ISSN 2087 2429

Analisis Resiko Teknologi Informasi Sistem Terintegrasi iGracias Berbasis Risk Assesment Menggunakan SNI ISO-IEC 27001-2009

Periyadi
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
periyadi@tass.telkomuniversity.ac.id

Abstrak—Sistem terintegrasi merupakan tantangan menarik dalam *software development* karena proses pengembangannya harus mengacu pada konsistensi sistem, agar sub-sub sistem yang sudah ada secara operasional masih tetap berfungsi sebagaimana mestinya, baik ketika proses mengintegrasikan sistem maupun setelah terintegrasi [1]. Universitas Telkom memanfaatkan fasilitas *e-Learning* untuk membantu proses pembelajaran dalam sistem terintegrasi. Aplikasi *e-Learning* Universitas Telkom bernama IDEA (*Integrated Distance Education Application*) dan pengelolaan aktivitas manajemen di dalam sistem tersebut, saat ini dapat diakses melalui portal sistem informasi Universitas Telkom, iGracias (*Telkom University Integrated Information System*). Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan risiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Proses analisis ini akan menghasilkan hasil analisis resiko mengenai aset fisik beserta kemungkinan risiko yang muncul Berbasis *Risk Management* menggunakan SNI ISO-IEC 27001-2009 pada sistem terintegrasi iGracias. Pada akhirnya organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas risiko.

Kata kunci—Telkom University; Sistem Terintegrasi; iGracias; Risk Management; SNI ISO-IEC 27001-2009; Teknologi Informasi

Abstract—Integrated system is an interesting challenge in software development since the development process must be based on the consistency of the system, so that sub-systems that already exist operationally still function properly either when or after the process of integrating the integrated system. Telkom University uses e-learning to assist the learning process in an integrated system. E-Learning applications at Telkom University named IDEA (Integrated Distance Education Application) and management activities within the management of the system, is now accessible through the portal of information systems Telkom University, iGracias (Telkom University Integrated Information System). However, it is undeniable that the possibility of a wide range of threats and risks can hamper even paralyze activity in the system, one of which is caused by the use of information technology. This analysis process will produce results of risk analysis regarding the physical assets and possible emerging risks Based Risk Management using ISO-IEC 27001-2009 in the integrated system iGracias. In the end, the organization can do prevention, treatment and improvements for the future in accordance with the priority level of risk.

Keywords—Telkom University; Integrated System; iGracias; Risk Management; SNI ISO-IEC 27001-2009; Information Technology

I. LATAR BELAKANG

Universitas Telkom (Tel-U) menyediakan layanan sistem informasi terintegrasi untuk mendukung proses layanan yang berlangsung di dalam melayani seluruh kegiatan pembelajaran. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan risiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan.

Sehingga menjadi sebuah kebutuhan untuk melakukan analisis risiko terhadap berbagai kemungkinan risiko yang terjadi pada sistem iGracias. Dari hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan risiko yang muncul. Karena itu perlu dilakukan analisis risiko teknologi informasi berbasis *risk management* menggunakan SNI ISO-IEC 27001-2009 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem terintegrasi iGracias.

Berdasarkan pada latar belakang tersebut, dapat dirumuskan permasalahan yaitu bagaimana analisis risiko teknologi informasi terhadap sistem terintegrasi iGracias menggunakan SNI ISO-IEC 27001-2009 dengan menentukan tingkat risiko teknologi informasi terintegrasi iGracias.

Adapun tujuan dari penelitian ini adalah melakukan tahapan dan proses analisis risiko teknologi informasi terintegrasi iGracias berbasis *risk management* sesuai dengan standar dan kerangka kerja SNI ISO-IEC 27001-2009 dengan mengetahui tingkat risiko teknologi informasi terintegrasi iGracias.

Manfaat dari penulisan ini diharapkan akan menjadi acuan untuk proses penentuan tingkat risiko di Universitas Telkom agar bisa dimanfaatkan sebagai satu alternatif bentuk *awareness* dari sisi risiko yang mungkin terjadi.

II. LANDASAN TEORI

A. *Risk Assesment*

Risiko berhubungan dengan ketidakpastian. Ketidakpastian ini terjadi oleh karena kurang atau tidak tersedianya cukup informasi tentang apa yang akan terjadi.

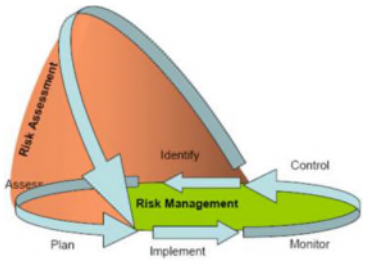
Sesuatu yang tidak pasti (*uncertain*) dapat berakibat menguntungkan atau merugikan, ketidakpastian yang menimbulkan kemungkinan menguntungkan dikenal dengan istilah peluang (*opportunity*), sedangkan ketidakpastian yang menimbulkan akibat yang merugikan dikenal dengan istilah risiko (*risk*) [2].

Dalam bentuk formula *risk* dapat digambarkan sebagai berikut [3];

$$RISK = \frac{(Threat * Vulnerability)}{countermeasure} * Value \quad (1)$$

Vulnerability : suatu keadaan atau kondisi yang dapat menyebabkan atau berpotensi sistem kita akan rusak karena gangguan.
Threat : probabilitas terjadinya suatu (eksternal) kejadian yang tidak diinginkan karena mengeksploitasi kerentanan
Countermeasure : cara tindakan yang dilakukan untuk menghentikan ancaman
Value : nilai dari informasi yang menjadi ukuran

Proses menentukan dari sebuah risiko tersebut yang akan menentukan perlu adanya tindakan terhadap nilai (informasi/aset) yang akan diamankan.



Gambar 1 *Risk Management* [1]

Gambar 1 merupakan gambaran dari *Risk Management*. Langkah yang bisa dilakukan adalah mencoba memperkecil risiko dengan memindahkan risiko ke pihak lain, mencoba menghindari risiko itu sendiri, mengurangi nilai dari risiko yang ditimbulkan, menampung semua atau sebagian risiko pada kasus-kasus tertentu dengan tidak mengurangi nilai/aset dari yang mengalami risiko itu sendiri.

Ancaman ini bisa disebabkan oleh berbagai elemen seperti teknologi, *human error*, lingkungan, politik maupun dari organisasi.

Secara umum *risk assesment* memiliki beberapa tahapan, yaitu:

1. *Identifikasi Risiko*

Kegagalan dalam tahapan ini akan berpengaruh besar terhadap tahapan manajemen resiko selanjutnya dan tentu akan mempengaruhi reliabilitas bagi proyek karena banyaknya kerentanan/celah yang mungkin akan terjadi di masa yang akan datang.

Tujuan utama dalam identifikasi resiko adalah untuk mengetahui daftar–daftar resiko yang potensial dan berpengaruh terhadap tujuan / proses bisnis suatu organisasi [4]. Langkah yang diambil dalam tahap ini adalah dengan melakukan:

a. Mengidentifikasi aset dalam ruang lingkup Sistem Manajemen Keamanan Informasi (SMKI) dan pemilik-pemilik aset.
b. Mengidentifikasi ancaman-ancaman terhadap aset
c. Mengidentifikasi kelemahan yang mungkin dieksploitasi oleh ancaman.
d. Mengidentifikasi dampak hilangnya kerahasiaan, integritas dan ketersediaan.

2. *Analisis Risiko*

Pada tahap ini dilakukan analisis resiko dengan melakukan pengukuran risiko dengan cara melihat potensial terjadinya seberapa besar *severity* (kerusakan) dan probabilitas terjadinya risiko tersebut. Langkah yang diambil antara lain:

a. Mengases dampak bisnis bagi organisasi yang mungkin berasal dari kegagalan keamanan, yang mempertimbangkan konsekuensi hilangnya kerahasiaan, integritas atau ketersediaan aset.
b. Mengases kemungkinan terjadinya kegagalan keamanan yang realistik, berkenaan dengan ancaman dan kelemahan, dan dampak yang terkait dengan aset serta pengendalian yang diterapkan saat ini.
c. Memperkirakan tingkat risiko.
d. Menetapkan apakah risiko dapat diterima atau memerlukan perlakuan.

3. *Evaluasi Risiko*

Proses yang biasa digunakan untuk menentukan manajemen risiko dengan membandingkan tingkat risiko terhadap standar yang telah ditentukan, target tingkat risiko dan kriteria lainnya.

Penilaian dan evaluasi resiko meliputi kegiatan-kegiatan sebagai berikut:

a. Menentukan kritikalitas aset berdasarkan data aset TI yang telah diinvetarisasi.
b. Menentukan kriteria penilaian resiko yang terdiri dari kriteria dampak dan kecenderungan/probabilitas yang dituangkan dalam metodologi penilaian resiko.
c. Melaksanakan penilaian risiko yang terdiri dari kegiatan identifikasi, evaluasi, dan analisis risiko.
d. Menentukan rencana mitigasi risiko sebagai bagian dari proses penerapan SMKI dan meminimasi dampak dari risiko tersebut.
e. Menyusun suatu profil risiko yang menggambarkan kondisi keamanan informasi.

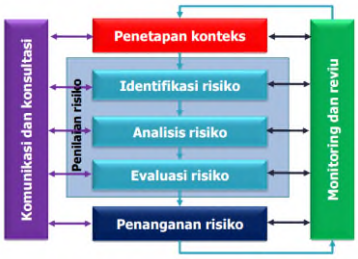
[1] https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms

4. Penanganan Risiko

Proses penanganan risiko yang mencakup identifikasi, evaluasi dan pengendalian risiko yang dapat mengancam kelangsungan usaha atau aktivitas perusahaan atau organisasi.

Jenis-jenis cara mengelola risiko, yang ditunjukkan juga pada Gambar 2:

a. Menghindari risiko (*risk avoidance*).
b. Berbagi risiko (*risk sharing/risk transfer*).
c. Mitigasi (*mitigation*).
d. Menerima risiko (*risk acceptance*).



Gambar 2 Tahapan *Risk Assesment* [5]

B. Teknologi Informasi

Teknologi Informasi adalah teknologi yang menggabungkan komputasi (komputer) dengan jalur komunikasi berkecepatan tinggi yang membawa data, suara, dan video [6].

Teknologi Informasi adalah salah satu alat yang digunakan para manajer untuk mengatasi perubahan yang terjadi. Dalam hal ini perubahan yang dimaksud adalah perubahan informasi yang sudah diproses dan dilakukan penyimpanan sebelumnya di dalam komputer [7].

Dari pengertian di atas, menurut penulis kesimpulan dari teknologi informasi adalah penggunaan alat atau perangkat (komputer) tertentu yang bisa membantu manusia untuk mengolah, mengorganisasikan data atau pesan untuk di sampaikan kepada objek yang dituju baik melalui jaringan komunikasi atau tidak menggunakan jaringan komunikasi.

C. Sistem Terintegrasi

Sistem terintegrasi akan menggabungkan komponen sub-sub sistem ke dalam satu sistem dan menjamin fungsi-fungsi dari sub sistem tersebut sebagai satu kesatuan sistem.

Ada beberapa metode yang dapat dipergunakan dalam membangun sistem terintegrasi, sebagaimana yang direferensikan berdasarkan artikel dari Wikipedia yaitu:

a. *Vertical Integration.*
b. *Star Integration.*
c. *Horizontal Integration*.

D. SNI ISO-IEC 27001-2009

SNI ISO/IEC 27001 [3] yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

Pendekatan proses mendorong pengguna menekankan pentingnya:

a. Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi.
b. Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan.
c. Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
d. Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.

Model *PLAN – DO – CHECK – ACT* (PDCA) diterapkan terhadap struktur keseluruhan proses SMKI. Dalam model PDCA, keseluruhan proses SMKI dapat dipetakan seperti Tabel 1.

TABEL 1 TABEL PETA PDCA DALAM PROSES SMKI

PLAN (Menetapkan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dan sasaran.
DO (Menerapkan dan mengoperasikan SMKI)	Menerapkan dan mengoperasikan kebijakan SMKI, kontrol, proses dan prosedur-prosedur.
CHECK (Memantau dan melakukan tinjau ulang SMKI)	Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya.
ACT (Memelihara dan meningkatkan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

Standar menyatakan persyaratan utama yang harus dipenuhi menyangkut:

a. Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi).
b. Tanggung jawab manajemen.
c. Audit internal SMKI.
d. Manajemen tinjau ulang SMKI.
e. Peningkatan berkelanjutan.

Disamping persyaratan utama di atas, standar ini mensyaratkan penetapan sasaran kontrol dan kontrol-kontrol keamanan informasi meliputi 11 area pengamanan sebagai berikut:

a. Kebijakan keamanan informasi.
b. Organisasi keamanan informasi.
c. Manajemen aset.
d. Sumber daya manusia menyangkut keamanan informasi.
e. Keamanan fisik dan lingkungan.
f. Komunikasi dan manajemen operasi.

g. Akses kontrol.
h. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi.
i. Pengelolaan insiden keamanan informasi.
j. Manajemen kelangsungan usaha (*business continuity management*).
k. Kepatuhan.

Dalam penelitian yang dilakukan penulis menitik beratkan pada bagaimana menganalisis risiko pada sistem informasi terintegrasi di lingkungan Universitas Telkom.

III. METODE PENELITIAN

Metodologi Penelitian Ilmiah [8] adalah cara memperoleh dan menyususun pengetahuan. Metodologi yang digunakan pada penelitian ini adalah mengunakan pedekatan kualitatif (*Interpretative Research*) dengan teknik pengumpulan data dan pengolahan data merujuk pada pendekatan *Prefers*, sebagai berikut:

a. Merumuskan masalah,
Pada penelitian ini penulis menitikberatkan pada masalah analisis risiko teknologi informasi pada sistem informasi iGracias di Universitas Telkom.
b. Menelaah kepustakaan,
Mempelajari sumber-sumber pustaka yang dapat berupa buku, *paper*, dan halaman-halaman web mengenai analisis risiko teknologi Informasi dan ISO SNI-IEC 27001-2009.
c. Merancang pendekatan penelitian,
Pendekatan yang diilakukan adalah menggunakan metoda *prefers* (2008) [9].
d. Mengumpulkan data,
Melibatkan seluruh pihak yang menggunakan teknologi informasi dan informasi pada sistem iGracias di Universitas Telkom dengan cara melakukan obeservasi dan wawancara terhadap pihak terkait serta diuji dengan cara triangulasi, yaitu pengecekan data dari berbagai sumber dengan berbagai cara, dan berbagai waktu. Proses uji data yang diperoleh ini tidak terlepas dari *credibility* (validitas internal), *transferability* (validitas eksternal), *Dependability* (reliabilitas), dan *confirmability* (obyektivitas), baik di lingkungan Universitas Telkom maupun berkaitan dengan kajian literatur yang digunakan.
e. Analisis data,
Menganalisis permasalahan dari hasil pengumpulan data sebelumnya yang berkaitan dengan objek penelitian yaitu keamanan data dan informasi pada sistem informasi iGracias di Universitas Telkom dan melakukan pemetaan terhadap SNI ISO/IEC 27001,
f. Menulis laporan,
Penulisan penelitian ini mengacu pada proses manajemen risiko sesuai pada Gambar 2.

IV. PEMBAHASAN

Tahapan proses penilaian risiko dibagai kedalam beberapa tahapan yaitu:

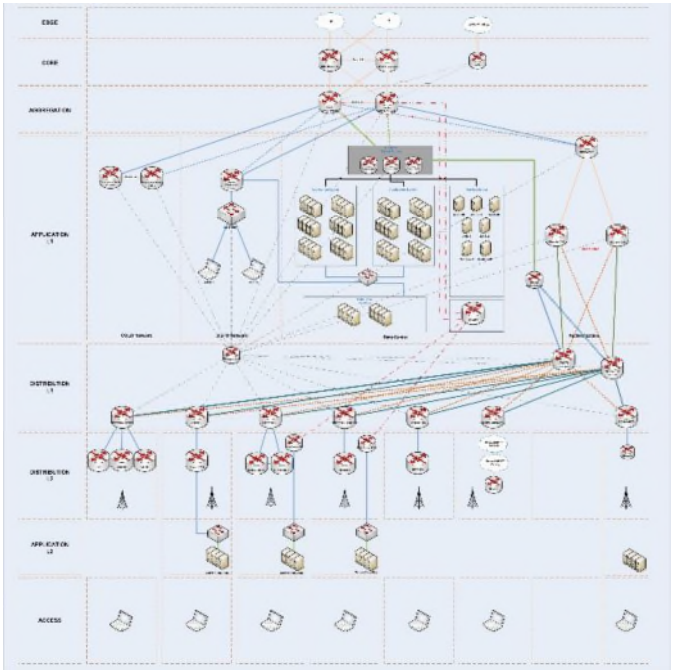
A. *Identifikasi Risiko*

Tahap identifikasi risiko [10] bertujuan untuk mengidentifikasi berbagai kemungkinan risiko yang muncul pada aset melalui proses studi literatur dan *interview* (wawancara). Proses ini dimulai dari mengidentifikasi berbagai kemungkinan risiko yang muncul pada teknologi dan infrastruktur sistem iGracias serta sistem informasi.

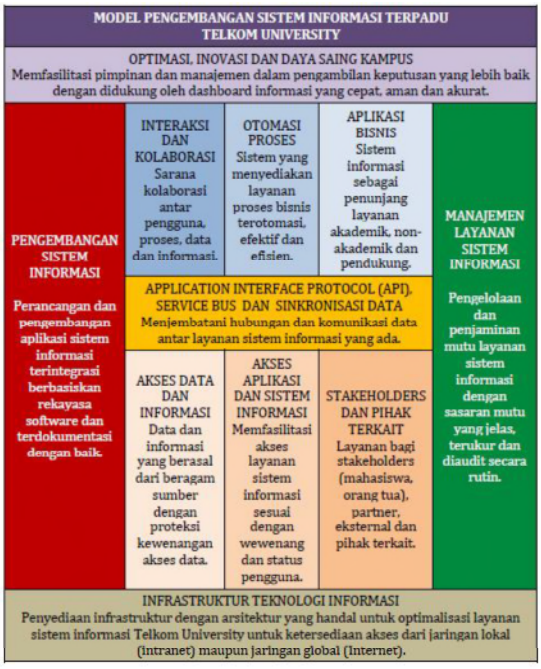
1. Mengidentifikasi aset dalam ruang lingkup SMKI dan pemilik-pemilik) aset.

Aset yang dimiliki oleh sistem terintegrasi Universitas Telkom terbagi ke dalam dua bagian, yang ditunjukkan pada Gambar 3-5.

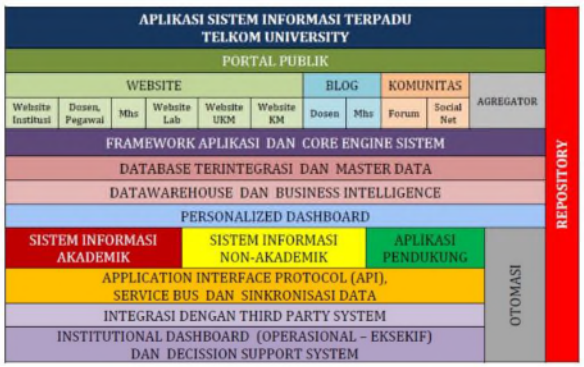
- Infrastruktur.
- Sistem informasi.



Gambar 3 Jaringan Infrastruktur Universitas Telkom



Gambar 4 Infrastruktur Teknologi Informasi



Gambar 5 Aplikasi Sistem Informasi Terpadu

2. SWOT

Sebagai analisis awal terhadap kondisi situasional yang ada di Universitas Telkom, dilakukan analisis untuk mengidentifikasi *strengths* (kekuatan), *weakness* (kelemahan), *opportunities* (peluang) dan *threats* (ancaman) yang berkaitan dengan pengembangan sistem informasi di Universitas Telkom [11].

1. *Strengths* (Kekuatan)
   a. Memiliki master data terintegrasi yang dibangun sendiri oleh Direktorat Sistem Informasi (*in-house development*) sebagai acuan sistem basis data untuk seluruh layanan sistem informasi yang digunakan di Universitas Telkom.
   b. Memiliki *framework* sistem informasi terintegrasi yang berbasis master data, yang dikembangkan secara sendiri oleh Direktorat Sistem Informasi (*in-house development*).
   c. Memiliki aplikasi sistem informasi terintegrasi yang menggunakan sistem *Single Sign On* (SSO) yang memungkinkan dapat diaksesnya seluruh aplikasi sistem informasi dari satu portal.
   d. Sistem informasi iGracias telah teruji dan digunakan oleh seluruh sivitas akademik Universitas Telkom untuk mendukung proses bisnis yang dijalankan.
   e. Sistem Informasi dibangun secara *in-house development* sehingga fleksibel dalam pengembangan, tidak tergantung pada pihak eksternal dan terdokumentasi dengan lengkap.
   f. Memiliki infrastruktur *data center* yang terdiri dari *main data center* dan *collocation data center* yang berada di Universitas Telkom, serta *backup data center* yang berada di dua lokasi terpisah.
   g. Memiliki infrastruktur jaringan *gigabit intranet* yang menghubungkan seluruh gedung menggunakan kabel *fiber optic* dan terkoneksi dengan *data center,* serta interkoneksi dengan jaringan internet melalui dua jalur *fiber optic*.
   h. Memiliki tim dan personel yang cukup memadai dengan kompetensi yang berbeda-beda sesuai dengan bidang layanan dan unit lokasi kerja, serta dukungan struktur organisasi yang memadai.

2. *Weakness* (Kelemahan)
   a. Aplikasi sistem informasi terintegrasi yang telah selesai dibangun dan telah dioperasikan, beberapa di antaranya masih memerlukan pemahaman dan penguasaan dalam penggunaannya oleh pemilik proses di Universitas Telkom.
   b. Pengguna belum memiliki keseragaman pemahaman dalam metode dan prosedur pengembangan sistem informasi terpadu.
   c. Proses bisnis, prosedur, instruksi kerja dan/atau ketetapan yang teridentifikasi oleh unit satuan mutu belum siap pakai sebagai acuan pengembangan aplikasi sistem informasi, sehingga menghambat proses identifikasi dan analisis kebutuhan aplikasi sistem informasi.
   d. Keterbatasan anggaran investasi dan operasional yang mengharuskan optimalisasi.
   e. Kecepatan proses logistik yang belum sepenuhnya mendukung pengadaan perangkat teknologi informasi untuk mendukung investasi maupun operasional yang dibutuhkan oleh Universitas Telkom.
   f. Ketidakpastian jenjang karir sumber daya manusia dan tingginya *turn over* pegawai alih-daya, khususnya bagi pranata layanan TIK di Direktorat Sistem Informasi Universitas Telkom.
   g. Belum adanya standard remunerasi yang sesuai dengan tugas dan tanggung jawab sumber daya manusia pengelola TIK.
   h. Belum terimplementasikannya tata kelola layanan sistem informasi yang berbasiskan standard *Information Technology Service Management* (ITSM).

3. *Opportunities* (Peluang)
   a. Pengembangan Direktorat Sistem Informasi Universitas Telkom tidak hanya sebagai unit *cost center*, namun berkembang menjadi unit *profit center*.
   b. Pendapatan *non-tuition fee* (NTF) jika aplikasi sistem informasi terpadu yang telah dibangun, dapat dipaketkan dan digunakan oleh institusi lain.
   c. Sinergi dengan program studi dan fakultas untuk menjalankan *join research* yang terkait dengan pengembangan sistem informasi di Universitas Telkom.
   d. Sinergi dengan lembaga pendidikan lain di bawah Telkom Foundation untuk implementasi sistem informasi terpadu dalam ruang lingkup yang lebih luas.
   e. Peningkatan peran sistem informasi Universitas Telkom yang didukung dengan kebijakan teknologi informasi dan sistem informasi di Universitas Telkom, untuk meningkatkan fungsi layanan sistem informasi sebagai *enabler* bagi Universitas Telkom, sesuai dengan pernyataan visi Universitas Telkom.

4. *Threat* (Ancaman)
   a. Ketidakpastian jenjang karir sumber daya manusia pengelola layanan TIK Direktorat Sistem Informasi Universitas Telkom dan rendahnya standar remunerasi, yang menyebabkan tingginya *turn over* pegawai.
   b. Ketidakpastian atas ketetapan dan ketersediaan anggaran investasi maupun operasional Direktorat Sistem Informasi Universitas Telkom, yang menyebabkan terhambatnya proses pengadaan dan penyediaan layanan teknologi infromasi dan sistem informasi.

c. Perbedaan cara pandangan dari unit/program studi/fakultas maupun personel struktural yang berkaitan dengan strategi pengelolaan dan pengembangan sistem informasi.

Selain data SWOT diperoleh data lain untuk mendukung penelitian ini dilakukan wawancara dengan pihak terkait dan studi literatur. Dari identifikasi data yang diperoleh dihasilkan dari hasil di bawah ini dengan mengacu pada:

1. *Vulnerability.*
2. *Threat.*
3. *Tools* atau metode [10] untuk penilaian kerentanan:
   a. *Automated vulnerability scanning tool*
   b. *Security testing and evaluation*
   c. *Penetration testing*
   d. *Code review*
   e. *Interview people and users*
   f. *Questionnaires*
   g. *Physical inspection*
   h. *Document analysis*

Pada Tabel 2 ditunjukkan tentang identifikasi risiko berdasarkan sumber-sumber risiko.

TABEL 2 IDENTIFIKASI RISIKO

Sumber Risiko	Risiko	*Vulnerability* (V) *or Threat* (T)		ID *Risk*
Alam	Kebakaran		T	1
	Gempa bumi		T	2
	Kebanjiran		T	3
	Badai		T	4
	Petir		T	5
	Gunung meletus		T	6
	Bangunan roboh		T	7
Manusia	Pencurian		T	8
	Human error		T	9
	Hacking		T	10
	Cracking		T	11
	Kebocoran data atau informasi internal perusahaan / institusi	V		12
	Pelanggaran hak akses *user ID*		T	13
	Data loss		T	14
	Bekas karyawan/dosen/ mahasiswa yang masih memiliki akses	V		15
	Akses fisik tidak sesuai dengan fungsi dan tanggung jawab	V		16
	Staff/unit yang memiliki akses meyalahgunakan aksesnya	V		17
	Cybercrime		T	18
	Cybervandalism		T	19
	Pemahaman penggunaan aplikasi	V		20
	Ketidakjelasan jenjang karir	V		21
	High turnover staff SISFO		T	22
	Perbedaan cara berfikir mengenai sistem	V		23
Teknologi Informasi dan Infrastruktur	Kerusakan perangkat / *Hardware*		T	24
	Misconfiguration	V		25
	Teknologi *absolut*	V		26
	Database sistem *crash/down*		T	27
	Application server down		T	28
	Masalah jaringan kelistrikan		T	29
	Bentrok pengalamatan jaringan	V		30
	Overcapacity network	V		31
	Sign on failure		T	32
	Virus	V		33
	Routing table	V		34
	Unprotected storage	V		35
	Ketersediaan Anggaran	V		36
	Tidak berjalannya rencana update teknologi		T	37
Sistem Informasi	Kerusakan perangkat lunak			38
	Malfunction perangkat lunak		T	39
	Malfunction sistem operasi		T	40
	Gagal *update*		T	41
	Backup failure		T	42
	Overload		T	43
	Overcapacity data		T	44
	Software malfunction		T	45
	Lack of efficient configuration change control	V		46
	Complicated user interface	V		47
	Network down		T	48

B. Analisis Risiko

Proses ini mencakup cara melihat potensial terjadinya seberapa besar *severity* (kerusakan) dan probabilitas terjadinya risiko tersebut (*like hood*). Penentuan probabilitas terjadinya suatu *event* sangatlah subyektif dan lebih berdasarkan nalar dan pengalaman. Data penilaian menggunakan teknik wawancara dengan pihak terkait yang berhubungan langsung dengan sistem terintegrasi iGracias.

Risk Assessment dengan metode kualitatif dinyatakan dengan hubungan antara dampak yang ditimbulkan oleh suatu hazard (*qonsequence*) dengan kemungkinan kejadian *hazard* di masa yang akan datang (*likelihood*), yang ditampilkan dalam sebuah *Risk Matrix* atau *Risk Ranking*. Indikator *consequence* diekspresikan dengan istilah kualitatif seperti *low, moderate*, *high* dan *extreme*, sedangkan *likelihood* diekspresikan dengan istilah *unlikely*, *possible, likely,* dan *very likely*.

1. Consequence

Consequence [12] merupakan dampak dari suatu *hazard* diekspresikan dalam beberapa aspek risiko seperti kemungkinan kehilangan/kerugian (*potential loss*) atau ketidakpastian/kemungkinan kejadian pada periode tertentu (*uncertainty/probability as well as period of time*). Pada penelitian ini pembagian kriteria *consequence* diltunjukkan pada Tabel 3.

TABEL 3 *CONSEQUENCE*

Rank	*Description*	*Criteria*
1	*Very Low*	*2% likely to happen or a one in fifty chance → Temporary Relocation*
2	*Low*	*5% likely to happen or a one in twenty chance → Closure a few days*
3	*Medium*	*10% likely to happen or a one in ten chance*

Rank	*Description*	*Criteria*
4	*High*	*20% likely to happen or a one in five chance or loss of 50% Capability*
5	*Very High*	*50% or over or a one in two chance or more likely to happen than not → long term disruption*

2. Likelihood

Likelihood [12] dinyatakan dalam kemungkinan kejadian di masa yang akan datang, dan *scoring*, kemudian dikategorikan dalam *rare, unlikely, possible, probable,* dan *high probable*, dengan uraian penjelasan pada Tabel 4.

TABEL 4 *LIKELIHOOD*

Level	***Descriptor***	**Menunjukkan Kesempatan yang Akurat dalam Waktu 5 Tahun**	***Description***
1	*Rare*	1% or less	Dapat terjadi hanya dalam keadaan luar biasa, mungkin terjadi sekali setiap lima tahunan atau lebih
2	*Unlikely*	2%-25%	Tidak diharapkan terjadi, dan/atau tidak ada insiden rekaman bukti masalah, dan/atau tidak ada insiden baru-baru ini di organisasi terkait fasilitas atau masyarakat, dan/atau sedikit kesempatan, alasan, atau sarana untuk terjadi, mungkin terjadi sekali setiap satu sampai lima tahun
3	*Possible*	26%-50%	Mungkin terjadi pada beberapa waktu , dan/atau beberapa, jarang, insiden acak direkam atau bukti masalah kecil, dan/atau sangat sedikit insiden dalam organisasi, fasilitas, atau masyarakat terkait atau sebanding; dan/atau beberapa kesempatan, alasan atau berarti terjadi; mungkin terjadi sekali dalam 2 tahun.
4	*Probable*	51%-75%	Mungkin atau dapat terjadi/berulang setiap tahun; insidendirekam biasa atau bukti masalah yang kuat dan mungkin terjadi dalam banyak situasi
5	*High Probable*	76%-100%	Mungkin atau dapat terjadi/berulang setiap 5 tahun atau kurang; tingkat tinggi insiden dicatat dan/atau bukti yang kuat masalah

3. Risk Matrix

Kemudian tahap berikutnya adalah membuat *Risk Matrix* dengan memetakan *likelihood* dan qonsequence dengan *range score* yang disepakati, seperti yang ditunjukkan pada Tabel 5.

TABEL 5 *RISK MATRIX*

Impact	*Likelihood*				
	Rare	*Unlikely*	*Possible*	*Probable*	*High Probable*
Major	L	M	H	H	Vh
Moderate	L	M	M	H	Vh
Minor	Vl	L	M	H	H
Insignificant	Vl	Vl	L	M	H

Vl = *Very Low*
L = *Low*
M = *Medium*
H = *High*
Vh = *Very High*

C. Evaluasi Risiko

Tujuan dari evaluasi risiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Untuk menentukan peringkat risiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan pemetaan matrik risiko dalam Tabel 6.

TABEL 6 PEMETAAN RSK MATRIX TERHADAP RISIKO

Impact	**Likelihood**				
	Rare	**Unlikely**	**Possible**	**Probable**	**High Probable**
Major	3	12,24,25	14,40	31,38,39, 41,42,33	Vh
Moderate	15	9	10,11,13, 22,29,30	16,32,26	27
Minor	1	7	17,20,21, 23,26	34,35	37
Insignificant	2,4,6	5	8,47	18,19,45, 46	43,55

Dari hasil pemetaan pada Tabel 6 diperoleh nilai risiko paling tinggi adalah untuk *server down* dan *database down*. Diluar itu tersebar dalam skala lebih rendah.

TABEL 7 LEVEL RISIKO DENGAN ASET YANG TERKAIT

Level Risiko	**Risiko**	**Nama Aset**
Very Low	Kebakaran	*Data Center*
	Gempa bumi	*Data Center*
	Badai	*Data Center*
	Petir	*Data Center*
	Gunung meletus	*Data Center*
Low	Kebanjiran	*Data Center*
	Bangunan roboh	*Data Center*
	Pencurian	*Hardware*
	Bekas karyawan/dosen/mahasiswa yang masih memiliki akses	Aplikasi
	Complicated user interface	Aplikasi
Medium	*Human error*	Aplikasi, *Database*
	Hacking	Aplikasi, *Database*

Level Risiko	Risiko	Nama Aset
	Cracking	Aplikasi, *Database*
	Kebocoran data atau informasi internal perusahaan / institusi	Aplikasi, *Database*
	Pelanggaran hak akses *user ID*	Aplikasi, *Database*
	Staff/unit yang memiliki akses meyalahgunakan aksesnya	Aplikasi, *Database*
	Cybercrime	Aplikasi, *Database*
	Cyber vandalism	Aplikasi, *Database*
	Pemahaman penggunaan aplikasi	Aplikasi, *Database*
	Ketidakjelasan jenjang karir	
	High turnover staff sisfo	
	Perbedaan cara berfikir mengenai sistem	Aplikasi, *Database*
	Kerusakan perangkat / *Hardware*	*Hardware*
	Misconfiguration	*Network*
	Teknologi *absolute*	*Hardware, Software*
	Masalah jaringan kelistrikan	*Network, Data center*, Aplikasi
	Bentrok pengalamatan jaringan	*Network*
	Software malfunction	Aplikasi, *Database*
	Lack of efficient configuration change control	*Network*, Aplikasi
High	*Data loss*	Aplikasi, *Database*
	Akses fisik tidak sesuai dengan fungsi dan tanggung jawab	*Hardware, Data Center, Network*
	Overcapacity network	*Network*
	Sign on failure	*Network*, Aplikasi
	Virus	*Network*, Aplikasi
	Routing table	*Network*
	Unprotected storage	*Data Center*
	Ketersediaan anggaran	*Network, Hardware, Software*
	Tidak berjalannya rencana *update* teknologi	*Hardware, Software*
	Kerusakan perangkat lunak	*Software*, Aplikasi
	Malfunction perangkat lunak	*Software*, Aplikasi
	Malfunction sistem operasi	*Software*, Aplikasi
	Gagal *update*	*Software*, Aplikasi
	Backup failure	*Database*, Aplikasi
	Overload	*Database*, Aplikasi
	Overcapacity data	*Database*, Aplikasi
Very High	*Database* sistem *crash/down*	*Database*, Aplikasi
	Application server down	*Network, Data center*, Aplikasi, *Database*
	Network down	*Network*, Aplikasi, *Database*

D. Penanganan Risiko

Dalam uraian sebelumnya penanganan risiko dilakuakn dengan beberapa cara, dalam penelitian ini penulis memfokuskan pada risiko yang memiliki level *Very High* Penanganan risiko difokuskan pada risiko-risiko yang berada pada *Level Very High* yaitu *Database Server Down, Server Down* dan *Network Down*.

Database server down berdampak pada seluruh layanan iGracias yang tidak dapat berjalan/diakses.

Application server down, *server* aplikasi dan *database* di dalam sistem iGracias dibuat terpisah, sehingga saat aplikasi *server*nya lumpuh maka akan berdampak pada layanan informasi secara keseluruhan.

Network Down, semua sistem terintegrasi iGracias berjalan di atas jaringan infrastruktur terintegrasi, apabila sistem jaringanya *down* maka yang terjadi semua aktivitas dan layanan informasi bahkan komunikasi antar pengguna dapat terhenti.

Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika risiko tersebut terjadi.

Dalam mengambil langkah-langkah untuk menangani risiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini:

1. Apa pemicu terjadinya *database*, *application server* dan network *down* pada sistem iGracias?
2. Seberapa sering *database*, application *server* dan network *down* tersebut terjadi pada sistem iGracias?
3. Kapan biasanya *database*, application *server* dan network *down* paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya risiko *database server down* antara lain:

1. *Overheat,*
2. *Overcapacity,*
3. *Overload,*
4. Tingginya jumlah user dalam satu waktu,
5. *Virus.*

Database, *application server* dan network *down* biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki kejadian tertentu seperti pada saat registrasi mata kuliah, registrasi geladi, *input* nilai, perwalian, penerimaan mahasiswa baru. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja *server* dan jaringan semakin bertambah dan dapat memicu terjadinya *server*/jaringan *down*.

Penanganan yang memungkinan adalah dengan mengusulkan membangun sistem yang dapat menjaga *availability* dan performansi sistem jaringan maupun layanan informasi dengan membangun beberapa hal di bawah ini:

1. *High Performance Computing.*
2. Menambah atau memperbaharui sistem pendingin pada *Data Center*.
3. Sistem Jaringan *cluster.*

4. Membangun sistem *server* yang berisi aplikasi deteksi serangan (*virus*) yang terpisah dari sistem utama.

V. SIMPULAN DAN SARAN

Berdasarkan hasil analisis risiko yang dilakukan pada penelitian ini dapat disimpulkan bahwa:

1. Dari hasil penelitian ini seluruh proses pada analisis risiko dengan mengacu pada ISO SNI-IEC 27001-2009 diperoleh tingkatan risiko pada sistem iGracias. Risiko yang berada pada level tinggi adalah risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem iGracias, risiko yang memiliki nilai risiko paling tinggi adalah *database*, *application server* dan *network down* yang ditimbulkan apabila risiko tersebut terjadi adalah seluruh layanan iGracias tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap risiko tersebut.
2. Dari hasil temuan dengan adanya tingkat risiko yang mungkin muncul diusulkan beberapa alternatif teknologi yang bisa memperkecil risiko yang muncul.

Adapun saran dari penulisan ini adalah:

1. Perlu di kaji kembali risiko yang ada pada level *high* agar menjadi prioritas untuk mengurangi terjadinya risiko yang lebih merugikan pada sistem iGracias.
2. Diharapakan apa yang sudah di kaji dalam penelitian ini dapat menjadi masukan untuk penelitian berikutnya terkait dengan risiko.

DAFTAR PUSTAKA

[1] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann and P. Sommerlad, Security Patterns:Integrating Security and Systems Engineering, John Wiley & Sons Ltd, 2006.

[2] R. M. Wideman and P. Fellow, Project and Program Risk Management; A Guided to Managing Project and Opportunities, USA: Project Management Institute, 1992.

[3] "ISO 73:2009; Risk management — Vocabulary — Guidelines for use in standards," 13 November 2015. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

[4] "http://www2.mitre.org," [Online]. Available: http://www2.mitre.org/work/sepo/toolkits/risk/compliance/files/RiskProcessGuidelines.doc.

[5] "BS ISO/IEC 27005-2008," British Standard, United Kingdom, 2008.

[6] . B. Williams and S. Sawyer, Using Information Technology 11th Edition, McGraw-Hill Education, February 4, 2014.

[7] . K. C. Laudon, Management Information Systems: Managing the Digital Firm (14th Edition) 14th Edition, Prentice Hall, January 15, 2015.

[8] P. Suryana, M.Si, METODOLOGI PENELITIAN, Model Prakatis Penelitian Kuantitatif dan Kualitatif, Universitas Pendidikan Indonesia, 2010.

[9] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems,* vol. Volume 24 , no. Issue 3, pp. pp. 45-78., 2007.

[10] D. J. Landoll, The Security Risk Assesment Handbook; A Complete Guide for Performing Risk Assesments, New york: Aurbach Publications; Taylor & Francis Group, 2006.

[11] D. S. I. *Rencana Strategis Sistem Informasi Universitas Telkom Periode 2014-2018 - Direktorat Sistem Informasi Telkom University - Revisi Juni 2015,* Bandung, 2014.

[12] M. E. Whitman and H. J. Mattord, Management of Information Security 3rd Edition, USA, 2010.