pada P *drive*. Departemen IT memberikan jaminan kepada *user* terhadap kerahasiaan, integritas, dan ketersediaan data yang tersimpan pada P *drive*.

   Jaminan keamanan dalam bentuk enkripsi data dalam pertukaran data serta pemberian perlindungan pada *network drive* dengan menggunakan aplikasi *drive encryption* menggunakan *BitLocker Recovery Tools* serta menerapkan *antivirus* pada seluruh PC.

b. Pertanyaan:

   Bagaimanakah kejelasan mengenai adanya peraturan tentang tanggung jawab karyawan untuk melindungi data perusahaan?

   Jawaban:

   Perusahaan memberikan hak akses kepada *user* sesuai kewajiban dan tanggung jawab. Sebagai contoh: Departemen IT berhak mengakses data *user* demi pengamanan data *user*. Jaminan bahwa pihak IT tidak menyalahgunakan data *user* adalah adanya kontrak kerja tentang hak, kewajiban, dan tanggung jawab pihak IT terhadap keamanan data perusahaan beserta risiko-risiko yang akan diterima apabila menyalahgunakan data perusahaan.

   Penjelasan tentang kewajiban IT adalah melakukan *backup* data secara terjadwal yang menggunakan perintah *robocopy* dengan *remote backup*. Data yang sudah di-*backup* kemudian disimpan di *storage*. Tetapi proses *robocopy* memiliki kekurangan:

   - Apabila data yang akan di-*copy* sedang terbuka, data tersebut tidak bisa ter-*copy* sehingga proses *remote backup* dengan *robocopy* tidak

dapat menjamin keamanan 100% data pekerjaan *user*. Kemudian dua minggu setelah *backup* dilaksanakan, data *user* akan dihapus dari *storage* jika tidak ada *complain* tentang data yang hilang.

- Tidak menjamin keamanan data secara *real time*. Jika saat data hilang berbeda dengan saat data di-*backup* oleh IT, data yang disimpan pada rentang waktu antara backup dan data pada *local drive* hilang tidak ter-*backup* sehingga data tidak terselamatkan.

c. Pertanyaan:

   Bagaimanakah kontrol akses pada perusahaan diterapkan? Keamanan kontrol akses yang bertujuan untuk memasuki sistem?

   Jawaban:

   Perusahaan telah menerapkan sistem keamanan dalam pengamanan data *user*. Penerapan sistem keamanan tersebut adalah berupa pemberian *smartbadge*, *user ID*, dan *password* apabila akan mengakses PC.

d. Pertanyaan:

   Bagaimana tanggung jawab yang dilakukan oleh seluruh *user* terhadap pengamanan data?

   Jawaban:

   Pengamanan data adalah tanggung jawab seluruh karyawan perusahaan. *User* diwajibkan memantau data mereka supaya tidak diakses oleh pihak yang tidak berkepentingan untuk mencegah penyalahgunaan data. *User* tidak boleh menyebarkan data perusahaan keluar dari lingkup perusahaan.

e. Pertanyaan:

   Bagaimanakah sosialisasi mengenai sistem dan kebijakan pengamanan data diterapkan sehingga dapat dipahami oleh *user*?

   Jawaban:

   Perusahaaan memberikan sosialisasi terkait kebijakan pengamanan data dengan menggunakan penjelasan yang mudah dipahami oleh seluruh *user*.

f. Pertanyaan:

Apakah ada keyakinan bahwa aturan dapat melindungi data?

Jawaban:

Peraturan yang diterapkan dalam perusahaan adalah tiap *user* diwajibkan melindungi data perusahaan. Penjagaan data berlaku untuk semua data baik data pekerjaan personal *user* maupun data *confidential* perusahaan. *User* tidak boleh menyebarkan data kepada pihak yang tidak berkepentingan untuk mencegah tindakan penyalahgunaan data.

User dihimbau untuk melakukan *backup* data pekerjaan mereka menggunakan media portabel pribadi yang telah dienkripsi. *Backup* dilakukan supaya apabila kinerja *server* dan jaringan sedang buruk, *user* tetap dapat mengerjakan pekerjaan kantor dengan data yang telah disimpan dalam media portabel pribadi yang telah dienkripsi tersebut.

g. Pertanyaan:

Apakah ada keyakinan bahwa aturan dapat dipatuhi oleh seluruh *user*?

Jawaban:

Perusahaan mengadakan penilaian kepada *user* mengenai kebijakan pengamanan data. Penilaian dilakukan untuk mengetahui apakah kebijakan yang diterapkan dapat dipatuhi oleh *user* atau tidak. Penilaian dari *user* terhadap kebijakan pengamanan data digunakan sebagai acuan dalam pembuatan kebijakan berikutnya.

h. Pertanyaan:

Apakah ada peran khusus yang dilakukan *user* lain (teman) ataupun atasan kepada seorang *user* dalam menghimbau tentang kebijakan pengamanan data?

Jawaban:

Perusahaan menerapkan budaya *information risk awareness*. Perusahaan juga menerapkan peraturan yang ditujukan kepada para atasan untuk menghimbau bawahannya untuk mematuhi kebijakan pengamanan data.

i. Pertanyaan:

Apakah sosialisasi mengenai kebijakan pengamanan data di perusahaan telah disampaikan dengan jelas?

Jawaban:

Sosialisasi yang diadakan dikaitkan dengan tujuan bisnis perusahaan, dijelaskan keuntungan dalam penyimpanan data di P *drive* dan dampak-dampak yang dapat terjadi apabila tidak menyimpan data di P *drive*.

Dalam pengamanan data, perusahaan melakukan metode penyimpanan data user pada P drive. Folder "*My Documents*" secara *default* tersimpan di P *drive*.

j. Pertanyaan:

Apakah seluruh *user* bersedia menanggung risiko apabila tidak patuh terhadap kebijakan pengamanan data?

Jawaban:

Terdapat kebiasaan *user* yang menyimpan data di C *drive*. Departemen IT diberikan tugas untuk dapat tetap menjaga keamanan data *user* dengan melakukan *backup* secara terjadwal terhadap data user yang tersimpan di C *drive*.

Apabila terjadi kehilangan data *user* yang tersimpan di C *drive*, departemen IT berusaha untuk membantu *recovery* data *user* dengan menggunakan *software recovery tools*. Apabila terjadi kehilangan data di P *drive* yang disebabkan oleh kelalaian *user*, *user* diwajibkan segera menghubungi pihak IT untuk *recovery* data.

k. Pertanyaan:

Apakah ada evaluasi terhadap pengaksesan dan penyimpanan data pada P drive terkait segi kemudahan, efisiensi waktu, dan kenyamanan?

Jawaban:

Perusahaan menerapkan sistem penyimpanan dan pengaksesan data pada P *drive* dengan mempertimbangkan segi kemudahan, kenyamanan, dan efisiensi waktu supaya proses tersebut tidak mengganggu pekerjaan *user*.

Perusahaan melakukan evaluasi terhadap sistem pengamanan data setiap tahunnya.

l. Pertanyaan:

Apakah ada evaluasi terkait utilisasi dalam penunjang penyimpanan maupun pengaksesan data di P drive?

Jawaban:

Pengadaan *monitoring* kepada *user* mengenai penilaian terhadap P *drive*. Apabila terjadi masalah, dapat dilaporkan dan dilakukan pembuatan penanganan ataupun kebijakan baru untuk kedepannya.

Perusahaan melakukan evaluasi terhadap sistem pengamanan data setiap tahunnya.

Lampiran 7. Hasil Wawancara kepada Karyawan

Responden 1:

Pertanyaan:

Apakah terdapat faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan penyimpanan data di P *drive*?

Jawaban:

Ya memang ada perilaku dari beberapa *user* yang takut untuk menyimpan data perkerjaan di *network drive*, faktor-faktornya adalah:

a. Jaminan keamanan data yang tersimpan di P *drive*. Kebanyakan *user* takut kalau data mereka tidak aman atau bahkan hilang.
b. Kenyamanan bagi *user* dalam menyimpan dan mengakses data di P *drive*.
c. Kemudahan dalam menyimpan data dan mengakses data di P *drive*. Kemudahan berarti *user* dapat langsung membuka data di P *drive* sendiri tanpa bantuan IT.
d. Intensitas perusahaan dalam memberikan sosialisasi terhadap kebijakan penyimpanan data.
e. Pengaruh *user* lain seperti: teman dan atasan dalam himbauan mengenai kepatuhan terhadap kebijakan pengamanan data. *User* akan lebih dapat melakukan sesuatu apabila mendapat ajakan dari pihak lain.
f. Tanggung jawab karyawan sendiri dalam pemantauan akses data. Apabila kurang adanya perilaku karyawan perusahaan dalam pemantauan akses data, dikhawatirkan IT juga berperilaku demikian. Sehingga dikhawatirkan data karyawan yang tersimpan di P *drive* akan mudah diakses oleh pihak lain yang tidak bertanggung jawab.
g. Tingkat kecepatan LAN perusahaan. Kecepatan LAN perusahaan yang ada harus mampu mengirimkan data ketika data disimpan maupun diakses.
h. Besar kapasitas P *drive*. Kapasitas P drive yang ada harus besar karena P *drive* menampung data pekerjaan untuk seluruh karyawan.
i. Terjadinya *server down*. Apabila masalah *server* down kerap terjadi, *user* juga menjadi enggan untuk menyimpan data mereka di P *drive*.

Responden 2:

Pertanyaan:

Apakah terdapat faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan penyimpanan data di P *drive*?

Jawaban:

Ya, yang dapat mempengaruhi *user* itu adalah hal-hal seperti ini:

a. Kenyamanan *user* sendiri untuk menyimpan data di P *drive*.
b. Efisiensi waktu dalam menyimpan dan mengakases data di P *drive*. Apakah cara penyimpanan pada P *drive* memakan waktu yang lebih lama daripada penyimpanan data yang biasa. Soalnya *user* repot apabila setiap menyimpan data harus diarahkan ke "*My Documents*" yang terarah P *drive*.
c. Apakah perusahaan yakin bahwa peraturan yang diterapkan aman, dengan kata lain mampu untuk melindungi data. Peraturan yang diterapkan apabila menjamin keamanan data, maka kemungkinan juga dapat meningkatkan tingkat kepatuhan *user* untuk menyimpan data di P *drive*.
d. Apakah perusahaan yakin bahwa peraturan yang diterapkan dapat dipatuhi oleh seluruh karyawan.
e. Besar kapasitas P *drive*. Kalau kapasitas P *drive* kecil, *user* tidak mau menyimpan data mereka di P *drive*.
f. Tingkat kecepatan LAN. Kalau jaringannya lambat, *user* juga tidak mau menyimpan data mereka di P *drive*. Karena apabila data dibutuhkan, data tersebut harus dapat segera diakses.
g. Kesediaan *user* menanggung risiko apabila terjadi kehilangan data yang tersimpan di P *drive*.
h. Adanya gangguan terhadap jaringan dan *server down* juga dapat mempengaruhi.
i. Pemahaman *user* sendiri terhadap kebijakan yang diterapkan.

Responden 3:

Pertanyaan:

Apakah terdapat faktor-faktor yang mempengaruhi tingkat kepatuhan karyawan terhadap kebijakan penyimpanan data di P *drive*?

Jawaban:

Ya, terdapat faktor-faktor yang mempengaruhi beberapa *user* sehingga kurang bersedia menyimpan data di P *drive*:

a. Data yang tersimpan di P *drive* bisa dijamin keamanannya atau tidak.
b. Kontrol akses di dalam suatu sistem pengamanan itu aman atau tidak.
c. Kemudahan dan kenyamanan *user* untuk menyimpan data di P *drive*.
d. LAN harus cepat karena data yang tersimpan ada juga data yang besar. Data yang besar lebih lama untuk mengaksesnya.
e. Kejelasan mengenai peraturan pengamanan data dan juga aturan yang menjelaskan tanggung jawab karyawan terhadap keamanan data perusahaan
f. Kejelasan mengenai sistem penyimpanan pada P *drive*, tata cara penyimpanan data yang ditujukan untuk seluruh *user*.
g. Masalah *server down* dapat mempengaruhi juga.