Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, Vol. 3, No. 2, Agustus 2017, Hal. 70-76
e-ISSN 2502-8995 p-ISSN 2460-8181

ANALISA PENGELOLAAN RISIKO PENERAPAN TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000

[1]Angraini, [2]Indri Dian Pertiwi
[1,2]Jurusan Sistem Informasi, Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru
Email: [1]angraini@uin-suska.ac.id, [2]indridianpertiwi4@gmail.com

ABSTRAK

Penggunaan teknologi informasi memiliki risiko bagi perusahaan. Risiko akan membawa dampak yang menyebabkan ancaman baru bagi perusahaan dan akan mempengaruhi dalam pengambilan keputusan. Perusahaan harus menyiapkan tindakan penanganan jika terjadi sebuah risiko dalam penggunaan software dan hardware. Salah satu bentuk tindakan yang dapat diambil organisasi yaitu menyiapkan sebuah standar operational terkait pengelolaan risiko teknologi informasi. saat ini perusahaan sudah memiliki Standard Operational Procedure manajemen risiko untuk karyawan yang berfungsi untuk meminimalisir risiko yang terjadi . Namun masih ditemukan masalah dalam kegiatan pengelolaan dokumen menggunakan aplikasi repository yaitu adanya uncontrolled document yang menyebabkan keterlambatan pengembalian dokumen dan kegiatan pengkajian yang tidak maksimal. Penelitian ini bertujuan untuk mengetahui diagram atau daftar risiko beserta peringkat risiko yang terjadi secara berangkai. Penggunaan framework manajemen risiko Teknologi informasi dengan ISO 31000 dapat membantu proses pengambilan keputusan peningkatan pengelolaan dokumen berdasarkan hasil asesmen yang dilakukan. Risiko yang berdampak terhadap tujuan dan stategis perusahaan dianjurkan harus selalu di monitor dan review, karena perubahan masa akan memerlukan teknik penanganan yang lebih efektif.

Kata kunci: risiko, ISO 31000, pengelolaan, ancaman, teknologi, informasi

A. PENDAHULUAN

Pengelolaan teknologi informasi pada proses pengelolaan data yang kurang baik akan menimbulkan beberapa permasalahan yang merupakan kelemahan (*vulnerabilities*) sehingga akan menimbulkan ancaman (*threats*) [1]. Risiko dan ancaman dapat dihadapi dengan membuat suatu pengelolaan (Manajemen Risiko) yang baik sehingga dapat memberikan pertimbangan kepada perusahaan secara terstruktur dengan memperhatikan segala bentuk ketidak pastian dalam pengambilan keputusan dan tindakan yang harus diambil guna menangani risiko tersebut. Sebuah institusi atau lembaga yang menggantungkan sebagian besar proses bisnisnya pada sistem informasi akan mengalami kendala yang serius ketika sistem yang diterapkan tidak berjalan dengan semestinya [2]

Pada penelitia terdahulu yang berjudul Analisis Tata Kelola Risiko Teknologi Informasi (*It Governance*) dengan *Framework Risk IT* (Studi Kasus: Badan Perencanaan dan Pembangunan (BAPPEDA) Pemerintahan Provinsi Riau)" [3]. Risiko yang timbul akibat kesalahan penerapan tata kelola TI yaitu risiko kehilangan data yang diakibatkan dari tidak adanya cadangan basisdata pada instansi, kerusakan *hardware* dan *software*, penginputan tidak dapat dilakukan dalam jumlah banyak sehingga harus melakukan input data satu per satu hal ini menyebabkan kemungkinan hilangnya data jika dilakukan dalam jangka panjang. Tujuan dari penelitian ini adalah memberikan rancangan risiko tata kelola TI terhadap pengembangan tata kelola TI (*IT Governance*) yang sudah ada sebelumnya pada Badan Perencanaan dan Pembangunan (BAPPEDA) Pemerintahan Provinsi Riau.

Pada penelitian safaat yang berjudul "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 (Studi Kasus: Sistem Infrastruktur TI Telkom Indonesia)" terdapat risiko-risiko yang mengganggu, baik itu risiko internal maupun risiko eksternal. Untuk risiko eksternal terdapat pada gangguan alam seperti petir, banjir, hujan dan angin yang menrusak infrastruktur TI sehingga menggungu kelangsungan proses bisnis [3]. Pada penelitian ini menyatakan bahwan penggunaan *Framework* manajemen risiko TI dengan ISO 31000:2009 dapat membantu proses pengambilan keputusan berdasarkan hasil *riskassessment* yang dilakukan.

Risiko adalah kemungkinan terjadinya penyimpangan dari harapan yang dapat menimbulkan kerugian. Risiko tidak cukup dihindari, tapi harus dihadapi dengan cara-cara yang dapat memperkecil kemungkinan terjadinya suatu kerugian. Risiko dapat datang setiap saat, agar risiko tidak menghalangi kegiatan, maka risiko harus dikelola dengan baik [5]

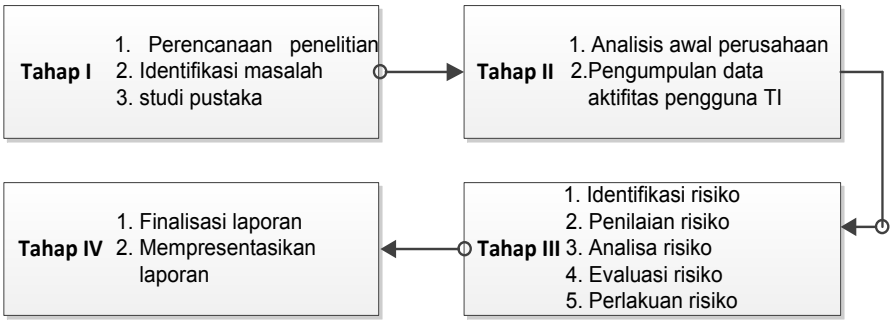
Manajemen risiko (*risk management*) adalah upaya terkoordinasi untuk mengarahkan dan mengendalikan kegiatan-kegiatan organisasi terkait risiko dalam operasional perusahaan untuk mengurangi berbagai kerugian dan untuk menetapkan sebuah standar operasional dalam sebuah perusahaan [6]. Manajemen risiko berperan

dalam memberikan jaminan yang wajar terhadap pencapaian sasaran organisasi, memberikan perlindungan kepada para pemangku jabatan terhadap akibat buruk yang mungkin terjadi yang disebabkan oleh risiko [7] Maka dapat dikatakan, bahwa manajemen risiko merupakan unsur yang ikut menentukan keberhasilan penerapan *Good Corporate Governance* (GCG) di dalam suatu perusahaan [9]

ISO *31000* "*Risk Management-Principle and Guidelines on Implementation*" adalah standar internasional pedoman penerapan manajemen risiko yang diterbitkan oleh *International Organization for Standardization* (*ISO*). Standar ini merupakan pengembangan standar *AS/NZS 4360:2004* yang dikeluarkan oleh *Standards Australia* [10]. Kelebihan ISO 31000:2009 dibandingkan dengan *framework* lain [8].

Framework ini akan menjadi dasar penataan yang mencakup seluruh kegiatan manajemen risiko disemua tingkatan organisasi. Selain itu, dapat membantu organisasi mengelola risiko secara efektif melalui penerapan proses manajemen risiko, memastikan informasi risiko yang lengkap dan memadai yang digunakan sebagai landasan untuk pengambilan keputusan. Kerangka kerja dalam mengelola risiko pada organisasi dapat dilihat pada Gambar 1.

Gambar 1. Kerangka kerja mengelola risiko [4]



Gambar 2. Metodologi penelitian

B. METODOLOGI

Metodologi penelitian yang akan dilakukan terdiri dari 4 (empat) tahapan. Secara sistematis dapat dilihat pada Gambar 2 dibawah ini:

B.1. Tahap Perencanaan

Pada tahap ini dilakukan penetapan permasalahan yang akan diteliti sehingga ditemukan dengan topik pengelolaan teknologi informasi pada EMP Bentu.

B.2. Tahap Pengumpulan Data

Tahap pengumpulan dan pengolahan data ini dilakukan untuk memperoleh bahan penelitian sesuai dengan tujuan penelitian yang telah ditetapkan. Adapun tahapan dalam mengumpulkan data adalah:

1) Observasi
2) Wawancara
3) Kuesioner

Tingkat kematangan pada kuesioner disusun oleh atribut-atribut sebagai berikut [2]:

a) Kesadaran dan komunikasi (*Awareness and Commmunication*)
b) Tanggung jawab (*Responsibility and Accountability*)
c) Penetapan dan Pengukuran pencapaian tujuan (*Goal Setting and Measurement)*
d) Kebijakan, standar dan Prosedur (*Policies, Standars and Procedures)*
e) Keahlian dan Keterampilan (*Skill and Expertise*)
f) Alat dan otomasi kontrol TI (*Tools and Automation*)

B.3. Tahap Pengolahan Data dan Analisa Data

Merupakan penjabaran dari data yang telah diperoleh sebelumnya. Tahap ini terdiri dari 6 tahap, yaitu:

1) Identifikasi risiko
2) Penilaian risiko
3) Analisis risiko
4) Evaluasi risiko
5) Perlakuan risiko

C. ANALISA DAN PEMBAHASAN

C.1 Analisa Kondisi Saat Ini

Saat ini pandangan nilai TI terhadap nilai bisnis organisasi tidak lagi bersifat parsial. TI tidak lagi dipandang sebagai *tool* (alat) yang terpisah (*separated*) dari perangkat organisasi, tetapi sudah dianggap sebagai salah satu sumber daya (*resources*) yang memiliki peran yang sama penting dengan sumber daya lain seperti *financial*, aset, dan SDM. Sumber daya TI yang diidentifikasi dapat dterangkan atau diidentifikasi sebagai berikut:

1) Aplikasi (*application*), merupakan suatu sarana atau tool yang digunakan untuk mengolah dan menyimpulkan prosedur manual maupun terprogram.
2) Informasi (*information*), adalah data-data yang telah diolah untuk kepentingan manajemen dalam membantu mengambil keputusan dalam menjalankan roda bisnis.
3) Infrasruktur (*insfrastrucure*), mencakup *hardware*, *software*, sistem operasi, sistem manajemen database, jaringan (*networking*), multimedia, dan fasilitas-fasilitas lainnya.
4) Sumber Daya Manusia/SDM (*people*), merupakan sumber daya yang paling penting bagi organisasi dalam pengelolaan dan operasionalisasi bisnis organisasi.

Kondisi yang terjadi pada pengelolaan dokumen ialah terjadinya kegiatan *uncontrolled document*. Terjadinya kegiatan pencetakan dokumen, yang sebelumnya telah didistribusikan berupa *soft copy* melalui aplikasi *repesotory document*. Dokumen yang sudah dicetak akan bersifat *unctrolled document,* yang dimaksud *unctrolled document* adalah dokumen yang sudah tidak dalam pengawasan pihak DCRM. Dokumen yang bersifat *unctrolled document* akan dikembalikan saat dokumen sudah kadaluarsa dengan masa berlaku dokumen 3 tahun. Namun berdasarkan ketentuan yang berlaku dokumen hanya dapat dipinjam dari unit DCRM yaitu 5 hari dengan maksimal 3 kali perpanjangan atau maksimal peminjaman 15 hari.

Pada kegiatan bisnis EMP Bentu sudah didukung oleh fasilitas-fasilitas penunjang seperti PC dengan jumlah 46 buah dan laptop 2 buah. Untuk pencetakan dokumen difasilitasi 11 buah printer dan 11 buah *scanner*. Pada penggunaan sistem aplilkasi sudah dapat diakses oleh seluruh pegawai menggunakan VPN. Namun untuk admin sistem hanya terdiri dari 1 orang yang merupakan staff TI perusahaan. Daftar mengenai data yang dioleh tahun 2017 dapat dilihat pada Tabel 1.

Tabel 1. Data yang diolah

No	Dokumen	Ada	Tidak
1.	Profil Perusahaan	✓	
2.	SOP Manajemen	✓	
3.	Panduan Manajemen	✓	
4.	Dokumen Risiko	✓	
5.	Struktur Organisasi	✓	

C.2. Pengelolaan Risiko pada Kegiatan Pengelolaan Dokumen EMP Bentu Menggunakan Asesmen ISO 31000

C.2.1. Identifikasi Risiko

Metode identifikasi risiko menggunakan *Risk Breakdown Structure* (RBS), Metode ini menyusun risiko-risiko dalam suatu kelompok atau kategori yang sesuai dengan sususan hierarkis organisasi, proyek atau proses. Pengelompokan risiko pada RBS ini berdasarkan sumber daya TI pada EMP Bentu yang dapat dilihat pada Gambar 3.

Kemudian dilakukan pengelompokkan risiko berdasarkan Sumber TI yang digunakan, dapat dilihat pada Tabel 2.

C.2.2. Penilaian Risiko

Risiko-risiko yang telah diidentifikasi dilakukan penilaian dengan cara memberikan nilai dari setiap risiko yang muncul berdasarkan frekuensi terjadinya risiko dan dampak risiko terhadap. Nilai frekuensi risiko (F) dan dampak risiko (D) akan dinyatakan dinyatakan dengan angka 1 hingga 5 [10]. Penjelasannya dapat dilihat pada Tabel 3 dan Tabel 4. Sedangkan hasil penilaian risiko tersebut secara detail dapat dilihat pada pada Tabel 5.

C.2.3. Analisa Risiko

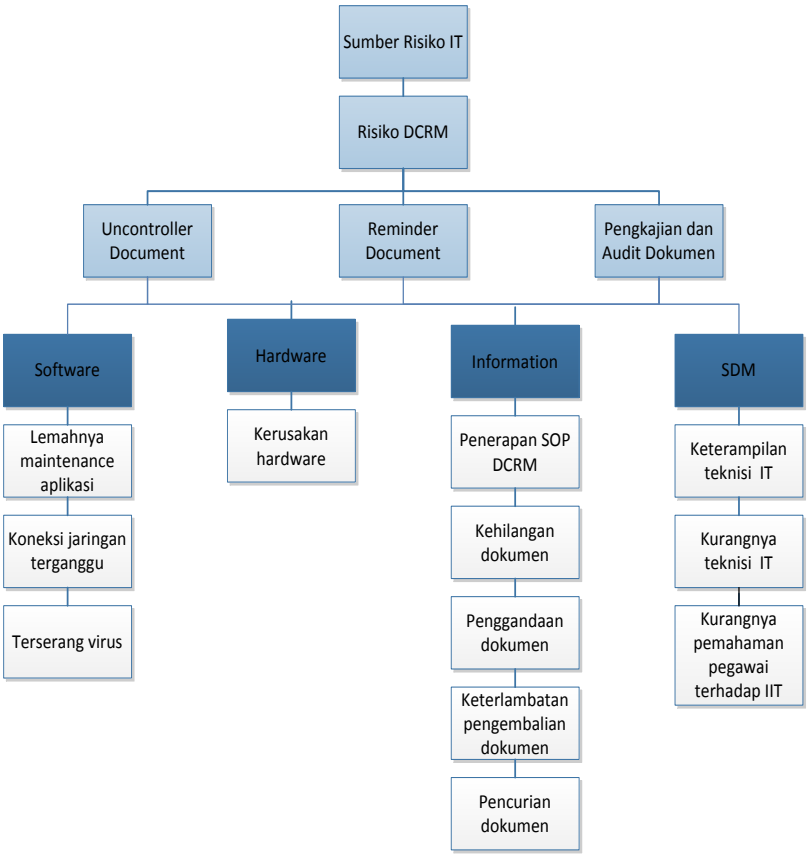
Metode analisa risiko yang digunakan adalah Analisis sebab akibat. Dalam merancang hubungan sebab akibat, terlebih dahulu akan dibuat diagram *FishBone* yang merupakan dasar dari pembangunan hubungan sebab akibat, yang menjelaskan penyebab-penyebab yang mungkin muncul dari masalah yang ingin dipecahkan. Diagram *fishBone* pada permasalahan yang terjadi dapat dilihat pada Gambar 4, 5 dan 6.

Pendistriusian dokumen dilakukan melalui interanet namun karna sulitnya akses intranet maka dilakukan pendistribusian melalui *burning* CD namun kegiatan *uncontrolled document* masi tetap terjadi, karena kurangnya pemahaman pekerja mengenai teknologi informasi sehingga pegawai merasa kesulitan mengoperasikan komputer dalam mengakses dokumen. Hal ini terjadi karena

kurangnya pelatihan dan minat pegawai untuk mempelajari teknologi informasi.

Pada kegiatan ini masi terdapat keterlambatan dalam pengembalian dokumen hal ini terjadi karena kurangnya respon divisi-divisi dilokasi terhadap pemberitahuan pengembalian dokumen karena cenderung masih adanya budaya menunda pekerjaan.

Pengkajian dan audit dokumen perlu dilakukan karena ketika terjadi perubahan pada sistem atau peralatan. Proses yang terjadi saat ini pengkajian dan audit tidak masksimal dilaksanakan, pekerja hanya melakukan pengkajian dokumen saat masa berlaku dokumen habis (3 tahun). Pekerja merasa pengkajian cukup dilakukan 3 tahun sekali, meskipun di SOP kegiatan pengkajan dokumen harus selalu dilakukan secara periodik.



Gambar 3. Struktur RBS

Tabel 2. Identifikasi risiko

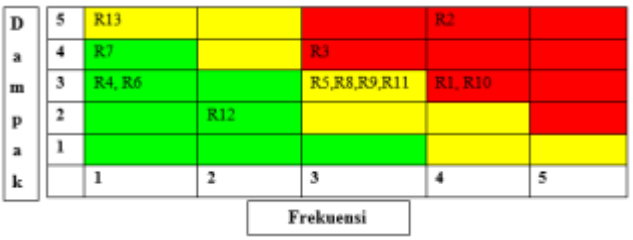
No	IT Resources		Identifikasi Risiko
1.	Software	Ms. Office dan intranet	- Lemahnya maintenance aplikasi - Koneksi jaringan terganggu - Terserang virus
2.	Hardware	PC, web server, database server, jaringan intranet, wifi, sistem operasi, UPS, AC, CCTV	- Kerusakan hardware
3.	Information	Dokumen dan list dokumen perusahaan	- Penerapan SOP DCRM - Kehilangan dokumen - Penggandaan dokumen - Keterlambatan pengembalian dokumen - Pencurian dokumen
4.	People	Karyawan, supervisi DCRM, maintanance/staff IT	- Keterampilan teknisiIT - Kurangnya teknisiIT - Kurangnya pemahaman pegawai terhadap IT

Tabel 3. Skala frekuensi risiko [10]

Nilai (F)	Frekuensi	Keterangan
5	Sangat Tinggi	Terjadi 11 hingga 100 kali setiap tahun
4	Tinggi	Terjadi 3 hingga 10 kali setiap 1 tahun
3	Sedang	Terjadi 1 hingga 4 kali setiap 4 tahun
2	Rendah	Terjadi 1 hingga 2 kali setiap 10 tahun
1	Sangat Rendah	Terjadi 1 hingga 9 kali setiap 100 tahun

C.2.4. Evaluasi Risiko

Evaluasi risiko dilakukan dengan menerapkan proses *mapping* pada grafik (x,y) yang menggambarkan peta risiko. Peta risiko yang dipergunakan mengadaptasi *risk mapping tool*. Pengelompokkan kategori risiko dapat dilihat pada kombinasi mapping risk pada Gambar 7 dibawah ini



Gambar 7. Pemetaan risiko

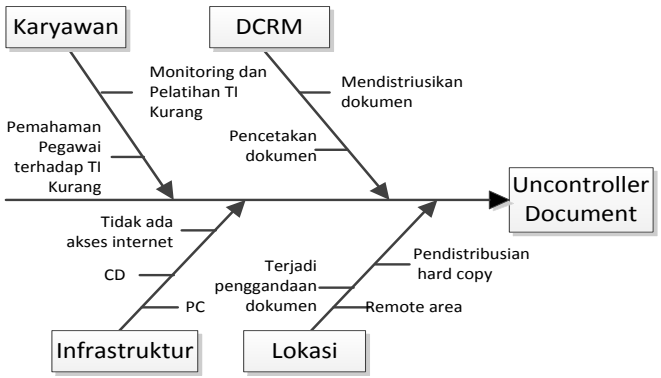
Hasil penilaian dan pemetaan risiko-risiko teknologi informasi kemudian diberikan peringkat berdasarkan nilai risiko. Tabel 6 menjelaskan peringkat risiko TI EMP Bentu.

Tabel 4. Skala dampak risiko [10]

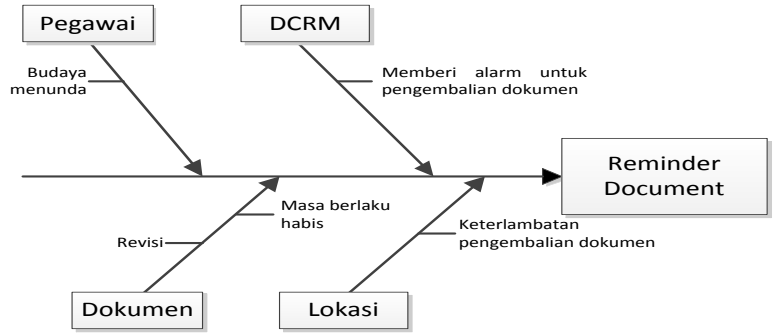
Nilai (D)	Dampak	Keterangan
5	Sangat Tinggi	Sangat mengganggu kelangsungan proses bisnis organisasi dan atau mengakibatkan kerugian finansial yang sangat besar.
4	Tinggi	Mengganggu kelangsungan proses bisnis organisasi dan atau mengakibatkan kerugian finansial yang besar.
3	Sedang	Cukup mengganggu kelangsungan proses bisnis organisasi dan atau mengakibatkan kerugian finansial yang tidak terlalu besar.
2	Rendah	Berpotensi mengganggu kelangsungan proses bisnis organisasi dan atau berpotensi mengakibatkan kerugian finansial yang tidak terlalu besar.
1	Sangat Rendah	Hampir tidak mengganggu kelangsungan proses bisnis organisasi dan atau hampir tidak mengakibatkan kerugian financial.

Tabel 5. Penilaian Frekuensi Risiko EMP Bentu

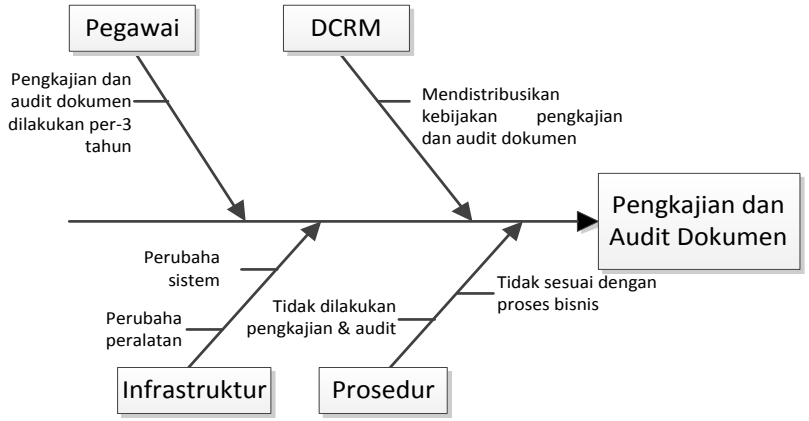
No	Identifikasi Risiko	F	D	D X F
1.	Lemahnya maintenance aplikasi/sistem	4	3	12
2.	Koneksi jaringan terganggu	4	5	20
3.	Penerapan SOP DCRM	3	4	12
4.	Penggandaan dokumen	1	3	3
5.	Keterlambatan pengembalian dokumen	3	3	9
6.	Kehilangan dokumen	1	3	3
7.	Pencurian dokumen	1	4	4
8.	Kerusakan hardware	3	3	9
9.	Infeksi virus computer	3	3	9
10.	Kurangnya teknisi TI	4	3	12
11.	Kurangnya pemahaman pegawai terhadap TI	3	3	9
12.	Kesalahan operasional	2	2	4
13.	Bencana Alam	1	5	5



Gambar 4. Diagram fishbone *uncontrolled document*



Gambar 5. Diagram fishbone *reminder document*



Gambar 6. Diagram *fishbone* pengkajian dan audit dokumen

Tabel 6. Evaluasi risiko berdasarkan *mapping risk* frekuensi-dampak

No	Risiko	Kategori Risiko	Usulan Tindakan Risiko
1.	Lemahnya *maintenance* aplikasi	Risiko Sedang	Lakukan *maintenance* pada *non-busy hour* atau gunakan mekanisme sistem cadangan sehinga tidak mengganggu proses operasional bisinis yang menggunakan TI.
2.	Koneksi jaringan terganggu	Risiko Tinggi	Review kinerja jaringan dengan teknisi TI. Lakukan monitoring sistem dan kinerja jaringan secara periodik, baik instalasi jaringan maupun *bandwidth.*
3.	SOP DCRM tidak sepenuhnya diterapkan	Risiko Tinggi	Melakukan review mengenai kegiatan yang tidak sesuai dengan SOP dengan mencari tahu penyebabnya dan memberi solusi agar kegiatan tersebut tidak terjadi lagi.
4.	Penggandaan dokumen	Risiko Tinggi	Meniadakan kegiatan *uncontrolled document* dan meningkatkan *security softcopy* dokumen.
5.	Keterlambatan pengembalian dokumen	Risiko Sedang	Memberi pemberitahuan pengembalian dokumen dan memberi sanksi terhadap keterlamabatan pengembalian dokumen.
6.	Kehilangan dokumen	Risiko Sedang	Meniadakan kegiatan pencetakan dokumen dan meningkatkan *security softcopy* dokumen dan memberi batasan waktu peminjaman dokumen. Memberi sanksi apa bila terjadi keterlambatan terhadap pengembalian dokumen.
7.	Pencurian dokumen	Risiko Tinggi	Melakukan review secara periodok mengenai penyebaran dokumen yang dilakukan pencetakan dan meniadakan kegiatan pencetakan terhadap dokumen.
8.	Kerusakan *hardware*	Risiko Rendah	Review kinerja pemeriksa operasional TI, perbaiki bila memungkinkan jika tidak segera lakukan penggantian
9.	Infeksi virus komputer	Risiko Sedang	Review kinerja antivirus pada PC operator, lakukan scan secara peridoik dan update antivirus
10.	Kurangnya supervisi TI	Risiko Sedang	Review mengenai kinerja teknisi TI dan meningkatkan SDM pada bagian TI.
11.	Kurangnya pemahaman TI	Risiko Tinggi	Memberikan pelatihan pada setiap pegawai mengenai penggunaan TI, pemahaman TI dan melakuakn review terhadap pegawai mengenai penggunaan TI.
12.	Kesalahan operasional	Risiko Sedang	Operasional pada SDM ICT dan DCRM tidak hanya satu orang, sebaiknya lebih dari satu orang agar kinerja lebih efektif dan meminimkan kesalahan pada operasional.
13.	Bencana alam	Risiko Tinggi	Memiliki lokasi penyimpanan *backup* data lebih dari satu yang memiliki risiko terkena bencana alam lebih kecil dibandingkan lokasi penyimpanan data utama Terapkan mekanisme *Disaster Recovery Planning* (DRP) untuk mengantisipasi kerusakan infrastruktur TI dikarenakan bencana alam, dan untuk mengatasi tersambar petir gunakan grounding sebagai penangkal petir.

D. KESIMPULAN

Setelah dilakukan analisa terhadap risiko TI khusunya risiko pengelolaan dokumen, menggunakan *framework* ISO 31000, dapat diambil kesimpulan sebagai berikut:

1) Penggunaan *framework* manajemen risiko TI dengan ISO 31000 dapat membantu proses pengambilan keputusan peningkatan pengelolaan dokumen berdasarkan hasil *asessmen* yang dilakukan.
2) Tingkat pengelolaan dokumen pada EMP Bentu saat ini sudah bernilai good. Risiko yang berdampak terhadap tujuan dan stategis perusahaan dianjurkan harus selalu di monitor dan *review*, karena perubahan masa akan memerlukan teknik penanganan yang lebih efektif.

Berdasarkan hasil analisa, ada beberapa saran yang dapat disampaikan yaitu:

1) Analisa permasalahan terhadap risiko teknologi informasi perlu dilakukan secara periodik dan program perbaikan perlu dipantau agar pelaksanaannya sesuai dengan harapan yang diinginkan.
2) Hasil temuan kondisi kematangan TI saat ini dapat dijadikan acuan untuk menumbuhkan pemahaman dan kesadaran terhadap risiko TI dan upaya pengelolaaan yang lebih baik.
3) Dilakukannya pengkajian ulang struktur organisasi divisi ICT dan menambahkan personil TI dalam melakukan penanganan permasalahan dan dilakukannya monitoring keseluruh pegawai.

REFERENSI

[1] Hartanto, Indra Dwi dan Tjahyanto, Aries. 2010. *Analisa Kesenjangan Tata Kelola Teknologi Informasi Untuk Proses Pengelolaan Data Menggunakan Cobit (Studi Kasus Badan Pemeriksa Keuangan Republik Indonesia)*. Program Studi Magister Manajemen Teknologi Bidang Keahlian Manajemen Teknologi Informasi Program Sarjana Institut Teknologi Sepuuh Nopember.

[2] Harris, Ivan Harris dan Tarigan, Muara Laut Adong. 2013. *Analisis Manajemen Risiko Pada Implementasi Sistem Informasi Keamanan Di Pt.Pupuk Sriwidjaja Dengan Framework Cobit* 4. Jurusan Sistem Informasi STMIK GI MDP.

[3] Kumala, Tuti Aznya. 2016. *Analisis Tata Kelola Risiko Teknologi Informasi dengan Framework Risk IT (Studi Kasus: Badan Perencanaan dan Pembangunan Pemerintahan Provinsi Riau)*. Dalam *Seminar Nasional APTIKOM (SEMNASTIKOM)*. 1-5.

[4] Safaat H, Nazruddin. 2011. *Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000*. Jurnal Sains, Teknologi dan Industri. 9(1): 1-15.

[5] Kasidi. 2010. *Manajemen Risiko*. Bogor: Ghalia Indonesia.

[6] ISACA. 2009. *The Risk IT Framework*.

[7] Susilo, Leo J dan Kaho, Victor Riwu. 2010. *Manajemen Risiko Berbasis ISO 31000 Industri Non-Perbankan*. Jakarta: PPM Manajemen.

[8] Pradana, Yana Ayu dan Rikumahu, Braddy. 2015. *Penerapan Manajemen Risiko terhadap Perwujudan Good Corporate Governance pada Perusahaan Asuransi*. Trikonomika Journal. 13(2): 195-204.

[9] Purdy, Grant. 2010. *ISO 31000: 2009—setting a new standard for risk management*. Risk Analysis. 30(6): 881-886.

[10] Budiraharjo R. 2013. *Model Pengelolaan Risiko IT Menggunakan Risk IT di ITENAS Bandung*. *Konferensi Nasional Sistem Informasi STMIK Bumigora Mataram*. Dalam KNSI.