Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000

Francisca Lady Nice[1], Radiant Victor Imbar[2]

***Abstrak*— Tujuan dari manajemen risiko adalah untuk mengelola risiko dalam mendapatkan hasil yang optimal. Teknologi informasi merupakan sistem pertukaran data dari alat penelitian secara *online*. SWIFTS merupakan *website* yang menunjang kinerja sistem dan mendukung jalannya proses bisnis LAPAN. Diperlukan analisis risiko untuk mendapatkan gambaran terhadap berbagai kemungkinan yang muncul di dalam sistem dan aset pendukung kinerja sistem, yang dinilai dapat menghambat bahkan melumpuhkan aktivitas sitem sehingga mengganggu proses bisnis LAPAN. Analisis risiko manajemen yang digunakan pada LAPAN adalah ISO 31000:2009. Penerapan dari analisis risiko meliputi identifikasi risiko, penilaian risiko dan pemeliharaan risiko. Dari hasil penelitian maka didapatkan nilai risiko yang telah terdokumentasi, sehingga LAPAN dapat melakukan pencegahan, penanganan dan pemeliharaan terhadap sistem dan aset pendukung kinerja sistem di masa depan.**

***Kata Kunci:* International Organization for Standardization (ISO) 31000, Manajemen Risiko, Teknologi Infromasi.**

***Abstract* — Risk Management goal is to manage risk to obtain optimal results. Information technology is a data exchange system of online research tools. Swifts is a website that supports the performance of the system and support the path of business processes LAPAN. Risk analysis is required to get an overview of the various possibilities that arise in the system and asset performance support system, which was considered to inhibit even disabling system activity that disrupts business processes LAPAN. Management Risk analysis that used in LAPAN is using ISO 31000:2009. The application of risk analysis includes risk identification, risk assessment and risk maintenance. The research purposes to get the value of risk that has been documented, so LAPAN can do prevention, treatment and maintenance of the system and the system performance support assets in the future.**

Keywords— International Organization for Standardization (ISO) 31000, Management Risk, Information Technology.

[1] *Alumni, Jurusan Sistem Informasi Fakultas Teknologi Informasi Universitas Kristen Maranatha, Jl. Prof. drg. Surya Sumantri, M.P.H No. 65 Bandung- 40164, Jawa Barat, Indonesia (tlp: 021-2012186; fax: 022-2015154;e-*

I. PENDAHULUAN

A. *Latar Belakang*

Lembaga Penerbangan dan Antariksa Nasional (LAPAN) adalah Lembaga Pemerintah Non Departemen Indonesia yang bertugas melaksanakan tugas pemerintahan di bidang penelitian dan pengembangan kedirgantaraan dan pemanfaatannya serta bertanggung jawab kepada Presiden Republik Indonesia.

Dalam pelaksanaan tugasnya dikoordinasikan oleh menteri yang bertanggung-jawab di bidang riset dan teknologi. LAPAN memiliki visi untuk meningkatkan peran Iptek Kedirgantaraan dalam mewujudkan kesejahteraan berkelanjutan. Penyampaian informasi ditujukkan kepada masyarakat dalam bentuk *website*. Oleh karena itu, LAPAN memiliki sebuah unit dalam penerapan *website* tersebut, bernama Divisi IT.

Divisi IT (*Information Technology*) adalah unit pelaksana sistem informasi yang berperan sebagai media dalam pemenuhan kebutuhan informasi berupa pengembangan dan pelayanan teknologi informasi guna mendukung visi dan misi LAPAN. Salah satu *website* yang digunakan oleh LAPAN adalah SWIFTS (*Space Weather Information and Forecast Services*). Kehadiran SWIFTS dinilai penting dalam penyampaian informasi kepada masyarakat, hal ini membuat sistem SWIFTS harus berjalan optimal dan konsisten.

Namun berbagai kemungkinan ancaman dan risiko yang muncul dapat mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Kemungkinan ancaman dan risiko tersebut dapat berasal dari berbagai faktor. Berangkat dari permasalahan di atas, perlu dilakukan suatu analisis manajemen risiko menggunakan ISO 31000, sehingga LAPAN dapat menghasilkan dokumentasi terhadap kemungkinan ancaman dan risiko yang muncul pada setiap aset yang merupakan kesatuan dari *website* SWIFTS untuk dapat dilakukan pengelolaan risiko secara keseluruhan dalam pencegahan, penanganan dan perbaikan di masa depan.

B. *Rumusan Masalah*

Dari latar belakang di atas, maka diambil rumusan masalah sebagai berikut :

- Bagaimana analisis risiko teknologi informasi terhadap *website* SWIFTS menggunakan ISO 31000 di Divisi IT Lembaga Penerbangan dan Antariksa Nasional (LAPAN) ?

- Bagaimana mengetahui tingkat risiko yang terjadi pada *website* SWIFTS pada Divisi IT Lembaga Penerbangan dan Antariksa Nasional (LAPAN) ?

C. Tujuan Pembahasan

Tujuan pembahasan dalam penelitian tugas akhir ini adalah :

- Melaksanakan tahapan dan proses analisis risiko teknologi informasi berbasis *risk management* sesuai dengan standar dan kerangka kerja ISO 31000 pada *website* SWIFTS.
- Mendokumentasikan tingkat risiko dan perlakuan terhadap risiko teknologi informasi *website* SWIFTS di LAPAN.

D. Ruang Lingkup

Penelitian dilakukan dengan analisis manajemen risiko berdasarkan ISO 31000 pada *website Space Weather Information and Forecaster Services* (SWIFTS) di Lembaga Penerbangan dan Antariksa Nasional (LAPAN), yang meliputi *risk identification, risk assessment* dan *risk treatment.*

II. KAJIAN TEORI

A. Risiko

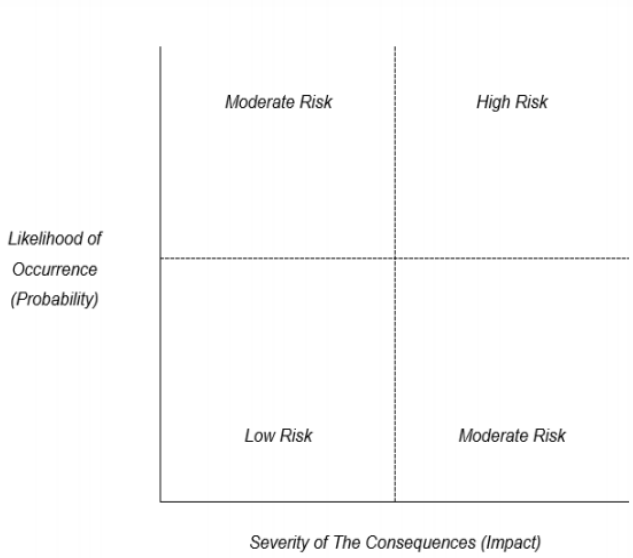
Semua risiko mewakili aktivitas-aktivitas yang tidak sah atau di luar dari yang diperbolehkan perusahaan. Aktivitas-aktivitas tersebut adalah: pengungkapan dan pencurian informasi, penggunaan secara tidak sah, pengrusakan dan penolakan dan modifikasi yang tidak dibenarkan [1].

Risiko juga dapat dikategorikan ke dalam beberapa bentuk diantaranya [2]:

- Risiko spekulatif
  Adalah suatu keadaan yang dihadapi perusahaan yang dapat memberikan keuntungan dan juga dapat memberikan kerugian.
- Risiko murni (*pure risk*)
  Adalah sesuatu yang hanya dapat berakibat merugikan atau tidak terjadi apa-apa dan tidak mungkin menguntungkan. Salah satu contoh adalah kebakaran, apabila perusahaan menderita kebakaran, maka perusahaan tersebut akan menderita kerugian.
- Risiko fundamental
  Adalah suatu peristiwa yang baik sebab maupun akibat yang ditimbulkannya bukan berasal dari individu dan dampaknya pada umumnya menimpa orang banyak dan biasanya bersifat katastropal (dalam skala besar) seperti perang, inflasi, dan lain-lain.
- Risiko partikular
  Adalah suatu risiko yang penyebabnya disebabkan oleh individu-individu dan dampaknya terbatas, dimana kita dapat menunjuk individu/sesorang yang menyebabkannya. Misalnya, kebakaran, pencurian, kecelakaan dan sebagainya. Ketidakpastian dapat menimbulkan dua akibat yang berbeda yaitu positif atau negatif.

Meskipun istilah risiko dan ketidakpastian sering digunakan secara berdampingan, keduanya memiliki arti yang berbeda. Risiko adalah suatu kondisi atau kejadian yang tidak pasti yang bila terjadi dapat memberikan dampak negatif maupun positif. Risiko terjadi secara kumulatif dan dapat mempengaruhi sebuah objektif [3].

Berbeda dengan ketidakpastian, yang hanya mempertimbangkan *event*-nya (kejadiannya) saja sedangkan kemungkinannya sama sekali tidak diketahui. Telah dijelaskan juga bahwa risiko memiliki tiga elemen utama *the event*, *the probability,* dan *the impact/consequences* atau *impact. Event* atau kejadian adalah deskripsi dari risiko yang mungkin saja terjadi. Deskripsi dari *event* sangat penting. Tanpa penjelasan yang jelas, menggali *probability* dan *impact* dari sebuah risiko menjadi jauh lebih sulit. Gambar 1 menjelaskan tentang konsep risiko, maka dapat diketahui *level of risk* (tingkatan risiko).

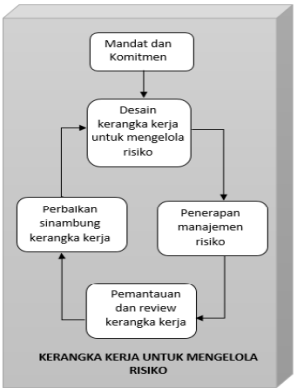


Gambar 1. *Concept of Risk* [4]

B. Manajemen Risiko

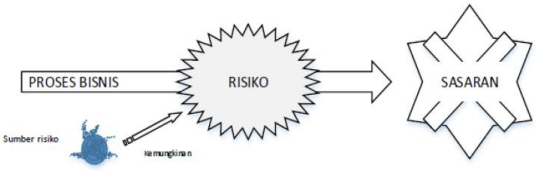
Manajemen risiko adalah suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manejemen risiko bertujuan untuk mengelola risiko sehingga dapat memperoleh hasil yang optimal. Agar dapat berjalan dengan baik, manajemen risiko diletakkan dalam suatu kerangka manajemen risiko. Kerangka kerja ini akan menjadi dasar dan penataan yang mencakup seluruh kegiatan manajemen risiko di segala tingkatan organisasi, selain itu juga akan membantu organisasi mengelola risiko secara efektif melalui penerapan proses manajemen risiko. Kerangka kerja ini tidak dimaksudkan sebagai sebuah sistem manajemen,

tetapi lebih ditujukan untuk membantu organisasi mengintegrasikan manajemen risiko ke dalam keseluruhan sistem manajemen organisasi. Oleh karena itu, organisasi harus mengadopsi komponen-komponen dari kerja ini ke dalam kebutuhan khas organisasi. Gambar 2 adalah kerangka kerja untuk mengelola risiko.



Gambar 2. Kerangka Kerja Untuk Mengelola Risiko [5]

1) *Prinsip dari Manajemen Risiko:* Prinsip dasar untuk penerapan manajemen risiko pada proses bisnis adalah Pertama, memahami apa saja sasaran (objektif) proses bisnis tersebut. Kedua, mengidentifikasi apa saja yang dapat menghambat tercapainya sasaran bisnis proses tersebut. Ketiga, pengendalian apakah yang harus dilakukan agar risiko-risiko tersebut dapat ditiadakan atau dikurangi. Prinsip dasar ini dapat dilihat pada gambar 3 [5].



Gambar 3. Prinsip Dasar Manajemen Risiko **[5]**

Manajemen risiko bekerja dalam serangkaian prinsip, yaitu [3] :

- *Proportionate* (Sepadan);
- *Aligned* (Sesuai);
- *Comprehensive* (Komprehensif);
- *Embedded* (Melekat);
- *Dynamic* (Dinamis).

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organization.
Aligned	Risk management activities need to be aligned with the other activities in the organization.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organization.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

Gambar 1. *Principles of Risk Management* **[3]**

Ganbar 4 merupakan deskripsi aturan yang terdapat pada manajemen risiko, berikut penjelasannya, *Proportionate* berarti manajemen risiko harus sepadan dengan tingkat risiko yang terdapat dalam suatu organisasi. *Align* berarti manajemen risiko harus sesuai dengan seluruh aktifitas bisnis yang terjadi dalam suatu organisasi. *Comprehensive* berarti manajemen risiko harus dilakukan secara sistematis dan terstruktur. *Embeded* berarti manajemen risiko harus melekat pada setiap bisnis proses yang terdapat dalam suatu organisasi. Dan *dynamic* berarti manajemen risiko harus dapat dilakukan berulang-ulang dan responsif terhadap perubahan yang terjadi [3].

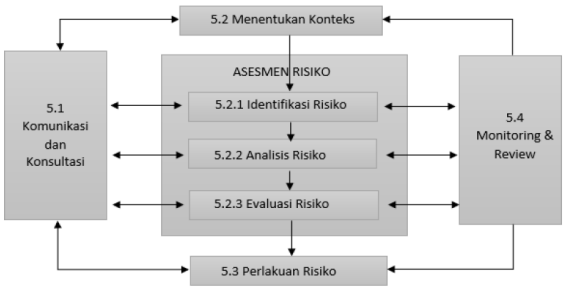
2) *Kerangka Kerja Manajemen Risiko:* Kerangka kerja manajemen risiko ISO 31000: 2009 *Risk Management – Principles and Guidelines* dimulai dengan pemberian mandat dan komitmen. Pemberian mandat dan komitmen merupakan hal yang sangat penting karena menentukan akuntabilitas, kewenangan, dan kapabilitas dari pelaku manajemen risiko. Hal-hal penting yang harus dilakukan pada pemberian mandat dan komitmen adalah [5]:
   - Membuat dan menyetujui kebijakan manajemen risiko;
   - Menyesuaikan indikator kinerja manajemen risiko dengan indikator kinerja perusahaan;
   - Menyesuaikan kultur organisasi dengan nilai-nilai manajemen risiko;
   - Menyesuaikan sasaran manajemen risiko dengan sasaran strategis perusahaan;
   - Memberikan kejelasan peran dan tanggung jawab;
   - Menyesuaikan kerangka kerja manajemen risiko dengan kebutuhan organisasi.

   Setelah pemberian mandat dan komitmen, kerangka kerja ISO 31000: 2009 dilanjutkan dengan kerangka implementasi "*Plan, Do, Check, Act*", yaitu dengan melakukan [5]:
   - Perencanaan kerangka kerja manajemen risiko;
   - Penerapan manajemen risiko;
   - *Monitoring* dan *review* terhadap kerangka kerja manajemen risiko;
   - Perbaikan kerangka kerja manajemen risiko secara berkelanjutan.

   Perencanaan kerangka kerja manajemen risiko mencakup pemahaman mengenai organisasi dan konteksnya, menetapkan kebijakan manajemen risiko, menetapkan akuntabilitas manajemen risiko, mengintegrasikan manajemen risiko ke dalam proses bisnis organisasi, alokasi sumber daya manajemen risiko, dan menetapkan mekanisme komunikasi internal dan eksternal. Setelah melakukan perencanaan kerangka kerja, maka dilakukan penerapan proses manajemen risiko. Dalam penerapan manajemen risiko, perlu

dilakukan *monitoring* dan *review* terhadap kerangka kerja manajemen risiko. Setelah itu, kerangka kerja manajemen risiko perlu diperbaiki secara berkelanjutan untuk memfasilitasi perubahan yang terjadi pada konteks internal dan eksternal organisasi. Proses-proses tersebut kemudian berulang kembali untuk memastikan adanya kerangka kerja manajemen risiko yang mengalami perbaikan berkesinambungan dan dapat menghasilkan penerapan manajemen risiko yang andal [5].

3) *Proses Manajemen Risiko:* Proses manajemen risiko merupakan salah satu tahapan dalan mengelola risiko. Proses ini meliputi lima kegiatan, yaitu komunikasi dan konsultasi, menentukan konteks, asesmen risiko, perlakuan risiko, serta *monitoring* dan *review*. Tahapan pada proses manajemen risiko ditunjukan pada gambar. Aktivitas-altivitas tersebut dan pendokumentasiannya akan diuraikan pada bagian selanjutya.



Gambar 2. Proses Manajemen Risiko **[6]**

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 menetapkan konteks dan identifikasi risiko [6].

C. Risk Management Framework

Secara umum diakui bahwa *risk management* framework (kerangka kerja manajemen risiko) merupakan dokumen yang menghasilkan informasi pada proses manajemen risiko. Dalam banyak kerangka kerja manajemen risiko, aktivitas manajemen risiko harus dilakukan dalam konteks lingkungan bisnis, organisasi dan risiko yang dihadapi oleh organiasi. Agar konteks dapat dijelaskan dan didefinisikan, kerangka kerja diperlukan dalam mendukung prosesnya. Symantec adalah *Risk Management* Report, yaitu Teknologi Informasi (TI) secara luas dan mendalam telah menjadi saling berhubungan dengan operasi bisnis, risiko TI sendiri pun telah tumbuh menjadi bagian dari keseluruhan komponen operasional.

Gambar 6. IT *Risk Classification* [7]

Untuk membantu organisasi dalam memahami dan menganalisa risiko TI dan mengatur strategi mitigasi, maka dibuat framework (kerangka kerja) klasifikasi risiko berdasarkan dampaknya terhadap organisasi. Kerangka kerja tersebut mengklasifikasikan risiko TI sebagai [7]:

- *Security Risk* atau risiko keamanan – bahwa informasi dapat dirubah, diakses atau digunakan oleh pihak yang tidak bertanggung jawab.
- *Availability Risk* atau risiko ketersediaan – bahwa informasi atau aplikasi tidak dapat diakses karena system failure (kegagalan sistem) atau bencana alam, termasuk masa pemulihan (*recovery*).
- *Performance Risk* atau risiko kinerja – bahwa kinerja yang kurang dari system, aplikasi, personil, atau TI secara keselruhan, dapat mengurangi produktivitas atau nilai bisnis.
- *Compliance Risk* atau risiko pemenuhan – bahwa penanganan atau pengolahan informasi gagal memenuhi peraturan, TI atau persyaratan kebijakan bisnis (*business policy requirements*).

D. Pengertian Audit

Audit adalah suatu proses yang sistematis untuk memperoleh dan menilai bukti-bukti secara objektif, yang berkaitan dengan tindakan-tindakan dan kejadian-kejadian ekonomi untuk menentukan tingkat kesesuaian dengan kriteria yang telah diterapkan dan mengkomunikasikan hasilnya kepada pihak-pihak yang berkepentingan. Definisi diatas mengandung arti yang luas dan berlaku untuk segala macam jenis auditing atau pengauditan yang memiliki tujuan berbeda-beda. Adapun kalimat-kalimat kunci dalam definisi audit sebagai berikut [8]:

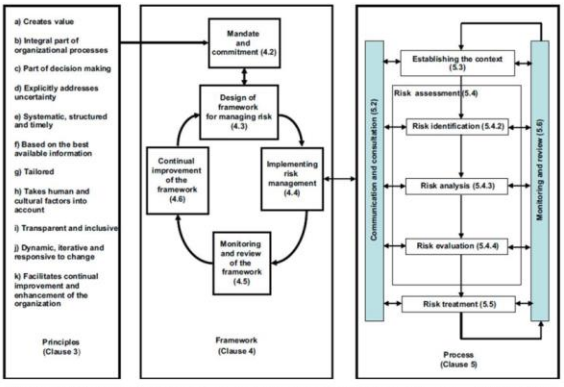
1) Proses yang sistematis
   Yaitu mengandung makna sebagai rangkaian langkah atau prosedur yang logis, terencana, dan terorganisasi.
2) Memperoleh dan Menilai Bukti Secara Obyektif
   Yaitu mengandung arti bahwa auditor memeriksa dasar-dasar yang diapaki untuk membuat aserasi

atau pernyataan oleh manajemen dan melakukan penilaian tanpa sikap memihak.

3) Tindakan-tindakan dan kejadian - kejadian Ekonomi
   Yaitu pernyataan tentang kejadian ekonomi yang merupakan informasi hasil proses akuntansi yang dibuat oleh individu atau suatu organisasi. Hal penting yang perlu dicatat adalah bahwa asersi-asersi tersebut dibuat oleh penyusun laporan keuangan, yaitu manajemen perusahaan atau pemerintah, untuk selanjutnya dikomunikasikan kepada para pengguna laporan keuangan, jadi bukan merupakan asersi dari auditor.
4) Mengkomunikasikan Hasilnya kepada Pihak-pihak yang Berkepentingan
   Yaitu kegiatan terakhir dari suatu auditing atau pengauditan adalah menyampaikan temuan-temuan dan hasilnya kepada pengambil keputusan. Hasil dari auditing disebut pernyataan pendapat (opini) mengenai kesesuaiannya antara asersi atau pernyataan tersebut dengan kriteria yang ditetapkan.
5) Tingkat Kesesuaian Kriteria yang Telah Ditetapkan
   Yaitu secara spesifik memberikan alasan mengapa auditor tertarik pada pernyataan bukti-bukti pendukungnya. Namun agar komunikasi tersebut efisien dan dapat dimengerti dengan bahasa yang sama oleh para pengguna, maka diperlukan suatu kriteria yang disetujui bersama.

E. International Organization for Standardization (ISO 31000:2009).

ISO 31000 merupakan standar yang berkaitan dengan manajemen risiko yang dikodifikasi oleh *International Organization for Standardization* (ISO) atau Organisasi Internasional untuk Standarisasi. Tujuan dari ISO 31000 sendiri adalah untuk memberikan prinsip-prinsip dan pedoman untuk manajemen risiko. ISO 31000 juga memberikan paradigma yang diakui secara *universal* bagi para praktisi dan organisasi yang memperkerjakaan proses manajemen risiko untuk menggantikan standar yang ada, metodologi dan paradigma yang berbeda antara industri, materi dan daerah.



Relationships between the risk management principles, framework and process based on ISO 31000:2009

Gambar 7. Hubungan Antara Prinsip, Kerangka Kerja, dan Proses Manajemen Risiko [3]

Menurut ISO 31000:2009, manajemen risiko suatu organisasi harus mengikuti 11 prinsip dasar agar dapat dilaksanakan secara efektif. Berikut penjabaran prinsip-prinsip tersebut [3]:

- Manajemen risiko menciptakan nilai tambah (*creates value*) Manajemen risiko berkontribusi terhadap pencapaian nyata objektif dan peningkatan, antara lain, kesehatan dan keselamatan manusia, kepatuhan terhadap hukum dan peraturan, penerimaan publik, perlindungan lingkungan, kinerja keuangan, kualitas produk, efisiensi operasi, serta tata kelola dan reputasi perusahaan.
- Manajemen risiko adalah bagian integral proses dalam organisasi (*an integral part of organizational processes*) Manajemen risiko adalah bagian tanggung jawab manajemen dan merupakan suatu bagian integral dalam proses normal organisasi seperti juga merupakan bagian dari seluruh proses proyek dan manajemen perubahan. Manajemen risiko bukanlah merupakan aktivitas yang berdiri sendiri yang terpisah dari aktivitas-aktivitas utama dan proses dalam organisasi.
- Manajemen risiko adalah bagian dari pengambilan keputusan (*part of decision making*) Manajemen risiko membantu pengambil keputusan mengambil keputusan dengan informasi yang cukup. Manajemen risiko dapat membantu memprioritaskan tindakan dan membedakan berbagai pilihan alternatif tindakan. Pada akhirnya, manajemen risiko dapat membantu memutuskan apakah suatu risiko dapat diterima atau apakah suatu penanganan risiko telah memadai dan efektif.
- Manajemen risiko secara eksplisit menangani ketidakpastian (*explicitly addresses uncertainty*) Manajemen risiko menangani aspek-aspek ketidakpastian dalam pengambilan keputusan, sifat alami dari ketidakpastian itu, dan bagaimana menanganinya.
- Manajemen risiko bersifat sistematis, terstruktur, dan tepat waktu (*systematic, structured and timely*) Suatu pendekatan sistematis, tepat waktu, dan terstruktur terhadap manajemen risiko memiliki kontribusi terhadap efisiensi dan hasil yang konsisten, dapat dibandingkan, serta andal.
- Manajemen risiko berdasarkan informasi terbaik yang tersedia (*based on the best available information*) Masukan untuk proses pengelolaan risiko didasarkan oleh sumber informasi seperti pengalaman, umpan balik, pengamatan, prakiraan, dan pertimbangan pakar. Meskipun demikian, pengambil keputusan harus terinformasi dan harus mempertimbangkan segala keterbatasan data atau model yang digunakan atau kemungkinan perbedaan pendapat antar pakar.

- Manajemen risiko dibuat sesuai kebutuhan (*tailored*) Manajemen risiko diselaraskan dengan konteks eksternal dan internal organisasi serta profil risikonya.
- Manajemen risiko memperhitungkan faktor manusia dan budaya (*takes human and cultural factors into account*) Manajemen risiko organisasi mengakui kapabilitas, persepsi, dan tujuan pihak-pihak eksternal dan internal yang dapat mendukung atau malah menghambat pencapaian tujuan organisasi.
- Manajemen risiko bersifat transparan dan inklusif (*transparent and inclusive*) Pelibatan para pemangku kepentingan, terutama pengambil keputusan, dengan sesuai dan tepat waktu pada semua tingkatan organisasi, memastikan manajemen risiko tetap relevan dan mengikuti perkembangan. Pelibatan ini juga memungkinkan pemangku kepentingan untuk cukup terwakili dan diperhitungkan sudut pandangnya dalam menentukan kriteria risiko.
- Manajemen risiko bersifat dinamis, iteratif, dan responsif terhadap perubahan (*dynamic, iterative and responsive to change*) Seiring dengan timbulnya peristiwa internal dan eksternal, perubahan konteks dan pengetahuan, serta diterapkannya pemantauan dan peninjauan, risiko-risiko baru bermunculan, sedangkan yang ada bisa berubah atau hilang. Karenanya, suatu organisasi harus memastikan bahwa manajemen risiko terus menerus memantau dan menanggapi perubahan.
- Manajemen risiko memfasilitasi perbaikan dan pengembangan berkelanjutan organisasi (*facilitates continual improvement and enhancement of the organization*) Organisasi harus mengembangkan dan mengimplementasikan strategi untuk memperbaiki kematangan manajemen risiko mereka bersama aspek-aspek lain dalam organisasi mereka.

Menurut ISO 31000, proses manajemen risiko meliputi lima kegiatan yaitu:

- *Communication and Consultation* (Komunikasi dan konsultasi).
  Proses ini berjalan secara internal dalam organisasi, divisi, dan unit bisnis atau eksternal ditujukan pada *external stakeholder*.
- *Establish the Context* (Menentukan konteks).
  Dengan ditetapkannya konteks berarti manajemen organisasi menentukan batasan atau *internal parameter* (parameter internal) dan *external parameter* (parameter eksternal) yang dijadikan pertimbangan dalam pengelolaan risiko, menentukan lingkup kerja, dan kriteria risiko untuk proses-proses selanjutnya.
- *Risk Assesment* (Penilaian Risiko), meliputi *Risk Identification* (Identifikasi Risiko), *Risk Analysis* (Analisis Risiko), dan *Risk Evaluation* (Evaluasi Risiko).
  Risk Identification atau identifikasi risiko adalah proses penentuan risiko yang berpotensi mempengaruhi organisasi dalam mencapai tujuannya.
  Risk Analysis atau analisis risiko adalah upaya untuk memahami risiko lebih dalam.
  Risk Evaluation atau evaluasi risiko adalah proses mengevaluasi tingkat kegawatan masing-masing risiko menggunakan kriteria yang telah ditentukan pada saat menentukan konteks.
- *Risk Treatment* (Perlakuan Risiko).
  Perlakuan risiko meliputi upaya untuk menyeleksi pilihan-pilihan yang dapat mengurangi atau meniadakan dampak serta kemungkinan terjadinya risiko, kemudian menerapkan pilihan tersebut.
- *Monitoring* dan *Review*.
  Monitoring dan *Review* adalah bagian dari manajemen risiko yang memastikan bahwa seluruh tahapan proses dan fungsi manajemen risiko berjalan dengan baik [10].

F. Sistem Informasi

Informasi merupakan salah satu sumber daya penting dalam suatu organisasi; digunakan sebagai bahan pengambilan keputusan. Menurut Burch dan Grudnitski (1989), kualitas informasi ditentukan oleh tiga faktor yaitu relevansi, tepat waktu dan akurasi. Akurasi berarti bahwa informasi bebas dari kesalahan. Relevansi berarti bahwa informasi benar-benar beguna bagi suatu tindakan keputusan yang dilakukan oleh seseorang. Tepat waktu berarti bahwa informasi datang pada saat dibutuhkan sehingga bermanfaat untuk pengambilan keputusan [9].

Informasi merupakan hasil dari pengolahan data, akan tetapi tidak semua hasil dari pengolahan tersebut bisa menjadi informasi, hasil pengolahan data yang tidak memberikan makna atau arti serta tidak bermanfaat bagi seseorang bukanlah merupakan informasi bagi orang tersebut [11].

Satzinger, Jackson, & Burd (2015) dalam bukunya yang berjudul *System Analysis and Design In a Changing World* menjelaskan bahwa sistem informasi adalah "kumpulan komponen yang saling berkaitan dengan komputer yang megambil, memproses, menyimpan dan menyediakan informasi sebagai kebutuhan untuk menyelesaikan tugas bisnis [12]."

Sistem Informasi menurut O'Brien & Marakas (2005) adalah gabungan antara orang, *hardware*, *software*, jaringan komunikasi, sumber data, serta kebijakan dan prosedur yang saling terorganisir untuk menyimpan, mengambil, mengubah dan menyebarkan informasi dalam sebuah organisasi [13].

G. Website

Website adalah keseluruhan halaman-halaman web yang terdapat dalam sebuah domain yang mengandung informasi. Sebuah *website* biasanya dibangun atas nama banyak nama halaman web yang saling berhubungan. Hubungan antara satu halaman web dengan web yang

lainnya disebut dengan *hyperlink*, sedangkan teks yang dijadikan media penghubung disebut *hypertext* [14].

III. ANALISIS DAN EVALUASI

A. *Analisis Manajemen Risiko IT*

Analisis manajemen risiko TI pada *website* SWIFTS pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) melibatkan penggunaan aplikasi secara sistematis dari pengelolaan kebijakan, proses dan prosedur hingga proses dalam penentuan konteks, mengidentifikasi, menilai, memperlakukan risiko yang terdapat pada *website* SWIFTS.

B. *Asesmen Risiko*

Asesmen Risiko atau *Risk Assesment* atau penilaian risiko terhadap risiko pada *website* SWIFTS merupakan gabungan proses yang terdiri dari *risk identification* (identifikasi risiko), *risk analysis* (analisis risiko) dan *risk evaluation* (evaluasi risiko).

1) *Identifikasi Risiko*

- *Identifikasi Aset*

Tahapan identifikasi aset dapat memberikan suatu gambaran terhadap aset-aset yang berhubungan dengan sistem SWIFTS, melalui proses obervasi dan wawancara dengan pihak-pihak yang terlibat langsung. Detail identifikasi aset terdapat pada Tabel I.

TABEL I
IDENTIFIKASI ASET SWIFTS

No	Komponen Sistem Informasi	Aset SWIFTS
1	Data	Data hasil penelitian
		FRF (*Forecast* Report Form) Online
		SWIFtS Weekly Space Weather News
2	Perangkat Lunak	Sistem Informasi Space Weather Information And *Forecast* Services (SWIFTS)
No	**Komponen Sistem Informasi**	**Aset SWIFTS**
3	Perangkat Keras	Personal Computer (PC) beserta komponen / perangkatnya (PC alat)
		Server SWIFTS
		Router Mikrotik
		Modem
		Access Point
		Switch
		Kabel *Fiber Optik*
		Kabel UTP (Unshielded Twisted Pair)
		RJ 45

- *Identifikasi Kemungkinan Risiko*

Tahap identifikasi kemungkinan risiko adalah proses untuk mengidentifikasi berbagai kemungkinan risiko yang muncul terhadap aset-aset informasi sistem SWIFTS. Detail identifikasi kemungkinan risiko terdapat pada Tabel II.

TABEL II
IDENTIFIKASI KEMUNGKINAN RISIKO

Faktor	Risiko
Alam / Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
Manusia	Pencurian perangkat
	Human Error
	Tidak dijalankannya Tata Kelola
	Kurangnya SDM
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server Down
	Overheat
	Koneksi jaringan terputus
	Sistem *Crash*
	Overcapacity
	Overload
	Data Korup
	Back up Failure
	Kurang baiknya kualitas jaringan

- *Identifkasi Komponen Risiko*

Risiko dalam manajemen risiko bukan hanya sekedar suatu kejadian, peristiwa, atau kondisi yang dapat berkembang/terjadi, namun mencakup pula berbagai informasi yang terkait dengan kejadian, peristiwa, atau kondisi tersebut, yang mencakup :

- Sumber risiko : benda atau kondisi yang dapat memicu timbulnya risiko
- Konsekuensi : dampak terhadap sistem SWIFTS

- *Identifikasi Dampak Risiko*

Menindaklanjuti hasil dari identifikasi kemungkinan risiko yang terjadi, maka dilakukan identifikasi terhadap dampak yang terjadi pada *website* SWIFtS. Detail identifikasi dampak risiko terdapat pada Tabel III. ID adalah pengkodean yang diberikan terhadap setiap risiko yang ada.

TABEL III
IDENTIFIKASI DAMPAK RISIKO

Komponen/ Sumber Daya Aset IT	ID	Risiko	Dampak
Data	R1	Kebakaran	Proses pengolahan

			informasi SWIFtS tidak dapat dilakukan, sehingga infomasi pada website tidak dapat diperbaharui.
	R1	Kebakaran	Kehilangan data. Perusahaan mengalami kerugian secara finansial. Kehilangan aset. Menggangu proses bisnis lainnya.
	R2	Petir	Alat rusak. Ketersedian data terhambat. Data yang digunakan dalam proses *forecast* menggunakan data dari institusi lain, yang berdampak kepada validitas informasi. Perusahaan mengalami kerugian secara finansial.
	R28	*Human Error*	Sistem operasi tidak dapat berjalan. Melakukan perubahan terhadap konfigurasi yang telah berjalan. Gagal melakukan update. Data dari *server* stasiun tidak dapat ditarik ke *server* utama. Data tidak dapat diakses sementara waktu. Data tidak dapat disimpan tampil ke log -konsolidasi untuk memperbaiki sistem.
Komponen/ Sumber Daya Aset IT	**ID**	**Risiko**	**Dampak**
Perangkat Keras	R41	Debu/ Kotoran	Alat mengalami kerusakan.
	R42	Radiasi Panas	Alat mengalami kerusakan.
	R43	Suhu yang bervariasi	Kerusakan alat. Kebocoran pada kapasitor. *Server* mati.

2) Analisis Risiko

Tahapan analisis risiko dilakukan penilaian terhadap risiko-risiko yang muncul pada sistem SWIFTS. Hal ini mencakup penilaian terhadap kemungkinan terjadi risiko (*likelihood*) dan dampak (*impact*) apabila suatu risiko terjadi.

- *Qualitative dan Semi-quantitative analysis*

Tahap ini menjelaskan setiap risiko yang telah teridentifikasi, kemudian diberikan penilaian berdasarkan *likelihood* dan *impact*. Berikut adalah kriteria penilaian *likelihood* dan *impact* yang dapat dilihat pada Tabel IV dan Tabel V.

TABEL IV
NILAI PADA *LIKELIHOOD*

Likelihood		**Deskripsi**	**Frekuensi per tahun**
Rating	**Kriteria**		
1	*Rare*	Hampir tidak pernah terjadi	>2 tahun
2	*Unlikely*	Kemungkinan terjadi ada tetapi kecil (jarang)	1 – 2 tahun
3	*Possible*	Mungkin saja terjadi (kadang-kadang)	7 – 12 bulan / tahun
4	*Likely*	Kemungkinan besar terjadi (sering)	4 – 6 bulan / tahun
5	*Almost Certain*	Hampir selalu terjadi	1 – 3 bulan / tahun

TABEL V
NILAI PADA *IMPACT*

Likelihood		**Deskripsi**
Rating	**Kriteria**	
1	*Insignificant*	Tidak menyebabkan gangguan operasional bisnis
2	*Minor*	Proses bisnis mengalami gangguan, namun aktivitas tugas pokok dapat diajalankan secara normal
3	*Moderate*	Proses bisnis mengalami gangguan yang menyebabkan sebagian bisnis mengalami penundaan
4	*Major*	Proses bisnis mengalami gangguan yang menyebabkan aktivitas bisnis mengalami penundaan
5	*Catastrophic*	Proses bisnis mengalami gangguan total hingga keseluruhan proses bisnis tidak tercapai

Setelah menentukan nilai pada *likelihood* dan *impact* maka penilaian pada masing-masing risiko yang telah didefinisikan pada proses sebelumnya dapat dilakukan. Penilaian *likelihood* dan *impact* dilakukan dengan melakukan wawancara dan *checklist*, hasil penelitian terdapat pada Tabel VI dan Tabel VII.

TABEL VI
IDENTIFIKASI *LIKELIHOOD* DAN IMPACTPADA RISIKO

Komponen/ Sumber Daya Aset	**ID**	**Risiko**	***Likelihood***	***Impact***

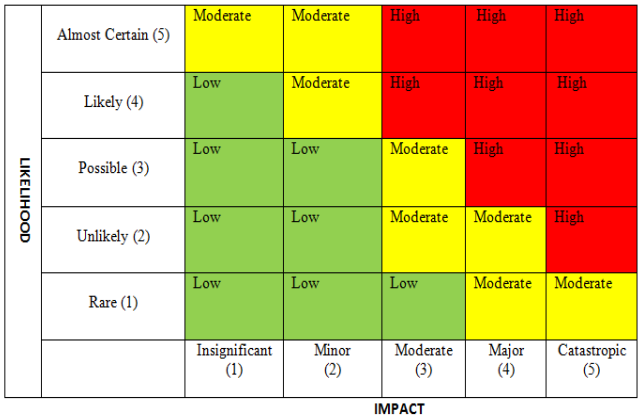
IT				
Data	R1	Kebakaran	*Rare*	*Catastropic*
	R2	Petir	*Unlikely*	*Major*
Perangkat Lunak	R27	Debu / Kotoran	*Likely*	*Insignificant*
	R28	*Human Error*	*Likely*	*Modeerate*
Perangkat Keras	R41	Debu/ Kotoran	*Likely*	*Insignificant*
	R42	Radiasi Panas	*Likely*	*Major*
	R43	Suhu yang bervariasi	*Likely*	*Major*

TABEL VII
PENILAIAN IDENTIFIKASI *LIKELIHOOD* DAN IMPACT PADA RISIKO

Komponen / Sumber Daya Aset IT	**ID**	**Risiko**	***Likelihood***	***Impact***
Data	R1	Kebakaran	1	5
	R2	Petir	2	4
Perangkat Lunak	R27	Debu/ Kotoran	4	1
	R28	*Human Error*	4	3
Komponen / Sumber Daya Aset IT	**ID**	**Risiko**	***Likelihood***	***Impact***
Perangkat Keras	R41	Debu / Kotoran	4	1
	R42	Radiasi Panas	4	4
	R43	Suhu yang bervariasi	4	4

3) Evaluasi Risiko

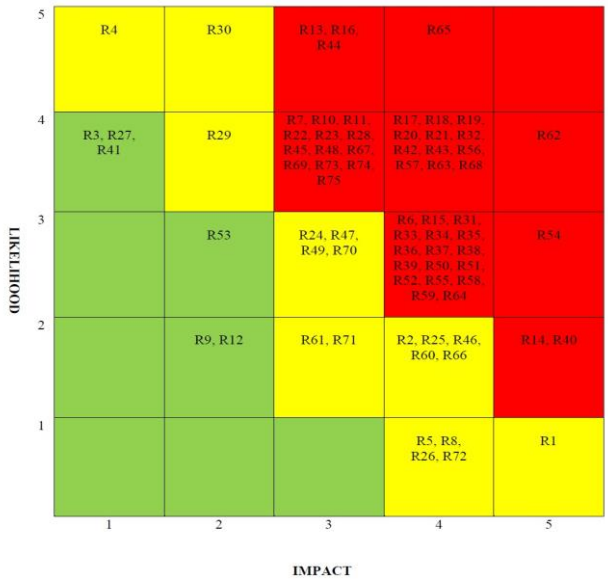
Tahap *risk evaluation* atau evaluasi risiko, adalah mengevaluasi risiko pada *website* SWIFTS apakah risiko dapat ditoleransi atau tidak berdasarkan pada *level of risk* atau tingkatan risiko yang diperoleh dari hasil analisis risiko pada tahap sebelumnya. Gambar 8 adalah matrik risiko yang digunakan dalam memetakan setiap risiko yang ada dengan nilai *likelihood* dan *impact* yang telah didapatkan pada tahapan analisis sebelumnya. Untuk deskripsi penggambaran lebih lengkap terkait nilai setiap warna dapat dilihat pada Gambar 9.



Gambar 8. Matrik Evaluasi Risiko

High Risk – Risiko Tinggi	Risiko yang berbahaya yang harus diatasi secepatnya. Risiko yang berada pada level ini menjadi perhatian penuh Direksi dalam pengelolaannya.
Moderate Risk – Risiko Sedang	Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan. Risiko yang berada pada level ini menjadi perhatian penuh General Manager dan Direksi.
Low Risk – Risiko Rendah	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil. Risiko yang berada pada level ini menjadi sepenuhnya dalam tanggung jawab pengelolaan ditingkat operasional.

Gambar 9. *Level of risk*



Gambar 10. Matrik Evaluasi Risiko berdasarkan *likelihood* dan *impact*

Gambar 10 merupakan matrik yang telah diisi menggunakan nilai yang telah sesuai dengan nilai yang telah diberikan pada analisis sebelumnya (dapat dilihat padaTabel VI dan Tabel VII) dan diberikan warna sesuai dengan tingkatan risiko yang terdapat pada Gambar 8.

TABEL VII
LEVEL OF RISK PADA RISIKO

Sumber Daya Aset IT	**ID**	**Risiko**	***Likelihood***	***Impact***	***Level of Risk***
Data	R1	Kebakaran	1	5	*Moderate*
	R2	Petir	2	4	*Moderate*
Perangkat Lunak	R27	Debu/ Kotoran	4	1	*Low*
	R28	*Human Error*	4	3	*High*
Perangkat Keras	R41	Debu / Kotoran	4	1	*Low*
	R42	Radiasi Panas	4	4	*High*
	R43	Suhu yang bervariasi	4	4	*High*

C. Perlakuan Risiko

Pada tahap ini dapat dilihat tindakan yang dilakukan oleh LAPAN dalam mengatasi banyak risiko yang telah teridentifikasi pada *website* SWIFtS. Menentukan usulan strategi perlakuan risiko yang tepat dalam mengatasi permasalahan yang sesuai dengan pencegahan risiko. Berdasarkan nilai yang diperoleh pada tahap analisis risiko, matrik risiko menghasilkan bahwa setiap risiko yang terjadi pada aset baik data, perangkat lunak, perangkat keras, sumber daya manusia dan prosedur yang terkait pada sistem SWIFtS memiliki nilai tingkatan risiko dari terendah, menengah dan tinggi. Perlu adanya perlakuan yang diberikan pada setiap risiko guna meminimalisir atau mencegah dan mengurangi setiap risiko yang ada. Berikut Tabel VIII adalah hasil usulan perlakuan risiko pada *website* SWIFtS.

TABEL VIII
HASIL USULAN PERLAKUAN RISIKO PADA SWIFTS

Komponen / Sumber Daya Aset IT	**ID**	**Risiko**	**Perlakuan**
Data	R1	Kebakaran	Menyediakan hardware yang baru. Melakukan pemindahan data dari setiap stasiun ke *server* baru. Melakukan pemindahan data secara berkala. Perusahaan menyediakan alat pemadam kebakaran. Pemilihan lokasi data *center* yang tepat.
	R2	Petir	Menyediakan penangkal petir. Melakukan *back up* data sebelum terjadi petir, sehingga *forecaster* dapat tetap melakukan *forecast*. Melakukan cek pada setiap stasiun. Melakukan *monitoring* data secara berkala. Menerapkan tata kelola standar data *center* meliputi standar prosedur operasi, standar prosedur perawatan, standar dan rencana pemulihan dan mitigasi bencana serta jaminan kelangsungan bisnis.
Perangkat Lunak	R27	Debu / Kotoran	Melakukan pengecekan jaringan. Melakukan pengecekan pada *server* utama. Melakukan *restart* sistem operasi.
Perangkat Lunak	R28	*Human Error*	Melakukan teguran lisan, apabila masih melakukan kesalahan yang sama maka akan diberikan teguran secara tertulis. Melakukan pelatihanterhadap sumber daya manusia. Melakukan pemetaan terhadap kemampuan masing-masing invidu. Melakukan pembagian tugas yang sesuai dengan kemampuan masing-masing individu.
Perangkat Keras	R41	Debu / Kotoran	Melakukan perawatan secara manual terhadap *server*. Melakukan analisis terhadap kebersihan lokasi alat dan *server*. Melakukan prosedur perlengkapan dalam melakukan perawatan alat dan *server*.
Komponen / Sumber Daya Aset IT	**ID**	**Risiko**	**Perlakuan**

	R42	Radiasi Panas	Menyediakan pendingin ruangan. Melakukan pemeliharaan terhadap alat secara berkala.
	R43	Suhu yang bervariasi	Melakukan pemeliharaan pendingin ruangan. Melakukan pengecekan terhadap alat.

IV. KESIMPULAN

A. Kesimpulan

Berdasarkan hasil analisis manajemen risiko pada *website* SWIFtS, terdapat beberapa poin yang menjadi simpulan, diantaranya :

- Analisis terhadap *website* SWIFtS menggunakan ISO 31000 dilakukan dalam beberapa tahapan antara lain komunikasi dan konsultasi, menetapkan konteks, asesmen risiko dan perlakuan risiko. Pada asesmen risiko terdiri dari beberapa proses didalamnya seperti identifikasi risiko, analisis risiko dan evaluasi risiko.
- Setelah dilakukan serangkaian proses manajemen risiko berdasarkan ISO 31000, maka didapatkan hasil tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi adalah asset, baik data perangkat lunak, perangkat keras, sumber daya manusia dan prosedur yang terkait pada sistem SWIFtS yang dinilai dapat mengganggu proses bisnis LAPAN itu sendiri. Sehingga diperlukan peninjauan kembali oleh pihak kepala Divisi IT LAPAN dan penerapan pada perlakuan risiko yang disarankan.
- Berdasarkan hasil analisis, didapatkan bahwa hampir setiap aset dan perangkat pendukung sistem SWIFtS membutuhkan koneksi dan asupan listrik yang baik dan konstan, sehingga perangkat dapat berjalan dengan optimal dan tidak mengganggu proses bisnis perusahaan. Perlu untuk diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik dan optimal.

B. Saran

Berdasarkan hasil analisis manajemen risiko yang dilakukan pada *website* SWIFtS, Adapun saran yang dapat diberikan untuk penelitian selanjutnya, diantaranya :

- Perusahaan dapat menyediakan laporan-laporan auditor, data-data historis risiko serta dokumen-dokumen organisasi untuk memudahkan dalam proses pengumpulan informasi.
- Penanganan yang dilakukan pada *website* SWIFtS dan setiap aset yang terkait secara umum telah dilakukan, hanya saja Divisi IT LAPAN tidak memiliki dokumen *Standard Operational Procedure* atau SOP yang berhubungan dengan manajemen risiko TI di LAPAN. Strategi penanganan terhadap risiko yang memiliki fungsi control dan mencegah terjadinya risiko yang muncul. Sehingga disarankan untuk memiliki dokumen SOP untuk mempermudah sumber daya manusia dalam menjalankan system SWIFtS.
- Dengan mengimplemetasikan usulan *risk treatment* dan melanjutkan ke tahap *monitoring* dan *review*, diharapkan di masa depan nilai dari setiap tingkatan risiko pada setiap risiko yang terjadi pada *website* SWIFtS dapat menurun dan LAPAN dapat menghasilkan strategi penanganan risiko yang lebih baik.
- Disarankan perusahaan dapat mengambil studi kasus dalam memperluas penggunaan ISO 31000 secara menyeluruh pada perusahaan.

V. DAFTAR PUSTAKA

[1] M. J. Raymond and P. George, Sistem Informasi Manajemen Edisi Kesembilan, Jakarta: PT.Index, 2011.

[2] D. A, "ISO 31000 *Risk Management*," *The Golden Standard*, vol. 45, no. 5, p. 5, 2012.

[3] H. P, Fundamental of *Risk Management* : Understanding, Evaluating, and Implementing Effective *Risk Management*, London: Kogan Page, 2010.

[4] H. J.J, Fundamentals of Enterprise *Risk Management*: How Top Companies Assess *Risk*, Manage Exposesures, and Seize Opportunities, New York: AMACOM, 2009.

[5] G. Joyce, "ISO *Risk Management*," *Guidelines and Principles*, 2009.

[6] S. Leo J and R. K. Victor, Manajemen Risiko Berbasis ISO 31000 Untuk Industri Non Perbankan, Jakarta: PPM, 2010.

[7] G. M. Husein and R. V. Imbar, "Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document *Management* System di PT. Jabar Telematika (JATEL)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 1, no. 2, p. 4, August 2015.

[8] R. Fauzan and R. Latifah, "Audit Tata Kelola Teknologi Informasi Untuk Mengontrol Manajemen Kualitas Menggunakan Cobit 4.1 (Studi Kasus : PT Nikkatsu Electric Works)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 1, no. 3, p. 2, December 2015.

[9] A. Kadir and T. Triwahyuni, Pengantar Teknologi Informasi Edisi Revisi, Yogyakarta: ANDI, 2013.

[10] J. S. Leo and R. K. Victor, Panduan Manajemen Risiko Berbasis ISO 31000 Industri Non-Perbankan Cetakan ke-3, Jakarta: PPM, 2014.

[11] D. Darmawan and N. Kunkun, Sistem Informasi Manajemen, Bandung: PT REMAJA ROSDAKARYA, 2013.

[12] S. John W, J. Robert B and B. Stephen D, Systems Analysis and Design in a Changing World, 7th Edition, Boston: Course Technology, 2015.

[13] J. A. O'Brien and G. M. Marakas, Introduction to Information System, 13th, Boston: McGraw-Hill Irwin, 2007.

[14] Y. H. M. and R. Hidayat, CMM Website Interaktif MCMS Joomla (CMS), Jakarta: PT. Elex Media Komputindo, 2009.