PERANCANGAN KEAMANAN INFORMASI MENGGUNAKAN METODE ANALISIS RISIKO COBIT 5 PADA LAYANAN BISNIS PT POS INDONESIA

INFORMATION SECURITY DESIGN METHODS USING COBIT 5 RISK ANALYSIS IN PT POS INDONESIA BUSINESS SERVICES

Bahar Adi Purnomo[1], Lukman Abdurrahman[2], Rokhman Fauzi [3]

Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

[1]baharadi@student.telkomuniversity.com, [2] abdural@telkomuniversity.ac.id, [3] rokhmanfauzi@telkomuniversity.ac.id

Abstrak

Informasi merupakan asset penting dalam perusahaan. Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis. Pada penelitian ini mengambil referensi dari penelitian sebelumnya yang menggunakan kerangka kerja COBIT 5 pada BUMN serupa. Untuk mengoptimalkan layanan bisnis dan keamanan layanan IT pada PT POS INDONESIA, diperlukan perancangan dengan menerapkan COBIT 5 sebagai *framework* untuk menjaga keamanan informasi pada PT POS INDONESIA menggunakan domain DSS04 (*Manage Continuity*) dan DSS05 (*Manage Security Services*). Dengan menghitung persentase *capability level* untuk mengurangi dampak risiko yang akan terjadi. Metode yang digunakan pada penelitian ini adalah wawancara dan observasi, sehingga mendapatkan analisis risiko yang dibutuhkan. Hasil penelitian ini adalah rekomendasi kebijakan dan solusi dari analisis risiko yang telah di rancang berupa dokumen pengelolaan layanan bisnis dan keamanan layanan IT yang akan di ajukan sebagai usulan atau bahan pertimbangan untuk PT POS INDONESIA.

Kata kunci: COBIT5, Analisis Risiko, Keamanan Informasi, Kebijakan

Abstrac

Information is an important asset in the company. Information security is the protection of information from various threats in order to ensure the continuity of business processes. This study draws references from previous studies using the COBIT 5 framework in similar SOEs. To optimize business services and IT service security at PT POS INDONESIA, it is necessary to

design by implementing COBIT 5 as a framework to maintain information security at PT POS INDONESIA using the DSS04 (Manage Continuity) and DSS05 (Manage Security Services) domains by calculating the percentage of the capability level to reduce the impact of the risks that will occur. The methods used in this research are interviews and observations, so as to get a risk analysis. The results of this study are policy recommendations and solutions from risk analysis that have been designed in the form of business service management documents and IT service security that will be submitted as suggestions or consideration for PT POS INDONESIA.

Keywords: COBIT5, Risk Analysis, Information Security, Policy

1. Pendahuluan

PT. POS INDONESIA merupakan sebuah Badan Usaha Milik Negara (BUMN) Indonesia yang bergerak di bidang layanan pos. Bentuk usaha PT. POS INDONESIA berdasarkan peraturan pemerintah Republik Indonesia Nomor 5 Tahun 1995, berisi tentang pengalihan bentuk awal Pos Indonesia yang berupa perusahaan umum (perum) menjadi sebuah perusahaan (persero). (PT.POS INDONESIA,2020)

Dalam melaksanakan pelayanannya, PT. POS INDONESIA membagi sebelas wilayah daerah atau divisi regional dalam pengoperasiannya. Pembagian divisi tersebut mencakup semua provinsi yang ada di Indonesia. Setiap divisi meliputi beberapa provinsi yang menjadi bagian dari divisi tersebut, dan melakukan berbagai ekspansi agar dapat melakukan bisnis di dunia internasional. (PT.POS INDONESIA, 2020)

Seiring kemajuan dan perkembangan zaman, saat ini informasi merupakan *asset* berharga bagi perusahaan. Seiring dengan meningkatnya *asset* informasi, keinginan orang untuk mendapatkan akses informasi dan mengendalikannya juga meningkat. Dalam menghadapi usaha perolehan informasi secara ilegal, orang-orang berusaha mencegah tindak kriminal tersebut. (Mukhlis Amin, 2014)

Menurut G. J. Simons (1995), keamanan informasi adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan

lengkap (*right information*), informasi dipegang oleh orang yang berwenang (*right people*), dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan memberikan informasi pada format yang tepat (*right form*).

Informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasi, kebocoran informasi, dan kegagalan pada sistem yang dapat mengakibatkan kerugian baik pada sisi finansial maupunn produktifitas perusahaan. Keamanan secara umum dapat diartikan sebagai '*quality or state of being secure-to be free from danger*'. Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis untuk mengurangi risiko bisnis yang saat ini sangat penting dalam ruang lingkup pemerintahan karena kerentanan terhadap ancaman risiko yang tidak dapat diprediksi.

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting,yang menyebabkan seringkali jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) yang dapat menimbulkan kerugian bagi pemilik informasi. Pada keamanan informasi terdapat aspek-aspek keamanan informasi yang perlu diperhatikan seperti *Confidentiality* (kerahasiaan), *Integrity* (keutuhan) dan *Availability* (ketersediaan). Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan return of investment (ROI) serta peluang bisnis.

Untuk mengoptimalkan layanan bisnis dan keamanan layanan IT pada PT POS INDONESIA diperlukan analisis dan perancangan dengan menerapkan COBIT 5 sebagai *framework* untuk menjaga keamanan informasi pada PT POS INDONESIA yang belum seutuhnya dilakukan dengan baik, sehingga mengurangi dampak risiko yang akan terjadi.

Control Objectives for Information and Related Technology (COBIT) merupakan kerangka kerja yang dapat digunakan sebuah organisasi, pemerintahan, perusahaan atau enterprise untuk membantu mencapai tujuan yang diingingkan. Pada COBIT 5 sendiri terdapat bagian yang khusus membahas tentang keamanan informasi yang dikenal dengan nama COBIT 5 *for Information Security* dimana dapat memberikan panduan kepada perusahaan terkait aspek keamanan informasi pada sebuah perusahaan. Dalam melakukan pengolahan teknologi informasi dibutuhkan sebuah model pengelolaan yang dapat dijadikan sebagai acuan sesuai dengan strategi dan tujuan institusi maka dapat digunakan sebagai alat pengukuran di dalam mengatasi permasalahan-masalahan yang

terjadi di institusi seperti COBIT atau ITIL. *Control Objectives for Information And Relate Technology* (COBIT) merupakan sebuah kerangka kerja *Framework IT* yang diterbitkan oleh *Information System Audit and Control Association.*

Pada penelitian ini diperlukan untuk menghitung persentase capability level dengan menggunakan domain proses DSS04 (*Manage Continuity)* dan DSS05 (*Manage Security Services)* , untuk mengukur seberapa besar dampak untuk instansi jika risiko itu terjadi dan. Kemudian dilakukan audit terhadap risiko-risiko yang telah diidentifikasi menggunakan kerangka kerja COBIT 5 *for Information Security.*

Hasil penelitian ini adalah rekomendasi kebijakan dan solusi yang telah di rancang berupa dokumen pengelolaan layanan bisnis dan keamanan layanan it yang akan di ajukan sebagai usulan atau bahan pertimbangan untuk PT POS INDONESIA .

2. Dasar Teori

2.1 Informasi

Informasi dapat didefinisikan sebagai hasil dari pengolahan data dalam suatu bentuk yang lebih berguna dan lebih berarti bagi penerimanya yang menggambarkan suatu kejadian-kejadian (event) yang nyata (fact) yang digunakan untuk pengambilan keputusan [1].

2.2 Keamanan Informasi

Keamanan informasi merupakan upaya untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis [2]. Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara stimultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan [2].

2.3 Risiko

Risiko merupakan bagian yang tidak terpisahkan dari kehidupan, bahkan ada orang yang mengatakan bahwa tidak ada hidup tanpa risiko, terlebih lagi dalam dunia bisnis dimana ketidakpastian beserta risikonya merupakan sesuatu yang tidak dapat diabaikan begitu saja, melainkan harus diperhatikan secara cermat bila menginginkan kesuksesan.

2.6 Analisis

Analisis data merupakan metode yang digunakan untuk mengetahui bagaimana menggambarkan data, hubungan data, semantik data dan batasan data yang ada pada suatu sistem informasi [5].

2.7 Manajemen Risiko

Secara umum Manajemen Risiko didefinisikan sebagai proses, mengidentifikasi, mengukur dan memastikan risiko dan mengembangkan strategi untuk mengelolah risiko tersebut. Dalam hal ini manajemen risiko akan melibatkan proses-proses, metode dan teknik yang membantu manajer proyek maksimumkan probabilitas dan konsekuensi dari event positif dan minimasi probabilitas dan konsekuensi event yang berlawanan [3].

2.8 COBIT 5

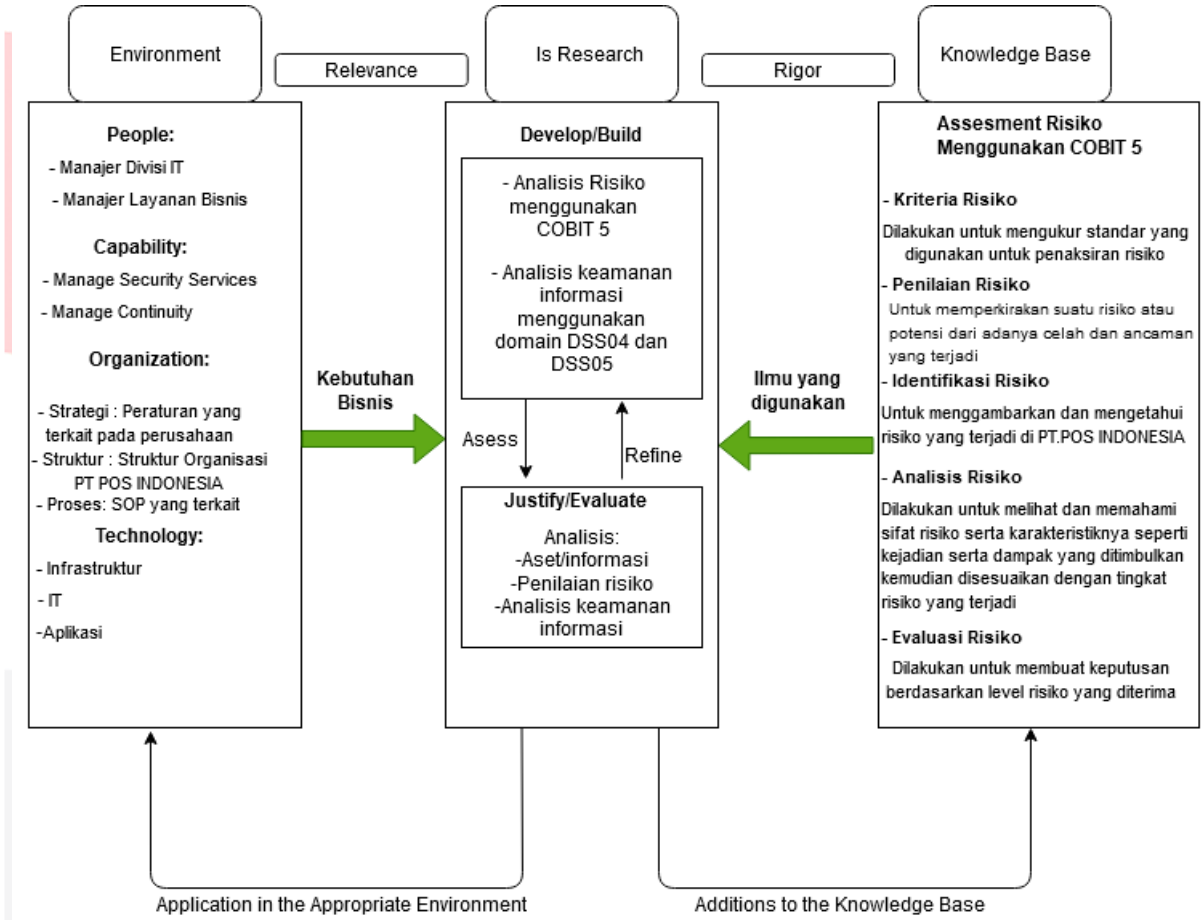
COBIT merupakan kerangka kerja yang dibuat oleh ISACA (*The Information Systems Audit and Control Association*) untuk manajemen dan tata kelola TI. COBIT adalah suatu panduan standar praktik manajemen teknologi informasi dan sekumpulan dokumentasi best practices untuk tata kelola TI yang dapat membantu auditor, manajemen, dan pengguna untuk menjembatani kesenjangan antara risiko bisnis, kebutuhan pengendalian, dan permasalahan – permasalahan teknis [4].

2.9 *IT Governance*

IT Governance adalah tanggung jawab eksekutif dan dewan direksi, dan terdiri dari pemimpin, struktur organisi dan proses yang memastikan bahwa TI perusahaan bertanggung jawab atas strategi dan tujuan organisasi. Dapat disimpulkan bahwa *IT Governance* adalah tanggung jawab dari pimpinan teratas dan eksekutif manajemen dari suatu perusahaan atau organisasi (*IT Governance Institute*, 2007).

3. Metodologi Penelitian

Model Konseptual adalah gambaran logis dari suatu masalah yang tergambar dalam susunan konsep berdasarkan aspek hipoteisi dan teoritis. Kerangka pola pikir yang dapat menjelaskan konsep dalam memecahkan masalah secara ringkas dan teratur dibutuhkan untuk menghasilkan *output* yang sesuai dengan tujuan. Model Konseptual akan dijelaskan pada gambar berikut :



Gambar 1 Model Konseptual

4. Hasil dan Pembahasan

A. Identifikasi Teknologi Eksisting

Proses ini merupakan teknologi pendukung pada perusahaan sebagai asset yang dimiliki untuk mencapai tujuan proses bisnis. Pada tabel 1 menjelaskan teknologi yang digunakan oleh perusahaan sebagai berikut :

Tabel 1 Aset

No.	Nama Asset
1	Database
2	PC
3	Firewall

4	Switch
5	Bridge
6	Antivirus
7	Router
8	Hub

B. Analisis Capability Level

Pada tahapan ini dilakukan analisis *Capability Level* untuk pengukuran keadaan organisasi berdasarkan COBIT 5 pada domain DSS04 (*Manage Continuity*) dan DSS05 (*Manage Security Services*) pada tabel 4-4 dan 4-5. Pengukuran ini didapat pada saat wawancara yang menghasilkan nilai *capability level* untuk domain DSS04 berada di level 1 dan DSS05 berada di level 1 dan level 2 yang artinya telah memenuhi target. (ISACA, 2012)

Tabel 2 Nilai Capability Level DSS04 & DSS 05

Proses	Level Kapabilitas	Persentase	PA 1.1	PA 2.1	PA 2.2	PA 2.3	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
DSS04	1	72%	L	N	N	N	N	N	N	N	N	N
Proses	Level Kapabilitas	Persentase	PA 1.1	PA 2.1	PA 2.2	PA 2.3	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
DSS05	2	87%	F	N	N	N	N	N	N	N	N	N

C. Analisis risiko

Analisis risiko dilakukan untuk melihat dan memahami sifat risiko serta karakteristiknya seperti kejadian serta dampak yang ditimbulkan kemudian disesuaikan dengan tingkat risiko yang terjadi. Setelah mengetahui tingkat kejadian serta dampak yang ada di PT Pos Indonesia lalu dikategorikan kedalam matriks risiko. Tabel 4.3.3.8.1 berikut adalah analisis risiko yang didapatkan dari kejadian dan dampak dari temuan risiko di PT Pos Indonesia :

:

Tabel 3 Analisis Risiko Pada DSS 04

No	Ancaman	Sebelum Penanganan				
		Tingkat kejadian	Tingkat dampak			
			Proyek	Hukum	Reputasi	Ketepatan
1	Salah pengambilan keputusan dalam penanganan insiden	2	2	2	2	2
2	Tidak terlaksananya rencana Business Continuity Plan secara maksimal	3	4	5*	2	3
3	Dapat menyebabkan perusahaan sulit berkembang dari segi proses bisnis maupun kemampuannya.	3	4	2	2	3
4	Pelatihan tidak fokus pada permasalahan yang ada	3	2	2	2	2
5	Kehilangan pelanggan	2	2	2	2	1
6	Dapat menyebabkan tidak dilakukan implementasi hasil pelatihan	2	2	2	2	1
7	Dapat menyebabkan masalah yang ada pada proses bisnis tidak dapat diselesaikan..	1	2	2	2	2

Dari analisis risiko yang sudah dilakukan dapat disimpulkan jumlah risiko berdasarkan level risiko yang sudah di perhitungkan dan di kelompokkan pada tabel dibawah ini.

Tabel 4 Rekap Data Level Risiko

Level Dampak	Tingkat Dampak
1 (1-5)	Sangat Rendah (SR)
2 (6-11)	Rendah (R)
3 (12-15)	Menengah (M)
4 (16-19)	Tinggi (T)
5 (20-25)	Sangat Tinggi (ST)

D. Perancangan Rekomendasi

Pada kegiatan ini peneliti membuat usulan rekomendasi berdasarkan hasil temuan kesenjangan yang sudah didapatkan sebelumnya. Setiap komponen rekomendasi yang diberikan berdasarkan kerangka kerja COBIT 5. Berikut adalah penjabarannya :

Tabel 5 Perancangan Rekomendasi Peningkatan Layanan Bisnis Pada Proses Domain DSS05

Proses Domain	Kesenjangan	Rekomendasi Kontrol	Rekomendasi Dokumen
DSS04 – 03 (*Develop and implement a business continuity response*)	Tindakan dan Komunikasi Respons insiden belum berjalan sepenuhnya	Menerapkan Tindakan dan komunikasi respon insiden dengan cara memonitoring terhadap proses yang mencurigakan serta melakukan analisis terhadap semua informasi yang berkaitan dengan insiden keamanan agar tidak terjadi insiden yang diinginkan.	Draf Penyusunan Kebijakan tentang tindakan komunikasi dan respons insiden yang belum berjalan sepenuhnya
DSS04 – 03	Belum adanya penjadwalan latihan	Melakukan penjadwalan latihan dan aktivitas	Draf Penyusunan Kebijakan tentang

(*Develop and implement a business continuity response*)	dan aktivitas pengujian yang ditentukan dalam rencana kontinuitas terkait *Business Continuity Plan*	pengujian pada staff bagian bisnis agar rencana kontinuitas terkait Business Continuity Plan tercapai dengan baik	Manajemen Kelangsungan Bisnis
DSS04 – 05 (*Review, maintain and improve the continuity plan*)	Tidak menetapkan persyaratan rencana pelatihan untuk melakukan penilaian risiko,penilaian dampak, dan perencanaan kontinuitas bisnis perusahaan	Melakukan pelatihan pada karyawan untuk melakukan penilaian risiko , penilaian dampak serta mempertimbangkan perencanaan kontinuitas bisnis pada perusahaan agar layanan bisnis tercapai.	Draf Penyusunan Kebijakan tentang Persyaratan Rencana Pelatihan
DSS04 – 04 (*Exercise, test and review the BCP)*	Kurangnya pengembangan kompetensi berdasarkan keterampilan untuk meningkatkan *customer experience*	Melakukan kompetensi pada divisi layanan bisnis untuk mengembangkan performa keterampilan karyawan untuk meningkatkan pengalaman pelanggan sehingga kontinuitas bisnis tercapai	Draf Perubahan Kebijakan tentang pengembangan kompetensi untuk meningkatkan pengalaman pelanggan
	Belum melakukan pembekalan dan analisis pasca latihan untuk mempertimbangkan pencapaian bisnis.	Memberikan pelatihan kepada semua karyawan sesuai dengan tugas masing-masing dengan tujuan untuk memberikan kesadaran terhadap pencapaian bisnis	Draf Penyusunan Kebijakan tentang Pembekalan Analisis pasca latihan untuk mempertimbangkan pencapaian bisnis.

	Belum melakukan analisis dan penilaian untuk mempertimbangkan pencapaian *Business Continuity Plan* terhadap ancaman yang menyebabkan dampak hilangnya kelangsungan bisnis	Mengidentifikasi tindakan yang akan mengurangi kemungkinan dan dampak melalui pencegahan yang lebih baik dan peningkatan ketahanan dengan cara melakukan penilaian risiko bisnis	Draf Penyusunan Kebijakan tentang Analisis Dan Penilaian Untuk Pencapaian Kelangsungan Bisnis (*Business Continuity Plan)*
	Belum adanya persyaratan kontinuitas untuk kemungkinan bisnis strategis dan opsi teknis	Menerapkan strategi bisnis pada semua karyawan agar kelangsungan bisnis tercapai	Draf Penyusunan Kebijakan tentang strategi proses bisnis

Tabel 6 Perancangan Rekomendasi Peningkatan Layanan Bisnis Pada Proses Domain DSS05

Proses Domain	Kesenjangan	Rekomendasi Kontrol	Rekomendasi Dokumen
DSS05 – 02 (*Manage network and connectivity security*)	Belum mendistribusikan semua perangkat lunak perlindungan secara terpusat (versi dan tingkat patch) menggunakan konfigurasi	Menerapkan sistem keamanan perangkat lunak secara terpusat dan melakukan control terhadap perangkat lunak dengan melakukan pencegahan dan pemulihan untuk melindungi perangkat lunak/software terhadap malware.	Draf Penyusunan Kebijakan tentang Perlindungan Keamanan Perangkat Lunak

	terpusat dan manajemen perubahan.		

5. Kesimpulan

Berdasarkan hasil dari penelitian yang dilakukan dalam perancangan keamanan informasi menggunakan metode analisis risiko COBIT 5 pada proses layanan bisnis di PT Pos Indonesia pada proses domain DSS04 , DSS05 dapat disimpulkan bahwa :

1. Kondisi penerapan keamanan informasi pada proses layanan bisnis masih belum optimal, karena berdasarkan pemetaan ada proses domain DSS04 dan DSS05 masih terdapat beberapa aktivitas yang belum dilakukan.
2. Berdasarkan analisis risiko yang sudah dilakukan pada proses domain DSS04 dan DSS05 diketahui bahwa :
   a. Penilaian proses layanan bisnis sesuai dengan DSS04 berada pada tingkat 1 dengan persentasi 72% yang termasuk dalam kategori *Large Achieved*. Pencapaian tersebut dikarenakan belum adanya kesadaran mengenai pengujian kontinuitas secara teratur dan menetukan tujuan dalam menjalankan dan pengujian dalam menjalankan BCP .
   b. Penilaian proses layanan bisnis sesuai dengan DSS05 berada pada tingkat 1 dengan persentasi 82% yang termasuk dalam kategori *Fully Achieved* . Pencapaian tersebut dikarenakan belum adanya kesadaran mengenai pengamanan perangkat lunak secara terpusat.
3. Rekomendasi untuk perancangan keamanan informasi pada proses layanan bisnis yaitu terdapat usulan rekomendasi berupa kebijakan dari kontrol risiko menggunakan COBIT 5 pada analisis risiko yang telah dibuat. Hasil yang telah didapat yaitu rekomendasi 8 kebijakan yang dapat membantu PT.POS INDONESIA dalam menjalankan proses bisnis dengan menangani risiko yang ada. Rekomendasi kebijakan yang dibuat yaitu Kebijakan Tindakan Komunikasi dan Respons Insiden, Kebijakan Manajemen Kelangsungan Bisnis, Kebijakan Persyaratan Rencana Pelatihan, Kebijakan Pengembangan Kompetensi Untuk Meningkatkan Pengalaman Pelanggan, Kebijakan Analisis Pasca Latihan Untuk Mempertimbangkan Pencapaian Bisnis, Analisis Dan Penilaian Untuk Pencapaian Kelangsungan Bisnis (*Business Continuity Plan*), Kebijakan Strategi Proses Bisnis, Kebijakan Perlindungan Keamanan Perangkat Lunak.

Daftar Referensi

[1] Priyanti, D. (2013). Sistem Informasi Data Penduduk Pada Desa Bogoharjo Kecamatan Ngadirojo Kabupaten Pacitan. *IJNS - Indonesian Journal on Networking and Security*, *2*(4), 56. ijns.org

[2] Utomo, M., Holil, A., Ali, N., & Affandi, I. (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik Its*, *1*(1), 2–7. http://ejurnal.its.ac.id/index.php/teknik/article/viewFile/900/462

[3] Soputan, G., Sompie, B., & Mandagi, R. (2014). Manajemen Risiko Kesehatan Dan Keselamatan Kerja (K3) (Study Kasus Pada Pembangunan Gedung Sma Eben Haezar). *Jurnal Ilmiah Media Engineering*, *4*(4), 99095.

[4] Handoyo, E., Umar, R., & Riadi, I. (2019). Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI). *Scientific Journal of Informatics*, *6*(2), 193–202. https://doi.org/10.15294/sji.v6i2.17387

[5] Edi, D., & Betshani, S. (2012). Analisis Data dengan Menggunakan ERD dan Model Konseptual Data Warehouse. *Jurnal Informatika*, *5*(1), 71–85.