# Analisis Risiko Teknologi Informasi Berbasis *Risk Management* Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University)

## *Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study* : i-Gracias Telkom University*)*

Andi Novia Rilyani[1]. Yanuar Firdaus A W ST., MT[2], Dawam Dwi Jatmiko ST., MT[3]
Departemen Teknik Informatika, Universitas Telkom
Jalan Telekomunikasi No.1, Dayeuhkolot Bandung 42057 Indonesia
[1]novia.rilyani@gmail.com, [2]yanuar@telkomuniversity.ac.id, [3]dawamdjs@telkomuniversity.ac.id

**Abstrak**

Sistem Informasi pada Direktorat SISFO merupakan salah satu sistem terintegrasi yang menjadi media penghubung antara civitas akademik. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. 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.

Untuk itu, perlu dilakukan analisis risiko terhadap berbagai kemungkinan risiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan risiko yang muncul pada aset tersebut. Analisis Risiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem i-Gracias.

Dari hasil penelitian didapatkan Nilai Prioritas Risiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap risiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas risiko.

**Kata Kunci** : Direktorat SISFO, ISO 31000, Manajemen Risiko, *Risk Management*, Sistem Informasi, Sistem, i-Gracias.

**Abstract**

Information System on Direktorat SISFO is one of integration system that connects between academic stakeholders. Every activities inside the system is a crucial thing to execute. The availability is the main priority to support the system to work. But, the possibility of having risk and threat will crash the system from any part, one of them is caused by information technology.

It is necessary to analyze the risks that possibly appear to crash the system. According to the result of the analyzing, it shows the result about the physical assets with its own risks. Information Technology Risk Analysis based on Risk Management using ISO 31000 focus on hardware and network infrastructure for i-Gracias System.

The research purposes is to get the Risk Priority Value based on the measurement process to all identified risk and analyzed. So that in the future, the organization will be able to prevent, handle and fix everything based on the risk priority level.

**Keyword** : Direktorat Sisfo, ISO 31000, Risk Management, Information System, System, i-Gracias.

## 1. Pendahuluan

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna.

Direktorat SISFO Telkom University merupakan salah satu lembaga pendidikan yang telah menerapkan dan mengembangkan sistem informasi dengan melibatkan teknologi informasi di dalamnya, salah satu karya Direktorat SISFO adalah *Integrated Academic Information System* atau sering disebut dengan i-Gracias. i-Gracias merupakan aplikasi akademik untuk mahasiswa, dosen, maupun

pegawai untuk semua Fakultas di lingkungan Telkom University. i-Gracias merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di Telkom University. Oleh sebab itu, kehadiran i-Gracias dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat i-Gracias harus tetap berjalan baik dan konsisten.

Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan risiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis risiko terhadap kemungkinan ancaman dan risiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan risiko tersebut.

Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan risiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai risiko yang diperoleh dari proses pengukuran tingkat risiko untuk tiap-tiap risiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Risiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem i-Gracias.

### 1.2 Perumusan Masalah

Permasalahan yang akan diselesaikan dalam Tugas Akhir ini adalah :

1. Bagaimana analisis risiko teknologi informasi terhadap sistem i-Gracias menggunakan iso 31000?
2. Bagaimana tingkat risiko teknologi informasi i-Gracias saat ini dan seperti apa perlakuan risiko yang diberikan?

### 1.3 Tujuan

Tujuan yang ingin dicapai dalam penelitian Tugas Akhir ini adalah :

1. Melakukan tahapan dan proses analisis risiko teknologi informasi berbasis risk management sesuai dengan standar dan kerangka kerja ISO 31000.
2. Mengetahui tingkat risiko teknologi informasi i-Gracias saat ini serta perlakuan risiko yang diberikan.

## 2. Tinjauan Pustaka

2.1 Manajemen Risiko

Manajemen risiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman; suatu rangkaian aktivitas manusia termasuk: penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan/ pengelolaan sumberdaya.

Strategi yang dapat diambil antara lain adalah memindahkan risiko kepada pihak lain, menghindari risiko, mengurangi efek negatif risiko, dan menampung sebagian atau semua konsekuensi risiko tertentu. Manajemen risiko tradisional terfokus pada risiko-risiko yang timbul oleh penyebab fisik atau legal (seperti bencana alam atau kebakaran, kematian, serta tuntutan hukum. [3]

Manajemen risiko dapat diterapkan ke seluruh organisasi, pada keseluruhan area kegiatan dan pada setiap tingkatan, setiap saat, baik pada suatu fungsi khusus, proyek, proses maupun suatu kegiatan. Adapun sasaran dan tujuan pelaksanaan manajemen risiko adalah untuk mengurangi risiko yang mungkin akan muncul (ancaman), mengukur dampak dari potensi ancaman, menentukan berapa besar kerugian yang diderita akibat hilangnya potensi bisnis. Ancaman ini bisa disebabkan oleh berbagai elemen seperti teknologi, human error, lingkungan, politik maupun dari organisasi.

Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga kita dapat memperoleh hasil yang optimal. Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini : [5]

1. **Identifikasi Risiko**
   Proses ini meliputi identifikasi risiko yang mungkin terjadi dalam suatu aktivitas usaha. Identifikasi risiko secara akurat dan komplet sangatlah vital dalam manajemen risiko. Salah satu aspek penting dalam identifikasi risiko adalah mendaftar risiko yang mungkin terjadi sebanyak mungkin. Teknik-teknik yang dapat digunakan dalam identifikasi risiko antara lain:
   a) Brainstorming
   b) Survei
   c) Wawancara
   d) Informasi historis
   e) Kelompok kerja, dll

2. **Analisis Risiko**
   Setelah melakukan identifikasi risiko, maka tahap berikutnya adalah pengukuran risiko dengan cara melihat potensial terjadinya seberapa besar severity (kerusakan) dan probabilitas terjadinya risiko tersebut. Penentuan probabilitas terjadinya suatu event sangatlah subyektif dan lebih berdasarkan nalar dan pengalaman. Beberapa risiko memang mudah untuk diukur, namun sangatlah sulit untuk memastikan probabilitas suatu kejadian yang sangat jarang terjadi. Sehingga, pada tahap ini sangatlah penting untuk menentukan dugaan yang terbaik supaya nantinya kita dapat memprioritaskan dengan baik dalam implementasi perencanaan manajemen risiko. Kesulitan dalam

pengukuran risiko adalah menentukan kemungkinan terjadi suatu risiko karena informasi statistik tidak selalu tersedia untuk beberapa risiko tertentu. Selain itu, mengevaluasi dampak severity (kerusakan) seringkali cukup sulit untuk asset immaterial. Hasil akhir dari analisis risiko adalah penentuan risiko (contoh: tingkat bahaya dan kemungkinan dari bahaya yang terjadi).

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.
   Tujuan Evaluasi yaitu :
   - Mengetahui yang memiliki tingkat prioritas tertinggi hingga terendah.
   - Menentukan risiko mana yang ditindaklanjuti dengan penanganan dan risiko mana saja yang hanya perlu dipantau.

4. **Pengelolaan Risiko**
   Jenis-jenis cara mengelola risiko :
   a. Menghindari risiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan risiko tersebut.
   b. Berbagi risiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya risiko atau dampak risiko.
   c. Mitigasi (mitigation), yaitu melakukan perlakuan risiko untuk mengurangi kemungkinan timbulnya risiko, atau mengurangi dampak risiko bila terjadi, atau mengurangi keduanya.
   d. Menerima risiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap risiko tersebut.

### 2.2 Teknologi informasi

Tekonologi Informasi (Information Technology) biasa disingkat TI, IT atau infotech. Dalam Oxford English Dictionary (OED2) edisi ke-2 mendefinisikan teknologi informasi adalah hardware dan software, dan bisa termasuk di dalamnya jaringan dan telekomunikasi yang biasanya dalam konteks bisnis atau usaha.
Secara singkat, istilah Teknologi Informasi juga dapat disimpulkan sebagai teknologi yang memanfaatkan komputer sebagai perangkat utama dalam mengolah data menjadi informasi yang bermanfaat.

### 2.3 Sistem Informasi

Secara umum Sistem informasi dapat didefinisikan sebagai suatu sistem di dalam suatu organisasi yang merupakan kombinasi dari orang-orang, fasilitas, teknologi, media prosedur-prosedur dan pengendalian yang ditujukan untuk mendapatkan jalur komunikasi penting, memproses tipe transaksi rutin tertentu, memberi sinyal kepada manajemen dan yang lainnya terhadap kejadian-kejadian internal dan eksternal yang penting dan menyediakan suatu dasar informasi untuk pengambilan keputusan. [10]

### 2.4 ISO 31000

ISO 31000 adalah suatu standar implementasi manajemen risiko yang diterbitkan oleh International Organization for Standardization pada tanggal 13 November 2009.

#### 2.4.1 Lingkup Penerapan ISO 31000

Standar international ini menyediakan prinsip dan panduan generik untuk penerapan manajemen risiko. Standar ini dapat digunakan untuk organisasi, perusahaan publik, perusahaan swasta, organisasi nirlaba, kelompok, ataupun perorangan. Oleh karena itu, standar ini bersifat generic dan tidak spesifik bagi industri atau sektor tertentu. Standar ini dapat digunakan selama masa hidup organisasi dan untuk berbagai kegiatan, proses, fungsi, proyek, produk, jasa, aset, operasi, dan pengambilan keputusan.
Walau standar ini menyediakan panduan generik, hal ini tidak dimaksudkan untuk membuat keseragaman penerapan manajemen risiko pada semua organisasi. Perencanaan dan penerapan manajemen risiko akan tergantung pada kebutuhan yang bervariasi dari setiap organisasi, khususnya sasaran dari setiap organisasi yang berbeda, konteks, struktur, produk, jasa, proyek, dan proses operasi, serta praktik-praktik khas yang digunakan.

Standar international ini bertujuan untuk melakukan harmonisasi proses manajemen risiko dalam berbagai macam standar yang sudah ada saat ini atau yang nantinya akan dibuat. Standar ini menyediakan pendekatan yang umum dan mendasar, sehingga dalam menangani risiko-risiko yang khas atau risiko pada bidang/sektor industri tertentu, tidak usah menggantinya dengan standar lain.

ISO 31000 telah menyediakan prinsip dan pedoman umum manajemen risiko. ISO 31000:2009, Manajemen Risiko - Prinsip dan pedoman, memberikan prinsip, kerangka kerja dan proses untuk mengelola risiko. Hal ini dapat digunakan oleh setiap organisasi terlepas dari ukurannya, kegiatan atau sektor. Menggunakan ISO 31000 dapat membantu organisasi meningkatkan kemungkinan mencapai tujuan, meningkatkan

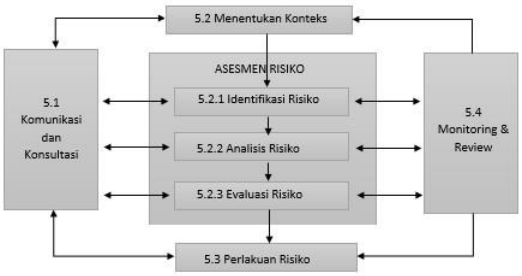
identifikasi peluang dan ancaman serta efektif dalam mengalokasikan dan menggunakan sumber daya untuk penanganan risiko [14]. ISO 31000 dapat diterapkan untuk semua jenis risiko, apapun sifatnya apakah positif atau negatif yang memiliki konsekuensi. Standar ini didukung oleh [15] :

- International Standard ISO/IEC 31010:2009–Risk Management.
- IEC/FDIS 31010 Risk Management–Risk Assessment Techniques and
- ISO Guide 73:2009–Risk Management–Vocabulary

## 3. Metode Penelitian

### 3.1 Proses Manajemen Risiko

Manajemen risiko adalah suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehinga dapat memperoleh hasil yang optimal. Proses manajemen risiko meliputi lima kegiatan, yaitu komunikasi dan konsultasi; menentukan konteks; asesmen risiko; perlakuan risiko; serta *monitoring* dan *review*. Proses manajemen risiko dapat ditunjukkan pada gambar di bawah ini.




Gambar 3.1 Proses Manajemen Risiko

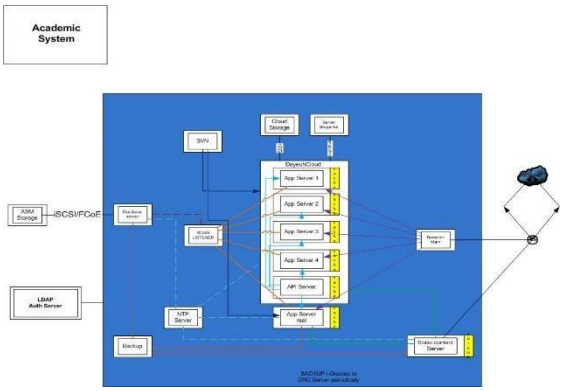
## 4. Pembahasan

### 4.1 Penilaian Risiko

Pada Penilaian risiko terdapat beberapa tahapan yang harus dilakukan antara lain :

#### 4.1.1 Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem i-Gracias dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait. Gambar di bawah ini merupakan mapping infrastruktur sistem i-Gracias.




Gambar 4. 1 Mapping Infrastruktur sistem i-Gracias

#### 4.1.1.2 Identifikasi Risiko

Tahap Identifikasi risiko bertujuan untuk mengidentifikasi berbagai kemungkinan risiko yang muncul pada aset melalui proses *studi literature* dan *interview*. Proses ini dimulai dari mengidentifikasi berbagai kemungkinan risiko yang muncul pada teknologi dan infrastruktur sistem i-Gracias. Setelah diperoleh daftar risiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari risiko tersebut.

Tabel 4.1 Identifikasi Risiko

| Sumber Risiko | Risiko |
|---|---|
| Alam / Lingkungan | Kebakaran |
| | Banjir |
| | Gempa bumi |
| | Petir |
| | Badai |
| | Embun |
| | Radiasi panas |
| | Suhu yang bervariasi |
| | Debu / kotoran |
| | Kelembaban |
| Manusia | Pencurian perangkat |
| | Informasi diakses oleh pihak yang tidak berwenang |
| | Kebocoran data atau informasi internal perusahaan / institusi |
| | Data dan informasi tidak sesuai fakta |
| | Penyalahgunaan hak akses / User ID |
| | Mantan user / karyawan masih memiliki akses informasi |
| | Akses fisik yang tidak terotorisasi |
| | Hilangnya data |
| | Human error |
| | Risiko kerusakan akibat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism |

| | |
|---|---|
| Sistem dan Infrastruktur | Kegagalan / kerusakan hardware |
| | Server down |
| | Overheat |
| | Koneksi jaringan terputus |
| | Sistem crash |
| | Overcapacity |
| | Overload |
| | Data corrupt |
| | Backup failure |
| | Gagal update |
| | Kurang baiknya kualitas jaringan |
| | Teknologi usang |
| | Risiko kerusakan akibat masalah catudaya / tegangan listrik |

**4.1.1.3 Analisis Risiko**

Analisis risiko adalah upaya untuk memahami risiko lebih dalam. Hasil analisis risiko ini akan menjadi masukan bagi evaluasi risiko dan proses pengambilan keputusan mengenai perlakuan risiko terhadap risiko tersebut. Analisis risiko meninjau dua aspek risiko, yaitu dampak dan kemungkinan. Tingkat risiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis risiko ini dilakukan penilaian terhadap risiko-risiko yang muncul pada sistem i-Gracias. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu risiko terjadi, serta kemungkinan terjadinya risiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

**4.1.1.3.1 Kuisioner**

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden dengan menggunakan kriteria yang telah ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu risiko terjadi, serta kemungkinan terjadinya risiko *(likelihood)* pada Teknologi dan Infrastruktur i-Gracias.

Tabel 3.1 Pilihan jawaban untuk kriteria kemungkinan

| Jawaban | Singkatan | Nilai |
|---|---|---|
| Sangat Kecil | SK | 1 |
| Kecil | K | 2 |
| Sedang | S | 3 |
| Besar | B | 4 |
| Sangat Besar | SB | 5 |

Tabel 3.2 Pilihan jawaban untuk kriteria dampak

| Jawaban | Singkatan | Nilai |
|---|---|---|
| Sangat Ringan | SR | 1 |
| Ringan | R | 2 |
| Sedang | S | 3 |
| Berat | B | 4 |
| Ekstrem | E | 5 |

**4.1.1.3.2 Uji Validitas**

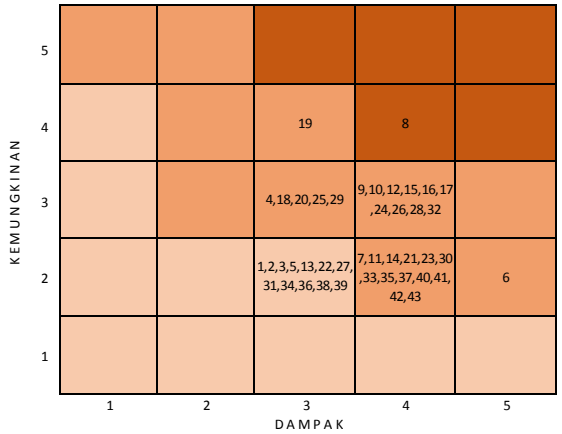
Tabel 4.2 Hasil Uji Validitas Kemungkinan Kuisioner Kedua

| Pernyataan | Corrected Total Item Correlation | Kesimpulan |
|---|---|---|
| Item B1 | 0.581 | Valid |
| Item B2 | 0.321 | Valid |
| Item B3 | 0.507 | Valid |
| Item B4 | 0.364 | Valid |
| Item B5 | 0.495 | Valid |
| Item B6 | 0.422 | Valid |
| Item B7 | 0.258 | Tidak Valid |
| Item B8 | 0.426 | Valid |
| Item B9 | 0.417 | Valid |
| Item B10 | 0.238 | Tidak Valid |
| Item B11 | 0.427 | Valid |
| Item B12 | 0.070 | Tidak Valid |
| Item B13 | 0.465 | Valid |
| Item B14 | 0.510 | Valid |
| Item B15 | 0.390 | Valid |
| Item B16 | 0.510 | Valid |
| Item B17 | 0.366 | Valid |
| Item B18 | 0.401 | Valid |

Setelah dilakukan uji validitas kuisioner sebanyak dua kali, terdapat beberapa item pernyataan yang masih **tidak valid**, diantaranya yaitu berada pada kriteria kemungkinan yaitu **item B7, B10, dan B12.** Maka dapat ditarik kesimpulan bahwa item yang tidak valid tersebut **TIDAK DIIKUTSERTAKAN** dalam proses-proses berikutnya.

**4.1.1.4 Evaluasi Risiko**

Tujuan dari evaluasi risiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut. Untuk menentukan peringkat risiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat risiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari risiko-risiko yang telah terdefinisi.




Gambar 4.2 Matriks Kemungkinan dan Dampak Risiko

Keterangan :

Risiko Tinggi

Risiko Menengah

Risiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa risiko yang memiliki nilai risiko paling tinggi adalah risiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran risiko menengah terdapat 30 risiko dan yang berada pada kuadran risiko rendah terdapat 12 risiko.

Tabel 4.3 Tingkat Keutamaan Risiko sistem i-Gracias

| Tingkat keutamaan | No Risiko | Risiko | Nama aset |
|---|---|---|---|
| Level I (High / Tinggi) | 8 | Database server down | Database Server |
| Level II (Medium / Menengah | 19 | Human error | Database Server |
| | 4 | Server down | NTP Server |
| | 18 | Backup failure | Database Server |
| | 20 | Gagal update | Database Server |
| | 25 | Kurang baiknya kualitas jaringan | APP Server |
| | 29 | Backup failure | Backup |
| | 9 | Koneksi database | Database Server |
| | 10 | Informasi diakses oleh pihak yang tidak berwenang | Database Server |
| | 12 | Penyalahgunaan hak akses / user ID | Database Server |
| | 15 | Overload | Database Server |
| | 16 | Hilangnya data | Database Server |
| | 17 | Data corrupt | |
| | 24 | Server down | APP Server |
| | 26 | Overcapacity | App Server |
| | 28 | Load balancer down | Load Balancer |
| | 32 | Jaringan terputus | Network Link |
| | 7 | Pencurian perangkat | Database Server |
| | 11 | Kebocoran data atau informasi internal perusahaan / institusi | Database Server |
| | 14 | Database crash | Database Server |
| | 21 | Risiko akibat bencana alam seperti kebakaran, banjir, gempa bumi, petir dll | APP Server |
| | 23 | Pencurian perangkat | APP Server |
| | 30 | Kerusakan hardware | Storage |
| | 33 | Kegagalan hardware | Core Router |
| | 35 | UPS tidak berfungsi | UPS |
| | 37 | Genset tidak berfungsi / rusak | Genset |
| | 40 | Risiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, aset dan lokasi data center | Data Center |
| | 41 | Risiko kerusakan akibat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalisme | Data Center |

| | | | |
|---|---|---|---|
| | 42 | Risiko kehilangan baik pada data maupun pada perangkat keras | Data Center |
| | 43 | Risiko kerusakan akibat masalah catu daya / tegangan listrik | Data Center |
| | 6 | Risiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi, petir dll | Database Server |
| Level III (Low / Rendah) | 1 | Risiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi, petir dll | NTP Server |
| | 2 | Pencurian perangkat | NTP Server |
| | 3 | Kegagalan / kerusakan hardware | NTP Server |
| | 5 | Overheat | NTP Server |
| | 13 | Mantan user / karyawan masih memiliki akses informasi | Database Server |
| | 22 | Kegagalan hardware | APP Server |
| | 27 | SVN down | SVN |
| | 31 | Penyimpanan penuh | Storage |
| | 34 | CDN down | CDN |
| | 36 | Baterai UPS lemah | UPS |
| | 38 | Baterai lemah atau mati | Genset |
| | 39 | AC mati | AC |

**4.1.1.5 Perlakuan Risiko**

Perlakuan risiko meliputi upaya untuk menyeleksi pilihan-pilihan yang dapat mengurangi atau meniadakan dampak serta kemungkinan terjadinya risiko. Secara umum, perlakuan terhadap suatu risiko dapat berupa salah satu dari empat perlakuan sebagai berikut :

- Menghindari risiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan risiko tersebut.
- Berbagi risiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya risiko atau dampak risiko.
- Mitigasi (mitigation), yaitu melakukan perlakuan risiko untuk mengurangi kemungkinan timbulnya risiko, atau mengurangi dampak risiko bila terjadi, atau mengurangi keduanya.
- Menerima risiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap risiko tersebut.

Penanganan risiko difokuskan pada risiko-risiko yang berada pada Level I (High / Tinggi) yaitu **Database Server Down.**

Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dll. Manfaat penggunaan database server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem i-Gracias sendiri.

Database server down berdampak pada seluruh layanan i-Gracias yang tidak dapat berjalan / diakses. 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 server down pada sistem i-Gracias?
2. Seberapa sering database server down tersebut terjadi pada sistem i-Gracias?
3. Kapan biasanya database server down paling sering terjadi?

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

- Overheat
- Overcapacity
- Overload
- Tingginya jumlah user dalam satu waktu

Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang

mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya risiko database server down, antara lain :

a. Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari risiko akibat overheat.
b. Menghilangkan log yang menggunakan kapasitas yang besar.
c. Melakukan restart database service.
d. Memprioritaskan query yang berat.

## 5. Kesimpulan dan Saran

### 5.1 Kesimpulan

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

1. Setelah melakukan serangkaian proses manajemen risiko, maka didapatkan hasil tingkatan risiko pada sistem i-Gracias. Risiko yang berada pada level tinggi adalah risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem i-Gracias, risiko yang memiliki nilai risiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila risiko tersebut terjadi adalah seluruh layanan i-Gracias tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap risiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem i-Gracias membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik.

## Daftar Pustaka


[1] [Online]. Available: https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Manager_. [Accessed 5 Juni 2015].

[2] [Online]. Available: http://mobelos.blogspot.com/2013/12/pengertian-manajemen-definisi-manajemen.html. [Accessed 15 Mei 2015].

[3] [Online]. Available: http://id.wikipedia.org/wiki/Manajemen_risiko. [Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/resiko-manajemen-risk-management/. [Accessed 14 Juni 2015].

[5] [Online]. Available: https://www.academia.edu/9860893/PROSES_MANAJEMEN_RISIKO. [Accessed 1 Juni 2015].

[6] [Online]. Available: http://chilem-iam.blogspot.com/2009/10/sistem-informasi-sistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online]. Available: http://dosen.gufron.com/artikel/pengertian-dan-definisi-teknologi-informasi/1/. [Accessed 3 Juni 2012].

[8] [Online]. Available: http://www.darakonsultanasuransi.com/index.php/risk-management-and-risiko/48-manajemen. [Accessed 16 November 2014].

[9] [Online]. Available: http://dosen.gufron.com/artikel/pengertian-dan-definisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].

[10] [Online]. Available: http://fisipuin.satugen.com/blog/Pengertian-Sistem-Informasi-Menurut-Para-Ahli-Definisi. [Accessed 17 Februari 2015].

[11] [Online]. Available: http://www.apb-group.com/asesmen-manajemen-risiko-berbasis-iso-310002009/. [Accessed 8 Maret 2015].

[12] L. J. Susilo, "Manajemen Risiko Berbasis ISO 31000".

[13] [Online]. Available: https://www.academia.edu/5170798/Uji_Validitas_Dan_Reliabilitas. [Accessed 6 Maret 2015].

[14] [Online]. Available: . http://setabasri01.blogspot.com/2012/04/uji-validitas-dan-reliabilitas-item.html. [Accessed 25 Februari 2015].

[15] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/resiko-manajemen-risk-management/. [Accessed 10 Juni 2015].