4 of 4

revisi paper

Inbox ×

Jurnal Edukasi dan Penelitian Informatika <jepin@untan.ac.id>
to me

Mon, Dec 14, 8:27 PM

Indonesian > English Translate message

Turn off for: Indonesian

Ysh Author
Dimohon untuk memperbaiki paper anda..silahkan liat hasil reviewer
Terima kasih

Salam,
Dewan Redaksi JEPIN

==========

e-ISSN: 2548-9364

printed ISSN: 2460-0741

http://jurnal.untan.ac.id/index.php/jepin/index

Wahyu Adi Prabowo <wahyuadi@ittelkom-pwt.ac.id>
to Jurnal

Wed, Dec 16, 12:05 PM

Ysh editor JEPIN

Terimakasih sebelumnya pak, untuk revisi sdh saya upload di sistem jepin

Regards

Wahyu Adi Prabowo

Faculty of Informatics and Industry
Telkom Institute of Technology Purwokerto

JEPIN - KELENGKAPAN ADMINISTRASI & BIAYA PENERBITAN

Inbox ×

Jurnal Edukasi dan Penelitian Informatika
to me

Fri, Dec 18, 10:45 AM (12 days ago)

Indonesian > English Translate message

Turn off for: Indonesian ×

Yth. Bapak/Ibu **Wahyu Adi Prabowo**

Bersama ini kami sampaikan bahwa paper dengan judul : "**Pemetaan Resiko Teknologi Informasi Dengan Integrasi IT Balanced Scorecard dan NIST SP 800-34 Rev.1**" telah **DITERIMA**.

Untuk dapat diterbitkan pada buku jurnal JEPIN edisi **Vol. 6 No. 3 Desember 2020**, mohon author dapat melengkapi hal-hal berikut selambat-lambatnya tanggal **Jumat, 18 Desember 2020**.

1. Mengisi formulir yang dapat diunduh di link berikut dan mengirimkannya kembali kepada kami melalui email ini.
https://drive.google.com/file/d/0BxTpSnf_8osMQlVoUTFhUy05TWs/view?usp=sharing

2. Mengirimkan biaya administrasi termasuk ongkos kirim 1 eks jurnal sebesar **Rp 1.000.000**,- ke No. Rekening : **BNI - 0696563721 a.n. Enda Esyudha**

3. Untuk **tambahan buku** jurnal dikenakan biaya sebesar **Rp 100.000,- / eksemplar**.

Formulir dan tanda bukti transfer dapat dikirim lewat email jepin@untan.ac.id.
Atas perhatiannya kami ucapkan terima kasih

Salam,
Dewan Redaksi JEPIN

==========

e-ISSN: 2548-9364

printed ISSN: 2460-0741

http://jurnal.untan.ac.id/index.php/jepin/index

JEPIN - FORMULIR...

JEPIN

(Jurnal Edukasi dan Penelitian Informatika)

ISSN(e): 2548-9364 / ISSN(p) : 2460-0741

Vol. x
No. y
mm yy

Pemetaan Resiko Teknologi Informasi Dengan Integrasi IT Balanced Scorecard dan NIST SP 800-34 Rev.1

Wahyu Adi Prabowo[#1], Marheni Eka Saputri[#2]

[#1]*Fakultas Informatika, Institut Teknologi Telkom Purwokerto*
Jl. DI Panjaitan 128, Purwokerto

[#2]*Fakultas Komunikasi dan Bisnis, Telkom University*

Jl. Telekomunikasi, Ters. Buah batu, Dayeuh Kolot, Bandung

[1]wahyuadi@ittelkom-pwt.ac.id
[2]marhenieka@telkomuniversity.ac.id

Abstrak **- Resiko Teknologi Informasi (TI) di lingkungan pendidikan tinggi merupakan suatu kejadian yang potensial untuk mengganggu berjalannya proses bisnis. Masih banyak resiko-resiko TI yang belum terpetakan sehingga masih ada ketidakseimbangan dalam proses identifikasi resiko yang menyebabkan tidak tercapainya tujuan visi misi pada Unit TI pendidikan tinggi. Untuk mengatasi ketidakseimbangan tersebut maka diperlukan untuk mengidentifikasi resiko TI untuk meningkatkan layanan TI agar tidak terhentinya proses bisnis pendidikan tinggi. Tujuan dari penelitian ini adalah untuk melakukan pemetaan yang terintegrasi antara tujuan dan risk, yaitu dengan menggunakan IT Balanced Scorecard dan NIST SP 800-34 Rev.1. Metode dari penelitian ini adalah dengan mengumpulkan beberapa data informasi terkait IT Balanced Scorecard dan NIST SP 800-34 Rev.1 lalu dianalisa untuk membuat sebuah perencanaan resiko Teknologi Informasi. Hasil dari penelitian ini dapat memberikan gambaran bahwa resiko dapat dipetakan ke dalam sasaran strategis yang ada dalam IT Balanced Scorecard, sehingga dapat menyeimbangkan antara kinerja dan resikonya agar dapat tercapainya visi misi Unit TI pendidikan tinggi.**

***Kata kunci*— IT Balanced Scorecard, NIST SP 800-34 Rev 1, Risk register**

I. PENDAHULUAN

Disaster Recovery Planning (DRP) terhubung dengan pemulihan sistem IT dan komponen infratrukturnya [1], [2]. Business Continuity Planning merupakan salah satu proses yang penting dalam menjalankan roda proses bisnis di suatu organisasi [2], [3]. DRP dan BCP merupakan suatu analisa risko yang saling terhubung antara satu dengan yang lain .[2], yang bahkan selama beberapa dekade ini manajemen resiko menjadi salah satu fungsi penting yang selalu terorganisir dengan baik dalam suatu institusi [4]. Pengorganisasian resiko ini diperlukan untuk mengantisipasi segala kemungkinan yang akan terjadi, agar secepatnya dapat ditindaklanjuti untuk mengurangi efek dampaknya, melalui perencanaan strategi yang baik [5]. Sebuah perencanaan pemulihan TI dari sebuah bencana meruapakan bukan tugas yang mudah [6]. Semua resiko harus diidentifikasi dengan baik dan tentu saja organisasi harus bisa untuk memahami resiko dan dapat memahami kebergantungan antar resiko-resiko tersebut [7].

Institusi pendidikan merupakan suatu oganisasi yang melakukan kegiatan pengajaran, penelitian, dan melakukan kegiatan komersial dalam berbagai spektrum multidisiplin ilmu [8]. Kegiatan-kegiatan yang ada di institusi pendidikan tentu saja beresiko terhadap proses bisnis yang sedang berjalan. Penerapan manajemen resiko sangat diperlukan dalam menghadapi dan mengurangi dampak risiko di institusi pendidikan [9]. Tantangan-tantangan yang dihadapi dalam menghadapi resiko ini tidak terlepas dari penggunaan teknologi informasi. Salah satu yang menjadi pusat perhatian adalah masalah keamanan dan kerentanan dari perluasan infrastruktur TI [10]. Selain itu gangguan manusia menjadi faktor penting dalam resiko TI [11]. Ancaman manusia ini dibagi menjadi 2 ancaman, yaitu pasif dan aktif. Ancaman aktif yaitu ancaman terhadap kecurangan dan kejahatan computer, ancaman pasif yaitu kegagalan sistem, kesalahan manusia dan bencana alam. [12].

Penelitian terdahulu yang melakukan sebuah penelitian terkait dengan resiko sudah dilakukan oleh beberapa peneliti

antara lain penelitian yang diteliti oleh kurniawati [13] yaitu dengan mengintegrasikan balanced scorecard dengan COSO ERM. Dengan mengintegrasikan balanced scorecard dengan COSO ERM, manajemen puncak dapat menterjemahkan visi misi ke dalam suatu strategi perusahaan dan dapat memperhatikan segala resiko-resiko agar tercapainya tujuan dan strategi perusahaan. Integrasi Balanced Scorecard dan COSO ERM juga dapat dianalogikan sebagai alat peneropong resiko, yaitu memetakan suatu resiko pada tahap awal penetapan strategi dan tindakan inisiatif agar tercapainya tujuan bisnis perusahaan.

Penelitian lain yang dilakukan oleh Sheikhpour [14], yaitu mengintegrasikan ITIL dan ISO 27001. Penelitian ini menjelaskan bahwa dengan menggabungkan framework layanan TI dan Keamanan informasi maka aktivitas terhadap perlindungan asset infrastruktur informasi, penyalahgunaan dan kerusakan dapat ditangani dengan baik. Dengan mengintegrasikan framework tersebut maka organisasi dapat memastikan tingkat resiko keamanan TI yang memadai dan dapat mengelola resiko infrastruktur TI secara efektif.

Penelitian lain dilakukan oleh Kumsuprom et all [15] dalam penelitian yang dilakukan dapat diambil kesimpulan bahwa dengan menganalisa resiko berdasarkan 2 pendekatan yaitu kerangka COBIT dan ISO/IEC 17799 dapat menunjukkan konstruksi yang baik dalam mengelola dan mengendalikan resiko. Kerangka kerja dari COBIT dapat bekerja secara top-down dalam manajemen resiko, dan ISO/IEC 17799 dapat bekerja secara bottom-up.

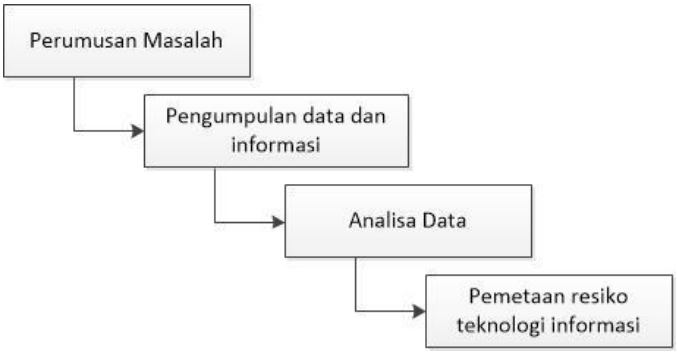
Dari penelitian-penelitian yang dilakukan oleh beberapa peneliti tersebut dapat dapat diambil kesimpulan bahwa pentingnya untuk mengelola resiko dalam organisasi. Perbedaan dari penelitian ini dengan penelitian sebelumnya adalah untuk membuat sebuah pemetaan resiko teknologi informasi dengan mengintegrasikan IT Balanced Scorecard dan NIST SP800-34 Rev1.

Perancangan IT BALANCED SCORECARD bertujuan untuk mengamati dari keseluruhan spektrum TI yang selaras dengan bisnis organisasi yang terdiri atas corporate contribution, customer orientation, operation excellence dan future orientation [16]. Setiap perspektif terdiri atas sasaran strategis yang dijadikan sebuah strategic map untuk meingkatkan investasi TI dari organisasi [17]. Untuk meningkatkan investasi TI yang sedang berjalan institusi pendidikan perlu untuk berupaya dalam melakukan strategi yang baik terhadap resiko layanan TI. Dengan mempertimbangkan resiko TI yang telah didapatkan, diharapkan institusi pendidikan dapat merancang sebuah strategi TI yang terintegrasi dengan resiko-resikonya. Karena peranan layanan TI telah membawa dampak yang signifikan bagi perkembangan institusi terutama adalah untuk mendukung kegiatan proses bisnis pendidikan, untuk itu dalam penelitian ini penting untuk membuat sebuah pemetaan resiko yang terintegrasi dengan IT Balanced Scorecard untuk mengatasi permasalahan terkait resiko IT dalam organisasi institusi pendidikan.

II. METODE

Dalam penelitian ini peneliti melakukan beberapa proses untuk implementasi pemetaan resiko teknologi informasi, peneliti juga membutuhkan data sekunder yang dikumpulkan dari unit IT *Support,* dan yang dijadikan objek integrasi IT Balanced Scorecard dan NIST SP800-34 Rev.1 ini adalah Institut Teknologi Telkom Purwokerto. Untuk melengkapi analisa pemetaan resiko yang akan dilakukan, metode penelitian ini akan dibagi beberapa tahapan yang dapat dilihat pada gambar 1. :

1. Perumusan Masalah
   Untuk mengidentifikasi kondisi permasalahan yang terjadi di saat ini terkait dengan kondisi TI yang ada di Institut Teknologi Telkom Purwokerto
2. Pengumpulan data dan informasi
   Untuk mendalami dari pemetaan resiko ini diperlukan data-data kualitatif yang berupa data resiko NIST SP800-34 Rev.1 dan IT Balanced Scorecard
3. Analisa data
   Data yang sudah dikumpulkan lalu dianalisa untuk diintegrasikan antara IT Balanced Scorecard dan NIST SP 800-34 Rev1.
4. Pemetaan Resiko Teknologi Informasi
   Perancangan strategi ini menggunakan kerangka kerja IT Balanced Scorecard dan NIST SP 800-34 yang memuat beberapa sasaran strategis yang sudah ada.



Gambar 1. Metode Penelitian

III. HASIL DAN PEMBAHASAN

A. Perumusan Masalah

Sesuai dengan nilai-nilai yang ada pada Institut Teknologi Telkom Purwokerto (ITTP) yaitu *continuous improvement*, maka ITTP menjadi perguruan tinggi yang memastikan mutu kinerja dalam pendidikan menjadi yang terbaik. Untuk menuju perbaikan yang bekelanjutan tersebut tentu saja ITTP harus

bisa untuk menjaga mutu di setiap lini unit-unitnya ,salah satunya adalah unit TI. Unit TI bertugas untuk memastikan proses bisnis layanan perndidikan terkait IT harus bisa dijaga selama 24 jam secara terus menerus. Untuk itu diperlukan identifikasi masalah terkait dengan resiko-resiko yang ada di unit TI tersebut. Untuk mengurangi resiko TI, organisasi harus fokus terhadap infrastruktur teknis TI, juga menciptakan budaya sadar akan resiko [18] oleh karena itu unit TI harus bisa mengontrol resiko yang dihadapinya.

B. Pengumpulan data dan Informasi

Data yang dikumpulkan dalam penelitian ini adalah data IT Balanced Scorecard yang terdiri dari 4 perspektif yaitu, perspektif corporate contribution, User orientation, Operational Excellence dan Future/Innovation. Data ini merupakan data rencana strategis unit IT pada tahun 2020. Dan data resiko yang dibutuhkan adalah data resiko yang telah di bentuk pada tahun 2020 yang telah disesuikan dengan framework NIST SP 800-34 Rev.1.

C. Analisa Data

Analisa sebuah resiko bertujuan untuk mengidentifikasi dan menilai resiko yang dihadapi terhadap TI agar dapat menjadi strategi yang baik untuk menghadapi segala resikonya [19]. Pengolahan hasil data untuk integrasi dari IT Balanced Scorecard dan NIST SP 800-34 Rev.1 diawali dengan menganalisa data dari identifikasi resiko yang sudah terdapat di ITTP dengan menggunakan NIST SP800-34 Rev.1 tujuannya adalah untuk memetakan asset-aset kritikal yang mempengaruhi proses bisnis yang ada di ITTP. Daftar resiko tersebut dapat dilihat pada table 1.

TABEL 1. TABEL RESIKO NIST SP800-34 REV1

No	Asset	Threat	Vulnerability	Kontrol	Likelihood	Impact Level	Risk Level
1	Sistem Informasi Akademik: i-Gracias	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	high	high	high
2	PMB Online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	high	moderate	medium
3	e-learning	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus,	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan,	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	moderate	moderate	Medium

		pencurian data dan merusak data	maintenance system				
4	Sistem Informasi Perpustakaan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	very low	very low	Low
5	E-journal	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	low	moderate	low
6	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	very low	very low	low
7	Website official ittelkom.ac.id	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	low	moderate	low
8	Blog dosen, mahasiswa, staff, UKM	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus,	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan,	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap,	low	moderate	low

		pencurian data dan merusak data	maintenance system	kunci keamanan ruang server			
9	Aplikasi Memo online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	very low	very low	Low
10	Aplikasi Nomor surat kesekretariatan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data	Kerusakan Server, kerusakan perangkat jaringan komputer, Jaringan internet down, pencurian, keamanan, maintenance system	Perlu ada CCTV di setiap sudut ruangan server, back up data secara berkala, antivirus, Password System, log activity, alat pemadam kebakaran, sensor asap, kunci keamanan ruang server	low	low	low

Dokumen resiko ini merupakan salah satu dokumen yang memuat resiko-resiko TI berdasarkan *value chain* yang telah diidentifikasi oleh unit TI. Menurut barney bahwa *value-chain analysis* digunakan untuk mengidentifikasi sumberdaya dan mengidentifikasi potensi kemampuan dari suatu organisasi [20]. Dalam identifikasi resiko pada tabel 1 bahwa yang paling banyak ditemui resiko adalah sebuah sistem**.** Ada beberapa resiko yang akan dihadapi dari teknologi Informasi seperti penghapusan file-file penting, hacker yang merusak sistem antarmuka web, sabotase sebuah sistem, virus yang dapat menghapus data seluruh organisasi dan badai yang dapat mengancam infrastruktur fisik teknologi informasi [21]. Selain itu masih ada kerentanan yang mengancam Infrastruktur TI, seperti bencana alam seperti gempa bumi, banjir, angin topan dan bencana yang diakbitkan dari manusianya sendiri seperti perang, ledakan bom, kebocoran bahan kimia, dll atau kecelakaan yang mengakibatkan kebakaran dahsyat maupun pesawat yang menabrak pusat data yang dapat menghancurkan blok-blok data penting [22]. Brar et al juga mengatakan bahwa bencana yang paling berbahaya adalah bencana yang diakibatkan dari kesengajaan, contohnya adalah karyawan ataupun mantan karyawan yang tidak puas terhadap perusahaan sehingga dapat membalas dendam dengan cara mencemari data perusahaan dengan virus sehingga dapat melumpuhkan kinerja perusahaan maupun mencuri data dengan sembunyi-sembunyi [22]. Kategori ini merupakan kategori dari spionase atau pengrusakan yang disebabkan oleh hacker. Resiko resiko yang disebutkan oleh Lallmahamood dan Brarr merupakan resiko bencana yang disebabkan oleh bencana alam maupun manusia, dan semua kategori yang telah disebutkan tersebut merupakan bencana yang sama, yang dapat menghancurkan sistem dan infrastruktur teknologi informasi.

Pada tabel *likelihood* (kemungkinan) merupakan kemungkinan resiko yang akan terjadi untuk suatu sistem layanan teknologi Informasi yang terdiri atas nilai tinggi (*high*), sedang (*moderate*), dan rendah (*low*). Manajemen Resiko fokus terhadap kegiatan yang memiliki efek untuk mengurangi kemungkinan terjadinya bencana daripada berfokus untuk meminimalkan dampak bencana. Menurut Bryson et al, kehandalan dari manajemen resiko TI adalah untuk mengukur kemungkinan resiko yang akan terjadi terhadap perencanaan strategi agar tercapainya kesinambungan, pemulihan sistem , dan restorasi sistem yang telah ditetapkan sebelumnya [23]. Karena implementasi dari manajemen resiko TI pada dasarnya adalah pemulihan aktivitas layanan dari proyek teknologi dan sistem informasi, yang sangat memungkinkan bahwa aktivitas proyek infrastruktur TI tersebut dapat gagal untuk diaktifkan.

Dalam penilaian peringkat resiko, melibatkan identifikasi resiko, analisis resiko dan penentuan prioritas resiko [24]. Hal ini sangat penting karena dapat menentukan penilaian resiko terhadap perubahan-perubahan yang akan terjadi [25]. Pada *impact level* menetapkan peringkat terhadap dampak resiko dengan nilai tinggi ,sedang, dan rendah terhadap resiko yang telah teridentifikasi. Peringkat ini ditentukan berdasarkan tingkat dampak terparah yang dihasilkan dari resiko yang diidentifikasi. Langkah ini juga bertujuan untuk mengidentifikasi besar kecilnya dampak yang terjadi pada gangguan operasional layanan TI terhadap organisasi serta mengidentifikasi sistem dan fungsi mana yang terganggu bagi keberlangsungan operasional bisnis. Analisa ini dilakukan untuk membuat keputusan yang penting bagaimana untuk membuat strategi terbaik dalam pemulihan bencana yang terjadi.

Tujuan dari untuk mengetahui *impact level* dan *risk level* adalah untuk menghitung tingkat resiko secara keseluruhan dengan nilai tinggi, sedang dan rendah untuk setiap resiko yang telah diidentifikasi. Dalam hal ini untuk menentukan tingkat resiko didasarkan pada kemungkinan-kemungkinan resiko yang terjadi dan dampaknya terhadap organisasi.

Integrasi IT Balanced Scorecard dengan NIST SP-800.34 Rev.1

ITTP merupakan insitusi pendidikan yang kompleks, dan banyaknya sistem yang saling terintegrasi, maka untuk itu top manajemen memerlukan suatu cara yang efektif dan efisien untuk mengidentifikasi resiko-resikonya. IT Balanced Scorecard dan NIST SP-800.34 merupakan sebuah perangkat umum yang digunakan dalam perusahaan. IT Balanced Scorecard digunakan untuk mengukur kinerja dan NIST SP800-34 digunakan untuk mengidentifikasi sebuah resiko. Masih banyak para pengguna framework ini untuk digunakan secara terpisah satu dengan yang lainnya.[13]. Dengan melakukan integrasi antara kinerja TI dan resiko tentu saja dapat menghasilkan nilai tambah yang bagus untuk institusi. Dengan memantau sasaran strategis yang ada pada IT Balanced Scorecard secara tidak langsung akan dapat memetakan resiko yang ada pada NIST SP 800-34. Rev.1 seperti pada tabel 2

TABEL 2. PEMETAAN RESIKO KE DALAM IT BALANCED SCORECARD

Perspektif	Sasaran Strategic	Risk	Threat
Perspektif Kontribusi perusahaan (Corporate Contribution)	1. Pengendalian Biaya TI (mengembangkan perencanaan pendanaan ITTP secara komprehensif yang dasarnya dapat diambil dari hasil monitoring dan evaluasi secara berkelanjutan).	Sistem Aplikasi Pelaporan Keuangan dari IT Telkom ke Yayasan (simonal)	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
Perspektif Orientasi Pengguna (User Orientation)	1. Meningkatkan Mutu Layanan TI	Website official ittelkom.ac.id	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data

		Blog dosen, mahasiswa, staff, UKM	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
	2. Menguatkan kerjasama pendidikan dengan berbagai pihak khususnya di bidang IT		
	3. Mewujudkan E-Campus sebagai pendukung sistem kelembagaan pendidikan	Aplikasi Nomor surat kesekretariatan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
		Aplikasi Memo online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
		Sistem Informasi Perpustakaan	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data

		PMB Online	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
Perspektif Penyempurnaan Operasional (Operational Execellence)	1. Meningkatkan kuantitas dan kualitas sarana dan prasarana IT untuk mendukung kegiatan E-Campus	Sistem Informasi Akademik: i-Gracias	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
		e-learning	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
	2. Meningkatkan pemeliharaan terhadap infrastruktur IT		
	3. Mengembangkan tata pamong kelembagaan yang baik di dalam sistem manajemen dan kinerja IT		
	4. Mewujudkan sistem informasi yang lengkap dan terintegrasi untuk mendukung business process dari ITTP	Sistem Informasi Akademik: i-Gracias	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data

	5. pengoptimalan terhadap aset, sumber daya, dan kapabilitas TI	E-journal	Runtuh/rusaknya Gedung server, gempa bumi, banjir, ledakan bom, kebakaran, listrik padam, Human Error, system error, over load traffic, System failure, Hacking, virus, pencurian data dan merusak data
Perspektif Orientasi Masa Depan (Future / Innovation).	1. Meningkatkan kapasitas dan kapabilitas tenaga IT		
	2. Tersedianya knowledge, keahlian, dan inisiatif untuk inovasi IT untuk mendukung kegiatan IT		
	3. Optimasi penggunaan IT		

Pada tabel 2. Terlihat pengintegrasian antara IT Balanced Scorecard dan NIST SP 800-34 Rev.1. Pada tahapan sebelumnya bahwa IT Balanced Scorecard dan NIST SP 800-34 Rev.1 merupakan data yang terpisah sehingga harus dilakukan mapping agar setiap sasaran strategis yang ada di IT Balanced Scorecard dapat diketahui resiko-resikonya. Untuk integrasi antara IT Balanced Scorecard dan NIST SP800-34 Rev 1 dapat digabungkan denganlangkah-langkah sebagai berikut :

1. Pada masing-masing sasaran strategis pada IT Balanced Scorecard sudah ditetapkan untuk melihat apa saja yang menjadi perhatian khususnya terhadap pencapaian sasran strategis dari Unit IT
2. Pada NIST SP 800-34 Rev.1 dapat memberikan nilai tambah untuk mengidentifikasi resiko berdasarkan sasaran strategis yang ada pada IT Balanced Scorecard. Pada tahapan ini resiko yang ada di kelompokkan sesuai dengan masing-masing perspektif pada IT Balanced scorecard sesuai dengan sasaran strategis.
3. Melakukan Analisa tambahan terhadap resiko yang sudah ditemukan.

Dapat dilihat pada tabel 2 bahwa dalam penetapan resiko ini masih ada beberapa resiko TI yang tidak terisi pada tiap-tiap sasaran strategisnya. Dapat dilihat juga proses pengintegrasian ini dapat memetakan kembali perencanaan resiko secara komprehensif sehingga institusi dapat memetakan tabel resiko secara lengkap untuk melengkapi resiko-resiko yang ada pada tiap-tiap sasaran strategis. Contoh sampel kelengkapan resiko dapat dilihat pada tabel 3. Sampel resiko perspektif orientasi masa depan.

TABEL3. SAMPEL RESIKO PERSPEKTIF ORIENTASI MASA DEPAN

Sasaran Strategis	Risk	Threat
1. Meningkatkan kapasitas dan kapabilitas tenaga IT	Tidak ada anggaran untuk pelatihan IT	RKA yang tidak mencukupi
2. Tersedianya knowledge, keahlian, dan inisiatif untuk inovasi IT untuk mendukung kegiatan IT	Tidak ada kemauan dari SDM untuk meningkatkan skill secara mandiri	Kurangnya sarana dan prasarana TI untuk mendukung kegiatan TI
3. Optimasi penggunaan IT	Proses kegagalan sistem	Kurang terjadwalnya service sistem

		secara berkala

IV. KESIMPULAN

Dari hasil penelitian yang dilakukan dalam merancang perencanaan resiko berdasarkan pendekatan IT Balanced Scorecard dan NIST SP 800-34 Rev.1, dapat diambil kesimpulan bahwa dengan membentuk risk berdasarkan pendekatan IT Balanced Scorecard dapat memetakan kembali *risk register* yang masih belum diidentifikasi pada tiap-tiap sasaran strategis yang ada pada IT Balanced Scorecard. Sehingga kemampuan operasional pada unit TI dapat bekerja secara maksimal untuk mencapai tujuannya. Dengan resiko yang telah diidentifikasi juga dapat mengurangi dampak resiko pada unit TI agar mengurangi kerugian pada Institut Teknologi Telkom Purwokerto. Dengan mengintegrasikan NIST SP 800-34 Rev.1 dan IT Balanced Scorecard dapat menyeimbangkan antara kinerja dan resiko, dan strategi yang telah ada tidak keluar pada jalurnya sehingga sesuai dengan visi misi dari unit TI.

UCAPAN TERIMA KASIH / ACKNOWLEDGMENT

Penelitian ini didukung oleh LPPM Institut Teknologi Telkom Purwokerto yang telah banyak membantu dan memberikan dukungan terkait dengan bantuan fasilitas penelitian, dan pendanaan internal terkait dengan penelitian ini

REFERENSI

[1] J. W. Toigo, “Disaster Recovery: Not Dead Yet,” *Virtualization Rev.*, no. Jul, 2015.

[2] S. Snedaker and C. Rima, *Business Continuity and Disaster Recovery Planning for IT Professionals: Second Edition*. 2013.

[3] R. Cegieta, “Selecting technology for disaster recovery,” in *Proceedings of International Conference on Dependability of Computer Systems, DepCoS-RELCOMEX 2006*, 2006, pp. 160–167, doi: 10.1109/DEPCOS-RELCOMEX.2006.49.

[4] M. Woods, “Linking risk management to strategic controls: A case study of Tesco plc,” *Int. J. Risk Assess. Manag.*, vol. 7, no. 8, pp. 1074–1088, 2007, doi: 10.1504/IJRAM.2007.015295.

[5] A. Campbell and M. Jones, “Rethinking business risk,” 2007.

[6] G. Ireland, “Rethink Your Disaster Recovery Plan,” *Credit Union Times*, 2014.

[7] H.-P. Berg, “Risk management: procedures, methods and experiences,” *Risk Manag.*, vol. 1, no. 17, pp. 79–95, 2010.

[8] M. Wu, D. Nurhadi, and S. Zahro, “Developing Risk Management as New Concept to Manage Risks in Higher Educational Institutions,” *Int. J. Risk Conting. Manag.*, vol. 6, no. 1, pp. 43–53, 2016, doi: 10.4018/ijrcm.2017010103.

[9] P. Tufano, “Managing risk in higher education,” *Forum Futur.*, pp. 58–61, 2011.

[10] I. Helsloot and W. Jong, “Risk management in higher education and research in the Netherlands,” *J. Contingencies Cris. Manag.*, vol. 14, no. 3, pp. 142–159, 2006, doi: 10.1111/j.1468-5973.2006.00490.x.

[11] J. Branchesi, “Human Being @ Risk. Enhancement, Technology , and the Evaluation of Vulnerability,” *Journal of Philosophical Studies*, vol. 26. pp. 271–275, 2014.

[12] Abdul Kadir, “Pengenalan Sistem Informasi Edisi Revisi,” *Edisi Revisi*. 2014.

[13] Kurniawati, “Integrasi Balanced Scorecard Dengan Coso Enterprise Risk Management Framework,” *J. Akunt. Bisnis*, vol. 4, no. 2, pp. 41–55, 2017.

[14] R. Sheikhpour and N. Modiri, “A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management,” *Indian J. Sci. Technol.*, vol. 5, no. 2, pp. 2170–2176, 2012, doi: 10.17485/ijst/2012/v5i3.1.

[15] S. Kumsuprom, B. Corbitt, and S. Pittayachawan, “ICT risk management in organizations: Case studies in Thai business,” in *ACIS 2008 Proceedings - 19th Australasian Conference on Information Systems*, 2008, pp. 513–522.

[16] W. Van Grembergen, “The balanced scorecard and IT governance,” *ISACA J.*, vol. 2, pp. 1–6, 2000, [Online]. Available: http://cab.org.in/IT Documents/The Balanced Scorecard and IT Governance.pdf%5Cn http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/The-Balanced-Scorecard-and-IT-Governance.p.

[17] T. B. Addo, C. Chow, and K. Haddad, “Development of

an IT Balanced Scorecard," *J. Int. Technol. Inf. Manag.*, vol. 13, no. 4, p. 1, 2004.

[18] N. E. Vincent and V. U. Vincent, "The Non-IT Manager ' s Role in Enterprise IT Risk Management," vol. 3, pp. 1–8, 2019.

[19] A. R. Ahlan and Y. Arshad, "Information technology risk management: the case of the International Islamic University Malaysia," *J. Inf. Syst. Res. Innov.*, vol. 1, pp. 58–67, 2012.

[20] J. B. Barney, *Gaining and sustaining competitive advantage*, vol. 104. 2002.

[21] M. Lallmahamood, "An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model," *J. Internet Bank. Commer.*, vol. 12, pp. 1–26, 2007.

[22] T. Pal, S. Brar, D. Sharma, and S. S. Khurmi, "Disaster Recovery and Business Continuity Planning for Electronic Banking : A Comparative Study," vol. 5976, pp. 64–71, 2015.

[23] K.-M. Osei-Bryson, H. Millar, A. Joseph, and A. Mobolurin, "Using formal MS/OR modeling to support disaster recovery planning," *Eur. J. Oper. Res.*, vol. 141, pp. 679–688, 2002, doi: 10.1016/S0377-2217(01)00275-2.

[24] B. W. Boehm, "Software risk management: Principles and practices," *Softw. Manag. Seventh Ed.*, pp. 365–374, 2007, doi: 10.1109/9780470049167.ch11.

[25] M. A. Rahman, R. Razali, and D. Singh, "A risk model of requirements change impact analysis," *J. Softw.*, vol. 9, no. 1, pp. 76–81, 2014, doi: 10.4304/jsw.9.1.76-81.