UNIVERSITAS KRISTEN MARANATHA

Volume 01 | Nomor 02 | Agustus 2015

JuTISI

Jurnal Teknik Informatika dan Sistem Informasi

9 772443 221007 >

ISSN: 2443-2210 | Halaman 053-193

ISSN: 2443-2210 Volume 1 Nomor 2 Agustus 2015

PENERBIT (PUBLISHER)
Maranatha University Press

ALAMAT PENYUNTING (EDITORIAL ADDRESS)
Sekretariat Jurnal Teknik Informatika dan Sistem Informasi
Fakultas Teknologi Informasi
Jl. Prof. Drg. Suria Sumantri, MPH, No.65 Bandung 40164
Telp. (022) 2012186 ext.1712, Fax (022) 2005915
E-mail: jutisi@it.maranatha.edu
Website: http://jutisi.maranatha.edu/

ISSN: 2443-2210 Volume 1 Nomor 2 Agustus 2015

DAFTAR ISI

Volume 1 Nomor 2

Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada *Document Management System* di PT. Jabar Telematika (JATEL)

Gilang M. Husein[#1], Radiant Victor Imbar[*2]

[#]*Jurusan Sistem Informasi, Universitas Kristen Maranatha Bandung*
[1]mchmd.hussein@gmail.com
[2]radiantv@gmail.com

Abstract — **ADEL (Aplikasi Dokumen Elektronik) and NADINE (Naskah Dinas Elektronik) are the use of information technology (IT) document management system (DMS) electronic archive product that used by JATEL to enhance information quality and to establish an information dan document workflow so it becomes easier, faster, and well-maintained. Electronic archive IT systems are designed to increase the value and benefits of information and able to control the documents distribution and disposition simultaneously that can increase JATEL business value and support business process automation. Information technology can assist organization but also present risks that need to be managed properly. To anticipate or reduce the likelihood of risk, information technology risk management is required. The implementation of information technology risk management involve risk identification, risk assessment, including risk analysis using bow-tie analysis, qualitative analysis also semi-quantitative analysis, and risk treatment so that risks can be identified, assess, and risk treatment strategy can be planned. With the implementation of information technology risk management at document management system in JATEL risks can be managed and prevented by eliminating sources of risk or reducing susbstantially the likelihood of occurrence.**

Keywords — ***risk identification, risk assessment, risk treatment, bow-tie analysis, qualitative analysis and semi-quantitative analysis.***

I. PENDAHULUAN

A. Latar Belakang

PT. Jabar Telematika (JATEL) merupakan anak perusahaan dari PT. Jasa Sarana, Badan Usaha Milik Daerah (BUMD) Pemerintah Provinsi Jawa Barat yang bergerak dibidang Infrastruktur. Melalui PT Jabar Telematika, PT Jasa Sarana mengembangkan 3 (tiga) layanan, yaitu: layanan akses internet kecepatan tinggi, layanan jaringan komunikasi data terintegrasi dan layanan *payment switching*. JATEL, sebagai perusahaan yang bergerak dibidang telematika, memiliki beberapa produk teknologi informasi yang digunakan untuk menunjang peningkatan kualitas informasi. Dalam membangun alur kerja informasi dan dokumen sehingga proses atau alur informasi dokumen menjadi lebih mudah, cepat, dan terkelola dengan baik JATEL menerapkan *Document Management System* arsip elektronik yaitu Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE). Sistem arsip eletronik ini dirancang untuk meningkatkan nilai dan manfaat informasi serta mampu mengawasi distribusi dan disposisi dokumen dalam waktu bersamaan sehingga berdampak pada peningkatan *business value* JATEL.

Melalui Teknologi Informasi (TI), berupa sistem arsip elektronik, JATEL dapat melakukan proses bisnis yang lebih efisien. Sistem TI juga mendukung otomatisasi proses bisnis dan penyediaan informasi untuk pengambilan keputusan. Namun dalam penerapannya, TI tidak selalu berjalan sesuai dengan yang diharapkan oleh perusahaan, sehingga akan menimbulkan risiko yang merugikan perusahaan. Untuk mengantisipasi atau mengurangi kemungkinan terjadinya risiko tersebut maka diperlukan analisis manajemen risiko teknologi informasi. Penerapan dari analisis manajemen risiko teknologi informasi meliputi *risk identification*, *risk assessment* serta *risk treatment*.

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan pada bagian sebelumnya, maka perumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana proses analisis manajemen risiko teknologi informasi pada *document management system* arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL?
2. Apa sajakah risiko yang terjadi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL?
3. Bagaimana hasil dari analisis manajemen risiko teknologi informasi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL?

C. Tujuan Pembahasan

Tujuan yang ingin dicapai dari pembahasan penelitian ini adalah dengan melakukan analisis menjemen risiko teknologi informasi maka dapat diidentifikasi risiko *(risk identification*) yang terjadi dalam penerapan *document menegement* sistem arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL. Melakukan penilaian risiko (*risk assessment*) serta perlakuan terhadapan risiko (*risk treatment*). Nantinya, hasil analisis manajemen risiko teknologi informasi pada *document management system* arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL diharapkan dapat mengantisipasi dan mencegah kemungkinan terjadinya risiko (*risk prevention*). Tujuan pembahasan dapat dirumuskan sebagai berikut:

1. Melakukan proses analisis manajemen risiko teknologi informasi pada *document management system* arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL.
2. Menganalisis risiko yang terjadi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL.
3. Menghasilkan analisis manajemen risiko teknologi informasi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL.

II. KAJIAN TEORI

A. Pengertian Risiko

Definisi *risk* atau risiko pada *The Oxford English Dictionary* adalah *'A chance or possibility of danger, loss, injury, or other adverse consequences'* [1]. Dan definisi *at risk* atau berisiko dari sumber yang sama adalah *'exposed to danger'* [1]. Dalam konteks ini risiko selalu dikaitkan dengan konsekuensi negatif namun menghadapi atau mengambil risiko juga dapat menghasilkan dampak positif. Kemungkinan lainnya risiko bisa berujung pada konsekuensi yang tidak dapat dipastikan.

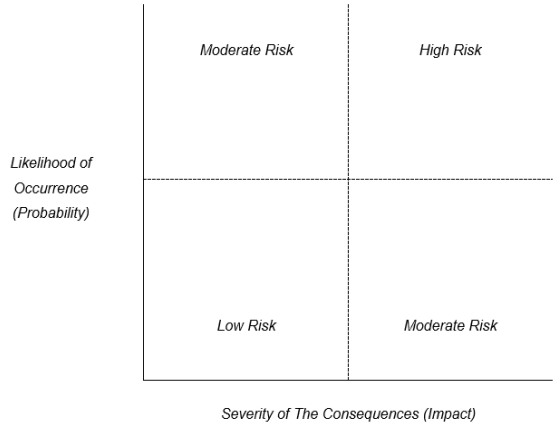
TABEL I
DEFINITION OF RISK[2]

Organization	Definition of risk
ISO Guide 73 ISO 31000	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.
Institute of Risk Management (IRM)	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.
"Orange Book" from HM Treasury	Uncertainty of outcome, within a range of exposure, arising from a combination of the impact and the probability of potential events.
Institute of Internal Auditors	The uncertainty of an event occurring that could have an impact on the achievement of the objectives. Risk is measured in terms of consequences and likelihood.
Alternative Definition by the author	Event with the ability to impact (inhibit, enhance or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and / or the delivery of stakeholder expectations.

Sedangkan risiko menurut ISO Guide 73 ISO 31000 adalah pengaruh ketidakpastian pada tujuan. Pengaruh bisa saja positif, negatif, atau penyimpangan dari yang diharapkan. Risiko juga sering digambarkan sebagai sebuah peristiwa, perubahan dalam keadaan atau konsekuensi. Menurut *Institute of Risk Management* (IRM) risiko merupakan gabungan antara kemungkinan sebuah kejadian beserta konsekuensinya. Konsekuensinya berkisar dari konsekuensi positif hingga konsekuensi negatif. *"Orange Book"* dari *HM Treasury* mendefinisikan risiko sebagai ketidakpastian hasil, dalam berbabagi paparan, timbul dari kombinasi antara dampak dan kemungkinan dari peristiwa. *Institute of Internal Auditors* menjelaskan bahwa risiko adalah ketidakpastian suatu peristiwa yang terjadi yang berdampak pada pencapaian sebuah tujuan. Risiko diukur dengan konsekuensi dan kemungkinan. Sedangkan menurut Paul Hopkins, risiko merupakan suatu peristiwa dengan kemampuan untuk mempengaruhi (menghambat, meningkatkan, atau menyebabkan keraguan) misi, strategi, proyek, operasi rutin, tujuan, proses inti, kunci dependensi dan/atau harapan dari *stakeholder* [2].

B. Konsep Risiko

Risiko, seperti telah dijelaskan pada bagian sebelumnya, 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 [2].



Gambar 2 *Concept of Risk* [3]

Berdasarkan Gambar 1 tentang konsep Risiko maka dapat diketahui *level of risk* (tingkatan risiko). Berdasarkan variabel yang digunakan, *probability* dan *impact*, maka *level of risk* dapat diklasifikasikan sebagai berikut [3]:

1. *Low Probability Low Impact = Low Risk.*
   Risiko ini adalah risiko dengan tingkat pengaruh yang paling kecil dibandingkan dengan risiko lainya sehingga, dengan kebijakan tertentu, risiko ini dapat diabaikan.

2. *Low Probability High Impact = Moderate Risk.*
   Risiko dengan tingkat pengaruh menengah, meskipun begitu risko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan tergantung dari dampak yang diberikan.
3. *High Probability Low Impact = Moderate Risk.*
   Risiko dengan tingkat pengaruh menengah. Berbeda dengan *low probability high impact* risiko ini hanya perlu dimonitor.
4. *High Probability High Impact = High Risk.*
   Risiko dengan pengaruh yang paling tinggi dibandingkan dengan lainnya. Merupakan risiko berbahaya yang harus diatasi secepatnya.

C. Pengertian Manajemen Risiko

Manajemen risiko mengacu pada budaya, proses dan struktur yang diarahkan pada pengelolaan ketidakpastian [4]. Proses pada manajemen risiko terjadi secara sistematis, terus menerus dan diterapkan dalam segala aspek [2]. Dalam konteks organisasi, manajemen risiko diterapkan dalam seluruh bidang yang terdapat dalam organisasi tersebut.

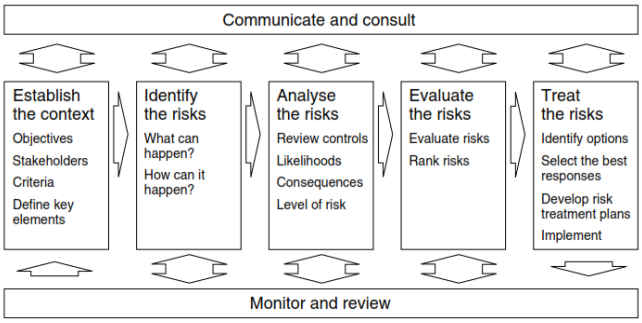
TABEL II
DEFINITION OF RISK MANAGEMENT [2]

Organization	Definition of risk management
ISO Guide 73 BS 31100	Coordinated activities to direct and control an organization with regard to risk
Institute of Risk Management (IRM)	Process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure
HM Treasury	All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress
London School of Economics	Selection of those risks a business should take and those which should be avoided or mitigated, followed by action to avoid or reduce risk
Business Continuity Institute	Culture, processes and structures that are put in place to effectively manage potential opportunities and adverse effects

Menurut ISO Guide 73 BS31100 manajemen risiko adalah aktivitas yang terkoordinasi untuk mengarahkan dan mengendalikan organisasi dari hal-hal yang berkaitan dengan risiko. *Institute of Risk Management* (IRM) mendefinisikan manajemen risiko sebagai proses yang bertujuan untuk membantu organisasi memahami, menilai dan mengambil tindakan pada semua risiko dengan maksud untuk meningkatkan kemungkinan keberhasilan dan mengurangi kemungkinan kegagalan. *HM Treasury* menjelaskan manajemen risiko sebagai semua proses yang terlibat dalam mengidentifikasi, menilai, dan mempertimbangkan risiko, menetapkan kepemilikan, mengambil tindakan untuk mengurangi atau mengantisipasi risiko, dan pemantauan dan peninjauan kemajuan. Sedangkan menurut *London School of Economics* risiko bisnis harus diambil dan dipilah yang harus dihindari dan dikurangi diikuti oleh tindakan menghindar atau mengurangi risiko. Sedangkan menurut *Business Continuity Institute* manajemen risiko merupakan budaya, proses dan struktur yang diletakan untuk mengelola potensi peluang dan efek merugikan secara efektif [2].

D. Proses Manajemen Risiko

Proses pada manajemen risiko melibatkan pengaplikasian secara sistematis dari pengelolaan kebijakan, proses dan prosedur hingga proses dalam penentuan konteks, mengidentifikasi, menilai, memperlakukan, mengamati, dan mengkomunikasikan risiko [4].



Gambar 3 *Risk Management Process* [4]

Proses dari manajemen risiko berfungsi membantu dalam melakukan pengambilan keputusan yang lebih baik dan meningkatkan efisiensi. Meskipun banyak cara dalam menggambarkan proses manajemen risiko, langkah-langkah dasar yang terdapat dalam proses ini hampir serupa dan biasanya mencakup tiga langkah utama yaitu: *risk identification, risk assessment,* dan *risk treatment*

1. *Risk Identification*
   Risk identification merupakan proses dalam menentukan apa, bagaimana, dan mengapa suatu kondisi atau kejadian dapat terjadi. Proses identifikasi risiko harus dilakukan secara komprehensif, harus terstruktur berdasarkan faktor-faktor utama agar nantinya risiko dapat dinilai secara sistematis [4]. Risiko dapat diidentifikasi melalui beberapa metode seperti; *checklist, interview* atau *focused group discussion* dan *questionnaries.*
   Checklist digunakan untuk menyederhanakan proses identtifikasi risiko. *Checklist* juga dirancang untuk menghindari atau meminimalkan risiko, seringkali *checklist* merupakan bagian dari prosedur dokumentasi dan jaminan kualitas organisasi.
   Questionnaries atau kuesioner merupakan instrumen penelitian yang terdiri dari serangkaian pertanyaan dan petunjuk lainnya dengan tujuan untuk mengumpulkan informasi tertentu dari responden.
2. *Risk Assesment*
   Risk assesment merupakan keseluruhan proses dari *risk analysis* dan *risk evaluation. Risk analysis* adalah

proses sistematis dalam menggunakan informasi yang ada untuk menentukan seberapa sering risiko dapat terjadi dan seberapa besar dampak yang dihasilkan bila risiko tersebut terjadi [4]. Proses penilaian risiko pada *risk analysis* dapat dilakukan dengan metode seperti; *bow-tie analysis*, *qualitative analysis*, dan *semi-quantitative analysis.* Sedangkan *risk evaluation* adalah proses dalam membandingkan risiko yang telah diperkirakan dengan kriteria risiko yang telah ditentukan [4]. Evaluasi risiko memperhitungkan apakah risiko dapat ditoleransi atau tidak didasarkan pada *level of risk* (tingkatan risiko) pada matriks risiko.
Bow-tie analysis pada *risk analysis* merupakan metode analisis yang digunakan untuk menggambarkan kegiatan manajemen risiko agar lebih mudah dimengerti dan diakses.

Gambar 4 *Bow-tie Analysis*

Sisi kiri dari dasi kupu-kupu merupakan sumber bahaya (*hazard*) tertentu dan menunjukan sistem klasifikasi yang digunakan oleh organisasi untuk sumber risiko. Sisi kanan dari dasi kupu-kupu menetapkan konsekuensi (*consequences*) dari peristiwa yang terjadi. Di bagian pusat, adalah *risk event* (kejadian risiko). Tujuan menggunakan ilustrasi dasi kupu-kupu adalah untuk menunjukan sistem klasifikasi risiko yang digunakan oleh organisasi. Kontrol (*control*) dapat diletakan untuk mencegah peristiwa yang terjadi dan diwakili oleh garis vertikal di sisi kiri dasi kupu-kupu. Pemulihan (*recovery*) dapat direpresentasikan dengan cara yang sama di sisi kanan dasi kupu-kupu [2]
Qualitative Analysis atau analisis kualitatif pada *risk analysis* didasarkan pada nominal atau skala deskriptif untuk menggambarkan *likelihood* dan *consequences* dari risiko, sedangkan *semi-quantitative analysis* atau analisis semi-kuantitatif pada *risk analysis* memperluas proses analisis kualitatif dengan mengalokasikan nilai numerik pada skala deskriptif.

3. *Risk Treatment*
   Risk treatment bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan [4]. *Risk treatment* merubah analisis sebelumnya, *risk identification* dan *risk assessment*, menjadi tindakan substantif untuk mengurangi risiko.

Terdapat beberapa *risk treatment* yang umumnya digunakan, yaitu; *risk prevention* (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, *risk mitigation* (mitigasi risiko) dengan tujuan untuk meminimalkan konsekuansi dari risiko, *risk sharing* (berbagi risiko) dengan tujuan untuk memindahkan risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupin individu, dan *risk retention* (retensi risiko) atau dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko.

E. 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 [2].

Berikut merupakan *risk management framework* yang digunakan dalam penelitian:

1. *Symantec: Risk Management Report*
   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 [7].

Gambar 5 *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*).

2. COBIT 5 *for Risk*

COBIT adalah kerangka kerja (*framework)* yang dibuat oleh ISACA untuk manajemen teknologi informasi (TI) dan tata kelola IT. COBIT adalah *toolset* yang memungkinkan penggunanya untuk menjembatani kesenjangan antara kebutuhan kontrol, masalah teknis dan risiko bisnis [8].

Sumber daya TI yang diidentifikasikan dalam COBIT dapat dijelaskan secara singkat sebagai berikut [9]:

- Aplikasi (*Application*), merupakan suatu sarana atau *tool* yang digunakan untuk mengolah dan menyimpulkan atau meringkas, baik prosedur manual maupun yang terprogram.
- Informasi (*Information*), adalah data-data yang telah diolah untuk kepentingan manajemen dalam membantu mengambil keputusan dalam menjalankan roda bisnisnya. Data-data terdiri obyek-obyek dalam pengertian yang lebih luas (yakni internal dan eksternal), terstruktur dan tidak terstruktur, grafik, suara dan sebagainya.
- Infrastruktur (*infrastructure*), mencakup *hardware, software,* sistem operasi, sistem manajemen database, jaringan (*networking*), multimedia, dan fasilitas-fasilitas lainnya.
- Sumber Daya Manusia/SDM (*People*), merupakan sumber daya yang paling penting bagi organisasi dalam pengelolaan dan operasionalisasi bisnis organisasi. Kesadaran dan produktivitasnya dibutuhkan untuk merencanakan, mengorganisasikan, melaksanakan, memperoleh, menyampaikan, mendukung, dan memantau layanan TI organisasi.

F. Document Management System

Manajemen dokumen, sering disebut sistem manajemen dokumen atau *Document Management System* (DMS), adalah penggunaan sistem komputer dan perangkat lunak untuk menyimpan, mengelola, dan untuk melacak dokumen elektronik dan gambar elektronik dari informasi berbasis kertas.

TABEL III
KOMPONEN *DOCUMENT MANAGEMENT SYSTEM*

Komponen	Deskripsi
Metadata	Metadata biasanya tersimpan dalam tiap dokumen. Salah satu contoh dari metadata adalah tanggal dokumen itu disimpan dan identitas pengguna yang menyimpannya. DMS juga dapat mengekstrak metadata dari dokumen secara otomatis atau meminta pengguna untuk menambahkan metadata. Beberapa sistem bahkan menggunakan *optical charater recogniton* pada gambar, atau melakukan *text extraction* pada dokumen elektronik. Hasil dari teks yang telah diekstraksi dapat digunakan untuk membantu pengguna dalam menemukan dokumen dengan mengidentifikasi kata kunci. Teks yang terekstraksi juga dapat disimpan sebagai komponen dari metadata, disimpan dengan gambar, atau disimpan secara terpisah sebagai sumber untuk mencari dokumen.
Integration	Banyak *document management system* berusaha untuk mengintegrasikan sistemnya langsung ke aplikasi lain, sehingga pengguna dapat mengambil dokumen yang ada secara langsung dari repositorinya, membuat perubahan, dan menyimpan dokumen yang telah dirubah kembali ke repositori sebagai versi yang baru tanpa meninggalkan aplikasi *document management system*. Integrasi tersebut umumnya tersedia untuk aplikasi perkantoran dan e-mail atau perangkat lunak kolaborasi atau *groupware*.
Capture	*Capture* melibatkan penerimaan dan pemrosesan gambar dari dokumen kertas ke pemindai (*scanner*) atau printer multifungsi. *Optical character recognition software* (OCR) sering digunakan, baik diintegrasikan dengan perangkat keras atau perangkat lunak yang berdiri sendiri (*stand-alone software*), untuk mengkonversi gambar digital ke dalam mesin teks yang dapat dibaca. *Optical mark recognition software* (OMR) kadang-kadang digunakan untuk mengekstrak isian kotak centang (*checkbox*) atau gelembung (*bubbles*)
Validation	*Visual validation registration system*. Contohnya kesalahan dokumen, tanda tangan yang hilang, kesalahan ejaan dapat dicetak pada dokumen atau gambar pada dokumen.
Indexing	*Indexing* dapat melacak dokumen elektronik. Meskipun hanya sesederhana melacak indeks dokumen yang unik tetapi *indexing* seringkali memiliki bentuk yang lebih kompleks seperti memberikan klasifikasi melalui metadata atau bahkan melalui indeks kata yang diekstrak dari isi dokumen. Fungsi utama *indexing* adalah untuk mendukung pengambilan (*retrieval*). Pembuatan index *topology* diperlukan untuk melakukan pengambilan cepat (*rapid retrieval*).
Storage	Menyimpan dokumen elektronik. Penyimpanan dokumen mencakup pengelolaan dokumen seperti: Di mana mereka disimpan, untuk berapa lama dokumen disimpan, migrasi dokumen dari satu media penyimpanan ke media penyimpanan lainnya dan pemusnahan dokumen akhir (*eventual document destruction*)
Retrieval	Mengambil dokumen dari storage. Meskipun gagasan mengambil dokumen tertentu sederhana, namun dalam pengambilan (*retrieval*) dalam konteks dokumen elektronik dapat menjadi sangat kompleks. Pengambilan dokumen tunggal secara sederhana dapat didukung dengan memungkinkan pengguna untuk menentukan indeks yang unik,

Komponen	Deskripsi
	memiliki sistem yang menggunakan indeks dasar (atau *non-indexed query* pada data store) untuk mengambil dokumen. Proses pengambilan dokumen yang lebih fleksibel memungkinkan pengguna untuk menentukan istilah pencarian parsial (*partial search terms*) yang melibatkan indeks dokumen dan/atau bagian dari metadata yang diharapkan. Dengan cara seperti ini, sistem akan memberikan daftar dokumen yang cocok dengan istilah pencarian (*search term*) pengguna.
Distribution	Dokumen yang diterbitkan untuk didistribusi harus memiliki format yang tidak dengan mudah diubah. Dokumen, dalam industri yang diatur oleh hukum, salinan asli dokumen tidak pernah digunakan untuk distribusi selain pengarsipan. Dokumen yang akan didistribusikan secara elektronik terlebih dulu harus divalidasi demikian pula sistem yang digunakan.
Security	Dalam *document management system* keamanan merupakan bagian penting. *Complience requirements* untuk dokumen-dokumen tertentu bisa saja sangat kompleks. Beberapa *document management system* memiliki modul manajemen hak yang memungkinkan administrator untuk memberikan akses ke dokumen berdasarkan kelompok orang tertentu atau *user group*. *Marking* (penandaan) pada dokumen saat pencetakan atau penciptaan PDF merupakan elemen penting untuk mencegah perubahan atau penggunaan yang tidak diinginkan.
Workflow	*Workflow* adalah proses yang kompleks dan *document management system* memiliki model alur kerja tersendiri (*built-in workflow module*). Ada berbagai jenis alur kerja. Penggunaannya tergantung pada lingkungan dimana *document management system* diterapkan. Panduan alur kerja mengharuskan pengguna untuk melihat dokumen dan memutuskan kepada siapa dokumen akan dikirim. Alur kerja berbasis aturan (*rule-based workflow*) memungkinkan administrator untuk membuat aturan yang mendikte aliran dokumen dalam organisasi: misalnya, faktur melewati proses persetujuan dan kemudian diteruskan ke departemen *account-payable*. Aturan yang dinamis memungkinkan dibuatnya cabang pada proses alur kerja. Contoh sederhananya adalah memasukan sejumlah faktur dan jika jumlahnya lebih rendah dari jumlah tertentu yang telah ditetapkan makan faktur tersebut akan mengikuti alur kerja organisasi yang berbeda. Mekanisme alur kerja yang canggih (*advance workflow mechanism*) dapat memanipulasi konten atau sinyal proses eksternal selagi aturan tersebut berjalan.
Collaboration	*Collaboration* harus melekat dalam *document management system*. Dalam bentuk dasarnya, *colabortive* DMS harus memungkinkan dokumen diambil dan dikerjakan oleh pengguna yang diizinkan (*authorized user*). Akses harus diblokir sementara untuk pengguna lain saat pekerjaan sedang dilakukan pada dokumen. Bentuk lain dari kolaborasi memungkinkan beberapa pengguna untuk melihat dan memodifikasi dokumen pada waktu yang bersamaan pada sesi kolaborasi. Dokumen yang dihasilkan harus dilihat dalam bentuk akhir, dan dalam waktu yang bersamaan juga menyimpan modifikasi yang dilakukan oleh tiap individu dalam sesi kolaborasi.
Versioning	*Versioning* adalah proses dimana dokumen masuk dan keluar diperiksa dalam *document management system*, yang memungkinkan pengguna untuk menggambil versi sebelumnya dan untuk melanjutkan pekerjaan dari titik acuan yang telah dipilih. *Versioning* sangat berguna bagi dokumen yang terus berubah dari waktu ke waktu dan yang memerlukan pembaharuan, tapi tetap dapat kembali atau mereferensi ke salinan sebelumnya.
Searching	Mencari dokumen dan berkas menggunakan atribut atau pencarian teks lengkap (*full text search*). Dokumen dapat dicari menggunakan berbagai atribut dan isi dokumen.
Publishing	*Document publishing* melibatkan prosedur *proofreading, public viewing, authorize, printing* dan *approving*. Penanganan yang tidak semestinya dapat menyebabkan ketidakakuratan dokumen. Dalam industri yang diatur oleh hukum beberapa prosedur harus dibuktikan oleh tanda tangan dan tanggal dimana okumen tersebut ditandatangani. Dokumen yang dipublikasikan harus dalam format yang tidak mudah diubah tanpa pengetahuan atau alat khusus.

III. ANALISIS DAN EVALUASI

A. Risk Identification

Pada proses identifikasi risiko dilakukan pengelompokan risiko berdasarkan sumber daya TI, yang didefinisikan oleh COBIT, yang berhubungan dengan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL.

Identifikasi yang dilakukan menghasilkan beberapa risiko yang mungkin terjadi pada setiap sumber daya TI yang dimiliki oleh PT. Jabar Telematika (JATEL) antara lain:

1. *Application*
   - *External Attacks*
   - *Malicious Code*
   - *Network Congestion*
   - *System Crash*
2. *Information*
   - *Database Failure*
   - *Data/Document Fraud*
3. *Infrastructure*
   - *Physical Damage*
   - *Hardware Failure*
   - *Power Outages*
   - *Force Majure*

4. *People*
   - *Inappropriate Access*
   - *Abuse of Position of Trus*
   - *Disgruntled Employees*

B. *Risk Assessment*

Pada proses ini dilakukan penilaian terhadap risiko yang terjadi *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL. Penilaian terhadap risiko merupakan gabungan proses yang terdiri dari *risk analysis* (analisis risiko) dan *risk evaluation* (evaluasi risiko).

Penilaian risiko terhadap risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dilakukan untuk mengevaluasi dan mengestimasi *level of risk* (tingkatan risiko) dari masing-masing risiko yang telah diidentifikasi pada proses identifikasi risiko dan menetapkan *acceptable level of risk* (tingkatan risiko yang dapat diterima) organisasi.

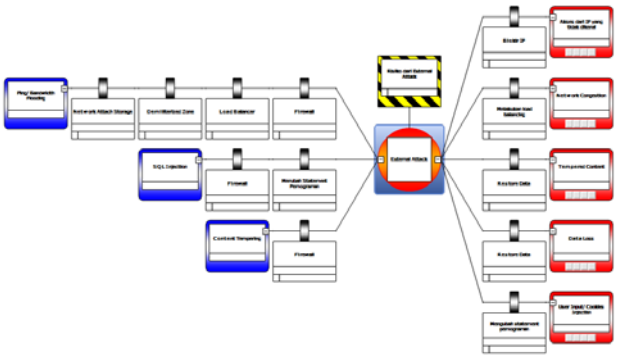
1. *Risk Analysis*
   Analisis risiko dilakukan untuk menentukan seberapa sering risiko pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dapat terjadi dan seberapa besar dampak yang dihasilkan apabila risiko tersebut terjadi.

o *Bow-tie Analysis*
   Bow-tie Analysis dilakukan agar proses analisis terhadap risiko menghasilkan *recovery* (pemulihan) dan *control* (kontrol).

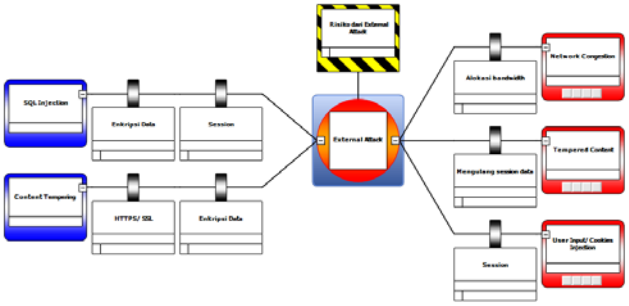
TABEL IV
TABEL *BOW-TIE ANALYSIS* PADA *EXTERNAL ATTACKS*

Threats	Impact/ Consequences	Recovery	Control
Ping Flooding	*Bandwidth Consuming.* Aplikasi tidak dapat diakses. Akses dari IP yang tidak dikenal. *Network Congestion.*	Menghentikan *packet data* dari IP yang tidak dikenal. Memblokir akses dari IP yang tidak dikenal. Melakukan *load balancing.* Mengalokasikan *bandwidth.*	*Firewall. Load Balancer. Network Attach Storage* (NAS). *Demiliterized Zone* (DMZ). *Virtual Private Network* (VPN).
Bandwidth Flooding			
SQL Injection	Manipulasi Data. Pencurian Data. *User Input Injection. Cookies*	*Restore Data.* Mengubah *statement* pemograman. *Session.*	*Firewall.* Enkripsi Data. Merubah statement pemograman, *Session.*
	Injection.		
Content Tempering	*Tempered Content.*	*Restore Data.* Mengulang *session data.*	

Pada Tabel IV diketahui bahwa terdapat empat ancaman yang dapat menyebabkan kemungkinan terjadinya *external attacks* pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL, yaitu *ping flooding, bandwidth flooding, SQL Injection,* dan *Content Tempering*. Pada tabel yang sama dapat juga dilihat *impact/consequences, recovery*, dan *control* untuk *external attacks.*



Gambar 6 Diagram *Bow-tie Analysis* Pada *External Attacks*



Gambar 7 Diagram *Bow-tie Analysis* Usulan Pada *External Attacks*

Gambar 5 dan Gambar 6 merupakan diagram yang dihasilkan dari tabel *bow-tie analysis* pada kelompok risiko *external attacks.*

o Klasifikasi *Impact/Consequences* Pada Kelompok Risiko
Pada tahap ini dilakukan klasifikasi *impact/ consequences* tiap kelompok risiko pada sumber daya IT yang mendukung penerapan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL.

TABEL V
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *APPLICATION*

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
External Attacks	*Ping Flooding*	*Bandwidth Consuming*	*Performance*
		Aplikasi tidak dapat diakses	*Availability*
	Bandwidth Flooding	Akses dari IP yang tidak dikenal	*Security*
		Network Congestion	*Performance*
	SQL Injection	Manipulasi Data	*Security*
		Pencurian Data	*Security*
		User Input Injection	*Security*
		Cookies Injection	*Security*
	Content Tempering	*Tempered Content*	*Security*
Malicious Code	*Trojan Horses*	*Data Loss*	*Availability*
		Backdoor Access	*Security*
		Network Usage	*Performance*
		Adanya *Backdoor Programing*	*Security*
	Worms	Replikasi Data	*Security*
		Network Traffic	*Performance*
	Viruses	Replikasi Data	*Security*
		Manipulasi Data	*Security*
		Infected Areas	*Security*
	Phising	Pencurian Data	*Security*
Network Congestion	*Slow Network Throughtput*	Layanan Terganggu	*Performance*
		Aplikasi tidak bias diakses	*Availability*
		Bottleneck	*Performance*
System Crash	*Application Crashes*	Aplikasi tidak dapat digunakan	*Availability*
		Data Loss	*Availability*
	Web Server Crashes	Aplikasi/ web server tidak dapat diakses	*Availability*
	Operation System Crashes	*Kernel Panic*	*Availability*

Pada Tabel V dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *application.*

TABEL VI
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *INFORMATION*

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
Database Failure	*Statement Failure*	*Looping*	*Performance*
		Memory Penuh	*Performance*
		Data tidak tersimpan	*Compliance*
	System Crash	*Error Connection Database*	*Availability*
		Application Crashes	*Availability*
		Web Server Crashes	*Availability*
		Operation System Crashes	*Availability*
	Human Error	Kesalahan Statement	*Performance*
		Kesalahan Prosedur yang menyebabkan kerusakan	*Compliance*
	Network Failure	Data tidak tersimpan karena kerusakan *network interface controller*	*Compliance*
		Error Connection Database	*Availability*
	Media Failure	Data tidak tersimpan karena ekstensi file tidak di *support*	*Compliance*
		Error Connection Database	*Availability*
	Disk Failure	*Bad Hardisk Sector*	*Availability*
	Corrupted File	*Corrupted Data*	*Availability*
Data/ Document Fraud	*Content Tempering*	*Tempered Content*	*Availability*
	Content Forging	*Forged Content*	*Availability*

Pada Tabel VI dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *information.*

TABEL VII
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *INFRASTRUCTURE*

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
Physical Damage	Pencurian Terhadap *Physical Asset*	Ketidak tersediaan infrastruktur	*Availability*
	Kerusakan Terhadap *Physical Asset*	Kerusakan Aset	*Availability*
		Data Loss	*Availability*
	Water Damage	Kerusakan Aset	*Availability*
		Data Loss	*Availability*
	Heat	Hardware tidak aktif	*Availability*
		Corrupted Data	*Availability*

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
		Data Loss	*Availability*
Hardware Failure	*Electrical Dischagrge*	Korsleting	*Availability*
		Kerusakan pada hardware/ modul	*Availability*
		Sengatan Listrik	*Compliance*
	Short Circuit	Kerusakan pada hardware/ modul	*Availability*
	Power Surges	*Server Interupts*	*Availability*
		Hard Bad Sector	*Availability*
	Overheating	Hardware tidak aktif	*Availability*
		Corrupted Data	*Availability*
		Data Loss	*Availability*
	Bad Hardisk Sector	*Hard Bad Sector*	*Availability*
		Soft Bad Sector	*Performance*
		Corrupted Data	*Availability*
		Data Loss	*Availability*
	Corrupted File	*Corrupted Data*	*Availability*
		Data Loss	*Availability*
	Human Error	Kerusakan Hardware	*Availability*
		Data loss	*Availability*
Power Outage	*Power Cut/ Power Blackout/ Power Failure*	Ketidak tersediaan Infrastruktur	*Availability*
Force Majure	Bencana Alam	Kerusakan Infrastruktur	*Availability*
		Kerusakan Hardware	*Availability*
		Data Loss	*Availability*

Pada Tabel VII dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *infrastructure.*

TABEL VIII
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *PEOPLE*

Kelompok Risiko	Threats	Impact/ Consequences	Klasifikasi
Inappropriate Access	*Unauthorized Access/ Man in The Middle*	Pencurian Data	*Security*
		Manipulasi Data	*Security*
		Akses yang tidak diinginkan	*Security*
Abuse of Position of Trust	*Inappropriate Access*	Manipulasi Data	*Security*
		Perubahan Konfigurasi	*Security*
	Content Tempering	*Tempered Content*	*Security*
	Content Forging	*Forged Content*	*Security*
	Penyebaran Informasi	Tersebarnya informasi rahasia	*Compliance*
Disgruntled Employees	*Unauthorized Access*	Manipulasi Data	*Security*
		Perubahan Konfigurasi	*Security*
	Penyebaran Informasi	Tersebarnya Informasi Rahasia	*Compliance*
	Lemahnya Pengetahuan Terhadap Aplikasi	*Output* dari aplikasi tidak optimal	*Performance*

Pada Tabel VIII dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *people.*

- *Qualitative* dan *Semi-Quantitative Analysis*

Qualitative dan *semi-quantitative analysis* dilakukan dengan memberikan nilai pada tiap risiko yang telah teridentifikasi berdasarkan *likelihood* dan *impact.*

Pada Tabel IX dan Tabel X dapat dilihat kriteria penilaian untuk risiko yang telah teridentifikasi dengan menggunakan metode *qualitative* dan *semi-quantitative analysis.*

TABEL IX
NILAI PADA *LIKELIHOOD*

Likelihood		Frekuensi per Tahun
Rating	Kriteria	
1	*Rare*	≤ 5 Kejadian
2	*Unlikely*	6 – 10 Kejadian
3	*Possible*	11 – 20 Kejadian
4	*Likely*	21 – 40 Kejadian
5	*Almost Certain*	≥ 41 kejadian

TABEL X
NILAI PADA *IMPACT*

Impact		Deskripsi
Rating	Kriteria	
1	*Insignificant*	Dampak mungkin diabaikan dengan aman.
2	*Minor*	Dampak kecil dan dapat diatasi dengan prosedur sederhana
3	*Moderate*	Dampak tergolong besar, namun dapat dikelola dengan menggunakan prosedur tertentu
4	*Major*	Dampak besar, berpotensi pada *financial cost* dan terhambatnya kinerja organisasi
5	*Catastrophic*	Dampak ekstrim, berpotensi pada *large financial cost* dan terhentinya kinerja organisasi, serta dampak pada reputasi organisasi

Setelah menentukan nilai pada *likelihood* dan *impact* maka penilaian pada masing-masing risiko yang telah didefinisikan pada proses sebelumnya dapat dilakukan. Penilaian risiko berdasarkan nilai *likelihood* dan *impact* secara detail dapat dilihat pada Tabel XI dan Tabel XII.

TABEL XI
IDENTIFIKASI *LIKELIHOOD* DAN *IMPACT*

No	Identifikasi Risiko	*Likelihood*	*Impact*
1	*External Attacks*	*Rare*	*Moderate*
2	*Malicious Code*	*Rare*	*Minor*
3	*Physical Damage*	*Rare*	*Moderate*
4	*Inappropriate Access*	*Rare*	*Major*
5	*Hardware Failure*	*Rare*	*Minor*
6	*Power Outages*	*Possible*	*Moderate*
7	*Database Failure*	*Rare*	*Moderate*
8	*Force Majure*	*Rare*	*Catastrophic*
9	*Network Congestion*	*Possible*	*Moderate*
10	*System Crash*	*Rare*	*Minor*
11	*Data/Documen Fraud*	*Rare*	*Major*
12	*Abuse of Position of Trust*	*Rare*	*Major*
13	*Disgruntled Employees*	*Unlikely*	*Minor*

TABEL XII
PENILAIAN *LIKELIHOOD* DAN *IMPACT*

No	Identifikasi Risiko	*Likelihood*	*Impact*
1	*External Attacks*	1	3
2	*Malicious Code*	1	2
3	*Physical Damage*	1	3
4	*Inappropriate Access*	1	4
5	*Hardware Failure*	1	2
6	*Power Outages*	3	3
7	*Database Failure*	1	3
8	*Force Majure*	1	5
9	*Network Congestion*	3	3
10	*System Crash*	1	2
11	*Data/Documen Fraud*	1	4
12	*Abuse of Position of Trust*	1	4
13	*Disgruntled Employees*	1	2

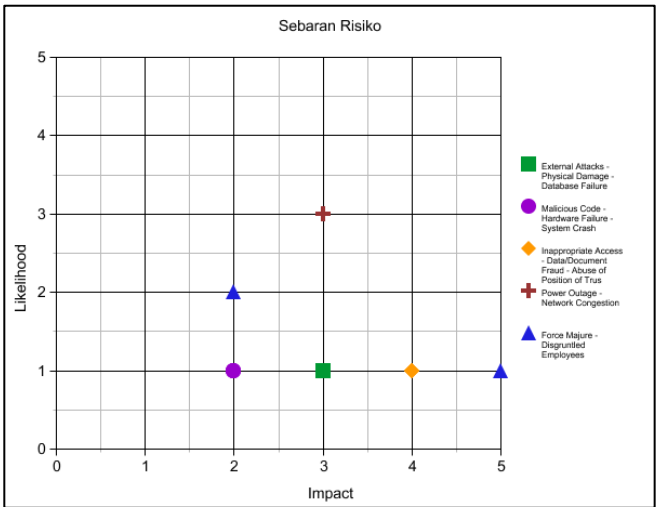
2. *Risk Evaluation*

Pada tahap evaluasi risiko, risiko yang telah teridentifikasi dievaluasi apakah risiko tersebut dapat ditoleransi atau tidak berdasarkan *level of risk* atau tingkatan risiko. Apabila risiko yang telah dinilai masuk kedalam kriteria yang ditetapkan maka risiko tersebut harus mendapatkan *treatment* (perlakuan) sebaliknya apabila risiko tidak termasuk kedalam kriteria yang ditetapkan maka perlakuan terhadap risiko tidak perlu dipertimbangkan lagi.

Evaluasi risiko dilakukan dengan menerapkan proses *mapping* pada grafik (x, y) yang menggambarkan hubungan antara *likelihood* atau frekuensi kejadian dan *impact* atau dampak yang diakibatkan oleh tiap-tiap risiko yang terjadi.

TABEL XIII
MATRIKS EVALUASI RISIKO

Likelihood					
5	Medium	Medium	High	High	High
4	Low	Medium	Medium	High	High
3	Low	Medium	Medium	Medium	High
2	Low	Low	Medium	Medium	High
1	Low	Low	Low	Medium	Medium
	1	2	3	4	5
			Impact		



Gambar 8 Grafik Sebaran Risiko Berdasarkan *Likelihood* dan *Impact*

Grafik hasil evaluasi tersebut dikategorikan menjadi 3 tingkatan *level of risk* yaitu, *low*, *medium*, dan *high* berdasarkan matriks evaluasi risiko. Matriks evaluasi risiko dapat dilihat pada Tabel XIII, sedangkan sebaran risiko berdasarkan *likelihood* dan *impact* dapat dilihat pada Gambar 10.

TABEL XIV
MATRIKS EVALUASI RISIKO BERDASARKAN *LIKELIHOOD* DAN *IMPACT*

Likelihood					
5					
4					
3			R6, R9		
2		R13			
1		R2, R5, R10	R1, R3, R7	R4, R11 R12	R8
	1	2	3	4	5
			Impact		

Keterangan:

R: Risiko	R7: *Database Failure*
R1: *External Attacks*	R8: *Force Majure*
R2: *Malicious Code*	R9: *Network Congestion*
R3: *Physical Damage*	R10: *System Crash*
R4: *Inappropriate Access*	R11: *Data/Document Fraud*
R5: *Hardware Failure*	R12: *Abuse of Position of Trust*
R6: *Power Outage*	R13: *Disgruntled Employees*

Tabel XIV – Matriks Evaluasi Risiko Berdasarkan *Likelihood* dan *Impact* memperlihatkan pengelompokan risiko berdasarkan kategori evaluasi *level of risk* risiko. Secara lebih lengkap evaluasi risiko berdasarkan *level of risk* dapat dilihat pada Tabel XV. Berdasarkan Sebaran Risiko dan *Likelihood-Impact* yang merupakan hasil penggabungan dari *mapping* grafik sebaran risiko dan matriks evaluasi risiko berdasarkan *likelihood* dan *impact.*

TABEL XV
EVALUASI *LEVEL OF RISK* BERDASARKAN SEBARAN RISIKO DAN *LIKELIHOOD-IMPACT*

No	Identifikasi Risiko	*Likelihood*	*Impact*	*Level of Risk*
1	*External Attacks*	1	3	*Low*
2	*Malicious Code*	1	2	*Low*
3	*Physical Damage*	1	3	*Low*
4	*Inappropriate Access*	1	4	*Medium*
5	*Hardware Failure*	1	2	*Low*
6	*Power Outages*	3	3	*Medium*
7	*Database Failure*	1	3	*Low*
8	*Force Majure*	1	5	*Medium*
9	*Network Congestion*	3	3	*Medium*
10	*System Crash*	1	2	*Low*
11	*Data/Documen Fraud*	1	4	*Medium*
12	*Abuse of Position of Trust*	1	4	*Medium*
13	*Disgruntled Employees*	1	2	*Low*

Dari Tabel X dapat dilihat bahwa dari 13 kelompok risiko yang terjadi di *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL 6 diantaranya memiliki *level of risk medium* sedangkan sisanya berada pada l*ow level of risk*. Risiko yang termasuk ke dalam *medium level of risk* meliputi *innapropriate access, power outage, force majure, network congestion, data/document fraud,* dan *abuse of position of trust.* Sedangkan risiko yang termasuk ke dalam *low level of risk* adalah *external attacks, malicious code, physical damage, hardware failure, database failure, system crash,* dan *disgruntled employees.*

3. *Risk Treatment*
Pada tahap ini dapat dilihat tindakan yang dilakukan oleh PT. Jabar Telematika (JATEL) dalam mengatasi risiko yang telah teridentifikasi pada aplikasi *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) dan memiliki *medium level of risk*. Pada tahap ini juga ditentukan usulan strategi perlakuan risiko yang tepat dalam mengatasi permasalahan yang sesuai dengan pembahasan ini yaitu dengan *risk prevention* (pencegahan risiko).
Berikut *Organization Risk Treatment* yang dilakukan oleh PT. Jabar Telematika (JATEL):

TABEL XVI
PENANGGULANGAN RISIKO DI JATEL

Organization Risk Treatment			
No.	**Identifikasi Risiko**	***Threats***	***Treatment* di JATEL**
1	*Inappropriate Access*	*Unauthorized Access*	Dari sisi internal terdapat prosedur *authentication, authorization,* dan *Log System.* Sedangkan dari sisi eksternal terdapat *firewall, NAS,* dan *DMZ.* Juga terdapat *Backup Scheduling.*
		Man in The Middle	Dengan memblokir akses dari IP yang tidak diinginkan dan memberikan *password* pada *access point* dan *router*.
2	*Power Outage*	*Power Cut/ Power Blackout/ Power Failure*	Penggunaan UPS atau *Uninterruptible Power Supply* dan penggunaan *Power Generator.*
3	*Force Majure*	Bencana Alama	Melakukan aset evakuasi berupa *backup data.*
4	*Network Congestion*	*Slow Network Througput*	Memindahkan *link* utama ke *link backup*. Mengatasi *bottleneck* dan mengalokasikan *bandwidth.*
5	*Data/ Document Fraud*	*Content Tempering*	Masih terbatas pada prosedur *authentication* dan *authorization* serta *workflow.*
		Content Forging	
6	*Abuse of Position of Trust*	Penyebaran Informasi Rahasia	Mencoba menghapus informasi yang tersebar sedangkan secara aplikasi terdapat prosedur *authentication, authorization,* dan *log system.*

Pada Tabel XVI dapat dilihat cara penanggulangan risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) yang dilakukan oleh JATEL. *Treatment* yang dilakukan oleh organisasi dalam memperlakukan risiko masih terbatas pada penanganan yang dilakukan apabila risiko tersebut terjadi dan perlakuan terhadap risiko tersebut hanya mengurangi konsekuensi dari risiko.

Setelah melihat cara penanggulangan yang dilakukan oleh JATEL, maka dibuatkan usulan untuk organisasi dalam memperlakukan risiko (*risk treatment*) yang memiliki fungsi untuk mencegah terjadinya risiko dan mengurangi secara substansial kemungkinan terjadinya risiko serta memberikan fungsi kontrol terhadap risiko.

TABEL XVII
USULAN *RISK TREATMENT*

Usulan *Organization Risk Treatment*			
No.	**Identifikasi Risiko**	***Threats***	**Usulan *Risk Treatment***
1	*Inappropriate Access*	*Unauthorized Access* *Man in The Middle*	Menerepkan *Safety IT Procedure* seperti; mengakhiri setiap akses, melindungi pc dan *terminals* dengan *password*. Menerapkn *Policy on Use of Network Services* seperti; hanya *user* dan *third parties* yang memeliki *user-id* yang dapat *log-on* kedalam sistem, tidak diizinkan melakukan aktifitas ilegal pada computer dan penggunaan computer harus di monitor oleh organisasi.
2	*Power Outage*	*Power Cut/ Power Blackout/ Power Failure*	Penggunaan 2 sumber listrik dari gardu yang berbeda untuk keperluan operasional dan infrastruktur jaringan. Serta menerapkan *Data Center Tier.*
3	*Force Majure*	Bencana Alam	Penerapan *Disaster Recovery System* atau *Disaster Recovery Procedure* juga dengan menerapkan *Data Center Tier*.
4	*Network Congestion*	*Slow Netrwork Troughput*	Melakukan monitoring *bandwidth*, dengan monitoring *bandwidth* penyempitan akses dapat dicegah dengan mengalokasikan *bandwidth* pada utilitas yang lebih besar.
5	*Data/Document Fraud*	*Content Tempering* *Content Forging*	Penggunaan HTTP/SLL yang didalamnya terdapat *Secure Socket Layer* (SLL) atau *Transport Layer Security* (TLS). Juga penerapan enkripsi data serta *checksum* untuk mencegah manipulasi konten.
6	*Abuse of Position of Trust*	Penyebaran informasi rahasia	Adanya prosedur pencegahan seperti; perlindungan dokumen organisasi, pemberian sanksi, dan dengan adanya kontrol dan audit sistem informasi.

Pada Tabel XVII dapat dilihat usulan strategi perlakuan terhadap risiko (*risk treatment*) untuk organisasi yang memiliki fungsi untuk mencegah terjadinya risiko (*risk prevention*) dan mengurangi secara substansial kemungkinan terjadinya risiko serta memberikan fungsi kontrol terhadap risiko.

IV. SIMPULAN DAN SARAN

Berdasarkan hasil analisis manajemen risiko teknologi infotmasi (TI) pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL), terdapat beberapa poin penting yang dapat disimpulkan dari uraian yang telah disampaikan, diantaranya:

1. Proses analisis manajemen risiko teknologi informasi terdiri dari *risk identification*, *risk assessment*, dan *risk treatment* dapat mengidentifikasi risiko, memberikan penilaian terhadap risiko serta memberikan perlakuan

yang lebih baik terhadap risiko yang mungkin terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL).

2. Dari hasil analisis pada aplikasi *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL) diketahui bahwa terdapat 13 risiko (*external attacks, malicious code, network congestion, system crash, database failure, data/document fraud, physical damage, hardware failure, power outage, force majure, inappropriate access, abuse of position of trust, dan disgruntled employees*) yang teridentifikasi dapat dikelompokan berdasarkan sumber daya TI (*application, information, infrastructure, dan people*) dan dapat diklasifikasikan *impact/consequences*nya berdasarkan *risk classification* (*security, availability, performance dan compliance*). Dari risiko yang telah teridentifikasi, 6 diantaranya pada grafik sebaran risiko dan evaluasi risiko berdasarkan *likelihood* dan *impact* diketahui memiliki tingakatan medium *level of risk.*
3. Penanganan organisasi terhadap risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) secara umum sudah dilakukan dan dapat dikatakan sudah baik hanya saja PT. Jabar Telematika (JATEL) tidak memiliki dokumen *Standard Operational Procedure* atau SOP yang berhubungan dengan manajemen risiko TI di organisasi. Strategi penanganan terhadap risiko yang memiliki fungsi kontrol dan mencegah terjadinya risiko (*risk prevention*) secara substantif dianggap sebagai strategi penanganan risiko yang paling baik. Penerapan *Data Center Tier* dan *Disaster Recovery Procedure* atau DRP juga memegang peranan penting pada implementasi manajemen risiko.

Lalu, berdasarkan hasil analisis manajemen risiko TI yang dilakukan pada aplikasi DMS arsip elektronik di JATEL, terdapat beberapa poin saran yang dapat diuraikan untuk pengembangan analisis manajemen risiko TI dan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL), diantaranya:

1. Diharapkan dengan adanya hasil analisis manajemen risiko TI pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL) dapat dijadikan dokumen inisiasi atau dokumen acuan oleh JATEL dalam mengembangkan *standard operation procedure* (SOP), strategi manajemen risiko, serta *disaster recovery plan* (DRP) sehingga dapat diimplementasikan oleh organisasi.
2. Dengan mengimplementasikan usulan risk treatment dan melanjutkan analisis manajemen risiko hingga tahap *monitoring and review* diharapkan nantinya nilai *lavel of risk* pada tiap-tiap risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) dapat menurun dan organisasi dapat menghasilkan strategi penanganan risiko yang lebih baik.
3. Adanya pengembangan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL) sehingga semua komponen *document management system* dapat terpenuhi. Komponen yang dimaksud adalah *capture, validation,* dan *collaboration* yang diharapkan dapat meningkatkan kinerja aplikasi dan *business value* dari JATEL serta mendukung otomatisasi proses bisnis.
4. Penerapan HTTPS/SLL, enkripsi, *session* dan *masking* yang dapat memberikan dukungan terhadap *security* pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL)

DAFTAR PUSTAKA

[1] A. Stevenson, Oxford Dictionary of English, Oxford: Oxford University Press, 2010.
[2] P. Hopkin, Fundamentals of Risk Management: Understanding, Evaluating, and Implementing Effective Risk Management, London: Kogan Page, 2010.
[3] J. J. Hampton, Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposures, and Seize Opportunities, New York: AMACOM, 2009.
[4] D. Cooper, S. Grey, G. Raymond and P. Walker, Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements, Chichester, West Sussex: John Wiley & Sons Ltd., 2004.
[5] L. J. Susilo and V. R. Kaho, Panduan Manajemen Risiko Berbasis ISO 31000 Industri Non-Perbankan, Jakarta: Penerbit PPM, 2014.
[6] N. R. Council, Improving Risk Communication, Washington DC: National Academy Press, 1989.
[7] Symantec, IT Risk Management Report, Cupertino, CA: Symantec, 2007.
[8] ISACA, COBIT 5 The Risk IT Framework: Principles, Process Details, Management Guidelines, Maturity Models, Rolling Meadows, IL: ISACA, 2009.
[9] ISACA, IT Governance Implementation Guide: Using COBIT and val ITTM, 2nd edition, ISACA, 2007.
[10] JATEL, PT Jabar Telematika: Annual Report 2013, Bandung: PT Jabar Telematika, 2013.
[11] E. E. Pratama and Suhardi, Analisis Nilai & Manajemen Risiko Teknologi Informasi (studi kasus PT. Bank Tabungan Negara), Bandung, 2013.
[12] N. B. Kurniawan, Manajemen Risiko Teknologi Informasi Pada Badan Pusat Statistik, Produk Layanan: Pelayanan Statistik Terpadu, Bandung, 2013.
[13] A. Y. Dewi, Analisis Nilai Teknologi Informasi & Implementasi ISO 31000 Sebagai Manajemen Risiko Teknologi Informasi (Studi Kasus Layanan Pada Direktorat Jendral Pajak Republik Indonesia), Bandung, 2013.