AUDIT SISTEM INFORMASI PADA LAMPUNG POST MENGGUNAKAN FRAMEWORK COBIT 5

Selamat Soni Harsono Wijaya[1], R.Z Abdul Aziz[2]

[12]Magister Teknik Informatika, Institut Informatika dan Bisnis Darmajaya
Jl. Z.A. Pagar Alam No.93, Bandar Lampung – Indonesia 35142
[1]Email : selamatsoni@gmail.com,
[2]Email : rz.aziz@gmail.com

ABSTRACT

Information is one of the most important factors at this time, especially for organizations that use information technology (IT) as a supporter of their business processes. Lampung Post is a company that uses IT to support its business processes. But in its development, technological progress is also used as an opportunity to commit crime in cyberspace or other media that are often known as cyber crime. Cyber crime is to take over the website and also change the contents of the website content that causes harm to the company and also company partners who are still in one group of companies. To maintain the security of corporate information systems, a technology or system with good information security management is needed to safeguard information assets and prevent activities that can harm the company. For this reason, an information system audit is needed to assess current and expected capability of corporate information technology governance. This research on auditing information systems uses the COBIT 5 framework to find solutions to improve corporate information technology governance systems and use a scale of 0-5 in determining the capability level assessment. The results of the information system audit show that the current value is on a scale of 3 (Established), while the value of the excpect is at level 5 (Optimizing).

Keywords : *Audit, Capability Level, Framework* COBIT 5 *, Information Systems*

ABSTRAK

Informasi merupakan salah satu faktor yang sangat penting saat ini, terutama terhadap organisasi yang menggunakan Teknologi Informasi (TI) sebagai pendukung proses bisnisnya. Lampung Post merupakan perusahaan yang menggunakan TI untuk mendukung proses bisnisnya. Namun dalam perkembangannya, kemajuan teknologi juga dijadikan peluang untuk melakukan kriminalitas di dunia maya atau media lainnya yang kerap dikenal dengan istilah kejahatan siber. Kejahatan siber yaitu dengan mengambil alih *website* dan juga mengubah isi *content website* yang menimbulkan kerugian bagi pihak perusahaan dan juga rekanan perusahaan yang masih berada dalam satu group perusahaan. Untuk menjaga keamanan sistem informasi perusahaan maka dibutuhkan suatu teknologi atau sistem dengan tata kelola keamanan informasi yang baik untuk menjaga aset informasi dan mencegah terjadinya aktivitas yang dapat merugikan perusahaan. Untuk itu perlu adanya audit sistem informasi untuk menilai *capability level* tata kelola teknologi informasi perusahaan saat ini dan yang diharapkan. Penelitian tentang audit sistem informasi ini menggunakan *framework* COBIT 5 untuk mencari solusi perbaikan sistem tata kelola teknologi informasi perusahaan dan menggunakan skala 0-5 dalam penentuan penilaian tingkat kapabilitas. Hasil dari audit sistem informasi menunjukkan bahwa nilai current ada pada skala 3 (*Established*), sedangkan nilai *excpect* berada pada level 5 (*Optimizing*).

Kata kunci : Audit, *Capability level*, *Framework* COBIT 5, Sistem Informasi

1. PENDAHULUAN

Informasi saat ini menjadi hal yang sangat penting, terutama terhadap organisasi yang menggunakan teknologi Informasi (TI) sebagai pendukung proses bisnis. Ketergantungan terhadap TI ini menuntut perhatian khusus pada tata kelola yang terdiri dari kepemimpinan, struktur organisasi, dan proses untuk memastikan bahwa TI di organisasi tidak hanya berkembang, namun juga menopang strategi dan tujuan perusahaan[1]. Lampung Post (Lampost) merupakan perusahaan yang menggunakan TI untuk mendukung proses bisnisnya. Penggunaan TI di Lampung Post bertujuan untuk meningkatkan kualitas layanan yang diberikan terhadap para *stakeholder* terutama informasi pemberitaan *online* maupun *offline* kepada masyarakat. Untuk itu perlu adanya dukungan keamanan informasi yang bertujuan agar informasi yang akan diberikan baik melalui media cetak maupun *online* dapat berjalan dengan lancar. Salah satu bentuk dukungan keamanan informasi adalah dengan adanya audit sistem informasi dengan tujuan agar risiko keamanan informasi dapat dikurangi atau dihindari. Keamanan informasi merupakan aspek penting dari tata kelola organisasi, kinerja TI akan terganggu jika keamanan informasi sebagai aspek penting dari keamanan informasi mengalami masalah terkait kerahasiaannya (*confidentiality*), keutuhannya (*integrity*), dan ketersediaannya (*availibility*). Gangguan pada sistem informasi secara tidak langsung akan mempengaruhi kegiatan operasional yang dilakukan oleh perusahaan.

Motto Lampung Post yaitu menyebarkan berita yang jujur, terkini, bermutu, dan paling berpengaruh di Provinsi Lampung. Kemajuan teknologi saat ini terkadang tidak hanya dimanfaatkan untuk kegiatan positif. Namun dalam perkembangannya, kemajuan teknologi juga dijadikan peluang untuk melakukan kriminalitas di dunia maya atau media lainnya yang kerap dikenal dengan istilah kejahatan siber. *Cyber crime* atau kejahatan siber dalam istilah hukumnya adalah mengacu pada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat dan sasaran kejahatan.

Belum lama ini terjadi aktivitas kejahatan siber di Lampost.co yang menimbulkan kerugian bagi pihak Lampost dan juga rekanan perusahaan yang masih berada dalam satu grup perusahaan. Untuk menjaga keamanan sistem informasi perusahaan maka dibutuhkan suatu teknologi atau sistem dengan tata kelola keamanan informasi yang baik untuk menjaga aset informasi dan mencegah terjadinya aktivitas yang dapat merugikan perusahaan.

Permasalahan ini membuat audit sistem informasi pada Lampung Post perlu dilakukan. Audit sistem informasi ini dibuat dengan mengacu pada *framework* COBIT 5. *Framework* COBIT 5 merupakan suatu kerangka kerja manajemen teknologi informasi yang diciptakan oleh *Information System Audit and Control Association (ISACA)* dan *IT Governance Institute (ITGI).* COBIT memiliki model kapabilitas (*capability*) yang bertujuan untuk mencapai tujuan secara keseluruhan dari proses penilaian dan proses dukungan perbaikan, yaitu untuk menyediakan sarana untuk mengukur kinerja dari setiap sisi sistem informasi yang kemudian diterapkan pada suatu penilaian kapabilitas proses.

2. METODE PENELITIAN

Metodologi audit operasional berkaitan dengan penggunaan secara ekonomis dan efisien atas sumber daya pencapaian tujuan serta sasaran yang diterapkan. Audit operasional memiliki 4 (empat) tahapan, yaitu perencanaan (*planning*), pekerjaan lapangan

(*fieldwork*), pelaporan (*reporting*), dan tindak lanjut (*follow up*).

2.1. Perencanaan (*Planning*)

Tahap perencanaan dilakukan dengan mengumpulkan data berikut.

2.1.1. Wawancara
Mewawancarai staf TI untuk mengidentifikasi masalah khususnya tentang tindakan yang pernah terjadi pada sistem informasi Lampost.

2.1.2. Observasi
Mengamati tata kelola sistem informasi Lampost.

2.1.3. Studi literatur
Mengumpulkan bahan referensi berupa teori yang berasal dari buku dan jurnal serta data sekunder berupa dokumen yang mendukung hasil penelitian.

2.1.4. Menentukan proses bisnis
Metode yang digunakan untuk menganalisis tata kelola keamanan informasi, yaitu *Framework* COBIT 5. *Framework* COBIT 5 merupakan standar kontrol yang umum terhadap teknologi informasi, dengan memberikan kerangka kerja dan kontrol terhadap teknologi informasi yang dapat diterima dan diterapkan secara internasional. *Framework* COBIT 5 dirancang dengan 5 (lima) domain yang masing-masing mencakup penjelasan rinci dan termasuk panduan secara luas dan bertujuan sebagai tata kelola dan manajemen TI perusahaan. 5 (lima) domain yang ada pada COBIT 5 adalah sebagai berikut.

a). EDM (*Evaluate, Direct and Monitor*)
b). APO (*Align, Plan and Organise*)
c). BAI (*Build, Acquire and Implement*)
d). DSS (*Deliver, Service, and Support*)
e). MEA (*Monitor, Evaluate and Assess*)

2.2. Pekerjaan Lapangan (*Fieldwork*)

2.2.1. Membuat kuisioner
Peneliti membuat pernyataan pada kuisioner berdasarkan pedoman pada *framework* COBIT 5 yang terkait dengan tata kelola keamanan sistem informasi untuk mencegah terjadinya tindakan *cracking* pada Lampost.

2.2.2. Menyebarkan kuisioner
Peneliti menyebarkan kuisioner kepada bagian TI Lampost sebanyak 6 (enam) orang dan redaksi Lampost sebanyak 24 orang yang dilakukan pada tanggal 3-31 Desember 2018 yang digunakan untuk mengukur kapabilitas tata kelola keamanan sistem informasi perusahaan.

2.3. Pelaporan (*Reporting*)

Kegiatan yang dilakukan pada tahap pelaporan adalah sebagai berikut.

2.3.1. Mengukur tingkat kapabilitas
Merekap pengisian kuisioner untuk menghitung dan mengukur tingkat kapabilitas tata kelola keamanan sistem informasi untuk dijadikan laporan hasil analisis. Tingkat kapabilitas setiap proses yang dinilai dinyatakan dalam level 0 sampai 5 (ISACA, 2013).

a) Level 0 : *incomplete*
b) Level 1 : *performed*
c) Level 2 : *managed*
d) Level 3 : *established*
e) Level 4 : *predictable*
f) Level 5 : *optimizing*

2.3.2. Menganalisa *gap /* kesenjangan
Menganalisa *gap/*kesenjangan tingkat kapabilitas untuk menemukan permasalahan yang terjadi pada tata kelola keamanan sistem informasi perusahaan.

2.4. Tindak Lanjut (*Followup*)

Kegiatan yang dilakukan pada tahap tindak lanjut adalah sebagai berikut.

2.4.1 Merekomendasikan perbaikan tata kelola keamanan sistem informasi.

Dari hasil *gap/*kesenjangan yang terjadi pada tingkat kapabilitas saat ini dan yang diharapkan perusahaan didapatkan temuan masalah yang kemudian akan diberikan rekomendasi perbaikan untuk meningkatkan kapabilitas tata kelola keamanan sistem informasi pada *website* Lampost.co.

2.4.2 Dokumentasi

Melakukan dokumentasi kegiatan penelitian tata kelola keamanan sistem informasi pada Lampost.

3. ANALISA DAN PEMBAHASAN

3.1. Hasil Identifikasi *Enterprise Goals*

Memetakan dan menentukan *enterprise goals* yang berkaitan dengan latar belakang masalah berdasarkan pedoman pada COBIT 5. Hasil pemetaan terhadap *enterprise goals* adalah sebagai berikut.

a) Penilaian produk dan pelayanan bersaing.
b) Pengaturan risiko bisnis (perlindungan aset).
c) Budaya pelayanan orientasi konsumen.
d) Pelayanan bisnis berkelanjutan dan ketersediaan.
e) Kecerdasan dalam merespon perubahan lingkungan bisnis.
f) Pengelolaan fungsi proses bisnis.
g) Pengaturan program perubahan bisnis.
h) Produktivitas staf dan operasional.
i) Pemenuhan kebijakan internal.
j) Keahlian dan motivasi perorangan.
k) Budaya inovasi bisnis & produk.

3.2 Hasil Identifikasi *IT Related Goals*

Memetakan dan menentukan *IT related goals* yang diselaraskan dengan *enterprise goals* yang telah dipilih sebelumnya dengan acuan dan pedoman pada COBIT 5. Berdasarkan pemetaan yang telah dilakukan, didapatkan 9 (sembilan) *IT related goals* yang diselaraskan dengan *enterprise goals*, yaitu :

a) Pengaturan risiko bisnis yang berhubungan dengan TI.
b) Transparasi biaya, manfaat, dan resiko TI.
c) Kecukupan kegunaan aplikasi, informasi, dan solusi teknologi.
d) Kecerdasan TI.
e) Keamanan informasi, aplikasi, dan infrastruktur pemrosesan.
f) Optimalisasi aset TI, sumber daya, dan kemampuan.
g) Pemenuhan TI dengan kebijakan internal.
h) Personal TI yang kompeten dan memiliki motivasi bisnis.
i) Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis.

3.3 Identifikasi Domain COBIT 5

Berdasarkan hasil pemetaan *IT related goals* yang diselaraskan dengan domain COBIT 5, domain yang akan digunakan dalam penelitian ini ada 2 (dua), yaitu DSS dan MEA.

3.4 Identifikasi Proses COBIT 5

Memetakan proses bisnis pada COBIT 5 yang diselaraskan dengan *IT enterprise goals.* Berdasarkan hasil pemetaan yang telah dilakukan, didapatkan 8 (delapan) proses bisnis yang akan digunakan dalam penelitian ini, yaitu APO013, DSS01, DSS02, DSS03, DSS05, DSS06, MEA01, dan MEA02.

3.5 Identifikasi Proses dan Aktivitas COBIT 5

Berdasarkan pemetaan proses bisnis pada *Framework* COBIT 5, digunakan 42 pernyataan yang merupakan turunan dari proses bisnis yang akan digunakan dalam penelitian yang akan dijadikan acuan dalam pembuatan kuisioner.

3.6 Uji Validitas Data Responden

Uji validitas dapat dihitung dengan bantuan SPSS versi 20.0 menggunakan persamaan sebagai berikut.

$$r_{yx} = \frac{n\sum XY - (\sum X)(\sum Y)}{\sqrt{\{n\sum X^2 - (\sum X)^2\}\{n\sum Y^2 - (\sum Y)^2\}}}$$

Keterangan :

r yx = koefisien korelasi Pearson Product Moment
X = skor item
Y = skor item total
n = jumlah responden

Pengujian ini diambil sampel sebanyak 30 orang responden yang terdiri dari 6 (enam) kategori responden manajemen dan 24 kategori responden user dan mengisi kuisioner yang diberikan. Data kuisioner yang diperoleh dari responden telah diuji validitasnya menggunakan SPSS. Kriteria pengambilan keputusan adalah :

Bila r $_{hitung}$ > r $_{tabel}$ maka instrumen valid. Bila r $_{hitung}$<r $_{tabel}$ maka instrumen tidak valid. Uji validitas pada penelitian ini dilakukan tiap item pernyataan pada kerangka kerja COBIT 5. Hasil uji validitas dari 42 pernyataan mendapatkan r $_{hitung}$ lebih besar daripada r $_{tabel}$ maka dengan ini kuisioner yang dinyatakan valid sebanyak 37 pernyataan sedangkan 5 (lima) diantaranya dinyatakan tidak valid. Kemudian dilakukan uji reliabilitas statistik pada data responden menggunakan metode alpha cronbach's dengan hasil yang dapat dilihat pada tabel 1 (satu).

Tabel 1. *Realibity Statistics* Data Responden

Cronbach's Alpha	N of Items
0,984	42

Dari nilai Cronbach Alpha diketahui *realibity statistics* data responden memiliki nilai 0,984.

3.7 Perhitungan *Capability Level*

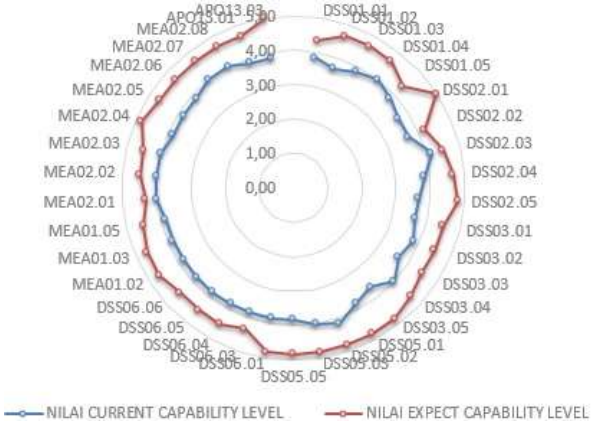
Perhitungan *capability level* merupakan rekapitulasi dari hasil kuisioner responden manajemen dan *user* dengan rumus berikut.

$$X = \frac{\sum Xi}{n}$$

Keterangan :

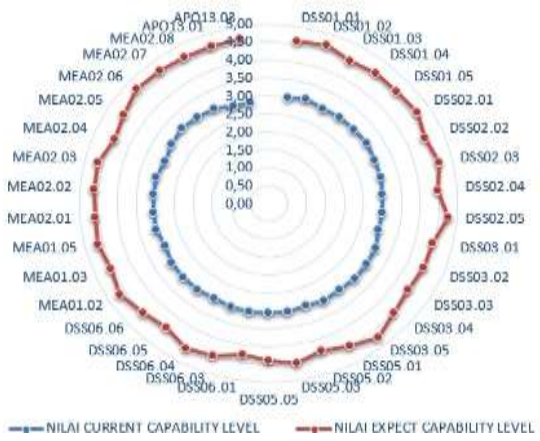
X = simbol untuk *mean* atau rata-rata hitung
∑ = simbol untuk penjumlahan keseluruhan
Xi = nilai berapa jumlah *X*, *I* = 1, 2, 3,..., n (nilai sampel ke-*i*)
n = jumlah sampel.

Hasil pengukuran *capability level* responden manajemen dapat dilihat dalam bentuk grafik radar pada gambar 1 berikut ini :



Gambar 1. Grafik Radar *Capability Level* Manajemen

Sedangkan hasil pengukuran *capability level* responden user dapat dilihat dalam bentuk grafik radar pada gambar 2 berikut ini :



Gambar 2. Grafik Radar *Capability Level* User

Berikut ini merupakan *gap* pada responden manajemen dan *user* yang dapat dilihat pada tabel 2 dan 3.

Tabel 2. *Gap Capablity Level Manajemen*

Proses	Current Capability Level Manajemen	Expect Capability Level Manajemen	Gap
APO13	3,83	4,83	1,00
DSS01	3,83	4,53	0,70
DSS02	3,80	4,63	0,83
DSS03	3,76	4,60	0,84
DSS05	3,95	4,83	0,88
DSS06	3,83	4,53	0,70
MEA01	3,83	4,61	0,78
MEA02	3,93	4,60	0,67

Tabel 3. *Gap Capablity Level user*

Proses	Current Capability Level User	Expect Capability Level User	Gap
APO13	2,85	4,62	1,77
DSS01	3,03	4,58	1,55
DSS02	3,03	4,60	1,57
DSS03	3,05	4,50	1,45
DSS05	3,04	4,42	1,38
DSS06	3,03	4,42	1,39
MEA01	3,01	4,61	1,60
MEA02	3,03	4,59	1,56

3.8 Analisa Kesenjangan

1. APO013 (pengaturan keamanan)
   a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses APO013 dengan nilai *current* 3,83 yang masuk ke dalam skala pengukuran *capability level* 4 (*predictable*), yang berarti bahwa proses pengaturan keamanan yang berjalan sekarang diimplementasikan dan telah ditetapkan. Sedangkan pada proses APO013 diperoleh nilai *expect* 4,83 sehingga pada APO013 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,00. Permasalahan yang ditemukan adalah pada keamanan sistem yang belum dilindungi secara baik sehingga diperlukan pengamanan sistem melalui jaringan dengan melakukan pengaman FTP, SMTP, Telnet dan pengaman Web Server.
   b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses APO013 dengan nilai *current* 2,85 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan keamanan yang berjalan sekarang telah diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses APO013 diperoleh nilai *expect* 4,62 sehingga pada APO013 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,77. Permasalahan yang sama ditemukan pada keamanan sistem yang belum dilindungi secara baik sehingga diperlukan pengamanan sistem melalui jaringan dengan melakukan pengaman FTP, SMTP, Telnet dan pengaman Web Server.
2. DSS01 (pengaturan operasi)
   a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses DSS01 dengan nilai *current* 3,60 yang masuk ke dalam skala pengukuran *capability level* 4 (*predictable*), yang berarti bahwa proses pengaturan operasi yang berjalan sekarang diimplementasikan dan

telah ditetapkan. Sedangkan pada proses DSS01 diperoleh nilai *expect* 4,53 sehingga pada DSS01 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 0,93. Permasalahan yang ditemukan adalah terhadap pengaturan fasilitas meliputi daya dan alat bantu komunikasi yang sejalan dengan hukum dan peraturan, teknik dan kebutuhan bisnis, kesehatan, dan petunjuk keamanan sehingga diperlukan pengaturan fasilitas yang baik untuk mendukung kegiatan operasional perusahaan dari sisi pemberdayagunaan alat komunikasi, Kesehatan dan Keselamatan Kerja (K3) serta adanya petunjuk keamanan kerja.

b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses DSS01 dengan nilai *current* 2,92 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan operasi yang berjalan sekarang diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses DSS01 diperoleh nilai *expect* 4,58 sehingga pada DSS01 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,66. Permasalahan yang sama ditemukan pada pengaturan fasilitas untuk mendukung kegiatan operasional perusahaan dari sisi pemberdayagunaan alat komunikasi, Kesehatan dan Keselamatan Kerja (K3) serta adanya petunjuk keamanan kerja.

3. DSS02 (pengaturan permintaan layanan dan insiden)

a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses DSS02 dengan nilai *current* 3,90 yang masuk ke dalam skala pengukuran *capability level* 4 (*predictable*), yang berarti bahwa proses pengaturan permintaan layanan dan insiden yang berjalan sekarang diimplementasikan dan telah ditetapkan. Sedangkan pada proses DSS02 diperoleh nilai *expect* 4,63 sehingga pada DSS02 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 0,73. Permasalahan yang ditemukan adalah pada perawatan *hardware* dan *update software* mendukung kebutuhan bisnis sehingga diperlukan perawatan *hardware* dan *software* secara rutin untuk mencegah terjadinya *cracking* dan penyebaran virus yang dapat menyerang dan merusak data yang bersifat penting yang diakibatkan adanya beberapa perangkat yang tidak *update*.

b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses DSS02 dengan nilai *current* 3,09 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan permintaan layanan dan insiden yang berjalan sekarang telah diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses DSS02 diperoleh nilai *expect* 4,60 sehingga pada DSS02 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,51. Permasalahan yang sama ditemukan pada perawatan *hardware* dan *update software* secara rutin untuk mencegah terjadinya *cracking* dan penyebaran virus yang dapat menyerang dan merusak data yang bersifat penting yang diakibatkan adanya beberapa perangkat yang tidak *update*.

4. DSS03 (pengaturan masalah)
   a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses DSS03 dengan nilai *current* 3,77 yang masuk ke dalam skala pengukuran *capability level* 4 (*predictable*), yang berarti bahwa proses pengaturan masalah yang berjalan sekarang diimplementasikan dan telah ditetapkan. Sedangkan pada proses DSS03 diperoleh nilai *expect* 4,60 sehingga pada DSS03 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 0,83. Permasalahan yang ditemukan adalah pada pengumpulan data operasional untuk mengidentifikasi masalah yang muncul sehingga diperlukan pengumpulan data operasional yang akan digunakan pihak manajemen untuk mengidentifikasi dan menganalisa masalah yang akan timbul, dan mencari solusi pemecahan masalah yang telah terjadi.
   b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses DSS03 dengan nilai *current* 3,26 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan masalah yang berjalan sekarang telah diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses DSS03 diperoleh nilai *expect* 4,50 sehingga pada DSS03 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,24. Permasalahan yang sama ditemukan pada pengumpulan data operasional untuk mengidentifikasi dan menganalisa masalah yang akan timbul, dan mencari solusi pemecahan masalah yang telah terjadi.
5. DSS05 (pengaturan layanan keamanan)
   a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses DSS05 dengan nilai *current* 3,40 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan layanan keamanan yang berjalan sekarang diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses DSS05 diperoleh nilai *expect* 4,83 sehingga pada DSS05 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,43. Permasalahan yang ditemukan adalah pada pengaturan data operasional tentang keamanan sistem informasi sehingga diperlukan pelaporan rutin kepada pihak manajemen untuk mengidentifikasi, menganalisis, dan mengatasi masalah yang akan muncul dengan cara mengumpulkan data operasional perusahaan yang berkaitan dengan tata kelola TI.
   b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses DSS05 dengan nilai *current* 3,13 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan layanan keamanan yang berjalan sekarang diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses DSS05 diperoleh nilai *expect* 4,44 sehingga pada DSS05 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,31. Permasalahan yang sama ditemukan pada pengumpulan data

operasional tentang keamanan sistem informasi. Diperlukan pelaporan rutin dengan cara menganalisa data operasi perusahaan yang terkait layanan keamanan untuk mencegah terjadinya gangguan baik dari dalam maupun dari luar lingkungan perusahaan.

6. DSS06 (pengaturan kendali proses bisnis)
   a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses DSS06 dengan nilai *current* 3,44 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan kendali proses bisnis yang berjalan sekarang diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses DSS06 diperoleh nilai *expect* 4,52 sehingga pada DSS06 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,08. Permasalahan yang ditemukan adalah pada tindakan pengoreksian kesalahan yang terjadi pada proses bisnis. Perusahaan perlu melakukan tindakan pengoreksian dan evaluasi terhadap pengelolaan kesalahan yang terjadi pada proses bisnis.
   b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses DSS06 dengan nilai *current* 3,08 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses pengaturan kendali proses bisnis yang berjalan sekarang diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses DSS06 diperoleh nilai *expect* 4,41 sehingga pada DSS06 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,33. Permasalahan yang sama ditemukan pada kegiatan evaluasi kesalahan sehingga perlu dilakukan tindakan pengoreksian terhadap pengelolaan kesalahan yang terjadi pada proses bisnis.
7. MEA01 (memonitor, mengevaluasi, dan menilai pelaksanaan dan penyesuaian)
   a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses MEA01 dengan nilai *current* 3,30 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses monitoring, evaluasi, dan penilaian pelaksanaan dan penyesuaian yang berjalan diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses MEA01 diperoleh nilai *expect* 4,67 sehingga pada MEA01 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,37. Permasalahan yang ditemukan adalah pada tindakan perbaikan penyimpangan pada proses bisnis. Pihak manajemen diharapkan dapat membantu *stakeholders* untuk mengidentifikasi, memprakarsai, dan memperbaiki penyimpangan yang terjadi pada proses bisnis.
   b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses MEA01 dengan nilai *current* 2,94 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses monitoring, evaluasi, dan penilaian pelaksanaan dan penyesuaian yang berjalan diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses MEA01

diperoleh nilai *expect* 4,56 sehingga pada MEA01 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,62. Permasalahan yang sama ditemukan pada pada tindakan evaluasi. Perlu adanya perbaikan tindakan evaluasi terhadap penyimpangan yang terjadi pada proses bisnis.

8. MEA02 (memonitor, mengevaluasi, dan menilai sistem kendali internal)
   a. Dari proses perhitungan penilaian kuisioner manajemen, diperoleh nilai rata-rata pada proses MEA02 dengan nilai *current* 3,56 yang masuk ke dalam skala pengukuran *capability level* 4 (*predictable*), yang berarti bahwa proses monitoring, evaluasi, dan penilaian sistem kendali internal telah diimplementasikan dan telah ditetapkan. Sedangkan pada proses MEA02 diperoleh nilai *expect* 4,60 sehingga pada MEA02 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,04. Permasalahan yang ditemukan adalah pada inisiatif perusahaan. Perusahaan perlu mendefinisikan dan menyetujui lingkup inisiatif berdasarkan tujuan penjaminan bisnis.
   b. Dari proses perhitungan penilaian kuisioner *user*, diperoleh nilai rata-rata pada proses MEA02 dengan nilai *current* 3,39 yang masuk ke dalam skala pengukuran *capability level* 3 (*established*), yang berarti bahwa proses monitoring, evaluasi, dan penilaian sistem kendali internal telah diimplementasikan dengan perencanaan dan pemantauan. Sedangkan pada proses MEA02 diperoleh nilai *expect* 4,56 sehingga pada MEA02 terdapat *gap* atau kesenjangan antara *current* dengan *expect* sebesar 1,17. Permasalahan yang sama ditemukan pada kegiatan layanan perusahaan terkait TI. Perlu adanya tim audit TI untuk mengawasi dan memantau kegiatan layanan perusahaan yang berkaitan dengan tata kelola teknologi informasi.

4. SIMPULAN

Hasil analisis penyebaran kuisioner pada responden manajemen dan *user* menghasilkan nilai *current* rata-rata pada proses APO013, DSS01, DSS02, DSS03, DSS05, DSS06, MEA01, dan MEA02, yaitu 3,42 yang berarti bahwa hasil penilaian pada sistem informasi Lampung Post memiliki *capability level* 3 (*established*). Keseluruhan proses bisnis yang berjalan telah diimplementasikan dengan perencanaan dan pemantauan.

Hasil analisis penyebaran kuisioner pada responden manajemen dan *user* menghasilkan nilai *expect* rata-rata 4,59 yang berada pada level 5 (*optimizing*) yang berarti bahwa proses diharapkan akan terus meningkatkan dan memenuhi tujuan bisnis yang relevan.

Antara *gap* manajemen dan *user*, ditemukan perbedaan penilaian terhadap *capability level* tata kelola sistem informasi perusahaan. Penilaian *gap* pada responden manajemen jauh lebih rendah dibandingkan penilaian *gap* yang terjadi pada responden *user*.

DAFTAR PUSTAKA

[1] Aziz, R. Z. A., & Nurlistiani, R. (2018). Audit sistem informasi menggunakan pendekatan cobit 5.0dan itil v3 pada sistem informasi akademik. *ICTB Darmajaya*, *1*(93), 1–6.

[2] Ciptaningrum, D., Nugroho, E., & Adhipta, D. (2015). Audit Keamanan Sistem Informasi Pada Kantor

Pemerintah Kota Yogyakarta Menggunakan Cobit 5. *Seminar Nasional Teknologi Informasi Dan Komunikasi*, *2015*(Sentika), 2089–9815.

[3] Mufti, R. G., & Mursityo, Y. T. (2017). Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk), *1*(12), 1622–1631.

[4] Sari, T. R., & Sari, W. S. (2016). Audit Tata Kelola Teknologi Informasi Berbasis COBIT 5 (DSS05) Untuk Evaluasi Keamanan Sistem Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Kendal, *5*(22 Mar). Retrieved from http://eprints.dinus.ac.id/id/eprint/1833.

[5] Atastina, I., Firdaus, Y., & Candra, R. K. (2014). Audit Teknologi Informasi menggunakan Framework COBIT 5 Pada Domain DSS (Delivery, Service, and Support) (Studi Kasus : iGracias Telkom University). *Eproc*, *2*(1), 1701–1706.

[6] Bartens, Y., De Haes, S., Lamoen, Y., Schulte, F., & Voss, S. (2015). On the way to a minimum baseline in IT governance: Using expert views for selective implementation of COBIT 5. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2015–March*(September), 4554–4563. https://doi.org/10.1109/HICSS.2015.543

[7] Hakim, A., Saragih, H., Suharto, A., Studi, P., Informatika, T., Tinggi, S., & Informatika, M. (2014). Jurnal Sistem Informasi (Journal of Information Systems). 2 / 10 (2014), 108-117 DOI : http://dx.doi.org/10.21609/jsi.v10i2.393, *10*, 108–117.

[8] Nugroho, H. (2014). Conceptual model of IT governance for higher education based on COBIT 5 framework. *Journal of Theoretical and Applied Information Technology*, *60*(2), 216–221. https://doi.org/ISSN: 1992-864

[9] Preittigun, A., & Chantatub, W. (2012). A Comparison between IT Governance Research and Concepts in COBIT 5. *International Journal of Research in Management & Technology*, *2*(6), 581–590.

[10] ISACA, 2013. *Kerangka COBIT 5, COBIT 4.1, BMI (Modeling Bussiness Information), Manajemen Tata Kelola, Jaminan Framework, Kerangka IT Risk.* Major ISACA.

[11] Sanyoto, 2015. *Audit Sistem Informasi*. Mitra Wacana Media, Jakarta.

[12] Sarno, 2009. *Audit Sistem & Teknologi Informasi*. ITS Press, Surabaya.

[13] Isaca. (2016). *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT-Executive Summary*. *Isaca.Org*. Retrieved from https://cobitonline.isaca.org/l3-main?book=framework#framework-preface02

[14] ISACA. (2013). *Process Assessment Model (PAM): Using COBIT 5*. *Isaca*. https://doi.org/10.1016/B978-012107151-6/50011-6.

[15] Liandi, O., & Fitria, F. (2019). Evaluasi Tata Kelola Framework COBIT 5 pada Dinas Kependudukan dan Pencatatan Sipil. *POSITIF: Jurnal Sistem dan Teknologi Informasi*, *5*(2), 111-115.