Audit Keberlangsungan Layanan Pada Perusahaan Jasa Pengiriman Berbasis Cobit 5 dan *National Institute of Standards and Technology* (NIST)

Zyas Esa Anarki[1], Basuki Rahmad, S.T.,M.T[2], M. Teguh Kurniawan, S.T.,M.T[3]
[1,2,3] Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom, Bandung
Jalan Telekomunikasi No.1 Terusan Buah Batu Bandung
[1]zyasesa@students.telkomuniversity.ac.id , [2]azkaku@gmail.com , [3]ujangtegoeh@gmail.com

Abstrak

Untuk mengukur permasalahan dan tingkat keberhasilan perusahaan terhadap keberlangsungan layanan/*Continuity Plan* diperlukan sebuah penelitian audit keberlangsungan layanan yaitu menilai kesiapan perusahaan dalam menangani gangguan/bencana dan lebih siap menghadapi bencana/gangguan yang akan terjadi. Penelitian yang dilakukan yaitu menilai efektifitas terkait kontrol-kontrol *Continuity Plan*, yaitu keberadaan struktur organisasi *Continuity Plan*, penerapan *Risk Assessment*, penerapan *Business Impact Analysis*, penerapan kontrol preventif, penerapan lingkup prosedur *backup* dan *recovery* dimasing-masing bagian, *Compliance Testing*, dan *Substantive Testing*. Penelitian yang dilakukan menggunakan framework COBIT 5 dan INTOSAI.

Hasil penelitian audit keberlangsungan layanan pada Jasa Pengiriman berupa rekomendasi dari proses hasil penilian efektifitas kontrol pada *Compliance testing* dan *Subtantive Testing* yang disusun pada proses analisa temuan. Sehingga dari penelitian audit keberlangsungan tersebut bisa memberikan sebuah solusi agar kedepannya perusahaan bisa mengetahui seberapa besar tingkat keberhasilan dan kesiapan dalam pengelolaan yang di terapkan pada sebuah perusahaan dan lebih memahami tentang kebutuhan yang tertinggal dalam pencapaian visi dan misi perusahaan.

Kata Kunci : COBIT 5, INTOSAI, Audit Keberlangsungan Layangan, *Continuity Plan*

Abstract

An audit survey is essential to measure the company success rate on Continuity Plan and also to evaluate the company readiness on disaster/problem handling. The survey conducted includes effectiveness assessment related to Continuity Plan controls specifically Continuity Plan organization structure, application of risk assessment, application of business impact analysis, application of preventive control, application of backup and recovery procedure in each sections, compliance testing, and substantive testing. The survey conducted using COBIT 5 and INTOSAI as frameworks.

The result of the service continuity survey in shipping service company are recommendation from the results of effectiveness control survey in compliance testing and substantive testing compiled in process analysis so that a solution can be provided for the company to determine the success rate and readiness in the company and better understanding of unachieved requirements in acquiring the vision and mission of the company.

Keywords: COBIT 5, INTOSAI, Service Continuity Audit, Continuity Plan

1. Pendahuluan

1.1 Latar Belakang

Pada era globalisasi sekarang ini perkembangan ilmu pengetahuan dan teknologi, terutama teknologi informasi begitu cepat. Diperlukan sistem informasi yang dapat menunjang perencanaan dan pelaksanaan kegiatan perusahaan. Saat ini informasi sangat dibutuhkan oleh pihak penggunanya dalam membangun suatu organisasi ,membangun perancangan suatu bisnis dan segala yang menyangkut kebutuhan akan informasi yang digunakan untuk mengambil keputusan yang efektif, strategis dan efisien. Saat ini berbagai macam masalah yang ditemukan

terjadi di Jasa Pengiriman baik itu dalam keamanan penyimpanan data transaksi pelanggan, transaksi pengiriman dan penerimaan barang kiriman. Salah satu faktor penyebab masalah terhentinya proses bisnis layanan pengiriman adalah terjadinya bencana yang dapat mengurangi kinerja TI sehingga menyebabkan akivitas bisnis terhambat atau bahkan terhenti. Bencana dapat berasal dari manusia, teknologi, alam. Semua orang tentu tidak mengharapkan terjadinya bencana. Namun, tidak dipungkiri bahwa bencana tetap terjadi pada waktu yang tidak pernah diketahui dan tidak mengenal hal siapa saja yang menjadi korbannya. Kerugian pun menjadi hal yang tak dapat dihindari. Bila perusahaan tidak mampu pulih, kebangkrutan malah menjadi ancaman berikutnya.

Kondisi inilah yang seharusnya dapat diterapkan oleh perusahaan dalam penerapan *Continuity Plan .Continuity Planning* yaitu prosedur bagaimana perusahaan tetap dapat menjalankan proses bisnisnya walaupun perusahaan sedang atau telah tertimpa bencana sehingga perusahaan tidak sampai mengalami kerugian besar (Ross & Moore, 2006). Perlunya PT XYZ memiliki *continuity plan* ini juga diperkuat dengan peraturan pemerintah yang menyampaikan bahwa penyelenggara sistem elektronik wajib memiliki *continuity plan* untuk menangani bencana/gangguan sesuai dengan risioko dari dampak yang ditimbulkan. Hal ini tertuang didalam Peraturan Pemerintah No. 82 Tahun 2012. Untuk mengukur permasalahan dan tingkat keberhasilan perusahaan terhadap keberlangsungan layanan diperlukan sebuah penelitian audit keberlangsungan layanan yaitu menilai kesiapan perusahaan dalam menangani gangguan/bencana dan lebih siap menghadapi bencana/gangguan yang akan terjadi, sehingga dari penelitian audit keberlangsungan tersebut bisa memberikan sebuah solusi agar kedepannya perusahaan bisa mengetahui seberapa besar tingkat keberhasilan dan kesiapan dalam pengelolaan yang di terapkan pada sebuah perusahaan dan lebih memahami tentang kebutuhan yang tertinggal dalam pencapaian visi dan misi perusahaan.

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, rumusan masalah yang terdapat pada penelitian ini yang bertujuan untuk mengetahui hal-hal apa saja yang bisa diperbaiki dan juga dioptimisasi kinerjanya untuk membantu perusahaan dalam mencapai visi dan misinya kedepan adalah sebagai berikut:

1. Bagaimana efektifitas kontrol terkait keberlangsungan layanan terhadap Jasa Pengiriman?
2. Bagaimana rekomendasi perbaikan dari hasil penilaian untuk meningkatkan kapabilitas terhadap keberlangsungan layanan fasilitas IT Jasa Pengiriman?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah dijelaskan diatas,maka tujuan utama dari penelitian ini yang nantinya dapat memberikan dampak positif ke pihak perusahaan adalah sebagai berikut:

1. Menilai efektifitas kontrol-kontrol sistem informasi terkait keberlangsungan Jasa Pengiriman.
2. Menyusun rekomendasi perbaikan terkait keberlangsungan layanan untuk meningkatkan efektifitas yang diperlukan Jasa Pengiriman

I.4 Batasan Penelitian

Berikut beberapa batasan masalah yang digunakan untuk batasan fokus penelitian kami seperti dibawah ini:

1. Studi kasus audit sistem informasi manajemen PT XYZ adalah hanya pada layanan Jasa Pengiriman area Bandung dengan mengkondisikan jadwal layanan pengiriman domestik di kantor PT.Pos Indonesia (persero) area Bandung.
2. Penilitian tidak dilakukan sampai tahap implementasi, sehingga hanya berupa usulan rekomendasi perbaikan untuk keterlanjutan bisnis.
3. Penelitian dibatasi pada proses-proses yang diprioritaskan atas kesepakatan dengan manajemen Jasa Pengiriman.
4. Pada penelitian audit sistem informasi manajemen ini menggunakan framework COBIT 5 dan domain *delivery, service and support.* Penelitian ini hanya menggunakan proses area pada DSS04 *Continuity Planning*.

I.5 Manfaat Penelitian

Manfaat pada penelitian ini diharapkan dapat berdampak positif baik dari sisi perusahaan maupun dari sisi pendukung lainnya,beberapa manfaat yang diperoleh dalam penelitian ini adalah sebagai berikut :

1. Metode evaluasi ini bertujuan untuk mengukur seberapa besar tingkat kematangan pengelolaan yang dilakukan pada sebuah organisasi dan lebih memahami tentang resiko yang tertinggal dalam pencapaian tujuan perusahaan.
2. Sebagai bahan masukan dan evaluasi bagi manajemen Jasa Pengiriman

2. Kajian Pustaka dan Metodelogi Penelitian

Sumber yang digunakan sebagai referensi dan acuan pada penelitian ini adalah sebagai berikut.

2.1 Business Continuity Plan

Continuity Planning atan *Business Continuity Plan* (BCP) adalah proses otomatis atau pun manual yang dirancang untuk mengurangi ancaman terhadap fungsi-fungsi penting organisasi, sehingga menjamin kontinuitas layanan bagi operasi yang penting. Perencanaan keberlangsungan bisnis dibuat untuk mencegah tertundanya aktivitas bisnis normal (Putri, 2008). *Continuity Planning* dirancang untuk melindungi proses bisnis vital dari kerusakan atau bencana yang terjadi secara alamiah atau perbuatan manusia, dan kerugian yang ditimbulkan dari tidak tersedianya proses bisnis normal. Business Continuity Plan merupakan strategi untuk meminimalisir efek dari ganguan dan mengupayakan berjalannya kembali proses bisnis suatu organisasi atau perusahaan.

2.2 *Disaster Recovery Plan* (DRP)

DRP berisikan prosedur untuk merespon kejadian darurat, menyediakan operasi *backup* cadangan selama sistem terhenti, dan mengelola proses pemulihan serta penyelamatan sehingga mampu meminimalisir kerugian yang dialami oleh organisasi (Blokdijk, 2002). Pada saat bencana terjadi, resiko yang dihadapi tentu tidak langsung kita disurutkan. Tentu membutuhkan waktu yang cukup banyak untuk mempertimbangkan apa saja yang perlu dilakukan agar proses bisnis kembali berjalan. Proses DRP meliputi:

- Proses *Disaster Recovery Planning*
- Pengujian *Disaster Recovery Plan*
- Prosedur pemulihan bencana

Tujuan utama dari *Disaster Recovery Planning* adalah untuk menyediakan kemampuan atau sumber daya dalam melaksanakan proses yang paling kritis pada lokasi cadangan sementara waktu dan mengembalikan lokasi utama menjadi normal dalam batas waktu yang telah ditetapkan, dengan menjalankan prosedur pemulihan yang cepat, dan untuk meminimalisir kerugian organisasi.

2.3 Audit Sistem Informasi

Berikut ini adalah definisi Audit Sistem Informasi dari berbagai sumber, yaitu:

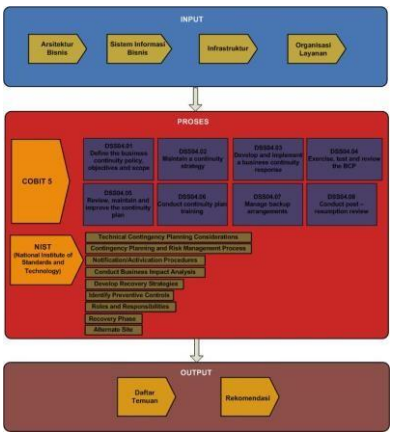
a. Audit Sistem Informasi merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (Weber, 2003).
b. Audit Sistem Informasi adalah sebuah proses yang sistematis dalam mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan bahwa sebuah sistem informasi berbasis komputer yang digunakan oleh organisasi telah dapat mencapai tujuannya (Budisusetyo, Subroto, Rosidi, & Solimun, 2013).
c. Audit sistem informasi (sebagai audit tersendiri dan bukan bagian dari audit keuangan) juga perlu dilakukan untuk memeriksa tingkat kematangan atau kesiapan suatu organisasi dalam melakukan pengelolaan teknologi informasi (Hendarti, 2007).
d. Audit sistem informasi didefinisikan sebagai proses pengumpulan dan evaluasi fakta/*evidence* untuk menentukan apakah suatu sistem informasi telah melindungi aset,menjaga integritas data, dan memungkinkan tujuan organisasi tercapai secara efektif dengan menggunakan sumber daya secara efisien (Karya, 2004).

2.4 COBIT 5 (*Control Objectives for Information and Related Technologies*)

COBIT memberikan kontribusi yang membantu perusahaan untuk mencapai tujuan bisnisnya. Dari hasil proses akan didapatkan informasi yang dibutuhkan oleh perusahaan untuk menentukan investasi TI dimasa mendapatang. Informasi harus memenuhi tujuh kriteria informasi; yaitu efisien, efektif, utuh, rahasia, reliabel, dan patuh terhadap kebijakan yang dibuat. Dari hasil proses COBIT juga membantu perusahaan dalam mengelola dan melakukan kontrol terhadap sumber daya TI; yaitu aplikasi, teknologi, data, fasilitas, dan manusia. Didalam COBIT memiliki lima domain yang sejalan dengan tanggung jawab penelitian audit teknologi informasi seperti merencanakan, membangun, menjalankan dan memonitor (COBIT 5, 2012). Domain dari area audit teknologi informasi yaitu, *Evaluate, Direct and Monitor* (EDM), Align, Plan and Organise (APO), *Build, Acquire and Implement* (BAI), *Deliver, Service ans Support* (DSS), *Monitor, Evaluate and Assess* (MEA)

2.5 Model Konseptual

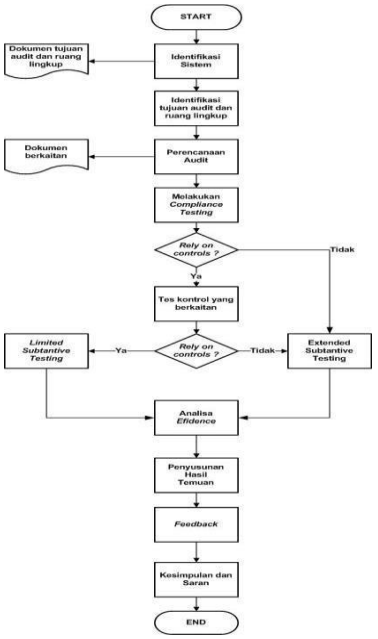
Kegunaan dari model konseptual sangat erat dengan teori referensi/literature yang digunakan. Fungsi kegunaan dari metode konsepual, peneliti dapat menunjukan bagaimana menjelaskan tahapan proses audit. Berikut merupakan model konseptual dari penelitian ini.



Gambar 1 Metode Konseptual

2.6 Sistematika Penelitian

Pada tahap sistematika penelitian mengikuti langkah-langkah pada INTOSAI (INTOSAI - International Organization of Supreme Audit Institutions, 2007). Tahapan pada proses sistematika penelitian meliputi identifikasi sistem, identifikasi tujuan dan ruang lingkup, perencanaan audit, *compliance testing*, *substantive testing*, analisa *evidence*, penyusunan hasil temuan, kesimpulan dan saran.



Gambar 2 Sistematika Penelitian

3. Pengumpulan Data dan Analisis

3.1 *Risk Assessment*

Merupakan langkah pengidentifikasian terhadap resiko yang kemungkinan terjadi, mulai dari bencana alam, bencana dari faktor manusia, dan bencana teknis (*environmental*) pada proses bisnis Jasa Pengiriman. Secara umum pengidentifikasian resiko pada *Risk Assessment* terpaku pada tiga faktor yang dijelaskan diatas, tetapi didalam pengidentifikasian resiko pada proses bisnis Jasa Pengiriman mempunyai empat faktor resiko yaitu berasal dari bencana alam (*natural*), faktor manusia (*human*), bencana teknis (*environmental*).

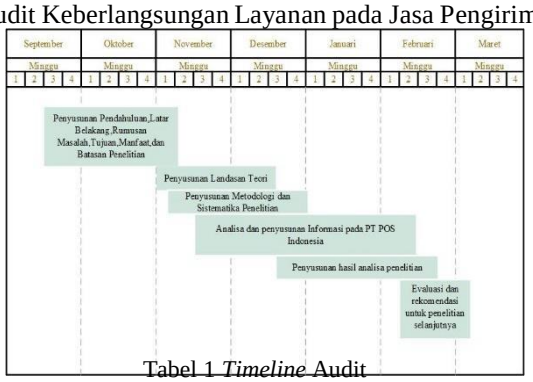
Dari hasil *Risk Assessment*, ada tujuh resiko yang dapat mengganggu kontinuitas layanan yaitu serangan jaringan, serangan data, kerusakan perangkat keras, ketiadaan daya, kerusakan perangkat lunak, *water damage*, kehilangan jaringan.

3.2 Program Audit

Program audit pada penelitian Audit Keberlangsungan bertujuan untuk mengatur secara sistematis dan struktur berbagai pertanyaan terkait tentang keberadaan *Continuity Plan* pada Jasa Pengiriman.

3.3 *Timeline* Audit

Berikut merupakan timeline audit yang bertujuan untuk mengetahui waktu yang diperlukan oleh tim *auditee* dalam merancang hasil analisis dan rekomendasi yang berasal dari hasil temuan penelitian audit. Berikut merupakan table *timeline* audit pada penelitian Audit Keberlangsungan Layanan pada Jasa Pengiriman.



Tabel 1 *Timeline* Audit

3.4 *Compliance Testing*

Tahap selanjutnya melakukan *Compliance Testing* yang bertujuan menilai dan memeriksa terkait kepatuhan struktur organisasi Jasa Pengiriman dalam memahami gangguan/bencana, mematuhi kebijakan terkait standarisasi perusahaan, dan kesiapan perusahaan dalam menangani gangguan/ancaman.

Berikut merupakan hasil temuan yang bernilai tidak efektif terhadap kontrol "Penerapan Struktur Organisasi *Continuity Plan*" pada proses *compliance testing*, yaitu Jasa Pengiriman belum menerapkan keberadaan DRP kedalam struktur organisasi sehingga belum terbentuk struktur organisasi ke dalam aspek *Continuity Plan* sehingga tidak terdapat team *Continuity Plan* didalam struktur organisasi.

Berikut merupakan hasil temuan yang bernilai tidak efektik terhadap kontrol "Penerapan *Risk Assessment*" pada proses *compliance testing*, yaitu

a. Belum mengimplementasikan proses *Risk Assessment* secara formal ke dalam aspek *Continuity Plan*, Jasa Pengiriman menerapkan identifikasi resiko bencana secara umum.

Berikut merupakan hasil temuan yang bernilai tidak efektik terhadap kontrol "Penerapan kontrol preventif" pada proses *compliance testing*, yaitu

a. Kondisi eksisting penerapan kontrol preventif di masing-masing bagian belum sepenuhnya optimal dikarenakan kontrol preventif terhadap masing-masing bagian belum memenuhi kriteria kontrol ideal.

Berikut merupakan hasil temuan yang bernilai tidak efektik terhadap kontrol "*Business Impact Analysis*" pada proses *compliance testing*, yaitu

a. Kondisi eksisting pada saat ini Jasa Pengiriman belum mengimplementasikan BIA terhadap masing-masing proses bisnis dan bagian infrastruktur dikarenakan belum merapkan pengelolaan struktur organisasi DRP secara formal, sehingga Jasa Pengiriman tidak mempunya dokumen BIA untuk acuan dalam menentukan batas pemulihan (RTO) dan batas kehilangan data (RPO)
b. Dampak yang ditimbulkan tidak mengimplementasikan BIA yaitu tidak dapat menentukan prioritas durasi batas pemulihan dan batas kehilangan data pada aplikasi layanan pengiriman

Berikut merupakan hasil temuan yang bernilai tidak efektik terhadap kontrol lingkup prosedur *backup* data pada proses *compliance testing*, yaitu

a. Tipe *backup* data secara *incremental* yang dilaksakanakan setiap hari dalam 1 kali pukul 00:00 wib yaitu menyebabkan mengalami dampak resiko kehilangan data pada 1 hari, sehingga dikhawtirkan sebelum pukul 00:00wib data pada Data Center mengalami gangguan/hilang sehingga belum sempat di *backup* di DRC sebelum waktu yang ditentukan.

Berikut merupakan hasil temuan yang bernilai tidak efektik terhadap kontrol lingkup prosedur *backup network* pada proses *compliance testing*, yaitu

a. Alternatif jaringan menggunakan metode *Warm Standby* berdampak terdapat suatu waktu dimana dimana sistem utama dan sistem kedua memiliki data yang berbeda atau data yang berbeda versi.

3.5 *Subtantive Testing*

Pada proses *substantive testing* terdapat beberapa pengujian kontrol terhadap kondisi eksisting struktur organisasi keberlangsungan layanan Jasa Pengiriman yaitu pengujian kontrol yang masih diterapkan oleh perusahaan dilakukan pengujian *substantive testing* untuk menganalisa apakah kontrol yang selama ini diterapkan masih layak digunakan untuk memenuhi target RTO 0 detik dan RPO 0 detik pada arsitektur teknologi.

Berikut merupakan hasil analisis *substantive testing* terhadap kondisi eksisting penerapan kontrol pada penggunaan teknologi *backup* dan *recovery* aplikasi, yaitu:

a. *Disk Replication*, pada mekanisme replikasi data pada redundansi server, tipe *incremental backup* yang diterapkan dan durasi *backup* data yang dilaksanakan 1x24jam pada pukul 00:00 wib kurang efektif dikarenakan berpotensi mengalami resiko kehilangan data sebanyak 1 hari karena dikhawatirkan sebelum pukul 00:00 wib terjadi kehilangan data dan data belum ter-*backup*
b. Penggunaan RAID 5 kurang efektif dikarenakan kemampuan RAID 5 dalam menunjang performansi tidak sesuai dengan kebutuhan proses bisnis disetiap layanan pengiriman Jasa Pengiriman yang bersifat kritikal.
c. Penerapan implementasi SAN pada arsitektur teknologi kurang efektif dikarenakan beberapa kelemahan yang dimiliki pada SAN, yaitu:
   - Kapasitas *bandwidth* yang dimiliki SAN lebih kecil dibandingkan kapasitas yang dimiliki NAS
   - SAN tidak bisa melakukan pengelolaan yang dilakukan NAS
d. Jasa Pengiriman belum menerapkan keamanan aplikasi untuk mencegah pelacakan IP

Berikut merupakan hasil analisis *substantive testing* terhadap kondisi eksisting penerapan kontrol pada penggunaan teknologi *backup* dan *recovery Network*, yaitu:

a. Penggunaan teknologi *Dual* ISP *connections* kurang efektif dikarenakan hanya menyediakan 2 ISP, sedangkan kebutuhan ketersediaan jaringan internet Jasa Pengiriman cukup tinggi dikarenakan jaringan sangat bedampak pada proses bisnis layanan Jasa Pengiriman, sehingga belum memenuhi untuk mencapai nilai target RTO 0 detik.
b. Implementasi *Cluster Server* pada redundansi *server* kurang efektif dikarenakan integrasi masing-masing *server* cukup rumit, khususnya pada perangkat lunak yang digunakan harus memiliki *setting* yang sama antar *server* anggota *cluster*. Selain itu *failover cluster* terbatas untuk beberapa *protocol* seperti HTTP, samba.
c. Penggunaan mekanisme alternatif jaringan *warm standby* kurang efektif dikarenakan terdapat suatu waktu dimana sistem utama dan sistem kedua memiliki data yang berbeda, atau data yang berbeda versi sehingga tidak memenuhi kriteria untuk mengejar target RPO 0 detik
d. Melakukan pembaharuan versi keamanan terhadapap semua tingkatan pengamanan jaringan secara rutin dan berkala (tidak di semua sistem internal)
e. Pada penerapan ACL *standard*, bila dibandingkan dengan ACL *extended*, performansi ACL standard kurang memenuhi kriteria kebutuhan Jasa Pengiriman yang membutuhkan kemampuan untuk membuat keputusan-keputusan lebih spesifik ketika mengontrol lalu lintas.
f. Tidak adanya perlindungan pada setiap *port* yang terdapat pada sebuah *switch* akan menyebabkan seseorang dapat mengkoneksikan komputernya kedalam sebuah jaringan melalui port pada switch tersebut
g. Jasa Pengiriman belum menerapkan pengamanan titik akses ke jaringan komputer (*hub* dan *switch*)
h. Jasa Pengiriman belum menerapkan perlindungan terkait aplikasi jaringan terhadap serangan pencurian data
i. Jasa Pengiriman belum menerapkan BGP (*Border Gateway Protocol*) dalam penggunaan ISP (*Internet Service Provider*) sehingga belum optimal dalam menentukan jalur terbaik pengiriman paket data.

Berikut merupakan hasil analisis *substantive testing* terhadap kondisi eksisting penerapan kontrol pada penggunaan teknologi *backup* dan *recovery* Data, yaitu:

a. Pada penerapan MD5 terkait enkripsi data, penerapan AES lebih efektif digunakan pada perusahaan besar dikarenakan pemilihan AES didasarkan pada 3 kriteria utama yaitu keamanan, harga, dan karateristik algoritma beserta implementasinya
b. Jasa Pengiriman melakukan implementasi enkripsi data sesuai dengan klasifikasi hanya untuk beberapa sistem internal
c. Jasa Pengiriman tidak mempunyai dokumen terkait tentang enkripsi data, seperti dokumentasi implementasi enkripsi data

d. Jasa Pengiriman tidak melakukan implementasi enkripsi informasi dalam sebuah media penyimpanan, seperti melakukan enkripsi dalam sebuah *server*
e. Jasa Pengiriman tidak melakukan perbaikan terhadap enkripsi informasi, seperti update enkripsi untuk informasi yang masuk

4. Kesimpulan

Dari hasil penelitian audit keberlangsungan layanan Jasa Pengiriman, hasil kesimpulan yang didapat dapat diambil secara garis besar terkait penilaian efektifitas kontrol dan penilaian hasil audit oleh pihak perusahaan adalah:

1. Hasil audit menunjukkan bahwa kontrol yang tidak efektif antara lain kontrol struktur organisasi *Continuity Plan*, penerapan *Risk Assessment*, penerapan kontrol preventif, penerapan *Business Impact Analysis*, lingkup prosedur *backup* data, lingkup prosedur *backup network*, penggunaan teknologi *backup* dan *recovery* aplikasi, penggunaan teknologi *backup* dan *recovery network*, penggunaan teknologi *backup* dan *recovery* data.
2. Dari hasil penelitian audit keberlangsungan layanan kesimpulan yang didapat menunjukan bahwa kontrol yang efektif yaitu prosedur *backup* dan *recovery hardware*, prosedur *backup* dan *recovery software*, prosedur *recovery* data, dan prosedur *recovery network*.
3. Hasil *feedback* keseluruhan atas rekomendasi yang dibuat, menunjukkan bahwa rekomendasi dalam penelitian ini baik untuk diimplementasikan di perusahaan, sehingga berdasarkan hasil dari penilaian penelitian oleh pihak divisi perancangan teknologi informasi, dan *network* dan *security* dapat disimpulkan bahwa:
    - Hasil penelitian audit keberlangsungan layanan dapat menilai tingkat efektifitas kontrol dan dapat memberikan rekomendasi perbaikan untuk meningkatkan efektifitas kontrol
    - Hasil penelitian audit keberlangsungan layanan dapat menjadi bahan masukan bagi pihak perusahaan Jasa Pengiriman dalam menjaga strategi keberlangsungan layanan
    - Hasil penelitian audit keberlangsungan layanan dapat memenuhi kebutuhan proses bisnis layanan Jasa Pengiriman
    - Penelitian audit keberlangsungan layanan dapat dipahami dan dimengerti
    - Dokumen hasil penelitian audit keberlangsungan layanan dapat diimplementasi dan dikembangkan lebih lanjut
    - Terdapat perbedaan *feedback* yang diberikan terkait perbaikan penelitian audit, yaitu *feedback* yang diberikan oleh pihak perancangan teknologi informasi adalah *scope* penelitian audit dapat diperkecil ruang lingkupnya, misalnya pada bidang nwtwork atau data. Namun *feedback* yang diberikan oleh pihak *network* dan *security* tidak ada perbaikan yang diperlukan terkait penelitian audit.
    - Tanggapan mengenai keseluruhan terhadap penelitian audit keberlangsungan layanan oleh pihak perusahaan adalah penelitian telah dilaksanaakan dengan baik dan sesuai dengan objek penelitian.

Daftar Pustaka

Blokdijk, G. (2002). *Disaster Recovery 100 Success Secrets.*

Budisusetyo, S., Subroto, B., Rosidi, & Solimun. (2013). Mencari Karakter Moral: Awal Mula Tugas Auditor. *Journal of Economics, Business, and Accountancy Ventura Volume 16, No. 3, December 2013. ISSN 2087-3735*, 503-514.

COBIT 5. (2012). ISACA.

Hendarti, H. (2007). *Pengelolaan Fungsi Audit Sistem Informasi.* Jakarta: Mitra Wacana Media.

INTOSAI - International Organization of Supreme Audit Institutions. (2007).

Karya, G. (2004). *Pengembangan Model Audit Sistem Informasi Berbasis Kendali.* Bandung: Bulettin Integral Vol.9.

Putri, S. W. (2008). *Pembangunan Disaster Recovery Plan Untuk Sistem Informasi Manajemen Terintegrasi ITB.* Bandung: Institut Teknologi Bandung.

Ross, C. F., & Moore, C. (2006). *Business Process Definition, Improvement, and Management.*

Weber, R. (2003). *Information Systems Control and Audit.*