JURNAL IPSIKOM Vol. 6 NO. 1 JUNI 2018 ISSN : 2338-4093

SISTEM INFORMASI MANAJEMEN RISIKO DENGAN MENGGUNAKAN *FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* PADA LEMBAGA PENDIDIKAN

Kukuh Harsanto
Program Study Sistem Informasi, STMIK Insan Pembangunan - Tangerang
Jl. Raya Serang Km 10 Bitung Tangerang, 15118 Telp. 59492836
Email : **kukuh.harsanto@outlook.com**
Deddy Hidayat
Program Studi Sistem Informasi, STMIK Insan Pembangunan - Tangerang
Jl. Raya Serang Km 10 Bitung Tangerang, 15118 Telp. 021-59492836
Email : rendy0477@gmail.com

ABSTRAK

Lembaga atau organisasi memanfaatkan teknologi informasi untuk menunjang keberlangsungan sistem informasi yang sedang berjalan, dimana keberhasilan pelayanan lembaga pendidikan bergantung kepada sejauh mana pengelolaan teknologi informasi yang dilakukan. Dalam penggunaannya muncul berbagai risiko yang dapat menggangu keberlangsungan sistem informasi sehingga mengakibatkan kerugian pada lembaga pendidikan. Risiko-risiko yang muncul perlu diatasi, supaya masalah yang ditimbulkan tidak mengakibatkan penggunaan teknologi informasi menghambat kinerja yang dapat merugikan lembaga pendidikan, baik material maupun inmaterial. Sehingga sangat penting dibutukan di lembaga pendidikan. NIST SP 800-30 merupakan kerangka kerja yang digunakan dalam manajemen risiko sistem informasi, dimana ada 3 tahapan dalam proses manajemen risiko, yaitu risk assessment, risk mitigation, dan risk evaluation. Untuk pengujiannya peneliti menggunakan user acceptance test. Hasil yang dari penelitian ini adalah munculnya sumber ancaman yang dapat menimbulkan risiko, yaitu ancaman manusia (hacker/cracker dan orang dalam) dan ancaman bencana alam (banjir, gempa bumi, kebakaran dan angin badai).

Kata kunci : *Sistem Informasi, Manajemen Risiko, Sistem Informasi Manajemen, National Institute of Standards and Technology, User Acepptance Test*

1. PENDAHULUAN

Risiko adalah suatu ketidakpastian dimasa yang akan datang tentang kerugian yang harus dipikul oleh organisasi. Risiko mengandung tiga unsur pembentukan risiko, yaitu : kemungkinan kejadian atau peristiwa, dampak atau konsekuensi (jika terjadi, risiko akan membawa akibat atau konsekuensi), kemungkinan kejadian (risiko masih berupa kemungkinan atau diukur dalam bentuk probabilitas [1]. Pada suatu instansi pendidikan, risiko bisa timbul dikarenakan oleh pihak eksternal dan pihak internal. Risiko yang berasal dari pihak eksternal dan internal. Risiko yang berasal dari pihak eksternal diantaranya diberlakukannya peraturan perundang-undangan baru, perkembangan teknologi, bencana alam dan gangguan keamanan. Sementara itu risiko yang bersumber dari pihak internal diantaranya adanya keterbatasan dana operasional, sumber daya manusia yang tidak kompeten, peralatan yang tidak memadai, kebijaan prosedur yang tidak jelas, suasana kerja yang tidak kondusif, adanya unsur sabotase dari pegwai dan sebagainya [1].

Manajemen merupakan suatu seni dalam ilmu dan proses pengorganisasian, pergerakan dan pengendalian atau pengawasan [2], dimana didalam manajemen tersebut mempunyai tujuan melindungi dari suatu risiko yang signifikan yang dapat menghambat pencapaian tujuan, memberikan kerangka kerja manajemen yang konsisten atas proses bisnis dan fungsi masing-masing yang ada pada lembaga pendidikan dan meningkat kinerja melalui penyediaan informasi tingkat risiko yang dituangkan dalam peta yang beguna bagi manajemen dalam pengembangan strategi dan perbaikan proses manajemen yang secara terus menerus dan

berkesinambungan [3]. Untuk mencapai tujuan tersebut maka dibutuhkan suatu *framework* yang mendukung untuk membantu dalam pemecahan masalah.

Framework National Institute of Standards and Technology (NIST) merupakan kumpulan standar atau langkah-langkah dan dapat memberikan pemahaman dalam proses manajemen risko [1], NIST mengeluarkan rekomendasi melalui publikasi khusus *framework* NIST SP 800-30 tentang *Risk Management Guide For Information Technology Sistem*. NIST lebih menyajikan langkah-langkah untuk mengukur tingkat risiko yang ada.

Berdasarkan uraian diatas, maka identifikasi masalah penelitiannya sebagai berikut :

1. Belum adanya Sistem Informasi Manajemen yang berkaitan dengan Manajemen Risiko di Lembaga Pendidikan.
2. Belum adanya dokumentasi terhadap risiko-risiko yang terjadi pada lembaga pendidikan khususnya pada infrastruktur TI di Lembaga Pendidikan.
3. Belum adanya pengelolaan manajemen risiko khususnya pada infrastruktur TI di Lembaga Pendidikan.

Berdasarkan identifikasi permasalahan diatas, maka permasalahan yang akan dijawab, yaitu :

1. Apa saja sumber ancaman yang muncul setelah dilakukan penilaian risiko dengan *framework* manajemen risiko NIST SP 800-30 pada lembaga pendidikan?
2. Bagaimana membangun prototipe Sistem Informasi Manajemen Risiko dengan menggunakan UML (*Unified Modeling Language*)?
3. Bagaimana melakukan pengujian sistem dengan menggunakan *User Acceptance Test* terhadap Sistem Informasi Manajemen Risiko yang dibangun?

2. LANDASAN TEORI

2.1. Risiko

Risiko adalah suatu ketidakpastian dimasa yang akan datang tentang kerugian yang harus dipikul oleh organisasi. Risiko mengandung tiga unsur pembentukan risiko, yaitu : kemungkinan kejadian atau peristiwa, dampak atau konsekuensi (jika terjadi, risiko akan membawa akibat atau konsekuensi), kemungkinan kejadian (risiko masih berupa kemungkinan atau diukur dalam bentuk probabilitas [1].

Risiko mempunyai dua karakteristik [4], yaitu :

1. Merupakan ketidakpastian atas terjadinya suatu peristwa.
2. Merupakan ketidakpastian yang bila terjadi akan menimbulkan kerugian.

Ada beberapa sumber yang dapat menyebabkan terjadinya suatu risiko [5], yaitu :

1. Risiko Internal, yaitu risiko yang berasal dari dalam lembaga pendidikan itu sendiri.
2. Risiko Eksternal, yaitu risiko yang berasal dari luar lembaga pendidikan atau lingkungan luar lembaga pendidikan.
3. Risiko Keuangan, risiko yang disebabkan oleh faktor-faktor ekonomi dan keuangan, seperti perubahan harga, tingkat bunga dan mata uang.
4. Risiko Operasional, adalah semua risiko yang tidak termasik operasional disebabkan oleh faktor-faktor manusia, alam dan teknologi.

Untuk menangulangi semua risiko yang terjadi, maka diperlukan sebuah manajemen untuk mengidentifikasi risiko tersebut.

2.2. Manajemen

Manajemen merupakan ilmu pengetahuan yang terdiri dari kegiatan perencanaan, pelaksanaan dan pengendalian terhadap sumber daya yang terbatas dalam mencapai tujuan tertentu dan sasaran yang efektif dan efisien [2]. Manajemen dibutuhkan oleh semua lembaga pendidikan karena tanpa manajemen, semua usaha akan sia-sia dan pencapaian tujuan akan lebih sulit. Tujuan dari manajemen adalah mendapatkan metode atau cara teknik yang paling baik agar sumber daya yang terbatas diperoleh hasil yang maksimal dalam hal ketepatan, kecepatan, penghematan dan keselamatan kerja komprehensif. Manajemen mempunyai empat fungsi utama [6], yaitu :

1. Perencanaan

Proses penentuan tujuan atau sasaran yang hendak dicapai dan menetapkan jalan dan sumber yang diperlukan untuk mecapai tujuan dan seefisien mungkin.

2. Pengorganisasian

Tindakan mengusahakan hubungan–hubungan kelakuan yang efektif antara orang-orang, sehingga mereka dapat bekerja sama secara efisien dan memperoleh kepuasan pribadi dalam melaksanakan tugas-tugas tertentu, dalam kondisi lingkungan tertentu guna mencapai tujuan atau sasaran tertentu.

3. Pelaksanaan

Usaha menggerakkan anggota-anggota kelompok sedemikian rupa hingga mereka berkeinginan dan berusaha untuk mencapai sasaran lembaga pendidikan dan sasaran anggota lembaga pendidikan tersebut.

Oleh karena itu para anggota juga ingin mencapai sasaran-sasaran tersebut.

4. Evaluasi

Proses pengumpulan dan analisis data secara sistematis yang diperlukan dalam rangka pengambilan keputusan.

Untuk mengontrol risiko tersebut dibutuhkan suatu sistem informasi manajemen untuk mencegah terjadinya risiko.

2.3. Sistem Informasi Manajemen Risiko

Sistem informasi manajemen risiko merupakan bagian dari sistem informasi manajemen yang harus dimiliki dan dikembangkan sesuai dengan kebutuhan, dalam rangka penerapan manajemen risiko yang efektif.

Sebagai bagian dari proses manajemen risiko, harus memiliki sistem informasi manajemen risiko yang dapat memastikan [7] tersedia secara akurat dan tepat waktu.

1. Risiko terukur secara akurat, relevansi dan tepat waktu, baik.
2. Mematuhi penerapan manajemen risiko terhadap kebijakan, prosedur dan penetapan limit risiko.
3. Hasil penerapan manajemen risiko ditetapkan oleh lembaga pendidikan sesuai dengan kebijakan dan strategi penerapan manajemen risiko.

Sistem informasi manajemen risiko harus dapat menerjemahkan risiko yang diukur dengan format kuantitatif sehingga menjadi format kuantitatif yang mudah dipahami. Sistem informasi manajemen risiko digunakan untuk mendukung pelaksanaan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko, maka diperlukan dukungan sistem informasi manajemen yang dapat mendukung pembuatan laporan yang akurat, informasi, relevan, lengkap, konsisten dan tepat waktu [7].

2.4. Kategori Risiko Teknologi Informasi

Dalam penggunaan teknologi informasi berisiko terhadap kehilangan informasi dan pemulihannya yang tercakup dalam 6 kategori, yaitu [8] :

1. Keamanan
   Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berwenang, misalnya saja kejahatan komputer, kebocoran internal dan terorisme *cyber*.

2. Ketersediaan
   Risiko yang datanya tidak dapat diakses setelah kegagalan sistem, karena kesalahan manusian (*human eror*), perubahan konfigurasi dan kurangnya penggunaaan arsitektur.

3. Daya pulih
   Risiko dimana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah terjadiya kegagalan dalam perangkat lunak atau keras, ancaman eksternal atau bencana alam.

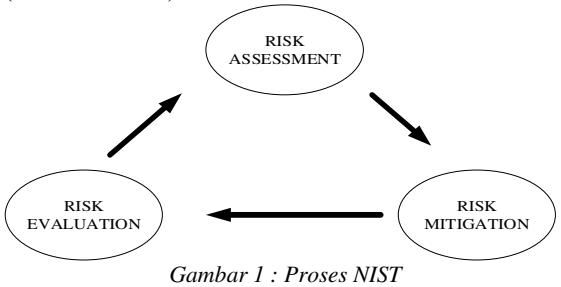
4. Performa
   Risiko dimana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaa yang tingga dan topografi informasi teknologi yang beragam.

5. Daya skala
   Risiko yang perkembangan bisnis, pengaturan *bottleneck* dan bentuk arsitekturnya membuatnya tidak mungkin menangani banyak aplikasi baru dan biaya bisnis secara efektif.

6. Ketaatan
   Risiko yang manajemen penggunaan informasinya melanggar keperluan dari pihak pengatur. Yang dipersalakan dalam hal ini mencakup aturan pemerintah, panduan pengaturan perusahaan dan kebijakan internal.

2.5. *National Institute Of Standards and Technology* (NIST)

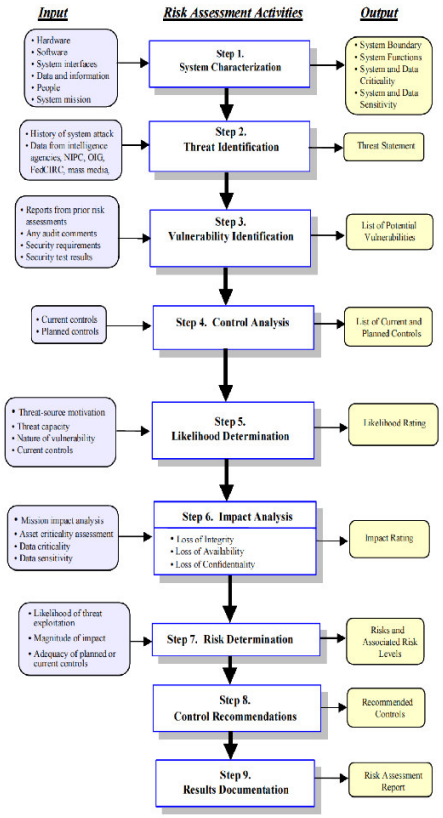
National Institute of Standards and Technology (NIST) merupakan organisasi pemeritah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standard an teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. Kegiatan utama adalah meneliti berbagai ilmu untuk mempromosikan dan meningkatkan infrastruktur teknologi [9]. Proses manajemen risiko terdapat 3 tahapan yaitu penilaian risiko (*risk assessment*), peringanan risiko (*risk mitigation*) dan evaluasi risiko (*risk evaluation*).



Gambar 1 : Proses NIST

1. *Risk assessment*
   Risk assessment merupakan proses tahap

pertama dalama metodologi manajemen risiko. Organisasi menggunakan *risk assessment* untuk menentukan sejauh mana ancaman dan risiko yang terkait dngan sistem IT sepanjang SDLC. Keluaran dari proses ini membantu mengidentifikasi pengendalian yang tepat untuk membuat atau menghilangkan risiko selama proses *risk mitigation* [10]. Untuk menentukan kemungkinan yang akan datang, ancaman terhadap sistem IT harus dianalisa yang berhubungan dengan potensi kerentanan dan pengendalian untuk sistem IT. Metodolgi *risk assessmet* terdiri dari sembilan langkah, yaitu [10] :



Gambar 2 : Risk Assesment Methodology Flowchart

a. *System Characterization*
Melihat sudut pandang *hardware, software infterface,* data dan lain-lain. Sudut pandang inilah yang akan menjadi *input* proses, sehingga akan menghasilkan *output* yaitu batasan sistem, fungsionalitas sistem, data dan tingkat sensitifitas, pengguna dan lain-lain.

b. *Threat Identification*
Mengenali berbagai sumber yang akan menjadi gangguan pada sistem. *Input* dari proses ini biasanya adalah laporan serangan yang pernah tejadi, data dari berbagai pihak baik media, agensi. Sementara *output* proses ini adalah *threat statement*, yaitu merupakan sekumpulan risiko yang mungkin terjadi serta sumber risiko yang dapat menimbulkan kerentanan pada sistem.

c. *Vulnerability Indetification*
Pada tahapan ini diidentifikasi berbagai kelemahan atau kekurangan dari sistem yang memungkinkan terjadi ancaman terhadap sistem.

d. *Control Analysis*
Tujuan utama dari tahap ini untuk menganalisis kontrol yang telah diterapkan atau yang akan diterapkan, untuk meminimalisasi kemungkinan terjadinya ancaman. *Input* dari tahapan ini adalah kontrol yang telah diterapkan dalam masing-masing risiko/kerentanan, sementara *output*nya adalah list dari kontrol terhadap risiko yang tengah diterapkan dan rencana kontrol yang akan diterapkan terhadap risiko yang mungkin terjadi.

e. *Likelihood Determination*
Digunakan untuk memperoleh nilai kecenderungan yang mungkin terjadi atas kelemahan dari sistem. *Input* dari tahapan ini adalah sumber risiko dan motivasi penyebab sumber risiko, kerentanan dan efektivitas dari kontrol yang diterapkan.

f. *Impact Analysis*
Menilai dampak yang terjadi terhadap serangan atas bagian lemah dari sebuah sistem. *Input* dari sistem ini adalah misi sistem serta tingkat sensitifitas data atau dengan kata lain bagaimana risiko akan berpengaruh pada misi sistem dan data yang diolah. Kemungkian yang menjadi pertimbangan adalah masalah integritas data, ketersediaan terhadap layanan dan kehilangan kepercayaan. *Output* dari sistem ini adalah definisi dampak dari risiko (*magnitude of impact definition)*

g. *Risk Determination*
Risk determination ini bertujuan untuk menilai tingkat risiko terhadap sistem, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan.

h. *Control Recommendations*
Tujuannya untuk mengurangi level risiko pada sistem ini TI sehingga mencapai level yang bias

diterima. *Input*nya adalah dari *output* dari tahapan sebelumnya yaitu risiko dan tingkat risiko, dari sini akan dihasilkan daftar rekomendasi kontrol.

i. *Result Documentatiom*
Merupakan laporan dokumentasi dari kegiatan yang ada, dimulai tahap karakteristik hingga rekomendasi kontrol.

2. *Risk Mitigation*
Tahapan ini merupakan tindakan peringanan terhadap risiko yang sudah terdokumentasi. Hasil dari penilaian risiko ini berupa profil risiko dengan berbagi rekomendasi yang sekiranya dapat menjadi solusi dalam proses meringankan risiko yang sesuai dengan kebutuhan sistem informasi.

Kegiatan *risk mitigation* ini meliputi prioritas, aksi ini dilakukan dengan mengacu hasil akhir penilaian risiko. Dimana risiko yang memiliki tingkat tertinggi yang harus dijadikan sebagai prioritas utama dalam proses peringanan risiko. Selain itu proses peringanan risiko ini juga harus menyesuaikan dengan biaya dan keuntungan yang akan timbul dalam upaya meminimalisir risiko yang sudah teridentifikasi dan hasil rekomendasi yang akan dilaksanakan. Peringanan risiko ini diharapkan dapat mengatasi permasalahan yang menggangu terhadap keberlangsungan sistem informasi.

3. *Risk Evaluation*
Kegitan evalusi risiko adalah kegiatan terhadap keberlangsungan proses mitigasi, pada umumnya jaringan yang diterapkan dalam organisasi akan mengalami perubahan atau pengembangan komponen *hardware,* pengembangan *software* dan aplikasi oleh versi yang lebih *up to date* dan lebih baru.

2.6. Tinjauan Studi

Tabel 1 : tinjauan studi

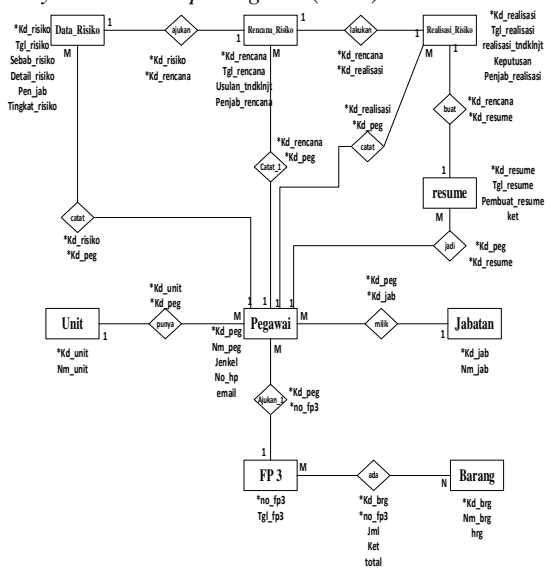
JUDUL PENELTIAN	TAHUN	METODE	HASIL PENELITIAN
MANAJEMEN RISIKO SISTEM INFORMASI PADA PERGURUAN TINGGI MENGGUNAKAN KERANGKA KERJA NIST SP 800-300	2016	NIST	Hasil dari penilaian risiko didapat beberapa sumber ancaman yang dapat menimbulkan pada sistem informasi, dengan menggunakan kerangka kerja NIST SP 800-30, dapat mendeskripsikan profil risiko yang dapat mengancam keberlangsungan sistem informasi
PENILAIAN RESIKO TEKNOIOGI INFORMASI & KEAMANAN SISTEM INFORMASI DENGAN MENGGUNAKAN FRAMEWORK COBIT 4.1 DAN GUIDELINES NIST SP 800-30 (Studi Kasus : Rumah Sakit Umum Dr Slamet Garut)	2011	COBIT 4.1 dan NIST	Mempunyai tingkat keamanan yang cukup untuk mendukung tujuan organisasinya akan tetapi untuk jangka menengah dan panjang
Manajemen Risiko Sistem Informasi pada Perguruan Tinggi Menggunakan Metoda Octave Allegro	2013	Octave Allegro	Dapat memberikan gambaran kemungkinan adanya ancaman pada asset kritikal dan mengambil langkah-langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi, pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga asset informasi kritikal tepat serta langkah-langkah pemulihan jika skenario ancaman benar-benar terjadi,
MANAJEMEN RISIKO PADA PERUSAHAAN JASA PELAKSANA KONSTRUKSI DI PROPINSI PAPUA (STUDY KASUS DI KABUPATEN SARMI)	2014	Metode penelitian deskriptif.	Berdasarkan analisis komponen utama diperoleh 8 aspek risiko untuk kemungkinan terjadinya kejadian,
PENGUKURAN MANAJEMEN RISIKO TEKNOLOGI DENGAN MENGGUNAKAN OCTAVE-S	2014	Octave-S	Mengetahui risiko-risiko dari penerapan teknologi informasi, mengidentifikasikan nilai dari risiko yang ditemukan pada perusahaan, mengidentifikasikan praktik

			keamanan yang cocok untuk penanggulangan risiko dan meminimalkan risiko, serta memaksimalkan kinerja dari Teknologi Informasi pada perusahaan
SISTEM INFORMASI MANAJEMEN RISIKO MENGGUNAKAN *FRAMEWORK NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY* PADA LEMBAGA PENDIDIKAN	2016	NIST	-

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Rancangan Basis Data

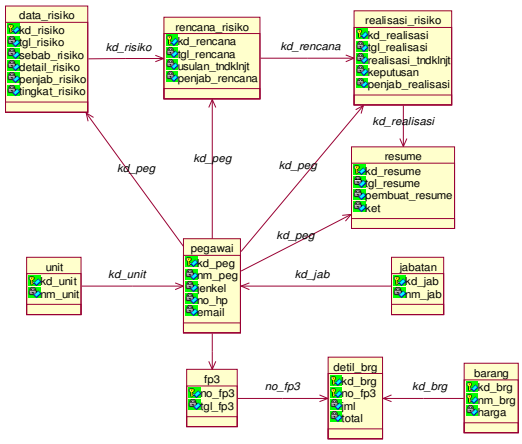
Rancangan basis data akan digambarkan dengan *Entity Relantionship Diagram* (ERD).



Gambar 3 : Rancangan Basis Data

3.2. Logical Record Structure

Berikut gambar *Logical Record Structure:*



Gambar 4 : Logical Record Structure

4. HASIL DAN PEMBAHASAN

Dalam pembahasan ini menggunakan *framework* NIST SP 800-30 untuk melakukan pengukuran risiko (*risk assessment*). Dalam melakukan pengukuran risiko (*risk assessment*) teknologi informasi, terdiri dari 9 langkah, yaitu [10]:

1. Karakterisasi Sistem (*System Characterization*)

Langkah pertama yang dilakukan adalah menentukan ruang lingkup usaha. Pada tahap ini batas-batas dari sistem TI diidentifikasi, bersamaan dengan sumber daya informasi yang merupakan sistem. Karakteristik sistem TI menetapkan ruang lingku penilaian usaha, izin operasional (akreditasi) batas-batas dan menyediakan informasi (*hardware, software, system connectivity*) dan divisi yang bertanggung jawab atau dukungan penting untuk menentukan risiko [10].

2. Identifikasi Ancaman (*Threat Identification*)

Ancaman merupakan suatu rintangan-rintangan utama bagi posisi instansi atau yang diinginkan dari instansi [11]. Suatu ancaman merupakan situasi utama yang tidak menguntungkan dalam lingkungan suatu instansi, maka kita harus mempertimbangkan berbagai sumber ancaman, ptensi kerentanan dan kontrol yang sudah ada.

3. Identifikasi Kerentanan (*Vulnerability Identification*)

Analisis ancaman terhadap suatu sistem TI harus mencakup analisis kerentanan yang terkait dengan sistem TI yang dievaluasi. Tujuannya adalah untuk mengembangkan daftar kerentanan sistem (kekurangan atau kelemahan) yang dapat dimanfaatkan oleh ancaman-sumber potensial [10]. Metode yang disarankan untuk mengidentifikasi kerentanan penggunaan sistem adalah kerentanan sumber, kinerja pengujian keamanan sistem dan daftar persyaratan pengembangan keamanan [10].

4. Analisis Pengendalian (*Control Analysis*)

Tujuan dari langkah ini adalah untuk menganalisis kontrol yang telah dilaksanankan atau direncakan untuk pelaksanaan, oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan adanya ancaman dan kerentanan sistem [10].

5. Penentuan Kemungkinan (*Likelihood Determinatioon*)

Untuk mendapatkan suatu penilaian secara keseluruhan yang menunjukkan kemungkina probabilitas bahwa potensi kerentanan dapat dilaksanan di dalam membangun lingkungan ancaman terkait [10].

6. Analisis Dampak (*Impact Analysis*)

Langkah penting berikutnya dalam mengukur tingkat risiko adalah menentukan dampak buruk dari akibat ancaman kerentanan tersebut.

Tabel 2 : Analisis Dampak

Ancaman	Dampak	Akibat
Virus dan hacker	Tinggi	a. Merusak data penting yang ada b. Mencuri informasi penting c. Merusak sistem keamanan d. Memanipulasi data e. Menyebarkan informasi penting lembaga pendidikan
Orang dalam	Rendah	Hanya merusak sebagian kecil asset

7. Penentuan Risiko (*Risk Determination*)

Tujuan dari langkah ini adalah untuk menilai tingkat risiko terhadap sistem TI [10]. Penentuan risiko untuk ancaman tersebut dapat dinyatakan sebagai berikut :

a. Kemungkinan ancaman dikurangi untuk melaksanakan suatu dampak kerentanan yang ada di dalam lembaga pendidikan.

   Artinya dampak kerentanan yang mungkin terjadi dapat mengurangi suatu risiko kerentanan yang ada di dalam lembaga pendidikan dan melakukan perbaikan agar roisiko tersebut dapat berkurang

b. Besarnya dampak harus menjadi sumber ancaman untuk melatih kerentanan

   Adanya dampak yang menyerang suatu sistem yang ada di dalam suatu lembaga pendidikan dan harus dapat dicegah segera mungkin agar risiko tersebut tidak menjadi besar dan juga dapat melakukan pencegahan agar mengurangi risiko yang ada

c. Kecukupan kontrol keamanan harus direncanakan untuk mengurangi risiko yang terjadi

8. Rekomendasi Pengendalian (*Control Recommendation*)

Tujuan dari direkomendasikan kontrol adalah untuk mengurangi tingkat risiko pada sistem TI dan data perusahaan pada tingkat yang memadai.

9. Hasil Dokumentasi (*Result Documentation*)

Setelah penilaian risiko telah selesai (sumber ancaman dan identifikasi kerentanan, penilaian risiko dan disarankan menyediakan kontrol), hasil harus didokumentasikan dalam sebuah laporan atau *briefing*.

Tabel 3 : Hasil Dokumentasi

Sumber Ancaman	Ancaman	Kontrol Yang Disarankan
Alam	a. Gempa bumi b. Kebakaran c. Banjir d. Angin badai	a. Sebelum melakukan pembangunan gedung harus dilakukan perencanaan terlebih dahulu untuk membuat model bangunan yang kokoh dan tahan gempa, sehingga apabila terjadi bencana gempa bumi bangunan tidak hancur/runtuh b. Diperlukan adanya *water fire protector* dan alat pemadaman apiyang cukup memadai. Hal ini dilakukan untuk mencegah kebakaran yang terjadi, sehingga dengan secepatnya api bisa dimatikan/dipadamkan
Manusia	a. Hacker b. Cracker c. Orang dalam	a. Memasang antivirus supaya hacker dan cracker tidak bisa memasuki sistem,mengambil data-data penting dan memanipulasi data di dalam perusahaan. b. Mengganti password sebulan sekali c. Memasang firewall di

		setiap sistem perusahaan untuk mencegah hacker memasuki sistem, firewall agar memberikan peringatan apabila sistem dimasuki oleh hacker/cracker d. Memperketat akses keamanan di dalam maupun di luar perusahaan e. Memasang cctv di setiap sudut perusahaan untuk memantau setiap orang yang memasuki perusahaan f. Harus mempunyai database untuk semua karyawan yang ada di perusahaan, hal ini dilakukan untuk mencegah orang-orang yang tidak berkepentingan atau orang-orang yang tidak kenal dapat memasuki perusahaan secara bebas g. Memberikan pelatihan untuk setiap karyawan agar selalu bersikap baik dan taat kepada peraturan-peraturan yang ada di dalam perusahaan h. Karyawan diberikan training untuk selalu bertanggung jawab atas tugas dan wewenang yang diberikan perusahaan

4.1. Pengujian Perangkat Lunak *User Acepptance Test* (UAT)

Responden diminta untuk mengisi kuesioner untuk pengujian dimana pengujian dilakukan untuk mengetahui kualitas dari prototype.

Tabel 4 : Pertanyaan Kuesioner

No	Pertanyaan	A	B	C	D	E
1.	Apakah tampilan prototype sistem informasi manajemen risiko ini mudah dipahami?	**5**	**12**	**3**	**0**	**0**
2.	Apakah menu-menu prototype sistem informasi manajemen risiko ini mudah dipahami?	**4**	**6**	**10**	**0**	**0**
3.	Apakah prototype sistem informasi manajemen risiko ini mudah dipahami?	**5**	**9**	**6**	**0**	**0**
4.	Apakah prototype sistem informasi manajemen risiko ini mempermudah mendapatkan informasi yang berhubungan dengan risiko khususnya infrastruktur IT?	**0**	**15**	**5**	**0**	**0**
5.	Apakah tampilan antarmuka sistem informasi manajemen risiko sesuai dengan kategori pengguna dalam prototype sistem informasi manajemen risiko?	**2**	**15**	**3**	**0**	**0**
6.	Apakah tidak membutuhkan waktu lama untuk memmahami prototype sistem informasi manajemen risiko?	**4**	**14**	**2**	**0**	**0**
7.	Apakah prototype sistem informasi manajemen risiko memberukan pesan jika terdapat kesalahan?	**2**	**14**	**4**	**0**	**0**
8.	Apakah prototype sistem informasi manajemen risiko (menampilkan halaman yang tidak sesuai dengan halaman yang diinginkan)?	**2**	**13**	**5**	**0**	**0**
9.	Apakah prototype sistem informasi manajemen risiko bersifat *user friendly*?	**2**	**15**	**3**	**0**	**0**
10.	Apakah prototype sistem informasi manajemen risiko sudah cukup baik?	**1**	**16**	**3**	**0**	**0**

Analisa pertanyaan pertama

$$\% \text{ skor aktual} = \frac{\text{Skor aktual}}{\text{Skor Ideal}} \times 100\%$$

$$= \frac{82}{100} \times 100\%$$

$$= 82\%$$

Dari hasil perhitungan diatas, dapat dilihat mayoritas responden setuju dengan presentase sebesar 82% dengan kriteria baik.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan beberapa hal sebagai berikut :

1. Setelah dilakukan penilaian risiko menggunakan *framework* NIST SP 800-30, maka muncul sumber ancaman yang dapat menimbulkan risiko sebagai berikut :
   a. Ancaman manusia (hacker/cracker, orang dalam)
   b. Ancaman bencana alam (banjir, gempa bumi, kebakaran, angin badai)
2. Sistem Informasi Manajemen Risiko menggunakan *framework* NIST SP 800-30 dapat menghasilkan aplikasi Sistem Informasi Manajemen Risiko, yang dapat diterapkan untuk pengelolaan manajemen risiko pada lembaga pendidikan.
3. Sistem Informasi Manajemen Risiko menggunakan pengujian UAT (*User Acepptance Test*) dengan jumlah total rata-rata 78.3%, sehingga Sistem Informasi Manajemen Risiko dapat diterima dengan baik oleh *user* pada lembaga pendidikan.

DAFTAR PUSTAKA

[1] U. Nugraha, "Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-

30," Mei 2016. http://www.slideshare.net/ 6 September 2016.

[2] Y. P. Nugroho, "Pengembangan Sistem Informasi Manajemen Proyek," 2012. http://eprints.undip.ac.id/38525/1/Tesis_PMIS_-_Yuliandri.pdf. 20 September 2016.

[3] PTPN XII, "Website GCG Online PTPN XII (Persero)," 2014. http://www.gcg.ptpn12.com. 20 April 2016.

[4] W. W. Yasa, I. G. B. S. Dharma and I. G. K. Sudipta, "Manajemen Risiko Operasional Dan Pemeliharaan Tempat Pembuangan Aakhir (TPA) Regional Bangki Di Kabupaten Bangli," Juli 2013. [Online]. https://www.academia.edu/Accessed 7 Oktober 2016.

[5] A. Lokobal, M. D. Sumajouw and B. F.Sompie, "Manajemen Risiko Pada Perusahaan Jasa Pelaksana Kontruksi Di Propinsi Papua (Study Kasus di Kabupaten Sarmi)," 2014. http://ejournal.unsrat.ac.id/. 20 September 2016.

[6] H. Salsabila, "Fungsi-Fungsi Manajemen; Perencanaan, Pengorganisasian, Pelaksanaan, Dan Evaluasi," 2016. [Online]. Available: https://www.academia.edu/. 18 April 2016.

[7] Ikatan Bankir Indonesia, Manajemen Risiko 1, Gramedia Pustaka Utama, 2015.

[8] F. Julianti, O. Yudianto and T. Fredy, "Library Binus," 9 Juli 2010. library.binus.ac.id. 9 September 2016.

[9] H. S. Firmansyah, "Implementasi Framework Manajemen Risiko Terhadap Penggunaan Teknologi Iinformasi Perbankan," 2010 Oktober 2010. http://jit.telkomuniversity.ac.id/index.php/aptikom10/article/download/174/159. 9 September 2016.

[10] g. Stonerburner, A. Goguen and A. Feringa, Juli 2002.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. 9 Sepetember 2016.

[11] D. Septianda, "Pendapat Para Ahli Tentang Analisis SWOT," 20 April 2012. http://dansseptianda.blogspot.co.id/ 14 November 2016.

[12] B. Susanto, "Seputar Pengetahuan," 10 Maret 2015.http://www.seputarpengetahuan.com/2015/03/pengertian-lembaga-pendidikan-menurut-para-ahli.html. 20 April 2016.

[13] Ikatan Bankir Indonesia, Manajemen Risiko 2, Gramedia Pustaka Utama, 2015, p. 230.