Buat paper dgn tema Proses Asesmen Resiko. Dengan ketentuan:

- Minimum kata 2000
- Struktur paper: Abstrak, Pendahuluan, Pembahasan, Kesimpulan, Dafar Pustaka

PERILAKU KECURANGAN AKADEMIK MAHASISWA DALAM PROSES PERKULIAHAN

Muhammad Iqbal Rizky Tanjung

ABSTRAK

Tujuan dari penelitian ini adalah untuk mengetahui cara kerja citra perilaku menyontek akademik siswa di Perkuliahan. Ini penelitian menggunakan data primer, Data primer melalui kuesioner dibagikan langsung kepada Mahasiswa. Teknik pengumpulan data dalam penelitian ini adalah daftar pertanyaan. Jumlah sampel dalam penelitian ini sebanyak 48 mahasiswa. Hasil tersebut menunjukkan bahwa perilaku akademis menyontek berada pada level sedang dimana siswa masih melakukan banyak kecurangan akademis yang bagus dalam ujian juga pemberian tugas sampai di perkuliahan.

PENDAHULUAN

Pendidikan merupakan sebuah sarana untuk meningkatkan kualitas sumber daya manusia. Pendidikan juga merupakan suatu kekuatan yang sangat mempunyai pengaruh besar terhadap perkembangan fisik, mental, etika dan seluruh aspek kehidupan manusia. Lembaga pendidikan formal mulai dari tingkat dasar, menengah, sampai dengan perguruan tinggi di harapkan mampu menghasilkan lulusan yang berkualitas.

Salah satu tolak ukur dari keberhasilan dan kualitas pendidikan adalah nilai evaluasi dari hasil pembelajaran. Setiap peserta didik, baik siswa pada jenjang dasar dan menengah maupun siswa pada level perguruan tinggi tentunya ingin mendapatkan nilai yang baik karena, nilai tersebut menjadi salah satu hal yang menjadi tolak ukur kesuksesan seseorang.

Perilaku kecurangan akademik (akademic cheating) merupakan suatu fenomena yang telah terjadi pada dunia pendidikan penelitian mengenai perilaku ini cukup banyak dilakukan namun demikian, para peneliti menggunakan banyak istilah yang berbeda dalam penelitian mereka. Evan dan Craig (dalam anderman 2006: 34) bahwa membuat defenisi mengenai perilaku kecurangan akademik sulit dilakukan karena tidak semua orang sepaham mengenai perilaku yang termasuk dalam perilaku kecurangan akademik. Perilaku kecurangan akademik secara umum dapat dijelaskan sebagai perilaku curang yanga di lakukan dalam setting akademik.

Fenomena yang cukup menarik di perguruan tinggi saat ini dan cukup mengancam dunia pendidikan akademik yaitu, banyak di temukan praktik ± praktik kecurangan yang terjadi. Sehingga segala upaya yang di lakukan agar dapat berhasil dalam ujian, termasuk dengan kecurangan. Nonis dan Swift (2001) melakukan penelitian akademik di dalam kelas maupun di tempat kerja. Didapati bahwa siswa

yang di menganggap tindakan curang merupakan tindakan yang sangat di terima, mereka akan cenderung untuk sering melakukannya. Selain itu dikatakan bahwa apabila seorang siswa sering melakukan tindakan di dalam kelas, nanti mereka akan melakukan hal yang sama di tempat kerja.

Ada banyak cara kecurangan yang dilakukan oleh mahasiswa pada saat proses ujian berlangsung disebabkan karena mahasiswa kurang menguasai materi, mahasiswa tidak siap dalam menguti ujian, dalam proses ujian berlangsung mahasiswa dapat mencari jawaban di internet menggunakan Handphone, menyontek pekerjaan teman lain di sebelah kiri atau kanan maupun dengan teman di sebelah depan maupun belakang, membuat diskusi kecil antara teman yang satu dengan teman yang lain untuk mendapatkan jawaban, membuat catatan ± catatan kecil yang dapat dipakai pada saat ujian. Hal ini yang biasanya yang dilakukan mahasiswa pada saaat ujian berlangsung di dalam kelas.

Selain kecurangan yang dilakukan oleh mahasiswa saat berada di dalam kelas, mahasiswa juga dapat melakukan kecurangan di luar kelas yaitu, mengcopy ± paste jawaban dari internet tanpa menulis sumber untuk mempermudah mahasiswa dalam mengerjakan tugas, menyalin jawaban dari teman lain. Selain itu tujuan utama mahasiswa melakukan kecurangan yaitu untuk mendapatkan nilai yang baik maka, mahasiswa cenderung untuk melakukan kecurangan hal ini disebabkan karena mahasiswa menganggap bahwa soal yang diberikan sulit untuk dikerjakan. Sehingga dengan mudah mahasiswa melakukan kecurangan.

PEMBAHASAN

Perilaku kecurangan akademik yang terjadi pada lingkungan mahasiswa sangat beragam. Perilaku kecurangan akademik yang dapat terjadi di kelas seperti ujian akhir semester atau ujian tengah semester, maupun pada perilaku kecurangan yang terjadi diluar kelas seperti dalam penyelesaian tugas. Perilaku kecurangan akademik antara lain dapat terjadi dengan penggunaan materi yang dialarang digunakan, melakukan kolaborasi yang dilarang saat ujian, plagiasi, pemalsuan, misrepresentataion, tidak berkontribusi secara layak pada tugas kelompok. Data yang diperoleh mengungkapkan hasil yang lebih rinci mengenai perilaku kecurangan akademik yang terjadi pada mahasiswa. Ketika perilaku kecurangan dibagi dalam perilaku ± perilaku yang berbeda maka dapat di tentukan bagaimana mahasiswa melakukan kecurangan akademik. Berdasarkan mean responden dalam tiap perilaku kecurangan akademik, terlihat bahwa perilaku kecurangan akademik untuk tiap perilaku berada pada tingkat sedang.

Perilaku pertama yaitu penggunaan materi yang dilarang gunakan. Kecurangan akademik yang terjadi pada program studi pendidikan ekonomi khususnya kecurangan

yang dilakukan oleh mahasiswa pada saat mengukuti ujian maupun pengumpulan tugas berada pada tingkat sedang. Hal ini disebabkan karena mahasiswa pada saat mengukuti ujian masih menggunakan kertas contekan, menggunkan handphone untuk mencari jawaban di internet, saling menanyakan teman pada saat ujian, dan saling menukar lembaran jawaban dengan teman yang lain.

Faktor – Faktor Yang Mempengaruhi Kecurangan Akademik

Hendricks (2004) dalam Endra Murti Sagoro (2013:57-59) mengelompokkan faktor penyebab kecurangan akademis ke dalam 4 kelompok yaitu faktor individual, kepribadian, kontekstual, dan situasional. Berikut penjelasannya:

1. Faktor Individual

   Faktor individual yang dapat digunakan untuk mengukur perilaku kecurangan akademik antara lain dapat berdasarkan usia, jenis kelamin,prestasi akademis, pendidikan orang tua, dan aktivitas ekstrakurikuleryang diikuti oleh seorang siswa.

   a. Usia

      Siswa yang berusia lebih muda lebih banyak melakukan kecurangan akademis daripada siswa yang lebih tua.

   b. Jenis Kelamin

      Siswa laki-laki lebih banyak melakukan kecurangan akademis dari pada siswa perempuan. Penjelasan utama dari pernyataan ini dapat dijelaskan oleh teori sosialisasi peran gender yakni wanita dalam bersosialisasi lebih mematuhi peraturan dari pada pria.

   c. Prestasi Akademis

      Hubungan antara kecurangan akademis dan prestasi akademis tidak seperti hubungan kecurangan akademis dengan usia ataupun jenis kelamin, hubungan antara kecurangan akademis dengan prestasi akademis bersifat konsisten. Siswa yang memiliki prestasi akademis rendah lebih banyak melakukan kecurangan akademis dari pada siswa yang memiliki prestasi yang lebih tinggi. Siswa yang memiliki prestasi akademis yang rendah berusaha memperoleh prestasi akademis yang lebih tinggi dengan cara berperilaku curang dan lebih mau mengambil risiko dari pada siswa yang memiliki prestasi akademis yang tinggi.

   d. Pendidikan Orang Tua.

      Siswa dari keluarga yang memiliki latar belakang pendidikan yang tinggi akan lebih baik dalam mempersiapkan diri dalam mengerjakan tugas yang

diberikan oleh sekolah. Selain itu, siswa tersebut juga akan memiliki komitmen yang cenderung tinggi dalam pendidikan yang dijalaninya. Komitmen yang tinggi ini dapat menjadi faktor pencegah kecurangan akademis.

e. Aktivitas Ekstrakulikuler.
   Banyak siswa yang memiliki tingkat kecurangan akademis yang tinggi dilaporkan terlibat di dalam aktivitas ekstrakurikuler. Siswa yang tergabung di dalam kegiatan ekstrakurikuler memiliki komitmen yang lebih rendah berkaitan dengan pendidikan. Dua aktivitas yang telah diteliti secara ekstensif adalah siswa yang tergabung di dalamorganisasi siswa dan kegiatan olahraga.

2. Faktor Kepribadian.
   Beberapa hal yang berkaitan dengan kepribadian siswa yang dapat memunculkan perilaku curang antara lain adalah:
   a. Moralitas.
      Siswa yang memiliki level kejujuran yang rendah akan lebih sering melakukan perilaku curang. Selain itu, siswa yang memiliki tingkat religiusitas yang rendah cenderung lebih banyak melakukan kecurangan akademis.
   b. Variable Yang Berkaitan Dengan pencapaian Akademis.
      Variabel yang berkaitan dengan kecurangan akademis adalah motivasi, pola kepribadian dan pengharapan terhadap kesuksesan. Motivasi berprestasi memiliki hubungan yang positif dengan perilaku curang. Selain itu, pola kepribadian dan pengharapan terhadap kesuksesan memiliki hubungan negatif dengan perilaku curang.
   c. Impulsivitas, afektivitas, dan variabel kepribadian yang lain.
      Terdapat hubungan antara perilaku curang dengan impulsivitas dan kekuatan ego. Selain itu siswa yang memiliki level tinggi dari tes kecemasan lebih cenderung melakukan perilaku curang.
3. Faktor Kontekstual yang mempengaruhi perilaku kecurangan akademik antara lain keanggotaan perkumpulan siswa, perilaku teman sebaya, dan penolakan teman sebaya terhadap perilaku curang.

   a. Keanggotaan Perkumpulan Siswa.
      Siswa yang tergabung dalam suatu organisasi siswa akan lebih sering melakukan kecurangan. Pada organisasi siswa diajarkan norma, nilai dan

kemampuan- kemampuan yang berhubungan dengan mudahnya perpindahan perilaku curang. Pada suatu perkumpulan, penyediaan catatan ujian yang lama, tugas laboratorium dan tugas akademis lain mudah untuk dicari dan didapatkan.

b. Perilaku Teman Sebaya.
   Perilaku teman sebaya memiliki pengaruh yang penting terhadap kecurangan akademis. Hubungan ini dapat dijelaskan dengan menggunakan teori pembelajaran sosial (Social Learning Theory) dari Bandura dan teori hubungan perbedaan (Differential Association Theory) dari Edwin Sutherland. Teoriteori tersebut mengemukakan bahwa perilaku manusia dipelajari dengan mencontoh perilaku orang lain dan individu yang memiliki hubungan dekat dengan individu lain yang memiliki perilaku menyimpang akan berpengaruh terhadap peningkatan perilaku individu yang menirunya.
c. Penolakan teman sebaya terhadap perilaku curang.
   Penolakan teman sebaya terhadap perilaku curang merupakan salah satu factor penentu yang penting dan dapat berpengaruh terhadap perubahan perilaku curang pada siswa.

4. Faktor Situasional.
   a. Belajar terlalu Banyak, Kompetensi Dan Ukuran Kelas.
      Siswa yang belajar terlalu banyak dan menganggap dirinya berkompetisi lebih cenderung melakukan kecurangan dibandingkan siswa yang tidak belajar terlalu banyak. Ukuran kelas juga menentukan kecenderungan perilaku curang siswa dimana siswa akan lebih berperilaku curang jika berada di dalam ruangan kelas yang besar.
   b. Lingkungan Ujian.
      Siswa lebih cenderung melakukan kecurangan di dalam ruangan ujian jika siswa tersebut berpikir bahwa hanya ada sedikit resiko ketahuan ketika melakukan kecurangan.

dilihat dari hasil perhitungan dan presentase yang menunjukan bahwa kecurangan akademik berada pada tingkat sedang dengan presentasi 72,3% , pada tingkat rendah 14,8% dan pada tingkat tinggi 12,7%. Pada perilaku kedua yaitu melakukan kolaborasi yang dilarang saat pelaksanaan ujian menunjukan bahwa kecurangan akademik yang dilakukan oleh mahasiswa berada pada tingkat sedang yang presentasenya 72,3%, tingkat rendah 17,0%, dan tinggi 10,6%. Hal ini dibuktikan dengan perhitungan dan presentase. Perilaku kecurangan akademik yang dilakukan

oleh mahasiswa sehingga berada pada kategori sedang. Dalam perilaku ini mahasiswa bekerja sama pada saat ujian, menyebarkan jawaban ujian pada sesama teman dengan sengaja memperlihatkan lembar jawaban pada teman lain, menggunakan bahasa tubuh dengan cara ini mahasiswa mudah untuk mendapatkan jawaban dari teman lain saat ujian.

Perilaku kecurangan akademik ketiga terjadi pada mahasiswa adalah dengan melakukan plagiasi. Dalam perilaku ini mahasiswa mengumpulkan tugas yang telah dikerjakan oleh orang lain ataupun dengan menyalin sebagaian maupun keseluruhan hasil pekerjaan atau tugas teman lain. Perilaku kecurangan akademik ini menunjukan bahwa kecurangan yang dilakukan oleh rmahasiswa berada pada kategori sedang. Hal ini dibuktikan dengan hasil perhitungan dan presentase menunjukan bahawa kecurangan akademik berada pada tingkat sedang. Dengan presentase 12,7% pada tingkat rendah 70,2% dan tinggi 17,0%.

Perilaku kecurangan akademik yang keemapat yang dilakukan oleh mahasiswa yaitu saat melakukan pemalsuan pada tugas. Dalam perilaku ini mahasiswa mengambil data dari internet dan buku tetapi tidak mencantumkan sumber/referensi. Perilaku kecurangan akademik ini menunjukan bahwa kecurangan yang dilakukan oleh mahasiswa berada pada tingkat sedang. Hal ini menunjukan dengan hasil perhitungan dan presentase menunjukan bahwa kecurangan akademik berada pada tingkat sedang dengan presentase 63,8%, pada tingkat rendah 14,8% dan pada tingkat tinggi 21,2%. Perilaku kecurangan yang kelima yang dilakukan oleh mahasiswa yaitu misrepresentation. Pada perilaku ini mahasiswa memberi alasan yang tepat dalam pengumpulan tugas atau ujian agar dapat mengumpulkan tugas atau mengikuti ujian. Pada perilaku ini menunjukan bahwa kecurangan akademik yang dilakukan oleh mahasiwa berada pada posisi sedang. Hal ini dibuktikan dengan hasil perhitungan dan presentase menunjukan bahwa kecurangan akademik berada pada tingkat sedang dengan presentase 72,3%, sedangkan 10,6% berada pada tingkat rendah dan 17,0% berada pada tingkat tinggi.

Perilaku kecurangan akademik yang terakhir yang dilakukan oleh yaitu tidak berkontribusi secara layak pada tugas kelompok. Dalam perilaku ini seseorang tidak turut membantu dalam menyelesaikan tugas kelompok, namun ia terdaftar sebagai anggota dalam menyelesaikan suatu tugas. Pada perilaku ini menunjukan bahwa kecurangan akademik yang dilakukan oleh mahasiswa berada pada posisi sedang. Hal ini dibuktikan dengan hasil perhitungan dan presentase yang menunjukan bahwa kecurangan akademik berada pada tingkat sedang dengan presentase 72,3% sedangkan 14,8% berada pada tingkat rendah dan 12,7% berada pada tingkat tinggi. Berdasarkan hasil wawancara yang dilakukan dengan dosen dapat diketahui bahwa kecurangan

akademik sering dilakukan oleh mahasiswa diantaranya mahasiswa masih banyak menggunakan contekan karena mereka menganggap bahwa soal di berikan sangat sulit untuk dikerjakan, selain itu mahasiswa tidak siap dalam mengikuti ujian sehingga pada saat ujian berlangsung mereka merasa gelisa, menggunakan sandi/bahasa tubuh, memperlihatkan jawaban kepada teman lain, menggunakan Handphone untuk bertanya/menyebarkan jawaban kepada teman lain, masih banyak mengedit naska tugas teman lain, menyalin jawaban dari teman lain, pengambilan data dari buku dan internet tetapi tidak mencantumkan sumber/referensi, terlambat mengumpulkan tugas, terlambat mengkuti ujian dengan alasan karena belum siap mengukuti ujian, dan pengerjaan tugas kelompok yang dilakukan tidak semua anggota kelompok aktif dalam pengerjaan tugas kelompok.

Dalam mengikuti ujian mahasiswa tidak pernah mendapatkan bocoran soal dari dosen, dan apabila mahasiswa didapatkan menyontek, menggunkan handphone dan sebagainya maka sanksi yang akan diberikan yaitu mahasiswa tersebut tidak mendapatkan nilai dan dinyatakan tidak lulus dalam ujian, handphone akan disita oleh dosen, mendapatkan potongan nilai, tugas akan dikembalikan apabila tidak mencantumkan sumber/referensi, apabila terdapat tugas yang dikerjakan secara bersama maka tugas tersebut akan dikembalikan. Untuk mengatasi adanya kecurangan yang dilakukan oleh mahasiswa maka dosen sering mengadakan ujian lisan agar tidak ada kemungkinan untuk mahsiswa melakukan kecurangan pada saat ujian berlangsung.

Berdasarkan penggolongan yang ditetapkan yang ditetapkan oleh Hetterington (dalam Anderman 2006:43) perilaku kecurangan akademik yang terjadi pada mahasiswa lebih banyak memiliki tipe sosial ± active cheating yang ditandai dengan perilaku kecurangan kecurangan akademik dengan menyalin pekerjaan teman lain. Berdasarkan model yang dibentuk oleh Whitley (2002:32) penyebab secara langsung perilaku kecurangan akademik adalah adanya intense dalam melakukan perilaku kecurangan akademik . intense tersebut sangat di pengaruhi oleg sikap, resiko terdektesi dan harapan mendapat keuntungan dalam perilaku kecurangan akademik. Berdasarkan tinjauan data perilaku kecurangan akademik para mahasiswa ini perilaku kecurangan akademik berada pada tingkat sedang. Hal ini dibuktikan dengan kuisioner yang dijawab oleh responden dalam penelitian.

KESIMPULAN

1. Perilaku kecurangan akademik sangat beragam,baik pada saat ujian tengah semester, ujian akhir semester maupun pemberian tugas diluar kelas.

2. Rata- rata perilaku kecurangan akademik pada mahasiswa yang telah di data ini berada pada kategori sedang.
3. Perilaku yang pantut mendapat perhatian karena banyak terjadi pada mahasiswa ini adalah perilaku kecurangan akademik dengan menggunakan materi yang dilarang untuk digunakan, melakukan kolaborasi pada saat ujian, plagiasi, pemalsuan, misrepresentation, berkontribusi pada tugas kelompok.
4. Perilaku kecurangan akademik paling banyak terjadi pada saat pemberian tugas.

DAFTAR PUSTAKA

Anderman, E. M. dan Murdock, T.B. (Eds). 2006. *Psikologi Kecurangan Akademik*. Burnington, MA: *Elsevier Academic Press*

Anderman, Eric M Murdock Tamera B. 2002, *Psychology of academic cheating* London: Elsevier.

Nonis, S., & Swift, C. O. (2001). *An examination of the relationship between academic dishonesty and workplace dishonesty: A multicampus investigation*. *Journal of Education for business, 77* (2), 69-77.

Hendricks (2004). Academic Dishonesty : A Study in The Magnitude of The Justification for Academic Dishonesty among College Undergraduate and Graduate Student. *Journal Of College Student Development*. Vol 35. Page 212-260.

Endra Murti Sagoro. (2011). "Pensinergian Mahasiswa , Dosen , dan Lembaga dalam Pencegahan Kecurangan Akademik Mahasiswa Akuntansi". *Jurnal Pendidikan Akuntansi Indonesia.*Vol. XI, No. 2. Hal. 54-67.

Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk Pada PT. Advisia Diantara

Abstrak

SAP (*System Application and Product in Data Processing*) merupakan jenis software ERP yang digunakan oleh PT. Advisia Diantara untuk menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan agar lebih efektif dan efisien. Untuk mengantisipasi timbulnya risiko yang dapat mengganggu jalannya proses bisnis perusahaan, PT. Advisia Diantara menerapkan manajemen risiko berdasarkan standart ISO 31000:2009. Dalam hal ini perlu dilakukan evaluasi untuk mnegetahui pencapaian penerapan manajemen risiko teknologi informasi pada PT. Advisia Diantara dengan menggunakan kerangka kerja COBIT 5 khususnya pada domain proses APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation). Untuk memperoleh data yang akurat, maka teknik pengumpulan data yang digunakan adalah dengan melakukan pengisian lembar kerja evaluasi, obeservasi langsung dan wawancara dengan pihak yang berwenang. Proses evaluasi tersebut terdiri dari beberapa tahapan, antara lain melakukan analisis *capability level,* analisis *gap* dan analisis *risk assessment* untuk mengidentifikasi risiko – risiko potensial serta menilai sejauh mana dampak yang dapat ditimbulkan. Berdasarkan hasil analisis tersebut, maka didapatkan nilai *capability level* untuk domain proses EDM03 berada pada level 2 dan domain proses APO12 berada pada level 3 serta menghasilkan 16 buah strategi mitigasi dan 9 buah rekomendasi yang dapat digunakan untuk membantu perbaikan penerapan manajemen risiko teknologi informasi di PT. Advisia Diantara.

1. PENDAHULUAN

Salah satu perusahaan yang telah memanfaatkan teknologi informasi dan menerapkan manajemen risiko teknologi informasi sebagai sarana pendukung untuk mencapai tujuan perusahaan adalah PT. Advisia Diantara. Untuk meningkatkan kualitas perusahaan dibidang teknologi informasi, PT. Advisia Diantara menerapkan sistem ERP – SAP yang terdiri dari sepuluh modul. Disamping itu PT. Advisia Diantara juga menerapkan beberapa aplikasi Non ERP untuk menunjang jalannya Sistem ERP-SAP. Dengan diterapkannya Sistem tersebut diharapkan mampu menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan secara efektif dan efisien. Namun pada kenyatannya, penerapan Teknologi Informasi (TI) pada perusahaan tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan perusahaan. Oleh karena itu untuk mengelola segala macam risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka PT. Advisia Diantara telah menerapkan manajemen risiko berdasarkan pada Standart ISO 31000 : 2009 sejak tahun 2003. Padatnya proses bisnis yang berjalan di PT. Advisia Diantara, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Risiko – risiko tersebut diantaranya berupa gangguan jaringan internet, gangguan arus listrik, kurang optimalnya dukungan teknis operasional ERP, gangguan komunikasi data antara user dengan server ERP dan lain sebagainya. Oleh arena itu perlu adanya evaluasi manajemen risiko Teknologi Informasi (TI) untuk mengetahui tingkat kapabilitas pengelolaan risiko yang telah dicapai, sehingga dapat meningkatkan kemampuan perusahaan dalam mengelola setiap risiko terkait penerapan sistem ERP-SAP pada PT. Advisia Diantara. Dari evaluasi tersebut menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko – risiko yang tidak diinginkan. Salah satu *framework* yang dapat digunakan untuk mengevaluasi anajemen risiko Teknologi Informasi (TI) pada PT. Advisia

Diantara ialah COBIT 5 khususnya pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisatin*). Digunakannya domain tersebut karena dalam COBIT 5, hanya ada dua domain yang membahas secara terperinci mengenai manajemen risiko Teknologi Informasi (TI).

2. PEMBAHASAN

2.1 Analisis *Capability Level*

Berdasarkan hasil pengisian lembar kerja evaluasi yang dilakukan oleh 3 responden dari Departemen TKP & MR dan Departemen TEKINFO PT. Advisia Diantara dapat diketahui bahwa nilai *capability level* yang telah dicapai subdomain EDM03 berada pada Level 2 dan nilai *capability level* yang telah dicapai subdomain APO12 berada pada tingkat Level 3. Hal tersebut dapat dilihat pada Tabel di bawah ini.

Tabel Rekapitulasi Hasil GAP Analysis

Nama Proses	Level Saat Ini	Level Target	*Gap*
EDM03	2	3	1
APO12	3	4	1

2.2 Analisis *Gap*

Berdasarkan hasil wawancara, diperoleh informasi bahwa level target yang ingin dicapai oleh Departemen TKP & MR dan Departemen TEKINFO PT. Advisia Diantara adalah naik satu level untuk setiap domain prosesnya, yaitu domain proses EDM03 berada pada Level 3 dan domain proses APO12 berada pada Level 4. Sehingga besarnya *gap* yang terbentuk antara level yang terjadi saat ini dan level target yang ingin dicapai pada domain proses EDM03 dan APO12 adalah sebesar 1.

2.3 *Risk Assessment*

Proses *Risk Assessment* dilakukan berdasarkan dua tahapan, antara lain:

1. *Risk Analysis*

   Risk Analysis bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, menentukan parameter *impact*, menentukan parameter *rating* risiko, melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*. Adapun pengelompokan risiko berdasarkan skenario risiko dapat dilihat dalam Tabel berikut ini.

Tabel Rekapitulasi Berdasarkan Skenario Risiko

No	Skenario Risiko	Jumlah *Risk Issue*
1	*New Technology*	1
2	*Software Implementation*	2
3	*Destruction of Infrastructure*	1
4	*IT Staff*	1
5	*IT Expertise and Skills*	2
6	*Software Integrity*	2
7	*Infrastructure (Hardware)*	3
8	*System Capacity*	2
9	*Malware*	1
10	*Logical Attacks*	1
11	*Utilities Performance*	1
12	*Data(base) Integrity*	2
13	*Logical Trespassing*	1
14	*Operational IT Errors*	2
15	*Acts of Nature*	1
	Total	23

Sedangkan untuk pengelompokan risiko berdasarkan aset dapat dilihat dalam Tabel berikut ini.

Tabel 4. Rekapitulasi Berdasarkan Aset

No	Kategori Aset	Jumlah *Risk Issue*	Persentase
1	Aplikasi	5	21,74 %
2	Fasilitas	1	4,35 %
3	Infrastruktur TI	3	13,04 %
4	Informasi / Data	7	30,43 %
5	Proses	4	17,39 %
6	SDM	3	13,04 %
Total	23	100 %	

Sebelum melakukan penilaian risiko terhadap *Inherent Risk* dan *Residual Risk*, terlebih dahulu menentukan standart penilaian berupa parameter *probability* (kecenderungan), parameter *impact* (dampak) dan parameter *Rating* Risiko. Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel berikut ini.

Tabel Penilaian *Inherent Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	0	0	4	0	1
2	Fasilitas	0	0	1	0	0
3	Infrastruktur TI	0	1	2	0	0
4	Informasi / Data	0	0	5	2	0
5	Proses	0	0	4	0	0
6	SDM	0	0	2	1	0
Total		0	1	18	3	1

Berdasarkan hasil wawancara dengan beberapa perwakilan dari Dept. TEKINFO dan Dept. TKP & MR, dapat diketahui bahwa setiap risiko – risiko yang teridentifikasi telah memiliki pengendalian tersendiri. Pengendalian tersebut digunakan sebagai dasar untuk melakukan penilaian Residual Risk. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel berikut ini.

Tabel Penilaian *Residual Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	4	0	1	0	0
2	Fasilitas	1	0	0	0	0
3	Infrastruktur TI	3	0	0	0	0
4	Informasi / Data	5	0	2	0	0
5	Proses	3	1	0	0	0
6	SDM	1	0	2	0	0
	Total	17	1	5	0	0

2. *Risk Evaluation*

Risk Evaluation bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk Evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan untuk mengatasinya. Adapun hasil pemetaan *Risk Map* dapat dilihat pada Tabel berikut ini.

Tabel Risk Map

Impact							
	Sangat Besar (5)	0	0	0	0	0	0
	Besar (4)	0	0	0	0	0	0
	Sedang (3)	1	0	0	0	0	1
	Kecil (2)	11	5	0	0	0	16
	Sangat Kecil (1)	3	3	0	0	0	6
	Total	15	8	0	0	0	23
		Sangat Jarang (1)	Jarang (2)	Kadang-kadang (3)	Sering (4)	Sangat Sering (5)	Total
		Probability					

Berdasarkan Tabel di atas, dapat diketahui bahwa terdapat 5 buah risiko yang termasuk dalam kategori Menengah (M) dan 1 buah risiko yang termasuk dalam kategori Menengah Rendah (LM). Kedua kategori tersebut termasuk dalam jenis risiko yang tidak dapat diterima oleh perusahaan, sehingga untuk mengurangi dampak terjadinya risiko perlu dilakukan tindakan mitigasi.

2.4 Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology,* 1 *Risk Issue* yang termasuk dalam *System Capacity,* 2 *Risk Issue* yang termasuk dalam *Data(base) Integrity* dan 2 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan untuk PT. Advisia Diantara dalam menyikapi beberapa *Risk Issue* dapat dilihat pada 4 buah Tabel berikut ini.

Tabel Langkah Mitigasi *New Technology*

Risiko	**Langkah Mitigasi**
1. Permintaan aplikasi diluar modul SAP tidak terpenuhi.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses perancangan dan pembuatan aplikasi. - Memberikan *training* dan pelatihan kepada seluruh Staff IT mengenai perkembangan teknologi informasi terkini. - Melakukan *Outsourcing* untuk memenuhi banyaknya permintaan aplikasi. - Melakukan analisis *cost-benefit* untuk menentukan investasi jangka panjang dan menentukan prioritas aplikasi yang harus dipenuhi terlebih dahulu

Tabel Langkah Mitigasi *System Capacity*

Risiko	**Langkah Mitigasi**
1. Operasional SAP lambat dan kurang optimal	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses monitoring dan evaluasi terhadap operasional SAP. - Mengadakan *User Licence* pada setiap unit kerja.

Tabel Langkah Mitigasi *Data(base) Integrity*

Risiko	**Langkah Mitigasi**
1. Gangguan komunikasi data antara PG dengan PIHC. 2. Gangguan transmisi data antar departemen.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam menjaga integritas dan keamanan data. - Menjalin kerja sama dengan Team IT dari PIHC. - Menyediakan *helpdesk* untuk menampung segala keluhan terkait dengan integritas data, sehingga dapat ditindak lanjuti dengan segera. - Menggunakan teknik *outomatic switch* jika terjadi *failure.*

Tabel Langkah Mitigasi *IT Expertise and Skills*

Risiko	**Langkah Mitigasi**
1. Dukungan teknis dari Team IT kurang optimal. 2. Adanya *gap* terkait kemampuan yang dimiliki Staff IT	- Meningkatkan kompetensi setiap Staff IT dengan menambah intensitas dalam mengadakan pelatihan atau training terkait dengan Sistem ERP - SAP. - Memperbaiki pola rekruitmen dan pelatihan SDM. - Mengasah kemampuan setiap Staff IT dengan memberikan penugasan atau pekerjaan yang berbeda – beda, agar Staff IT mampu menguasai segala bidang kompetensi yang berhubungan dengan IT. - Mengadakan monitoring dan evaluasi terhadap kinerja seluruh Staff IT. - Bekerja sama dengan Team IT dari PIHC untuk meningkatkan dukungan teknis operasional ERP – SAP. - Menyediakan *helpdesk* tersendiri untuk memudahkan Staff IT dalam menangani setiap keluhan.

3. KESIMPULAN

Berdasarkan hasil pembahasan terkait penerapan manajemen risiko teknologi informasi ada PT. Advisia Diantara maka dapat diperoleh kesimpulan sebagai berikut:

1. Proses evaluasi penerapan manajemen risiko teknologi informasi pada PT. Advisia Diantara menggunakan kerangka kerja COBIT 5 khususnya subdomain EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:
   a. Nilai *Capability Level* untuk subdomain EDM03 berada pada Level 2 yaitu *Managed Process*. Sedangkan Nilai *Capability Level* untuk subdomain APO12 berada pada Level 3 yaitu *Established Process*
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah diperoleh dengan nilai *capability level* yang ingin dicapai untuk subdomain EDM03 dan APO12 masing – masing adalah sebesar 1.
   c. Ditemukannya 23 *risk issue* yang terbagi dalam 15 skenario risiko. Dan dari kelima belas skenario risiko tersebut, terdapat 4 skenario risiko yang membutuhkan strategi dan Langkah mitigasi.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk perbaikan manajemen risiko teknologi informasi di PT. Advisia Diantara adalah sebagai berikut:
   a. Dibuatnya 9 buah rekomendasi agar nilai *Capability Level* pada subdomain EDM03 dapat mencapai Level 3 dan pada subdomain APO12 dapat mencapai Level 4.
   b. Dibuatnya 16 langkah mitigasi berdasarkan 6 buah *risk issue* yang termasuk dalam 4 buah skenario risiko, diantaranya *new technology, database integrity, system capacity* dan *IT expertise skills.* Langkah mitigasi tersebut dirancang untuk memenuhi permintaan aplikasi diluar modul SAP; untuk mengatasi gangguan transmisi data antara departemen dan departemen serta antara PG dengan pihak PIHC; untuk mengoptimalkan operasional SAP; untuk mengoptimalkan dukungan teknis dari team IT dan untuk mengurangi *gap* yang timbul akibat tidak meratanya kemampuan atau *skill* yang dimiliki oleh setiap staff IT.

4. DAFTAR PUSTAKA

Djojosoedarso, Soeisno, 2003. *Prinsip-Prinsip Manajemen Risiko dan Asuransi*, Edisi Pertama, Jakarta: Salemba Empat.

Dyahaloka, Astri, 2016. *Evaluasi Manajemen Risiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero)). Malang : Universitas Brawijaya*

Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu (DKPP). Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

ITGL., 2003. *Broad Briefing on IT Governance 2nd Edition.* Rolling Meadowa : IT Governace Institute.

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung.

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta)*. *SEMNASTEKNOMEDIA ONLINE*, 1(1), pp.23-1.

Husein, G.M. and Imbar, R.V., 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL)*. *Jurnal Teknik Informatika dan Sistem Informasi*, *1*(2).

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) engineering: a practitioner's approach*. United Kingdom : Palgrave Macmillan.

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri.* Jakarta : Universitas Indonesia.

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework*. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1 No.1

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus: PT OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

Wibisono, Diaz Mahardika, 2015. *Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 Manage Risk.* Surabaya : Universitas Airlangga.

Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk Pada PT. Advisia Diantara

Abstrak

SAP (*System Application and Product in Data Processing*) merupakan jenis software ERP yang digunakan oleh PT. Advisia Diantara untuk menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan agar lebih efektif dan efisien. Untuk mengantisipasi timbulnya risiko yang dapat mengganggu jalannya proses bisnis perusahaan, PT. Advisia Diantara menerapkan manajemen risiko berdasarkan standart ISO 31000:2009. Dalam hal ini perlu dilakukan evaluasi untuk mnegetahui pencapaian penerapan manajemen risiko teknologi informasi pada PT. Advisia Diantara dengan menggunakan kerangka kerja COBIT 5 khususnya pada domain proses APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation). Untuk memperoleh data yang akurat, maka teknik pengumpulan data yang digunakan adalah dengan melakukan pengisian lembar kerja evaluasi, obeservasi langsung dan wawancara dengan pihak yang berwenang. Proses evaluasi tersebut terdiri dari beberapa tahapan, antara lain melakukan analisis *capability level,* analisis *gap* dan analisis *risk assessment* untuk mengidentifikasi risiko – risiko potensial serta menilai sejauh mana dampak yang dapat ditimbulkan. Berdasarkan hasil analisis tersebut, maka didapatkan nilai *capability level* untuk domain proses EDM03 berada pada level 2 dan domain proses APO12 berada pada level 3 serta menghasilkan 16 buah strategi mitigasi dan 9 buah rekomendasi yang dapat digunakan untuk membantu perbaikan penerapan manajemen risiko teknologi informasi di PT. Advisia Diantara.

1. PENDAHULUAN

Salah satu perusahaan yang telah memanfaatkan teknologi informasi dan menerapkan manajemen risiko teknologi informasi sebagai sarana pendukung untuk mencapai tujuan perusahaan adalah PT. Advisia Diantara. Untuk meningkatkan kualitas perusahaan dibidang teknologi informasi, PT. Advisia Diantara menerapkan sistem ERP – SAP yang terdiri dari sepuluh modul. Disamping itu PT. Advisia Diantara juga menerapkan beberapa aplikasi Non ERP untuk menunjang jalannya Sistem ERP-SAP. Dengan diterapkannya Sistem tersebut diharapkan mampu menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan secara efektif dan efisien. Namun pada kenyatannya, penerapan Teknologi Informasi (TI) pada perusahaan tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan perusahaan. Oleh karena itu untuk mengelola segala macam risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka PT. Advisia Diantara telah menerapkan manajemen risiko berdasarkan pada Standart ISO 31000 : 2009 sejak tahun 2003. Padatnya proses bisnis yang berjalan di PT. Advisia Diantara, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Risiko – risiko tersebut diantaranya berupa gangguan jaringan internet, gangguan arus listrik, kurang optimalnya dukungan teknis operasional ERP, gangguan komunikasi data antara user dengan server ERP dan lain sebagainya. Oleh arena itu perlu adanya evaluasi manajemen risiko Teknologi Informasi (TI) untuk mengetahui tingkat kapabilitas pengelolaan risiko yang telah dicapai, sehingga dapat meningkatkan kemampuan perusahaan dalam mengelola setiap risiko terkait penerapan sistem ERP-SAP pada PT. Advisia Diantara. Dari evaluasi tersebut menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko – risiko yang tidak diinginkan. Salah satu *framework* yang dapat digunakan untuk mengevaluasi anajemen risiko Teknologi Informasi (TI) pada PT. Advisia

Diantara ialah COBIT 5 khususnya pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisatin*). Digunakannya domain tersebut karena dalam COBIT 5, hanya ada dua domain yang membahas secara terperinci mengenai manajemen risiko Teknologi Informasi (TI).

2. PEMBAHASAN

2.1 Analisis *Capability Level*

Berdasarkan hasil pengisian lembar kerja evaluasi yang dilakukan oleh 3 responden dari Departemen TKP & MR dan Departemen TEKINFO PT. Advisia Diantara dapat diketahui bahwa nilai *capability level* yang telah dicapai subdomain EDM03 berada pada Level 2 dan nilai *capability level* yang telah dicapai subdomain APO12 berada pada tingkat Level 3. Hal tersebut dapat dilihat pada Tabel di bawah ini.

Tabel Rekapitulasi Hasil GAP Analysis

Nama Proses	Level Saat Ini	Level Target	*Gap*
EDM03	2	3	1
APO12	3	4	1

2.2 Analisis *Gap*

Berdasarkan hasil wawancara, diperoleh informasi bahwa level target yang ingin dicapai oleh Departemen TKP & MR dan Departemen TEKINFO PT. Advisia Diantara adalah naik satu level untuk setiap domain prosesnya, yaitu domain proses EDM03 berada pada Level 3 dan domain proses APO12 berada pada Level 4. Sehingga besarnya *gap* yang terbentuk antara level yang terjadi saat ini dan level target yang ingin dicapai pada domain proses EDM03 dan APO12 adalah sebesar 1.

2.3 *Risk Assessment*

Proses *Risk Assessment* dilakukan berdasarkan dua tahapan, antara lain:

1. *Risk Analysis*

   Risk Analysis bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, menentukan parameter *impact*, menentukan parameter *rating* risiko, melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*. Adapun pengelompokan risiko berdasarkan skenario risiko dapat dilihat dalam Tabel berikut ini.

Tabel Rekapitulasi Berdasarkan Skenario Risiko

No	Skenario Risiko	Jumlah *Risk Issue*
1	*New Technology*	1
2	*Software Implementation*	2
3	*Destruction of Infrastructure*	1
4	*IT Staff*	1
5	*IT Expertise and Skills*	2
6	*Software Integrity*	2
7	*Infrastructure (Hardware)*	3
8	*System Capacity*	2
9	*Malware*	1
10	*Logical Attacks*	1
11	*Utilities Performance*	1
12	*Data(base) Integrity*	2
13	*Logical Trespassing*	1
14	*Operational IT Errors*	2
15	*Acts of Nature*	1
	Total	23

Sedangkan untuk pengelompokan risiko berdasarkan aset dapat dilihat dalam Tabel berikut ini.

Tabel 4. Rekapitulasi Berdasarkan Aset

No	Kategori Aset	Jumlah *Risk Issue*	Persentase
1	Aplikasi	5	21,74 %
2	Fasilitas	1	4,35 %
3	Infrastruktur TI	3	13,04 %
4	Informasi / Data	7	30,43 %
5	Proses	4	17,39 %
6	SDM	3	13,04 %
Total	23	100 %	

Sebelum melakukan penilaian risiko terhadap *Inherent Risk* dan *Residual Risk*, terlebih dahulu menentukan standart penilaian berupa parameter *probability* (kecenderungan), parameter *impact* (dampak) dan parameter *Rating* Risiko. Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel berikut ini.

Tabel Penilaian *Inherent Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	0	0	4	0	1
2	Fasilitas	0	0	1	0	0
3	Infrastruktur TI	0	1	2	0	0
4	Informasi / Data	0	0	5	2	0
5	Proses	0	0	4	0	0
6	SDM	0	0	2	1	0
Total		0	1	18	3	1

Berdasarkan hasil wawancara dengan beberapa perwakilan dari Dept. TEKINFO dan Dept. TKP & MR, dapat diketahui bahwa setiap risiko – risiko yang teridentifikasi telah memiliki pengendalian tersendiri. Pengendalian tersebut digunakan sebagai dasar untuk melakukan penilaian Residual Risk. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel berikut ini.

Tabel Penilaian *Residual Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	4	0	1	0	0
2	Fasilitas	1	0	0	0	0
3	Infrastruktur TI	3	0	0	0	0
4	Informasi / Data	5	0	2	0	0
5	Proses	3	1	0	0	0
6	SDM	1	0	2	0	0
	Total	17	1	5	0	0

2. *Risk Evaluation*

Risk Evaluation bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk Evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan untuk mengatasinya. Adapun hasil pemetaan *Risk Map* dapat dilihat pada Tabel berikut ini.

Tabel Risk Map

Impact							
	Sangat Besar (5)	0	0	0	0	0	0
	Besar (4)	0	0	0	0	0	0
	Sedang (3)	1	0	0	0	0	1
	Kecil (2)	11	5	0	0	0	16
	Sangat Kecil (1)	3	3	0	0	0	6
	Total	15	8	0	0	0	23
		Sangat Jarang (1)	Jarang (2)	Kadang-kadang (3)	Sering (4)	Sangat Sering (5)	Total
		Probability					

Berdasarkan Tabel di atas, dapat diketahui bahwa terdapat 5 buah risiko yang termasuk dalam kategori Menengah (M) dan 1 buah risiko yang termasuk dalam kategori Menengah Rendah (LM). Kedua kategori tersebut termasuk dalam jenis risiko yang tidak dapat diterima oleh perusahaan, sehingga untuk mengurangi dampak terjadinya risiko perlu dilakukan tindakan mitigasi.

2.4 Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology,* 1 *Risk Issue* yang termasuk dalam *System Capacity,* 2 *Risk Issue* yang termasuk dalam *Data(base) Integrity* dan 2 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan untuk PT. Advisia Diantara dalam menyikapi beberapa *Risk Issue* dapat dilihat pada 4 buah Tabel berikut ini.

Tabel Langkah Mitigasi *New Technology*

Risiko	**Langkah Mitigasi**
1. Permintaan aplikasi diluar modul SAP tidak terpenuhi.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses perancangan dan pembuatan aplikasi. - Memberikan *training* dan pelatihan kepada seluruh Staff IT mengenai perkembangan teknologi informasi terkini. - Melakukan *Outsourcing* untuk memenuhi banyaknya permintaan aplikasi. - Melakukan analisis *cost-benefit* untuk menentukan investasi jangka panjang dan menentukan prioritas aplikasi yang harus dipenuhi terlebih dahulu

Tabel Langkah Mitigasi *System Capacity*

Risiko	**Langkah Mitigasi**
1. Operasional SAP lambat dan kurang optimal	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses monitoring dan evaluasi terhadap operasional SAP. - Mengadakan *User Licence* pada setiap unit kerja.

Tabel Langkah Mitigasi *Data(base) Integrity*

Risiko	**Langkah Mitigasi**
1. Gangguan komunikasi data antara PG dengan PIHC. 2. Gangguan transmisi data antar departemen.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam menjaga integritas dan keamanan data. - Menjalin kerja sama dengan Team IT dari PIHC. - Menyediakan *helpdesk* untuk menampung segala keluhan terkait dengan integritas data, sehingga dapat ditindak lanjuti dengan segera. - Menggunakan teknik *outomatic switch* jika terjadi *failure.*

Tabel Langkah Mitigasi *IT Expertise and Skills*

Risiko	**Langkah Mitigasi**
1. Dukungan teknis dari Team IT kurang optimal. 2. Adanya *gap* terkait kemampuan yang dimiliki Staff IT	- Meningkatkan kompetensi setiap Staff IT dengan menambah intensitas dalam mengadakan pelatihan atau training terkait dengan Sistem ERP - SAP. - Memperbaiki pola rekruitmen dan pelatihan SDM. - Mengasah kemampuan setiap Staff IT dengan memberikan penugasan atau pekerjaan yang berbeda – beda, agar Staff IT mampu menguasai segala bidang kompetensi yang berhubungan dengan IT. - Mengadakan monitoring dan evaluasi terhadap kinerja seluruh Staff IT. - Bekerja sama dengan Team IT dari PIHC untuk meningkatkan dukungan teknis operasional ERP – SAP. - Menyediakan *helpdesk* tersendiri untuk memudahkan Staff IT dalam menangani setiap keluhan.

3. KESIMPULAN

Berdasarkan hasil pembahasan terkait penerapan manajemen risiko teknologi informasi ada PT. Advisia Diantara maka dapat diperoleh kesimpulan sebagai berikut:

1. Proses evaluasi penerapan manajemen risiko teknologi informasi pada PT. Advisia Diantara menggunakan kerangka kerja COBIT 5 khususnya subdomain EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:
   a. Nilai *Capability Level* untuk subdomain EDM03 berada pada Level 2 yaitu *Managed Process*. Sedangkan Nilai *Capability Level* untuk subdomain APO12 berada pada Level 3 yaitu *Established Process*
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah diperoleh dengan nilai *capability level* yang ingin dicapai untuk subdomain EDM03 dan APO12 masing – masing adalah sebesar 1.
   c. Ditemukannya 23 *risk issue* yang terbagi dalam 15 skenario risiko. Dan dari kelima belas skenario risiko tersebut, terdapat 4 skenario risiko yang membutuhkan strategi dan Langkah mitigasi.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk perbaikan manajemen risiko teknologi informasi di PT. Advisia Diantara adalah sebagai berikut:
   a. Dibuatnya 9 buah rekomendasi agar nilai *Capability Level* pada subdomain EDM03 dapat mencapai Level 3 dan pada subdomain APO12 dapat mencapai Level 4.
   b. Dibuatnya 16 langkah mitigasi berdasarkan 6 buah *risk issue* yang termasuk dalam 4 buah skenario risiko, diantaranya *new technology, database integrity, system capacity* dan *IT expertise skills.* Langkah mitigasi tersebut dirancang untuk memenuhi permintaan aplikasi diluar modul SAP; untuk mengatasi gangguan transmisi data antara departemen dan departemen serta antara PG dengan pihak PIHC; untuk mengoptimalkan operasional SAP; untuk mengoptimalkan dukungan teknis dari team IT dan untuk mengurangi *gap* yang timbul akibat tidak meratanya kemampuan atau *skill* yang dimiliki oleh setiap staff IT.

4. DAFTAR PUSTAKA

Djojosoedarso, Soeisno, 2003. *Prinsip-Prinsip Manajemen Risiko dan Asuransi*, Edisi Pertama, Jakarta: Salemba Empat.

Dyahaloka, Astri, 2016. *Evaluasi Manajemen Risiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero)). Malang : Universitas Brawijaya*

Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu (DKPP). Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

ITGL., 2003. *Broad Briefing on IT Governance 2nd Edition.* Rolling Meadowa : IT Governace Institute.

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung.

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta)*. *SEMNASTEKNOMEDIA ONLINE*, 1(1), pp.23-1.

Husein, G.M. and Imbar, R.V., 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL)*. *Jurnal Teknik Informatika dan Sistem Informasi*, *1*(2).

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) engineering: a practitioner's approach*. United Kingdom : Palgrave Macmillan.

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri.* Jakarta : Universitas Indonesia.

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework*. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1 No.1

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus: PT OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

Wibisono, Diaz Mahardika, 2015. *Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 Manage Risk.* Surabaya : Universitas Airlangga.

RISK ASSESSMENT CV MTI-NET

Abstrak

Teknologi informasi telah menjadi bagian penting dari kehidupan manusia sehingga dapat mempermudah suatu kegiatan bisnis. Meskipun begitu, penggunaan teknologi informasi tidak lepas dari resiko yang dapat mempengaruhi proses kegiatan tersebut. Adapun tujuan penelitian ini adalah untuk melakukan penilaian resiko terhadap potensi kerentanan dan ancaman yang dapat menyerang sistem CV MTI-NETsekaligus mempersiapan tindakan antisipasi terhadap hal-hal yang dapat mengganggu sistem. Untuk melakukan penilaian tersebut, study ini menggunakan framework NIST SP 800-30r-1 yang terdiri sembilan tahapan untuk dalam penilaian resiko yaitu karakteristik sistem yang digunakan, indentifikasi ancaman yang menyerang sistem, identifikasi vulnerability, pengendalian sistem, menentukan kemungkinan terjadi (*likelihood*), menentukan dampak (*impact*), penentuan resiko, rekomendasi pengendalian dan dokumentasi hasil. Hasil dari penilaian resiko terhadap sistem CV MTI-NET adalah terdapat tida resiko yang mengganggu aktifitas yang ada dalam sistem. Kemudian dari hasil penilaian resiko berupa rekomendasi yang digunakan untuk memperkecil resiko yang terjadi pada sistem.

Kata kunci:*NIST, Penilaian Resiko, Risk Management,*

PENDAHULUAN

Peran penting teknologi informasi dan komunikasi (TIK) adalah membantu meringankan pekerjaan kantor sehingga lebih cepat dan lebih akurat. Hal ini dapat dilihat dari semakin tergantungnya proses bisnis suatu organisasi di berbagai bidang kegiatan dengan teknologi ini.Bidang pendidikanpun tidak lepas dari penggunaan TIK terutama dalam pelayanan akademik. Secara eksternal, banyak aktifitas pelaporan kegiatan akademik mengharuskan lembaga pendidikan menggunakan TIK. Dukungan teknologi juga dipergunakan untuk mempercepat proses layanan akademik dalan suatu perguruan tinggi. Akibatnya semakin pentingnya peran TIK dalam mendukung kegiatan menimbulkan permasalah tersendiri bila fungsi TIK tersebut terganggu.Pemanfaatan juga TIK perlu untuk memperhatikan resiko yang berpotensi menganggu akibat pengelolaan yang kurang efektif. Pemanfaatan teknologi informasi dapat berjalan dengan efektif jika digunakan dengan baik (Suzanto and Sidharta 2015).

Pemanfaatan TIK yang tidak dimanfaatkan secara baik menimbulkan peluang untuk seseorang melakukan kejahatan dalam teknologi informasi.Pemanfaatan sistem informasi akademik dapat berjalan dengan baik jika dalam penggunaan dan pemanfaatan sistem dapat digunakan secara baik(Cahyaningdyah and Ressany 2012).Kejahatan TIK dapat digolongkan dari yang mengesalkan (*annoying*) sampai dengan sangat berbahaya. Dari yang dapat diatasi sampai yang tidak dapat diatasi yang dapat menimbulkan kehilangan aset terpenting dalam sistem. Untuk mengantisipasi resiko kehilangan aset, maka dibutuhkan sebuah keamanan sistem yang dibuat untuk melindungi teknologi informasi yang ada pada lembaga. Menurut Rahardjo (2002) berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu resiko keamanan yang bersifat fisik *(physical security)*, resiko keamanan yang berhubungan dengan orang (*personel*), resiko keamanan dari data dan media serta teknik komunikasi dan resiko keamanan dalam operasi.

Perumpamaan sebuah objek adalah sebuah CV warnet penyedia layanan akses internet, dll. Pada sesi khusus team peneliti membuat sebuah rencana dengan sebuah bisnis. Bisnis itu adalah warnet, objek direncakankan bernama CV NTI-NET, dimana lokasi objek yang memungkinkan paling strategis adalah dekat dengan pemukiman warga yang padat serta berdekatan dengan area sekolah. Kebutuhan bisnis disana yaitu untuk menyediakan layanan internet (Termasuk *gaming*, *printing*, *scanning*, serta jasa penyediaan untuk mengakses layanan internet). Perkiraan ruko ada dua lantai, lantai pertama digunakan untuk bisnis awal, sebesar 9 komputer (8 komputer *client*, 1 komputer *billing*). Bisnis ini baru dibuka dan kebutuhan awal adalah 9 komputer, namun dilantai 2 ada denah yang sama dengan kebutuhan komputer adalah 8 komputer yang harus terhubung juga ke internet. Namun ini masih sebatas rencana. Untuk mendukung prospek kedepannya, maka team peneliti dituntut agar memikirkan tehnologi seperti apa yang bisa dipakai untuk kebutuhan tersebut. Kebutuhan dari bisnis baru ini yaitu bahwa mereka membutuhkan jaringan komputer dengan skala kecil yang menggunakan setidaknya 10 pc dimana digunakan secara bergantian (selain pc *billing* dan server) oleh penggunjung dan dapat mengakses internet dengan jam kerja operasional 07.00 s.d

22.00 WIB.

Untuk dapat mendukung usaha tersebut, *owner* meminta kami untuk membangun suatu jaringan yang dapat diterapkan/diimplementasikan ditempat usaha tersebut. *Owner* juga meminta sebuah jaringan efektif dengan menyediakan anggaran dengan seminimal mungkin. Dari **proses bisnis** yang telah dijelaskan, tantangan kerja team adalah membangun jaringan yang efektif sesuai dengan anggaran yang ada. Dengan memikirkan, apakah usaha ini akan ada perubahan atau perluasan prospek usaha kedepannya. Maka strategi team adalah menggunakan teknologi diskless yaitu teknologi untuk membuat PC/Komputer bisa tetap running dengan normal tanpa menggunakan Harddisk, dimana PC Diskless berjalan dengan metode booting melalui jaringan dan mengambil seluruh OS dan aplikasi-aplikasi langsung dari PC Server, bukan dari harddisk lokal. Lalu yang menjadi permasalahan adalah resiko yang akan terjadi. Bagaimana hal ini dapat dijangkau, maka dalam penelitian ini adalah mencoba menganalisis kerja sistem yang ada.

2. METODOLOGI PENELITAN

2.1 Risk Management Framework

Risk management atau manajemen resiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman, suatu rangkaian aktivitas manusia termasuk penilaian resiko, pengembangan strategi untuk mengelolanya dan mitigasi resiko dengan menggunakan pembersayaan/pengelolaan sumberdaya (Hanafi 2014).Tujuan dari manajemen risiko adalah untuk mengenali risiko dalam sebuah proyek dan mengembangkan strategi untuk mengurangi atau bahkan menghindarinya, dilain sisi juga harus dicari cara untuk memaksimalkan peluang yang ada (Wideman 1992).*Framework* adalah kumpulan perintah atau fungsi dasar yang membentuk aturan-aturan tertentu dan saling berinteraksi satu sama lain sehingga dalam pembuatan aplikasi (Wardana and Si 2010).*Framework* yang digunakan oleh penulis adalah *framework* NIST SP 800-30r1 yang tepat digunakan dalam penelitian ini. NIST 800-30r1 adalah dokumen standar yang dikembangkan oleh *National Institute of Standards and Technology* yang mana merupakan kelanjutan dari tanggung jawab hukum dibawah undang-undang *Computer Security Act* tahun 1987 dan *the Information Technology Management Reform Act* tahun 1996 (NIST 2002). Terdapat tiga proses dalam manajemen resiko: *risk assessment, risk mitigation, and evaluation and assessment.Framework* NIST SP 800-30r1 mempunyai struktur dan tahapan proses yang terarah. Metode ini memberikan panduan untuk melakukan proses penilaian resiko langkah demi langkah. Tahapannya terdiri dari *Risk Assessment, Risk Mitigation* dan *Evaluation and Assessment.*

2.2 Teknik Penilaian Resiko

Teknik penilaian resiko menggunakan *framework NIST* SP 800-30r-1. *Framework* NIST SP 800-30r-1 merupakan panduan untuk memproses data yang sangat sensitif. NIST SP 800-30r-1 memiliki kontribusi lebih dalam melakukan penilaian resiko karena memberikan wawasan keamanan informasi yang sifatnya konsisten dan komprehensif bagi pengambilan kebijakan, pemodelan sumber daya yang terstruktur, wawasan keamanan dapat diterima oleh berbagai pengambil resiko, penentuan ancaman dapat diidentifikasi dengan mudah, pengambilan keputusan yang baik untuk setiap resiko yang diselidiki (Andani 2014). Dalam NIST SP 800-30r-1 ini terdapat sembilan langkah untuk melakukan analisa resiko yaitu karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, analisa kontrol, analisa kemungkinan terjadi, analisa dampak, penentuan level resiko dan rekomendasi pengendalian.

2.3 Teknik Pengumpulan Data

Pengumpulan data sangat penting dalam penelitian, karena data tersebut dimaksudkan untuk berkontribusi pada pemahaman kerangka teoretis yang lebih baik (Herdiansyah 2013). Pemilihan informan dengan metode *purposive sampling* bertujuan untuk penelitian yang dilakukan peneliti akan mendapatkan capaian yang baik dan sesuai dengan keinginan informan. Pemilihan informan yang dilakukan peneliti dalam menganalisis *assessment* resiko pada sistem yang akan diterapkan pada CV MTI-NET yaitu memilih sumber data yang benar-benar

bertanggung jawab atas sistem tersebut yaitu owner, team perancang dan strategy pengembangan jaringan (team strategy IT, Networking), konsumen, pekerja yang bertanggung jawab dan diantaranya pula merupakan orang – orang dalam ruang lingkup dimana sistem ini diterapkan, ini bersumber pada analisis team peneliti yaitu team perancang dan pengembang sistem dan strategi pengembangan jaringan komputer.

2.4 Metode Pennetuan Informan

Pengumpulan data sangat penting dalam penelitian, karena data tersebut dimaksudkan untuk berkontribusi pada pemahaman kerangka teoretis yang lebih baik (Herdiansyah 2013). Menentukan sampel dalam penelitian, terdapat teknik sampling yang digunakan salah satunya adalah teknik purposive sampling. *Purposive sampling* adalah teknik pengambilan sumber dengan pertimbangan tertentu. Misalnya akan melakukan penelitian tentang kualitas suatu makanan, maka sampel yang merupakan sumber data dari penelitian tersebut adalah orang yang ahli dalam makanan. Sampel ini digunakan untuk penelitian kualitatif atau penelitian-penelitian yang tidak melakukan generalisasi (Aryani and Rosinta 2011). Pemilihan informan dengan metode *purposive sampling* bertujuan untuk penelitian yang dilakukan peneliti akan mendapatkan capaian yang baik dan sesuai dengan keinginan informan. Pemilihan informan yang dilakukan peneliti dalam menganalisis *assessment* resiko pada sistem pada CV MTI-NET yaitu memilih sumber data yang benar-benar bertanggung jawab atas sistem tersebut yaitu owner, team perancang dan strategy pengembangan jaringan (team strategy IT, Networking), dan ruang lingkup sistem tersebut diterapkan konsumen, pekerja.

3. HASIL DAN PEMBAHASAN

Untuk melakukan penilaian resiko terhadap sistem CV MTI-NETada sembilan tahapan yaitu:

a. Karakteristik Sistem

- Karakteristik yang digunakan dalam sistem CV MTI-NET adalah perangkat keras yang digunakan PC dan sever lokal yang adalah satunya server merk dell yaitu T30 Xeon Quad E3-1225v5/16Gb/1TB// 2LAN PORT. *Software* yang digunakan berupa *Windows 7*. Teknologi yang digunakan adalah diskless yang merupakan teknologi untuk membuat PC/Komputer bisa tetap running dengan normal tanpa menggunakan Harddisk kemudiann dapat pula PC Diskless berjalan dengan metode booting melalui jaringan dan mengambil seluruh OS dan aplikasi-aplikasi langsung dari PC Server, bukan dari harddisk lokal. Dan jaringan akses internet yang digunakan adalah ISP Telkom Unlimited.

b. Identifikasi Ancaman

Ancaman-ancaman yang mengancam sistem CV MTI-NETadalah ancaman serangan pada *firewall* dan perubahan setting windows yang kemungkinan ada pada CV MTI-NET. Melakukan ancaman seperti *sniffing, scanning network, phising, flooding, wireless jamming, Ddos* pada sistem informasi yang bertujuan merusak sistem.

c. Identifikasi Kerentanan (*Vulnerability*)

Identifikasi kerentanan (*Vulnerability*) yang didapat dari hasil wawancara terlihat pada tabel 1.

Tabel 1: Identifikasi Kerentanan (*Vulnerability*)

Jenis Resiko	Kerentanan
Berasal dari dalam Lingkungan	- *Password cracking* untuk melakukan pencurian data pada sistem - Keterlambatan Dalam melakukan *updateantivirus* sehingga memungkinkan *malware* masuk kedalam sistem - Kelalaian konsumen dalam memindahkan sistem dalam menggunakan flash drive atau

	drive eksternal yang dapat menjadi sarana masuknya trojan. - pengaksesan website berisi iklan jahat, dll
Berasal dari luar lingkungan Bencana alam	- *Scanning tools* - Kebakaran - Gempa Bumi

d. Analisis Pengendalian

Hasil dari wawancara terstruktur analisis pengendalian telah tertuang dalam dokumen yang mencakup semua standar-standar dan prosedur-prosedur dalam pengoperasian sistem CV MTI-NET yaitu dokumen SOP (*Standard Operating Procedure).*Yang kedepannya seharusnya menjadi rencana pengerjaan.

e. Kemungkinan Terjadi (*Likelihood*)

Hasil dari kemungkinan terjadi (*Likelihood*) pada sistem CV MTI-NETberdasarkan tingkat kemungkinan terjadinya resiko ada tiga yaitu tinggi, sedang dan rendah. Kategori kemungkinan terjadi resiko pada sistem termasuk tinggi apabila sumber ancaman sangat mampu dan pengendalianuntuk mencegah kerentanan yang dilkaukan sudah tidak efektif lagi. Kategori kemungkinan terjadi resiko pada sistem termasuk sedang apabila sumber ancaman mampu dalam menembus pertahanan sistem namun belum sampai pada layer terdalam pada jaringan sehingga dapat menghambat kerentanan. Kategori kemungkinan terjadi resiko pada sistem termasuk rendah apabila sumber ancaman tidak memiliki kemampuan untuk menembus keamanan, setidaknya dapat menghambat namun dapat diatasi. Kemungkinan terjadi resiko pada sistem adalah (1) penyerangan yang dilakukan oleh orang dalam (bisa ditimbulkan dari staf, owner), dan orang luar adalah konsumen (2) terjadi kerusakan atau *disk error* pada penyimpanan data, (3) *firewall* yang tidak diamankan (4) malware, trojan, dan file-file jahat dari luar ketika mengakses website atau internet atau bahkan file yang membawa banyak script jahat.

f. Analisis Dampak (*Impact*)

Berdasarkan analisis hasil resiko yang menggambarkan dampak resiko (*impact*) terhadap sistem CV MTI-NETterlihat pada tabel 2.

Tabel 2: Dampak Resiko

Jenis Resiko	Dampak	Tingkat Dampak
Penyerangan yang dilakukan oleh orang dalam	- Tidak dapak masuk kedalam sistem - Kehilangan kontrol pada sistem - hilang setting - Pencurian data pengguna	Tinggi
Disk Error	- Tidak dapat melakukan proses penyimpanan data pada hardisk sistem	Sedang
Keamanan firewall; Malware, trojan sejenis file jahat atau script jahat dan asing dari internet.	- Merusak set-up, spy, data bocor, dan privacy	Tinggi

g. Risk Determination

Risk determination memperlihatkan jenis resiko yang menyerang sistem CV MTI-NET dari yang tinggi sampai ke resiko yang rendah yang akan terlihat pada tabel 3. Pada tabel 3

terlihat jenis resiko yang memiliki tingkat atau level resiko tinggi pada jenis resiko penyerangan yang dilakukan oleh orang dalam dan ancaman keamanan *firewall*. Level resiko sedang pada jenis resiko *disk error* atau kerusakan pada penyimpanan data.

Tabel 3:*Risk Determination*

Jenis Resiko	Nilai Kemungkinan Terjadi	Nilai Dampak	Nilai Resiko	Level Resiko
Penyerangan yang dilakukan oleh orang dalam	1,0	100	100	Tinggi
Disk Error	0,5	100	50	Sedang
Keamanan firewall; *Malware, trojan* sejenis file jahat atau *script* jahat dan asing dari internet.	0,1	100	100	Tinggi

h. Rekomendasi Pengendalian

Dari tingkat resiko tersebut dapatlah rekomendasi pengendalian yang digunakan untuk membuat prosedur untuk penanganan terhadap ancaman yang terjadi. Dari hasil penilaian maka direkomendasikan beberapa kontrol yang dapat dilakukan terhadap resiko yang terlihat pada tabel 4.

Tabel 4: Rekomendasi Pengendalian

Jenis Ancaman	Tingkat Ancaman	Rekomendasi Pengendalian
Penyerangan yang dilakukan oleh orang dalam	Tinggi	- Memperkokoh *firewall* yang digunakan oleh sisem pada CV MTI-NET. Memperkokoh keamanan server dan PC server. *Backup data, sistem maintenance berkala, dan re-setting dari pc server sehingga data awal dan jika terjadi perubahan sett-up pada sistem akan dikembalikan*
Disk Error	Sedang	- *ketika maintenance.*
Keamanan firewall; *Malware, trojan* sejenis file jahat atau *script* jahat dan asing dari internet.	Tinggi	- Pembatasan akses website tertentu. Dan antivirus setiap pc.

i. Dokumen Hasil

Dari hasil penilaian kemungkinan resiko teknologi pada implementasi sistem CV MTI-NET maka dibuatlah dokumen penanganan terhadap resiko yang mengancam sistem pada CV MTI-NEt. Dokumen ini berisi tentang tata cara penanganan resiko-resiko yang menyerang sistem informasi akademik.

4. KESIMPULAN

Dalam proses penilian resiko, penulis menggunakan tahapan resiko yang telah disediakan oleh *framework* NIST SP 800-30r-1 yang terdiri dari karakteristik sistem, mengidentifikasi ancaman, kontrol analisis, kemungkinan terjadi (*likelihood*), dampak (*impact*), level resiko *(risk determination*), rekomendasi resiko dan terakhir rekomendasi hasil. Diantara jenis ancaman ini terdapat 3 tingkat resiko setelah dilakukan penilaian. Resiko yang muncul adalah resiko yang dilakukan oleh orang dalam serta kegagalan infrastruktur. Selain itu adalah ancaman firewall yang bekas – bekas atau file jahat yang dibawa file yang diambil dari internet. Resiko dinilai mempunyai resiko tinggi karena penyerangan yang dilakukan terhadap sistem berasal dari orang dalam seperti staf, dll. Resiko ini dinilai mempunyai resiko sedang karena tempat

penyimpanan data rusak yang membuat aktifitas dalam sistem menjadi terganggu.

Paper terinspirasi dari (Meilani, dkk. 2019). Kasus ini merupakan kasus yang belum ada sistem. Sehingga analisis dilakukan dengan bertanya pada IT strategy dan pengembangan jaringan sistem CV MTI-NET dan dengan melihat pengalaman staf pada sistem yang serupa (lab komputer dll). Ini adalah virtual analisis resiko, dengan pengalaman kerja pada sistem yang memiliki teknologi yang serupa (diskless) serta melihat bagaimana kerja sistem warnet pada umumnya. sekian-

Referensi

Meilani, Yayuk Ike, Dedy Syamsuar, dan Yesi Novaria Kunang. 2019. "ASSESSMENT RESIKO TEKNOLOGI PADA IMPLEMENTASI SISTEM INFORMASI AKADEMIK E-UNIVERSITY." *Jurnal Bina Komputer* 1(1):54–60. doi: 10.33557/binakomputer.v1i1.154.

Andani, M. (2014). Manajemen Risiko Keamanan Aplikasi Sistem Informasi Laporan Harian Pks & Ppko Online Pada Ptpn V Menggunakan Metode Nist Sp 800-30, *Universitas Islam Negeri Sultan Syarif Kasim Riau.*

Aryani, D. and F. Rosinta (2011). Pengaruh kualitas layanan terhadap kepuasan pelanggan dalam membentuk loyalitas pelanggan. *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi.*

Cahyaningdyah, D. And Y.D. Ressany (2012), Pengaruh Kebijakan Manajemen Keuangan Terhadap Nilai Peusahaan, *Jurnal Dinamika Manajemen*.

Herdiansyah, H. (2013). *Wawancara, observasi, dan focus groups: Sebagai instrumen penggalian data kualitatif*. Jakarta: PT. Raja Grafindo Persada.

Mellisa, M. And F. A. Andono (2013). *Penerapan Enterprise Risk Management dalam Rangka Meningkatkan Efektifitas Kegiatan Operasional CV. Anugerah Berkat Calindo Jaya.*

NIST (2002). Sp 800-30. risk management guide for information technology systems.

Recomendation of National Institute of Standards and Technology Special Publication 800-30r-1.Rahardjo, B. (2002). Keamanan Sistem Informasi Berbasis Internet. *PT Insan Infonesia–Bandung & PT INDOCISC–Jakarta.*

Suzanto, B. and I. Sidharta (2015). Pengukuran End-User Computing Satisfaction Atas Penggunaan Sistem Informasi Akademik. *Jurnal Ekonomi, Bisnis & Entrepreneurship*.

Wardana, S. H. and M. Si (2010). *Menjadi Master PHP dengan Framework Codeigniter, Elex Media Komputindo,* www.scholar.google.co.id, *diakses:* 18 Maret 2018.

Wideman, R. M. (1992). Project and program risk management: a guide to managing project risks and opportunities, *University of Maribor, Faculty of Business and Economics*.

Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk Pada PT. Advisia Diantara

Abstrak

SAP (*System Application and Product in Data Processing*) merupakan jenis software ERP yang digunakan oleh PT. Advisia Diantara untuk menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan agar lebih efektif dan efisien. Untuk mengantisipasi timbulnya risiko yang dapat mengganggu jalannya proses bisnis perusahaan, PT. Advisia Diantara menerapkan manajemen risiko berdasarkan standart ISO 31000:2009. Dalam hal ini perlu dilakukan evaluasi untuk mnegetahui pencapaian penerapan manajemen risiko teknologi informasi pada PT. Advisia Diantara dengan menggunakan kerangka kerja COBIT 5 khususnya pada domain proses APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation). Untuk memperoleh data yang akurat, maka teknik pengumpulan data yang digunakan adalah dengan melakukan pengisian lembar kerja evaluasi, obeservasi langsung dan wawancara dengan pihak yang berwenang. Proses evaluasi tersebut terdiri dari beberapa tahapan, antara lain melakukan analisis *capability level,* analisis *gap* dan analisis *risk assessment* untuk mengidentifikasi risiko – risiko potensial serta menilai sejauh mana dampak yang dapat ditimbulkan. Berdasarkan hasil analisis tersebut, maka didapatkan nilai *capability level* untuk domain proses EDM03 berada pada level 2 dan domain proses APO12 berada pada level 3 serta menghasilkan 16 buah strategi mitigasi dan 9 buah rekomendasi yang dapat digunakan untuk membantu perbaikan penerapan manajemen risiko teknologi informasi di PT. Advisia Diantara.

1. PENDAHULUAN

Salah satu perusahaan yang telah memanfaatkan teknologi informasi dan menerapkan manajemen risiko teknologi informasi sebagai sarana pendukung untuk mencapai tujuan perusahaan adalah PT. Advisia Diantara. Untuk meningkatkan kualitas perusahaan dibidang teknologi informasi, PT. Advisia Diantara menerapkan sistem ERP – SAP yang terdiri dari sepuluh modul. Disamping itu PT. Advisia Diantara juga menerapkan beberapa aplikasi Non ERP untuk menunjang jalannya Sistem ERP-SAP. Dengan diterapkannya Sistem tersebut diharapkan mampu menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan secara efektif dan efisien. Namun pada kenyatannya, penerapan Teknologi Informasi (TI) pada perusahaan tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan perusahaan. Oleh karena itu untuk mengelola segala macam risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka PT. Advisia Diantara telah menerapkan manajemen risiko berdasarkan pada Standart ISO 31000 : 2009 sejak tahun 2003. Padatnya proses bisnis yang berjalan di PT. Advisia Diantara, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Risiko – risiko tersebut diantaranya berupa gangguan jaringan internet, gangguan arus listrik, kurang optimalnya dukungan teknis operasional ERP, gangguan komunikasi data antara user dengan server ERP dan lain sebagainya. Oleh arena itu perlu adanya evaluasi manajemen risiko Teknologi Informasi (TI) untuk mengetahui tingkat kapabilitas pengelolaan risiko yang telah dicapai, sehingga dapat meningkatkan kemampuan perusahaan dalam mengelola setiap risiko terkait penerapan sistem ERP-SAP pada PT. Advisia Diantara. Dari evaluasi tersebut menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko – risiko yang tidak diinginkan. Salah satu *framework* yang dapat digunakan untuk mengevaluasi anajemen risiko Teknologi Informasi (TI) pada PT. Advisia

Diantara ialah COBIT 5 khususnya pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisatin*). Digunakannya domain tersebut karena dalam COBIT 5, hanya ada dua domain yang membahas secara terperinci mengenai manajemen risiko Teknologi Informasi (TI).

2. PEMBAHASAN

2.1 Analisis *Capability Level*

Berdasarkan hasil pengisian lembar kerja evaluasi yang dilakukan oleh 3 responden dari Departemen TKP & MR dan Departemen TEKINFO PT. Advisia Diantara dapat diketahui bahwa nilai *capability level* yang telah dicapai subdomain EDM03 berada pada Level 2 dan nilai *capability level* yang telah dicapai subdomain APO12 berada pada tingkat Level 3. Hal tersebut dapat dilihat pada Tabel di bawah ini.

Tabel Rekapitulasi Hasil GAP Analysis

Nama Proses	Level Saat Ini	Level Target	*Gap*
EDM03	2	3	1
APO12	3	4	1

2.2 Analisis *Gap*

Berdasarkan hasil wawancara, diperoleh informasi bahwa level target yang ingin dicapai oleh Departemen TKP & MR dan Departemen TEKINFO PT. Advisia Diantara adalah naik satu level untuk setiap domain prosesnya, yaitu domain proses EDM03 berada pada Level 3 dan domain proses APO12 berada pada Level 4. Sehingga besarnya *gap* yang terbentuk antara level yang terjadi saat ini dan level target yang ingin dicapai pada domain proses EDM03 dan APO12 adalah sebesar 1.

2.3 *Risk Assessment*

Proses *Risk Assessment* dilakukan berdasarkan dua tahapan, antara lain:

1. *Risk Analysis*

   Risk Analysis bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, menentukan parameter *impact*, menentukan parameter *rating* risiko, melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*. Adapun pengelompokan risiko berdasarkan skenario risiko dapat dilihat dalam Tabel berikut ini.

Tabel Rekapitulasi Berdasarkan Skenario Risiko

No	Skenario Risiko	Jumlah *Risk Issue*
1	*New Technology*	1
2	*Software Implementation*	2
3	*Destruction of Infrastructure*	1
4	*IT Staff*	1
5	*IT Expertise and Skills*	2
6	*Software Integrity*	2
7	*Infrastructure (Hardware)*	3
8	*System Capacity*	2
9	*Malware*	1
10	*Logical Attacks*	1
11	*Utilities Performance*	1
12	*Data(base) Integrity*	2
13	*Logical Trespassing*	1
14	*Operational IT Errors*	2
15	*Acts of Nature*	1
	Total	23

Sedangkan untuk pengelompokan risiko berdasarkan aset dapat dilihat dalam Tabel berikut ini.

Tabel 4. Rekapitulasi Berdasarkan Aset

No	Kategori Aset	Jumlah *Risk Issue*	Persentase
1	Aplikasi	5	21,74 %
2	Fasilitas	1	4,35 %
3	Infrastruktur TI	3	13,04 %
4	Informasi / Data	7	30,43 %
5	Proses	4	17,39 %
6	SDM	3	13,04 %
Total	23	100 %	

Sebelum melakukan penilaian risiko terhadap *Inherent Risk* dan *Residual Risk*, terlebih dahulu menentukan standart penilaian berupa parameter *probability* (kecenderungan), parameter *impact* (dampak) dan parameter *Rating* Risiko. Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel berikut ini.

Tabel Penilaian *Inherent Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	0	0	4	0	1
2	Fasilitas	0	0	1	0	0
3	Infrastruktur TI	0	1	2	0	0
4	Informasi / Data	0	0	5	2	0
5	Proses	0	0	4	0	0
6	SDM	0	0	2	1	0
Total		0	1	18	3	1

Berdasarkan hasil wawancara dengan beberapa perwakilan dari Dept. TEKINFO dan Dept. TKP & MR, dapat diketahui bahwa setiap risiko – risiko yang teridentifikasi telah memiliki pengendalian tersendiri. Pengendalian tersebut digunakan sebagai dasar untuk melakukan penilaian Residual Risk. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel berikut ini.

Tabel Penilaian *Residual Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	4	0	1	0	0
2	Fasilitas	1	0	0	0	0
3	Infrastruktur TI	3	0	0	0	0
4	Informasi / Data	5	0	2	0	0
5	Proses	3	1	0	0	0
6	SDM	1	0	2	0	0
	Total	17	1	5	0	0

2. *Risk Evaluation*

Risk Evaluation bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk Evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan untuk mengatasinya. Adapun hasil pemetaan *Risk Map* dapat dilihat pada Tabel berikut ini.

Tabel Risk Map

Impact							
	Sangat Besar (5)	0	0	0	0	0	0
	Besar (4)	0	0	0	0	0	0
	Sedang (3)	1	0	0	0	0	1
	Kecil (2)	11	5	0	0	0	16
	Sangat Kecil (1)	3	3	0	0	0	6
	Total	15	8	0	0	0	23
		Sangat Jarang (1)	Jarang (2)	Kadang-kadang (3)	Sering (4)	Sangat Sering (5)	Total
		Probability					

Berdasarkan Tabel di atas, dapat diketahui bahwa terdapat 5 buah risiko yang termasuk dalam kategori Menengah (M) dan 1 buah risiko yang termasuk dalam kategori Menengah Rendah (LM). Kedua kategori tersebut termasuk dalam jenis risiko yang tidak dapat diterima oleh perusahaan, sehingga untuk mengurangi dampak terjadinya risiko perlu dilakukan tindakan mitigasi.

2.4 Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology,* 1 *Risk Issue* yang termasuk dalam *System Capacity,* 2 *Risk Issue* yang termasuk dalam *Data(base) Integrity* dan 2 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan untuk PT. Advisia Diantara dalam menyikapi beberapa *Risk Issue* dapat dilihat pada 4 buah Tabel berikut ini.

Tabel Langkah Mitigasi *New Technology*

Risiko	**Langkah Mitigasi**
1. Permintaan aplikasi diluar modul SAP tidak terpenuhi.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses perancangan dan pembuatan aplikasi. - Memberikan *training* dan pelatihan kepada seluruh Staff IT mengenai perkembangan teknologi informasi terkini. - Melakukan *Outsourcing* untuk memenuhi banyaknya permintaan aplikasi. - Melakukan analisis *cost-benefit* untuk menentukan investasi jangka panjang dan menentukan prioritas aplikasi yang harus dipenuhi terlebih dahulu

Tabel Langkah Mitigasi *System Capacity*

Risiko	**Langkah Mitigasi**
1. Operasional SAP lambat dan kurang optimal	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses monitoring dan evaluasi terhadap operasional SAP. - Mengadakan *User Licence* pada setiap unit kerja.

Tabel Langkah Mitigasi *Data(base) Integrity*

Risiko	**Langkah Mitigasi**
1. Gangguan komunikasi data antara PG dengan PIHC. 2. Gangguan transmisi data antar departemen.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam menjaga integritas dan keamanan data. - Menjalin kerja sama dengan Team IT dari PIHC. - Menyediakan *helpdesk* untuk menampung segala keluhan terkait dengan integritas data, sehingga dapat ditindak lanjuti dengan segera. - Menggunakan teknik *outomatic switch* jika terjadi *failure.*

Tabel Langkah Mitigasi *IT Expertise and Skills*

Risiko	**Langkah Mitigasi**
1. Dukungan teknis dari Team IT kurang optimal. 2. Adanya *gap* terkait kemampuan yang dimiliki Staff IT	- Meningkatkan kompetensi setiap Staff IT dengan menambah intensitas dalam mengadakan pelatihan atau training terkait dengan Sistem ERP - SAP. - Memperbaiki pola rekruitmen dan pelatihan SDM. - Mengasah kemampuan setiap Staff IT dengan memberikan penugasan atau pekerjaan yang berbeda – beda, agar Staff IT mampu menguasai segala bidang kompetensi yang berhubungan dengan IT. - Mengadakan monitoring dan evaluasi terhadap kinerja seluruh Staff IT. - Bekerja sama dengan Team IT dari PIHC untuk meningkatkan dukungan teknis operasional ERP – SAP. - Menyediakan *helpdesk* tersendiri untuk memudahkan Staff IT dalam menangani setiap keluhan.

3. KESIMPULAN

Berdasarkan hasil pembahasan terkait penerapan manajemen risiko teknologi informasi ada PT. Advisia Diantara maka dapat diperoleh kesimpulan sebagai berikut:

1. Proses evaluasi penerapan manajemen risiko teknologi informasi pada PT. Advisia Diantara menggunakan kerangka kerja COBIT 5 khususnya subdomain EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:
   a. Nilai *Capability Level* untuk subdomain EDM03 berada pada Level 2 yaitu *Managed Process*. Sedangkan Nilai *Capability Level* untuk subdomain APO12 berada pada Level 3 yaitu *Established Process*
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah diperoleh dengan nilai *capability level* yang ingin dicapai untuk subdomain EDM03 dan APO12 masing – masing adalah sebesar 1.
   c. Ditemukannya 23 *risk issue* yang terbagi dalam 15 skenario risiko. Dan dari kelima belas skenario risiko tersebut, terdapat 4 skenario risiko yang membutuhkan strategi dan Langkah mitigasi.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk perbaikan manajemen risiko teknologi informasi di PT. Advisia Diantara adalah sebagai berikut:
   a. Dibuatnya 9 buah rekomendasi agar nilai *Capability Level* pada subdomain EDM03 dapat mencapai Level 3 dan pada subdomain APO12 dapat mencapai Level 4.
   b. Dibuatnya 16 langkah mitigasi berdasarkan 6 buah *risk issue* yang termasuk dalam 4 buah skenario risiko, diantaranya *new technology, database integrity, system capacity* dan *IT expertise skills.* Langkah mitigasi tersebut dirancang untuk memenuhi permintaan aplikasi diluar modul SAP; untuk mengatasi gangguan transmisi data antara departemen dan departemen serta antara PG dengan pihak PIHC; untuk mengoptimalkan operasional SAP; untuk mengoptimalkan dukungan teknis dari team IT dan untuk mengurangi *gap* yang timbul akibat tidak meratanya kemampuan atau *skill* yang dimiliki oleh setiap staff IT.

4. DAFTAR PUSTAKA

Djojosoedarso, Soeisno, 2003. *Prinsip-Prinsip Manajemen Risiko dan Asuransi*, Edisi Pertama, Jakarta: Salemba Empat.

Dyahaloka, Astri, 2016. *Evaluasi Manajemen Risiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero)). Malang : Universitas Brawijaya*

Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu (DKPP). Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

ITGL., 2003. *Broad Briefing on IT Governance 2nd Edition.* Rolling Meadowa : IT Governace Institute.

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung.

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta)*. *SEMNASTEKNOMEDIA ONLINE*, 1(1), pp.23-1.

Husein, G.M. and Imbar, R.V., 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL)*. *Jurnal Teknik Informatika dan Sistem Informasi*, *1*(2).

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) engineering: a practitioner's approach*. United Kingdom : Palgrave Macmillan.

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri.* Jakarta : Universitas Indonesia.

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework*. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1 No.1

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus: PT OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

Wibisono, Diaz Mahardika, 2015. *Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 Manage Risk.* Surabaya : Universitas Airlangga.

Bhagaskara / 192420028

ASSESSMENT RESIKO TEKNOLOGI PADA

SISTEM INFORMASI STOK BARANG

Abstrak

Teknologi informasi telah menjadi bagian penting dari kehidupan manusia sehingga dapat mempermudah suatu kegiatan bisnis. Meskipun begitu, penggunaan teknologi informasi tidak lepas dari resiko yang dapat mempengaruhi proses kegiatan tersebut. Adapun tujuan penelitian ini adalah untuk melakukan penilaian resiko terhadap potensi kerentanan dan ancaman yang dapat menyerang sistem informasi stok barang sekaligus mempersiapkan tindakan antisipasi terhadap hal-hal yang dapat mengganggu sistem. Untuk melakukan penilaian tersebut, penelitian ini menggunakan framework NIST SP 800-30r-1 yang terdiri sembilan tahapan untuk dalam penilaian resiko yaitu karakteristik sistem yang digunakan, indentifikasi ancaman yang menyerang sistem, identifikasi *vulnerability*, pengendalian sistem, menentukan kemungkinan terjadi (*likelihood*), menentukan dampak (*impact*), penentuan resiko, rekomendasi pengendalian dan dokumentasi hasil. Hasil dari penilaian resiko terhadap sistem informasi stok barang adalah terdapat tiga resiko yang mengganggu aktifitas yang ada dalam sistem. Kemudian dari hasil penilaian resiko berupa rekomendasi yang digunakan untuk memperkecil resiko yang terjadi pada sistem.

1. PENDAHULUAN

Peran penting teknologi informasi dan komunikasi (TIK) adalah membantu meringankan pekerjaan kantor sehingga lebih cepat dan lebih akurat. Hal ini dapat dilihat dari semakin tergantungnya proses bisnis suatu organisasi di berbagai bidang kegiatan dengan teknologi ini. Bidang pendidikanpun tidak lepas dari penggunaan TIK terutama dalam pelayanan akademik. Secara eksternal, banyak aktifitas pelaporan kegiatan akademik mengharuskan lembaga pendidikan menggunakan TIK. Dukungan teknologi juga dipergunakan untuk mempercepat proses layanan akademik dalan suatu perguruan tinggi. Akibatnya semakin pentingnya peran TIK dalam mendukung kegiatan menimbulkan permasalah tersendiri bila fungsi TIK tersebut terganggu (Suzanto dan Sidharta 2015).

Pemanfaatan sistem informasi stok barang dapat berjalan dengan baik jika dalam penggunaan dan pemanfaatan sistem dapat digunakan secara baik. Menurut Rahardjo (2002) berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu resiko keamanan yang bersifat fisik *(physical security)*, resiko keamanan yang berhubungan dengan orang (*personel*), resiko keamanan dari data dan media serta teknik komunikasi dan resiko keamanan dalam operasi.

Sistem informasi stok barang adalah sebuah antarmuka yang menyediakan informasi-informasi seperti pemasukan barang, jumlah stok di gudang, pengeluaran barang, dan wadah yang digunakan oleh pengguna atau admin untuk memantau sistem. Dalam pengelolaannya, sistem informasi stok barang dikelola oleh tiga orang yaitu Kepala Gudang, *Programmer* dan staf jaringan yang mempunyai peranan masing-masing didalam sistem.

Terkadang dalam penerapan sistem informasi stok barang belum optimal seperti aktifitas dalam penggunaan sistem terhambat karena mendapatkan penyerangan dari penyusup berupa serangan *Ddos*, serangan *phising*, serangan terhadap *port-port* yang digunakan sistem, melakukan *scanning* sistem untuk memperoleh data penting yang ada pada sistem informasi stok barang sehingga membuat server menjadi *down*. Seiring berkembangnya teknologi sering kali dimanfaatkan oleh beberapa pihak yang tidak bertanggung jawab yang dapat menyebabkan munculnya ancaman dan resiko dari penggunaan teknologi. Permasalahan keamanan sistem informasi mendapatkan perhatian dari para *stakeholder* dan pengelola sistem informasi ketika sudah terjadi sebuah ancaman yang menimbulkan kerugian pada lembaga. Untuk memperkecil resiko, maka diperlukan penilaian terhadap resiko yang timbul karena kerentanan yang ada dalam sistem. Penilaian resiko terhadap sistem merupakan elemen penting dalam menyediakan pelayanan kepada pengguna sistem. Pelayanan informasi stok yang tepat dan cepat tergantung pada peranan sistem informasi yang didukung oleh teknologi informasi serta SDM (Sumber Daya Manusia) yang mencukupi dan terlatih dalam penggunaan sebuah teknologi informasi.

2. METODOLOGI PENELITAN

2.1 Risk Management Framework

Risk management atau manajemen resiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman, suatu rangkaian aktivitas manusia termasuk penilaian resiko, pengembangan strategi untuk mengelolanya dan mitigasi resiko dengan menggunakan pembersayaan/pengelolaan sumberdaya (Hanafi 2014).Tujuan dari manajemen risiko adalah untuk mengenali risiko dalam sebuah proyek dan mengembangkan strategi untuk mengurangi atau bahkan menghindarinya, dilain sisi juga harus dicari cara untuk memaksimalkan peluang yang ada (Wideman 1992).*Framework* adalah kumpulan perintah atau fungsi dasar yang membentuk aturan-aturan tertentu dan saling berinteraksi satu sama lain sehingga dalam pembuatan aplikasi (Wardana and Si 2010).*Framework* yang digunakan oleh penulis adalah *framework* NIST SP 800-30r1 yang tepat digunakan dalam penelitian ini. NIST 800-30r1 adalah dokumen standar yang dikembangkan oleh *National Institute of Standards and Technology* yang mana merupakan kelanjutan dari tanggung jawab hukum dibawah undang-undang *Computer Security Act* tahun 1987 dan *the Information Technology Management Reform Act* tahun 1996 (NIST 2002). Terdapat tiga proses dalam manajemen resiko: *risk assessment, risk mitigation, and evaluation and assessment. Framework* NIST SP 800-30r1 mempunyai struktur dan tahapan proses yang terarah. Metode ini memberikan panduan untuk melakukan proses penilaian resiko langkah demi langkah. Tahapannya terdiri dari *Risk Assessment, Risk Mitigation* dan *Evaluation and Assessment.*

2.2 Teknik Penilaian Resiko

Teknik penilaian resiko menggunakan *framework NIST* SP 800-30r-1. *Framework* NIST SP 800-30r-1 merupakan panduan untuk memproses data yang sangat sensitif. NIST SP 800- 30r-1 memiliki kontribusi lebih dalam melakukan penilaian resiko karena memberikan wawasan keamanan informasi yang sifatnya konsisten dan komprehensif bagi pengambilan kebijakan, pemodelan

sumber daya yang terstruktur, wawasan keamanan dapat diterima oleh berbagai pengambil resiko, penentuan ancaman dapat diidentifikasi dengan mudah, pengambilan keputusan yang baik untuk setiap resiko yang diselidiki (Andani 2014). Dalam NIST SP 800- 30r-1 ini terdapat sembilan langkah untuk melakukan analisa resiko yaitu karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, analisa kontrol, analisa kemungkinan terjadi, analisa dampak, penentuan level resiko dan rekomendasi pengendalian.

2.3 Teknik Pengumpulan Data

Pengumpulan data sangat penting dalam penelitian, karena data tersebut dimaksudkan untuk berkontribusi pada pemahaman kerangka teoretis yang lebih baik (Herdiansyah 2013). Pemilihan informan dengan metode *purposive sampling* bertujuan untuk penelitian yang dilakukan peneliti akan mendapatkan capaian yang baik dan sesuai dengan keinginan informan. Pemilihan informan yang dilakukan peneliti dalam menganalisis *assessment* resiko pada sistem informasi stok barang yaitu memilih sumber data yang benar-benar bertanggung jawab atas sistem tersebut yaitu Kepala Gudang, *Programmer* dan Staf jaringan yang bertanggung jawab dan terlibat langsung dalam sistem informasi stok barang.

2.4 Metode Penentuan Informan

Pengumpulan data sangat penting dalam penelitian, karena data tersebut dimaksudkan untuk berkontribusi pada pemahaman kerangka teoretis yang lebih baik (Herdiansyah 2013). Menentukan sampel dalam penelitian, terdapat teknik sampling yang digunakan salah satunya adalah teknik purposive sampling. *Purposive sampling* adalah teknik pengambilan sumber dengan pertimbangan tertentu. Misalnya akan melakukan penelitian tentang kualitas suatu makanan, maka sampel yang merupakan sumber data dari penelitian tersebut adalah orang yang ahli dalam makanan. Sampel ini digunakan untuk penelitian kualitatif atau penelitian-penelitian yang tidak melakukan generalisasi (Aryani and Rosinta 2011). Pemilihan informan dengan metode *purposive sampling* bertujuan untuk penelitian yang dilakukan peneliti akan mendapatkan capaian yang baik dan sesuai dengan keinginan informan. Pemilihan informan yang dilakukan peneliti dalam menganalisis *assessment* resiko pada sistem informasi stok barang yaitu memilih sumber data yang benar-benar bertanggung jawab atas sistem tersebut yaitu Kepala Gudang, *Programmer* dan Staf jaringan yang bertanggung jawab terhadap sistem.

3. HASIL DAN PEMBAHASAN

Untuk melakukan penilaian resiko terhadap sistem informasi stok barang ada sembilan tahapan yaitu:

1. Karakteristik Sistem
   Karakteristik yang digunakan dalam sistem informasi stok barang adalah perangkat keras yang digunakan PC dengan server luar dan sever lokal yang dalah satunya servernya menggunakan *cloud*. *Software* yang digunakan berupa linux *free* BSD. Untuk menjamin sistem yang digunakan aman dalam melakukan transaksi makan digunakan SSL *(Secure Socket Layer)*.

2. Identifikasi Ancaman
   Ancaman-ancaman yang mengancam sistem informasi stok barang adalah mengubah *plug in* dan tema yang ada pada sistem informasi stok barang. Melakukan ancaman seperti *sniffing, scanning network, phising, flooding, wireless jamming, Ddos* pada sistem informasi yang bertujuan merusak sistem.

3. Identifikasi Kerentanan (*Vulnerability*)
   Identifikasi kerentanan (*Vulnerability*) yang didapat dari hasil wawancara terlihat pada Tabel 1

Tabel 1. Identifikasi Kerentanan (*Vulnerability*)

Jenis Resiko	Kerentanan
Berasal dari dalam lingkungan	- *Password cracking* untuk melakukan pencurian data pada sistem - Keterlambatan dalam melakukan *update antivirus* sehingga memungkinkan *malware* masuk kedalam sistem - Kelalaian staf dalam memindahkan sistem menggunakan *flash drive* yang berisi *malware*
Berasal dari luar lingkungan Bencana alam	- *Scanning tools* - Kebakaran - Gempa Bumi

4. Analisis Pengendalian
   Hasil dari wawancara terstruktur analisis pengendalian telah tertuang dalam dokumen yang mencakup semua standar-standar dan prosedur-prosedur dalam pengoperasian sistem informasi stok barang yaitu dokumen SOP (*Standard Operating Procedure).*

5. Kemungkinan Terjadi (*Likelihood*)
   Hasil dari kemungkinan terjadi (*Likelihood*) pada sistem informasi stok barang berdasarkan tingkat kemungkinan terjadinya resiko ada tiga yaitu tinggi, sedang dan rendah. Kategori kemungkinan terjadi resiko pada sistem termasuk tinggi apabila sumber ancaman sangat mampu dan pengendalianuntuk mencegah kerentanan yang dilkaukan sudah tidak efektif lagi. Kategori kemungkinan terjadi resiko pada sistem termasuk sedang apabila sumber ancaman mampu dalam menembus pertahanan sistem namun belum sampai pada layer terdalam pada jaringan sehingga dapat menghambat kerentanan. Kategori kemungkinan terjadi resiko pada sistem termasuk rendah apabila sumber ancaman tidak memiliki kemampuan untuk menembus keamanan, setidaknya dapat menghambat namun dapat diatasi. Kemungkinan terjadi resiko pada sistem informasi stok barang adalah (1) penyerangan yang dilakukan oleh orang dalam

(bisa ditimbulkan dari staf), (2) terjadi kerusakan atau *disk error* pada penyimpanan data, (3) *plug in* yang terlambat diperbarui.

6. Analisis Dampak (*Impact*)
   Berdasarkan analisis hasil resiko yang menggambarkan dampak resiko (*impact*) terhadap sistem informasi stok barang terlihat pada Tabel 2.

Tabel 2. Dampak Resiko

Jenis Resiko	Dampak	Tingkat Dampak
Penyerangan yang dilakukan oleh orang dalam	- Tidak dapak masuk kedalam sistem - Pencurian data pengguna	Tinggi
Disk Error	- Tidak dapat melakukan proses penyimpanan data pada hardisk	Sedang
Plug in yang terlambat diperbarui	- Kerusakan kecil pada ditampilan interface sistem	Rendah

7. *Risk Determination*
   Risk determination memperlihatkan jenis resiko yang menyerang sistem informasi stok barang dari yang tinggi sampai ke resiko yang rendah yang akan terlihat pada Tabel 3. Pada Tabel 3 terlihat jenis resiko yang memiliki tingkat atau level resiko tinggi pada jenis resiko penyerangan yang dilakukan oleh orang dalam. Level resiko sedang pada jenis resiko *disk error* atau kerusakan pada penyimpanan data dan terakhir adalah *plug in* yang terlambat diperbarui yang memiliki level resiko rendah.

Tabel 3. *Risk Determination*

Jenis Resiko	Nilai Kemungkinan Terjadi	Tingkat Dampak	Nilai Dampak	Level Resiko
Penyerangan yang dilakukan oleh orang dalam	1,0	100	100	Tinggi
Disk Error	0,5	100	50	Sedang
Plug in yang terlambat diperbarui	0,1	100	10	Rendah

8. Rekomendasi Pengendalian
   Dari tingkat resiko tersebut dapatlah rekomendasi pengendalian yang digunakan untuk membuat prosedur untuk penanganan terhadap ancaman yang terjadi. Dari hasil penilaian maka direkomendasikan beberapa kontrol yang dapat dilakukan terhadap resiko yang terlihat pada Tabel 4.

Tabel 4. Rekomendasi Pengendalian

Jenis Ancaman	Tingkat Ancaman	Rekomendasi Pengendalian
Penyerangan yang dilakukan oleh orang dalam	Tinggi	Memperkokoh *firewall* yang digunakan oleh sisem informasi stok barang, tidak menampilkan jenis *web* editor apa yang digunakan untuk membangun sistem informasi stok barang
Disk Error	Sedang	*Backup Data*
Plug in yang terlambat diperbarui	Rendah	Memberikan pelatihan terhadap penggunaan sistem informasi stok barang

9. Dokumen Hasil
   Dari hasil penilaian resiko teknologi pada implementasi sistem informasi stok barang maka dibuatlah dokumen penanganan terhadap resiko yang mengancam sistem informasi stok barang. Dokumen ini berisi tentang tata cara penanganan resiko- resiko yang menyerang sistem informasi stok barang.

4. KESIMPULAN

Dalam proses penilaian resiko, penulis menggunakan tahapan resiko yang telah disediakan oleh *framework* NIST SP 800-30r-1 yang terdiri dari karakteristik sistem, mengidentifikasi ancaman, kontrol analisis, kemungkinan terjadi (*likelihood*), dampak (*impact*), level resiko *(risk determination*), rekomendasi resiko dan terakhir rekomendasi hasil. Diantara jenis ancaman ini terdapat 3 tingkat resiko setelah dilakukan penilaian. Resiko yang muncul adalah resiko yang dilakukan oleh orang dalam serta kegagalan infrastruktur. Resiko dinilai mempunyai resiko tinggi karena penyerangan yang dilakukan terhadap sistem berasal dari orang dalam. Resiko ini dinilai mempunyai resiko sedang karena tempat penyimpanan data rusak yang membuat aktifitas dalam sistem menjadi terganggu. Serta resiko ini dinilai mempunyai resiko rendah karena *plug in* yang terlambat diperbarui sehingga penyusup dapat mengubah beberapa menu pada tampilan *interface*.

Referensi

Andani, M. (2014). Manajemen Risiko Keamanan Aplikasi Sistem Informasi Laporan Harian Pks & Ppko Online Pada Ptpn V Menggunakan Metode Nist Sp 800-30, *Universitas Islam Negeri Sultan Syarif Kasim Riau.*

Aryani, D. and F. Rosinta (2011). Pengaruh kualitas layanan terhadap kepuasan pelanggan dalam membentuk loyalitas pelanggan. *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi.*

Cahyaningdyah, D. And Y.D. Ressany (2012), Pengaruh Kebijakan Manajemen Keuangan Terhadap Nilai Peusahaan, *Jurnal Dinamika Manajemen*.

Herdiansyah, H. (2013). *Wawancara, observasi, dan focus groups: Sebagai instrumen penggalian data kualitatif*. Jakarta: PT. Raja Grafindo Persada.

Mellisa, M. And F. A. Andono (2013). *Penerapan Enterprise Risk Management dalam Rangka Meningkatkan Efektifitas Kegiatan Operasional CV. Anugerah Berkat Calindo Jaya.*

NIST (2002). Sp 800-30. risk management guide for information technology systems.

Recomendation of National Institute of Standards and Technology Special Publication 800- 30r-1.Rahardjo, B. (2002). Keamanan Sistem Informasi Berbasis Internet. *PT Insan Infonesia–Bandung & PT INDOCISC–Jakarta.*

Suzanto, B. and I. Sidharta (2015). Pengukuran End-User Computing Satisfaction Atas Penggunaan Sistem Informasi Akademik. *Jurnal Ekonomi, Bisnis & Entrepreneurship*.

Wardana, S. H. and M. Si (2010). *Menjadi Master PHP dengan Framework Codeigniter, Elex Media Komputindo,* www.scholar.google.co.id, diakses: 18 Maret 2018.

Wideman, R. M. (1992). Project and program risk management: a guide to managing project risks and opportunities, *University of Maribor, Faculty of Business and Economics*.

Nama : Hendra Yada Putra
Nim : 192420034
Kelas : MTI Angkatan 21 Reguler B
Mata kuliah : ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEM
(M. IZMAN HERDIANSYAH, PhD)
Tugas : **PEPER 1 MINGGU KE 3**

RISK ASSESSMENT TERHADAP PERISAPAN AUDIT DENGAN MENGACU PADA ITAF

1. ABSTRAK

Dengan melihat audit sebagai evaluasi dari suatu kesesuaian proses operasi dari organisasi terhadap aturan dan kebijakan, tentunya untuk mencapai tujuan ini haruslah pelaksanaannya harus dipersiapakan sebaik mungkin.

Didalam framework ITAF, telah disusun sedemikian rupa terhadap rangakaian persiapan Audit, dan untuk menentukan proritas audit dari area lingkup audit yang telah direncanakan maka haruslah dilakukan kegiatan risk asssemen, dengan ketentuan dan korelasi apa saja dan keterkaitannya terhadap object pada COBIT 5

Penulis disini bermaksud meneliti terkait fungsi dari risk assessment yang telah disediakan dalam framework tersebut.

2. PENDAHULUAN

ITAF adalah model referensi pengaturan praktik yang komprehensif dan baik terhadap implemntasi Audit IS/IT, dimana didalamnya:

- Menetapkan standar yang membahas peran dan tanggung jawab profesional audit dan jaminan SI; pengetahuan dan kemampuan; dan persyaratan ketekunan, perilaku dan pelaporan
- Mendefinisikan istilah dan konsep khusus untuk jaminan SI
- Memberikan panduan dan alat serta teknik pada perencanaan, desain, pelaksanaan dan pelaporan tugas audit dan asurans SI.

Didalam referesni guidlinenya terdapat framework yang membimbing terkait kegiatan risk assessment, dimana dalam kegiatan audit sendiri umumnya merupakan kegiatan terpisah.

Berdasarkan hal tersebut penulis hendak meneliti lebih dalam menganai sejauh mana peran risk assessmen ini terhadap implementasi AUDIT SI/TI yang mengacu pada framework ITAF.

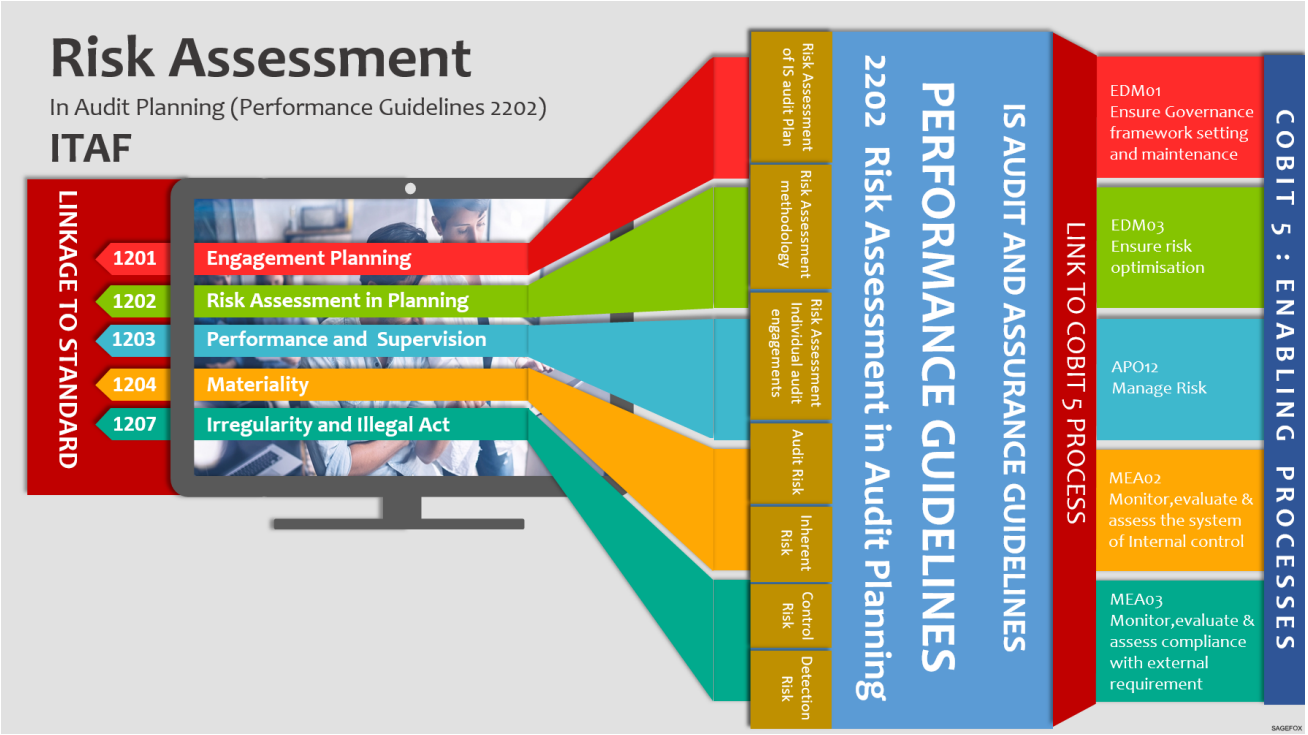
3. PEMBAHASAN

Didalam ITAF Risk Assemessment guideline terdapat pada poin 2202, yang mengacu pada standard:

1201 Engengement Planning

1202 Risk Assessement in Planning
1203 Performace and Supervision
1204 Materliality
1207 Irregularity and Legal ACT

Selain itu Framework ini juga terhubung dengan COBIT 5 Process, yaitu pada
EDM01 Ensure governance framework setting & Maintenance
EDM03 Ensure Risk Optimisation
AP012 Manage Risk
MEA02 Monitor, Evaluate, and Assess the system of internal Control
MEA03 Monitor,evaluate and assess compliance with external requirements



Gambar korelasi Risk Assessment pada ITAF terhadap COBIT 5

Didalam ITAF tersebut diatur mengenai 7 panduan yang meliputi:

1. Risk Assesment terhadap rencana Audit
2. Risk Assesment Metodelogi
3. Risk Assesment terhadap pendekatan individu
4. Audit Risk
5. Risiko yang melekat
6. Kontrol Risiko
7. Pendeteksian Risiko

Detil sebagai berikut:

1. Risk Assesment terhadap rencana Audit
    a. Pendekatan risk assessment dilakukan secara tahunan untuk peningkatan pengembangan audit IT itu sendiri.
    b. Lingkup audit ditentukan terkait dengan elemen pengembangan rencana audit, dan mewakili jangkauan dari semua aktivitas audit, proses yang melibatkan managemen, baik supervise, pemeriksaan hingga Pelaporan terkait isu dan risiko yang timbul
    c. Pelaksanaan risk assessment dengan melihat area mana yang menjadi perhatian lebih
    d. Persetujuan pendekatan risk assessment akan mejadi output yang akan diterima oleh stakeholder (keperayaan)
    e. Pengembangan audit IT Berdasarkan penilaian risiko melibatkan professional yang harus mengembangkan rencana audit SI yang berfungsi sebagai kerangka kerja audit IS dan aktivitas dimana diharuskan:
        - Adanya pertimbangkan persyaratan dan aktivitas audit IT
        - Diperbarui setidaknya setiap tahun,
        - Disetujui oleh pihak yang bertanggung jawab atas tata kelola
        - Mengatasi tanggung jawab yang ditetapkan oleh piagam audit

2. Risk Assesment Metodelogi
    a. Berbicara Metodology yang tepat, maka tidak ada metodologi penilaian risiko tunggal yang dapat diharapkan sesuai di semua situasi. Kondisi mempengaruhi audit dapat berubah seiring waktu. Secara berkala, para profesional harus mengevaluasi kembali kesesuaian
    b. Banyak metodologi penilaian risiko tersedia untuk mendukung proses penilaian risiko. Ini berkisar dari klasifikasi sederhana tinggi, sedang dan rendah, berdasarkan penilaian profesional, hingga lainnya
    c. Perhitungan kuantitatif dan ilmiah memberikan peringkat risiko numerik, dan lain-lain yang merupakan kombinasi di antara dua. Profesional harus mempertimbangkan tingkat kompleksitas dan detail yang sesuai untuk perusahaan atau subjek yang diaudit.
    d. Panduan khusus untuk melakukan penilaian risiko dapat ditemukan di ISACA publikasi COBIT 5 untuk Risiko.
    e. Semua metodologi penilaian risiko bergantung pada penilaian subjektif di beberapa titik dalam proses (misalnya, untuk menetapkan bobot ke berbagai parameter)
    f. Dalam memutuskan metodologi penilaian risiko yang paling tepat, para profesional audit harus mempertimbangkan hal-hal sebagai:

- Jenis informasi yang perlu dikumpulkan (beberapa sistem menggunakan pengaruh finansial sebagai satu-satunya ukuran ini tidak selalu sesuai untuk perikatan audit IT)
- Biaya perangkat lunak atau lisensi lain yang diperlukan untuk menggunakan metodologi
- Sejauh mana informasi yang dibutuhkan sudah tersedia
- Jumlah informasi tambahan yang perlu dikumpulkan sebelum keluaran yang andal dapat diperoleh, dan
- biaya pengumpulan informasi ini (termasuk waktu yang diperlukan untuk diinvestasikan dalam kegiatan pengumpulan)
- Pendapat dari pengguna lain tentang metodologi, dan pandangan mereka tentang seberapa baik metodologi tersebut membantu mereka dalam peningkatan efisiensi dan / atau efektivitas audit mereka
- Kesediaan pihak yang bertanggung jawab atas tata kelola area audit TI untuk menerima metodologi sebagai sarana untuk menentukan jenis dan tingkat pekerjaan audit yang dilakukan

3. Risk Assesment terhadap pendekatan individu
   Selama penilaian risiko, para profesional harus mempertimbangkan:
   a. Hasil laporan, tinjauan dan temuan audit sebelumnya, termasuk setiap aktivitas perbaikan
   b. Proses penilaian risiko perusahaan secara menyeluruh
   c. Kemungkinan terjadinya risiko tertentu
   d. Dampak risiko tertentu (dalam ukuran moneter atau nilai lainnya) jika terjadi
   e. Pemahaman lingkup
      Mereka harus meminta komentar dan saran dari pemangku kepentingan dan pihak lain yang sesuai. Hal ini diperlukan untuk menentukan dan memeriksa dengan tepat dampak dari kemungkinan risiko dalam perikatan audit.

4. Audit Risk
   a. Risiko terbentuknya kesimpulan yang salah terhadap temuan audit
   b. Tingkatan level Risiko
      Auditor harus mempertimbangkan setiap risiko dari komponen audit, karena dapat menentukan tingkat resiko secara keseluruhan
   c. Komponen Risiko Audit
      Terdiri dari:
      1. Control Risk
      2. Dectection Risk
      3. Inherent Risk

5. Risiko yang melekat
   Risiko inheren yang terkait dengan sistem operasi tanpa kontrol yang tepat biasanya tinggi, (karena dampak intergrasi, pengungkapan, data atau program) melalui kelemahan keamanan sistem operasi dapat mengakibatkan informasi manajemen yang salah atau kerugian kompetitif. Sebaliknya, risiko melekat yang terkait dengan keamanan untuk PC yang berdiri sendiri tanpa kontrol, jika analisis yang tepat menunjukkan bahwa ia tidak digunakan untuk tujuan bisnis yang penting, biasanya rendah.

6. Kontrol Risiko
   Melihat Risiko tidak dapat terdeteksi dan dicegah maupun diperbaiki pada saat tersebut oleh system pengendalian internal
   Auditor harus dapat menilai control risk dengan nilai tinggi kecuali, pengendalian internlnya:
   1. Selalu ada identifikasi
   2. Dievaluasi secare effektif
   3. Dilakukan Test dan pembuktian guna memastikan beroperasi dengan tepat

7. Pendeteksian Risiko
   Risiko deteksi yang terkait dengan identifikasi pelanggaran keamanan dalam sistem aplikasi biasanya tinggi karena log untuk keseluruhan periode audit tidak tersedia pada saat audit. Risiko deteksi yang terkait dengan mengidentifikasi kurangnya rencana pemulihan bencana biasanya rendah, karena keberadaannya dapat diverifikasi dengan mudah

4. KESIMPULAN

Dari hasil pembahasan diatas ditemukan bahwa, saat akan melakukan audit dengan dilakukannya terlebih dahulu risk assessment terhadap lingkup area yang akan diaudit akan membua audit menjadi tepat sasaran dimana risk assesmen ini dapat memberikan gambaran mengenai area-area yang menjadi proritas utama dalam proses audit, sehingga akan lebih effektif dan effisien dalam mencapai tujuan audit

Risk assessmen yang dilakukan dalam persiapan audi ini lebih kepada penilahan risiko terhadap object audit tidak pada mitigasinya sehingga proses risk assessmennya pun lebih cepat.

5. DAFTAR PUSTAKA

ISACA., 2014. *ITAF™: A Professional Practices Framework for IS Audit/ Assurance, 3rd Edition.* : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.