ISSN: 2477-5126
e-ISSN: 2548-9356

Analisis Risiko IT untuk Pemanfaatan *Genogram Tools* pada *Health care*

Sukmadiningtyas[1*)], M. Yoka Fathoni[2]
[1,2] Program Studi Sistem Informasi, Fakultas Informatika, Institut Teknologi Telkom Purwokerto, Banyumas
[1,2]Jln. DI. Panjaitan No.128 Purwokerto Selatan, Kabupaten Banyumas, 50272, Indonesia
email: [1]sukmatyas@ittelkom-pwt.ac.id , [2]myokafathoni@ittelkom-pwt.ac.id

Abstrak – *Genogram* merupakan representasi grafik Kesehatan keluarga, *Genogram* juga dapat dimanfatakan sebagai alat pendukung perbaikan kesehatan khususnya kesehatan keluarga dengan mengutamakan pencegahan hingga pelayanan berkelanjutan. Hal ini menjadi latar belakang masalah perlunya memanfaatkan genogram sebagai alat pelayanan kesehatan. *Genogram* dapat dimanfaatkan pada sarana kesehatan yang belum memiliki sistem terintegrasi khusunya untuk penanganan penyakit degeneratif. Penelitian ini bertujuan untuk melakukan analisis risiko penggunaan *genogram tools* sebagai media yang merekam *history* kesehatan seseorang sebagai media pendukung pada kesehatan. Penelitian ini menganalisis risiko pada sebuah Poliklinik yang akan menerapkan *genogram tools*. Proses analisis dilakukan dengan melakukan proses *risk identification* lalu *risk assessment* dengan menggunakan metode *COBIT for Risk IT* sebagai pemetaan tipe sumber daya IT, kemudian *qualitative analysis* untuk mengetahui *likelihood* dan *impact*, kemudian melakukan penilaian tingkat risiko sesuai dengan FGD dengan organisasi. Selanjutnya melakukan analisis dengan *bow tie analysis* sebagai metode pemetaan untuk risiko yang memungkinkan mendapat pemulihan risiko. Berdasarkan pemetaan analisis nilai *likelihood* kejadian dan *impact* risiko yang mungkin terjadi terdapat *impact* risiko adalah *low, middle, dan high.* Risiko dengan nilai evaluasi *high* adalah *inappropriate access, abuse of position* dan *lack of genogram technology.* Sedangkan untuk risiko *middle* adalah *Network congestion, power outages.* Terakhir risiko dengan tingkatan *low likelihood* tapi high *impact* adalah *External attack, database failure,* dan *Hardware failure.* Oleh karena itu diperlukan adanya *treatment* untuk risiko yang dapat dimitigasi sesuai dengan yang dapat ditangani oleh organisasi.
Kata Kunci – **COBIT *for Risk* IT, *Genogram tools,* identifikasi risiko,**

Abstract –
Genogram is a graphic representation of family health, Genogram can also be utilized as a supporting tool for health improvement, especially family health by prioritizing prevention to sustainable services. This is the basic of the problem that needs to utilize genograms as a health service tool. Genograms can be utilized in health facilities that do not have an integrated system, especially for handling degenerative diseases. This study aims to conduct a risk analysis of the use of genogram tools as a medium that records a person's health history as a supporting medium in health. This research analyzes the risks in a Polyclinic that will implement genogram tools. The analysis process is carried out by conducting a risk identification process and then risk assessment using the COBIT for Risk IT method as a mapping of IT resource types, then qualitative analysis to determine likelihood and impact, then assessing the level of risk according to FGDs with the organization. Next, analyze with bow tie analysis as a mapping method for risks that allow risk recovery. Based on the mapping analysis of the likelihood value of the event and the impact of the risks that may occur, there are low, middle, and high impact risks. Risks with high evaluation values are inappropriate access, abuse of position and lack of genogram technology. Meanwhile, the middle risks are Network congestion, power outages. Finally, risks with a low likelihood but high impact level are External attack, database failure, and Hardware failure. Therefore, treatment is needed for risks that can be mitigated according to what the organization can handle.

Translated with DeepL.com (free version)
Kata Kunci – ***Genogram tools,*** **risk identification, COBIT for Risk IT**

I. PENDAHULUAN

Genogram merupakan representasi grafik dari anggota keluarga serta hubungan mereka hingga setidaknya tiga generasi. Genogram juga digunakan sebagai alat penilaian visual, melacak pengaruh keluarga dalam berbagai konteks dan juga dalam sistem yang lebih luas [7]. Genogram sering kali digunakan sebagai alat untuk *concealling* untuk seseorang mahasiswa pasca sarjana, yang nantinya menghubungkan pendidikan dengan sistem keluarga [6]. *Genogram* juga menjadi alat pendukung dibidang pendidikan. Hal ini dilakukan oleh sosiolog klinis, untuk memperkenalkan dan membantu siswa memahami dasar sosiologis terapi keluarga dan untuk memperdalam kesadaran transmisi social keluarga [8]. Dari sudut pandang lain, *genogram* dapat dijadikan alat untuk terapi keluarga yang nantinya dapat digunakan untuk memahami perkembangan individu dalam konteks dinamika keluarga [7]. Penelitian kali ini memfokuskan pemanfaatan *genogram* sebagai pendukung perbaikan kesehatan khususnya kesehatan keluarga dengan mengutamakan pencegahan hingga pelayanan berkelanjutan. Hal ini dilatarbelakangi oleh pelayanan kesehatan yang belum memiliki sistem khusunya untuk penanganan penyakit degeneratif. Adanya Genogram tools diterapkan pada sebuah klinik diharapkan menjadi salah satu *tools* mendukung yang perbaikan pelayanan Kesehatan.

Pada penelitian ini diusulkan untuk diterapkan pada poliklinik sebagai arahan / saran perbaikan kesehatan seorang pasien sebelum mendapat pengobatan medis. Penggunaan alat penyembuhan dengan genogram ini dilakukan dengan menganalisis *Family tree.* Nantinya memiliki pengaruh yang

*) **penulis korespondensi**: Sukmadiningtyas
Email: sukmatyas@ittelkom-pwt.ac.id

cukup *significant* terhadap manajemen karena memungkinkan terjadinya perubahan manajemen organisasi dan proses bisnis.

Perubahan organisasi dapat terjadi dengan berbagai alasan yang nantinya tidak terlepas dari perubahan ekonomi global bahkan perubahan teknologi yang dinamis. *Michael Hammer* dan *James Champy* menuliskan bahwa ekonomi global berdampak terhadap 3 C, yaitu *customer, competition*, dan *change* [1]. Perubahan manajemen atau yang disebut *change management* merupakan pengelolaan perubahan pada perusahaan yang dapat digambarkan sebagai proses, alat dan teknik untuk mengatur proses perubahan untuk mencapai hasil yang diperlukan dan untuk merealisasikan perubahan secara efektif [3] .Untuk itu, perlu dilakukan analisis risiko terhadap berbagai kemungkinan risiko yang muncul ketika *Genogram tools* diterapkan. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan risiko yang muncul pada aset tersebut. Analisis Risiko dan manfaat penggunaan genogram terhadap change management sebuah *health care* berbasis *Risk Management* dengan menggunakan COBIT 5 *for Risk.* Berdasarkan *Cobit 5 For IT Risk* terdapat kelompok identifikasi risiko berdasarkan aplikasi, informasi, infrastruktur, sumber daya manusia [3].

Penelitian ini melakukan analisis risiko penggunaan *Genogram tools* pada sebuah organisasi *health care.* Organisasi yang kompleks, seperti rumah sakit dan sarana kesehatan lainnya memiliki karakteristik khusus sehingga membuat manajemen perubahan (*change manajemen)* lebih sulit dan kompleks utnuk dilaksanakan [4]. Hal ini dikarenakan pada sebuah perusahaan berbentuk *Health care* misalnya memiliki berbagai proses yang berinteraksi satu sama lain. Adanya analisis risiko pemanfaatan *Genogram tools* maka dapat memberi sudut pandang pada organisasi untuk melakukan persiapan sebelum melakukan *change management.*

II. PENELITIAN TERKAIT

Topik manajemen perubahan ini mengikat beberapa *sub topic* terkait. Sebelum melakukan sebuah perubahan pada suatu organisasi maka dibutuhkan adanya kesiapan untuk melakukan perubahan. Topik terkait lainnya adalah bagaimana analisis risiko dan manfaat yang akan dihadapi nantinya dan keterkaitannya. Paper berikut akan mengimplementasikan *businiss intelegent* pada perusahaan sehingga dibutuhkan proses penilaian kesiapan organisasi. Metode yang digunakan adalah *Participants and data collection* sebagai pengajuan point utama (*Key Point)* dalam melakukan penilaian kesiapan pada organisasi tersebut. Beberapa point utama yang dijadikan faktor penilaian adalah budaya, individual, management, strategi, dan BI *readiness*. Terdapat juga beberapa *variable* terkait yang terdapat pada perusahaan terkait yang mempengaruhi penilaian. Berdasarkan penelitian, hasilnya menampakkan adanya beberapa faktor yang mempengaruhi kesiapan organisasi untuk mengimplementasikan *change management*. Faktor yang paling berpengaruh adalah strategi perusahaan [5].

Penelitian selanjutnya membahas tentang bagaimana sebenarnya *Change management* dibutuhkan untuk sebuah peningkatan kualitas pelayanan perusahaan. Peningkatan kualitas pelayanan pada *Oman's Health Care* adalah melalui sebuah proses penelitian dengan metode *Focus group discussion*. Dilakukan dengan studi kualitatif deskriptif berlangsung antara Desember 2012 dan November 2013 di Departemen Pendidikan Kesehatan, Muscat, Oman. Sampel terdiri dari 20 peserta terdiri dari empat kelompok *Focus Grup Discussion*, dan tiga wawancara semi terstruktur. Focus Grup dilakukan dengan dekan, pengajar fakultas di lembaga masing-masing, fakultas program, dan anggota dari yayasan pusat terdiri dari empat kelompok. Hasil dari penelitian kesiapan sebuah pelayanan perusahaan ini adalah temuan menunjukkan bahwa perubahan menuju peningkatan lembaga pendidikan kesehatan saat ini ke perguruan tinggi memiliki dampak positif pada peserta, namun, tidak adanya visi yang jelas dan strategi manajemen perubahan mengakibatkan dampak psikologis yang merugikan pada peserta dalam perjalanan menuju pelaksanaan perubahan ini [6].

Penelitian lain menyebutkan terdapat parameter yang dapat dijadikan penilaian kesiapan sebuah perusahaan untuk melakukan perubahan. Faktor tersebut adalah psikologi masing-masing individu, terutama individu yang bertugas memegang kepetingan serta pengambil keputusan.

Pada penelitian ini memiliki sudut pandang, ketika sebuah *tools* diterapkan maka dapat memengaruhi proses bisnis sebuah organisasi sehingga perlu dilakukan analisis risiko sebelum sebuah *change management* dilakukan.

III. METODE PENELITIAN

A. Risiko

Risiko atau yang dapat disebut *Risk* adalah *'A chance or possibility of danger, loss, injury, or other adverse consequences'* [9]. Risiko sering kali disandingkan dengan kemungkinan yang akan terjadi adalah negative, walaupun tidak semua risiko menghasilkan konsekuensi yang negatif. Menurut ISO 31000/2009 risiko adalah pengaruh bias yang positif dan negative yang memengaruhi tercapainya tujuan. [12]. Sedangkan menurut COBIT 5 *for risk* mendefinisikan risiko merupakan bagian dari risiko bisnis terkait dengan penggunaan, kepemilikan, pengoperasian, keterlibatan, pengaruh, dan penerapan TI dalam suatu organisasi. Risiko TI terdiri dari peristiwa terkait TI yang dapat berdampak pada bisnis. Risiko TI dapat terjadi dengan frekuensi dan dampak yang tidak pasti serta dapat menimbulkan tantangan dalam mencapai tujuan strategis [7][13]. Risiko tidak selalu harus dihindari. Berbisnis adalah tentang mengambil risiko yang konsisten dengan selera risiko, yaitu, banyak proposisi bisnis memerlukan risiko TI untuk diambil untuk mencapai proposisi nilai dan merealisasikan tujuan perusahaan dan tujuan, dan risiko ini harus dikelola tetapi tidak harus dihindari. Sedangkan manajemen risiko didefinisikan sebagai identifikasi risiko melalui penggunaan sumber daya yang terkoordinasi dan ekonomis untuk meminimalkan, memantau, dan mengendalikan kemungkinan atau dampak kejadian buruk atau untuk memaksimalkan realisasi peluang, evaluasi, dan penentuan prioritas [11] [12].

B. *Change Management*

Change management atau yang disebut manajemen perubahan, merupakan pengelolaan perubahan pada perusahaan yang dapat digambarkan sebagai proses, alat dan teknik untuk mengatur proses perubahan pada sisi orang untuk mencapai hasil yang diperlukan dan untuk merealisasikan perubahan secara efektif melalui agen perubahan, tim dan sistem yang lebih luas [2]. *Change*

management berbentuk transisi yang dilakukan sebuah organisasi/perusahaan dalam melakukan perubahan dengan tujuan meningkatkan kinerja organisasi. Beberapa penggerak perubahan umum meliputi:

a) Menyesuaikan dengan pergeseran kondisi ekonomi
b) Menyesuaikan dengan lanskap yang berubah di pasar
c) Mematuhi peraturan dan pedoman pemerintah
d) Memenuhi kebutuhan klien
e) Memanfatkan teknologi baru
f) Mengatasi saran karyawan untuk perbaikan

C. *Genogram*

Genogram merupakan representasi grafik dari anggota keluarga serta hubungan mereka hingga setidaknya tiga generasi. *Genogram* juga digunakan sebagai alat penilaian visual, melacak pengaruh keluarga dalam berbagai konteks dan juga dalam sistem yang lebih luas [7]. *Genogram* sering kali digunakan sebagai alat untuk melihat *concealling* untuk seseorang mahasiswa pasca sarjana, yang nantinya akan menghubungkan pendidikan dengan sistem keluarga [6]. *Genogram* sebagai alat pendukung pendidikan hal ini dilakukan oleh sosiolog klinis, untuk memperkenalkan dan membantu siswa memahami dasar sosiologis terapi keluarga dan untuk memperdalam kesadaran transmisi social keluarga [8]. *Genogram* juga dapat dijadikan alat untuk terapi keluarga yang nantinya dapat digunakan untuk memahami perkembangan individu [7] dalam konteks dinamika keluarga.

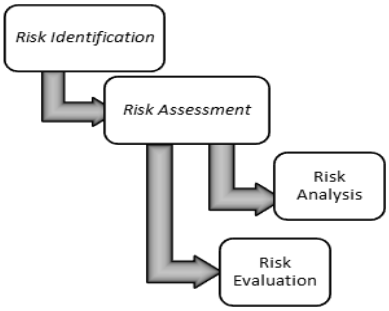
D. COBIT 5 *For IT Risk*

COBIT adalah manajemen teknologi informasi (TI) dan kerangka tata kelola TI yang dibuat oleh ISACA. COBIT adalah seperangkat alat yang memungkinkan pengguna menjembatani kesenjangan antara persyaratan kontrol, masalah teknis, dan risiko bisnis. [8]. Sumber daya TI yang diidentifikasi dalam COBIT secara sederhana dapat digambarkan sebagai berikut [10]:

a. Aplikasi (*Application*) adalah sarana atau alat untuk mengolah, melengkapi, atau merangkum prosedur baik manual maupun terprogram.
b. Informasi (*information*) adalah data yang diolah untuk keperluan administratif dalam rangka pengambilan keputusan bisnis bagi perusahaan. Data terdiri dari objek dalam arti luas (internal dan eksternal), terstruktur dan tidak terstruktur, grafik, suara, dll.
c. Infrastruktur (*infrastructure*) termasuk perangkat keras, perangkat lunak, sistem operasi, sistem manajemen basis data, jaringan, multimedia, dan peralatan lainnya;
d. Sumber Daya Manusia/SDM (*people*) merupakan sumber daya terpenting suatu organisasi dalam mengelola dan menjalankan bisnisnya. Merencanakan, mengatur, menerapkan, memperoleh, menerapkan, mendukung, dan memantau layanan TI organisasi memerlukan kesadaran dan produktivitas.

E. Analisis Risiko

Terdapat beberapa tahapan untuk melakukan analisis risiko.

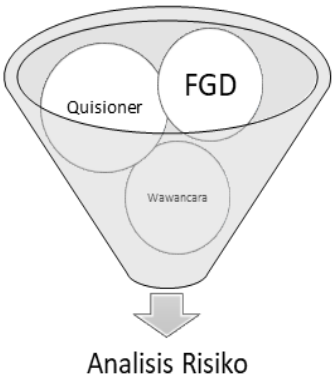


Gbr 1.Bagan proses analisis risiko

Berdasarkan pada Gbr 1, terdapat 2 (dua) proses utama yang dilakukan untuk mendapatkan hasil analisis yang dapat memberikan pertimbangan. Oleh karena itu diperlukan adanya Bow-tie Analysis agar proses analisis terhadap risiko menghasilkan *recovery* (pemulihan) dan *control* (kontrol).

1) Identifikasi Risiko (*Risk Identification)*

Pada proses identifikasi risiko dilakukan pengelompokan risiko dengan kondisi pertama merupakan prosedur dari pemeriksaan poliklinik kondisi sekarang (*as-is*) atau sebelum *genogram tools* diberlakukan dan kondisi yang diharapkan (*to-be*) setelah penggunaan *genogram tools*. Kemudian klasifikasikan berdasarkan definisi oleh *COBIT 5 For risk*, yang berhubungan dengan *rekam medis system*. *Risk Identification* dilakukan dengan cara pengambilan data dengan beberapa metode *penelitian Focus Grup discussion,* wawancara*, questionnaries* dengan penggunaan *checklist*. Selanjutnya perbandingan metode sekarang dan metode setelah menggunakan *genogram tools*. Proses ini diharapkan dapat berjalan secara komprehensif sehingga hasil identifikasi dapat memunculkan permasalahan sebagai bahan analisis lanjutan.



Gbr 2.Bagan Pemetaan Sumber Data

Berdasarkan Gbr 2, dilakukan penghimpunan data dengan wawancara, questioner dan FGD untuk melakukan identifikasi risiko dan menjadi inputan pada proses analisis risiko. Kemudian sumber data lain yang digunakan sebagai pendukung dalam penelitian ini adalah data sekunder. Data sekunder merupakan data yang diperoleh secara tidak langsung. Data sekunder ini diperoleh berupa dokumen-dokumen seperti buku-buku penelitian terdahulu yang memerlukan pengembangan lebih lanjut dan jurnal-jurnal yang relevan terkait dengan topik penelitian.

2) Penilaian Risiko (*Risk Assessment)*

Penilaian terhadap risiko merupakan gabungan proses yang terdiri dari *risk analysis* (analisis risiko) dan *risk evaluation* (evaluasi risiko). Pada penelitian ini penilaian risiko sesuai kegiatan pada *rekam medis system.*

a. Proses Analisis Risiko: Proses analisis *Bowtie* mencakup proses pemetaan *Hazard dan Top Event* kemudian analisis dampak. Kemudian mengevaluasi risiko dengan memberikan nilai pada risiko yang teridentifikasi berdasarkan nilai probabilitas dan dampaknya. Analisis *bowtie* dilakukan agar proses risiko mengarah pada pemulihan dan pengendalian. Hal itu dimulai dengan mengananlisis *likelihood* sesuai pada Tabel 1.

TABEL 1.
Tabel Nilai *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

Selanjutnya terdapat nilai *impact* dengan perangkingan 1-5. Pada Tabel 2 terdapat *impact* yang mungkin terjadi dan deskripsi yang akan terjadi.

TABEL 2.
Tabel Nilai *Impact*

Impact		**Deskripsi**
Rating	**Kriteria**	
1	*Insignificant*	Dampak mungkin diabaikan dengan aman/ dengan toleransi
2	*Minor*	Dampak kecil dan dapat diatasi dengan prosedure sederhana
3	*Moderate*	Dampak tergolong besar namun dapat dikelola dengan 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.* Proses selanjutnya adalah penilaian pada masing-masing risiko yang telah didefinisikan.

3) Evaluasi Risiko (*Risk Evaluation)*

Risk Evaluation adalah proses dalam membandingkan risiko yang telah diperkirakan dengan kriteria risiko yang telah ditentukan [14]. Fase penilaian risiko mengevaluasi risiko yang teridentifikasi dan menentukan apakah risiko tersebut dapat diterima oleh organisasi berdasarkan tingkat risiko.

Penilaian risiko dilakukan dengan menerapkan proses pemetaan pada grafik (x,y) yang merepresentasikan hubungan antara probabilitas atau frekuensi kejadian dengan dampak dari setiap risiko yang terjadi, seperti terlihat pada Tabel 3.

TABEL 3.
Nilai Evaluasi Likeihood dan impact

y *likelihood*					
1		Medium	High	High	High
2	Low	Medium	Medium	HIGH	HIGH
3	Low	Medium	Medium	Medium	HIGH
4	Low	Low	Low	Medium	HIGH
5	Low	Low	Low	Medium	Medium
	1	2	3	4	5 x

Nilai Impact

F. RESULT AND DISCUSSION

Pada proses penelitian ini dilakukan proses analisis risiko secara beruntut yang dimulai dengan proses identifikasi risiko, penilaian risiko, dan evaluasi risiko. Berikut merupakan uraian prosesnya:

4.1 Identifikasi risiko

Identifikasi risiko pertama dilakukan dengan menerjemahkan layanan yang sekarang *(as-is)* [9][15]. pada poliklinik lalu memberikan usulan pelayanan *(to-be)* dengan penerapan *genogram tools*. Berikut merupakan kegiatan utama pada Poliklinik sesuai pada Tabel 4:

TABEL 4.
Layanan Kesehatan poliklinik (*as-is*)

Aktivitas	***as-is***
Registrasi Pasien	Petugas admin melakukan registrasi dengan mencatat di kartu kendali secara manual
Antrian	Antrian dilakukan dengan menggunakan kartu nomer urut
Pemeriksaan	Dokter membaca data pasien dari kartu kendali kesehatan.
Diagnosis	Dokter menuliskan diagnosis pada kartu kendali kesehatan
Konsultasi	Dokter menyampaikan modul kesehatan secara keseluruhan pada saat tatap muka.
Pengambilan obat	Pasien mengambil obat menggunakan kertas resep yang diberikan dokter

Sedangkan terdapat layanan yang diharapkan untuk diterapkan sebagai usulan *(to-be)* pelayanan pasien pada Poliklinik, sesuai pada Tabel 5.

TABEL 5.
Usulan Pelayanan (*to-be*)

Aktivitas	**To-be**
Registrasi Pasien	Pasien dapat melakukan pendaftaran *online*, telah membawa identitas dan menunjukkan kartu kesehatan
Antrian	Antrian dilakukan dengan cara memanggil nama berdasarkan data yang di input kan oleh admin.

ISSN: 2477-5126
e-ISSN: 2548-9356

Pemeriksaan	Dokter mengisi form pada sebuah perangkat lunak yang digunakan untuk pengisian data *history* kesehatan pasien sembari pasien diskusi singkat. Memanfaatkan *genogram tools.*
Diagnosis	Dokter menulis diagnosis beserta penulisan resep/ rangkuman keluhan dan saran awal *treatment* penyembuhan.
Pengambilan obat	Pasien mengambil obat (resep)

Identifikasi kegiatan poliklinik yang memungkinkan terdapat risiko yang terjadi pada setiap sumber daya TI . Identifikasi ini menyesuaikan dengan COBIT *for IT Risk*.

1. Risiko yang memiliki kemungkinan terjadi risiko pada *Application* adalah :

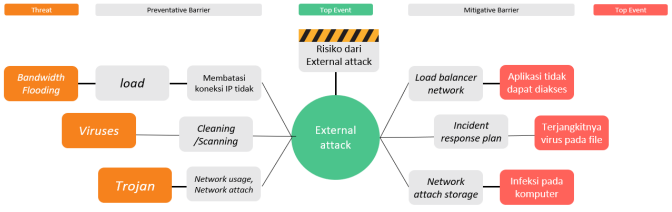
a) External Attacks (Serangan Eksternal)

External Attack merupakan risiko yang memiliki kemungkinan terjadi kesalahan pada proses perekaman data. Risiko ini bisa saja terjadi pada proses registrasi dan proses pendataan yang dilakukan oleh dokter. Proses analisis risiko sesuai pada Tabel 6. Analisis risiko dilakukan dengan mempertimpangkan *Threats, impact, recovery dan control issue.*

TABEL 6.
Tabel Risiko pada *External Attacks*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Bandwidth Flooding	Aplikasi tidak dapat diakses, pembatalan penyimpanan data	Terapkan *load balancing,* dan memutus akses untuk IP yang tidak dikenali	*Load balancer network*
Viruses	Terjangkitnya virus pada file	*Cleaning /Scanning viruses*	Menyiapkan anti virus
Trojan	Kehilangan data	*Network usage, Network attach storage*	*Network attach storage*

Berikut pada Gambar 3 merupakan proses analisis risiko pada *External attack* menggunakan *Bowtie analysis. Diagram* yang merupakan usulan untuk penanganan risiko pada *External attack.*



Gambar 3. Diagram *Bow Tie Analysis*

b) *Network Congestion* (Kesalahan Jaringan)

Network Congestion merupakan risiko yang memiliki kemungkinan terjadi kesalahan pada keseluruhan proses perekaman data. Karena hal ini merupakan hal utama dalam pemrosesan data. Berdaarkan Tabel 7 terdapat analisis risiko *network Congestion,* dengan mempertimbangkan *Threats, impact, recovery dan control issue.*

TABEL 7.
Tabel Risiko pada *Network Congestion*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Slow respon/ throughput	Layanan terganggung, proses penginputan data memakan banyak waktu	*Security load balancer*	Perjadwalan perawatan

c) System Crash (Kecelakaan sistem)

System Crash merupakan risiko yang memiliki kemungkinan terjadi kesalahan pada keseluruhan proses perekaman data yang berhubungan langsung dengan penggunaan aplikasi perekaman data. Karena hal ini merupakan hal utama dalam pemrosesan data, seperti pada Tabel 8 terdapat analisis risiko dengan *Threats, impact, recovery dan control issue.*

TABEL 8.
Risiko pada *System Crash*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Application Crash	*Not responding*, kehilangan data,aplikasi *crash*	*Task manager*	*Memory disk control usage*
Operating system crash	Kepanikan kernel	*Task manager*	*Memory disk control usage*

1. Risiko yang memiliki mungkin terjadi risiko pada *Infromation* adalah :

a) Database Failure (Kegagalan Basis Data)

Database Failure merupakan risiko yang memiliki kemungkinan terjadi kesalahan pada keseluruhan proses perekaman data yang berhubungan langsung dengan penggunaan aplikasi perekaman data, baik saat perekaman maupun penyimpanan data, sesuai dengan analisis risiko pada Tabel 9 yang mempertimbangkan *Threats, impact, recovery dan control issue.*

TABEL 9.
Risiko pada *Database Failure*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Statement failure	*Looping, memory* penuh,*not responding*	*Rollback plans, inciden response plan*	*Error handling*
Human error	Kehilangan data, kesalahan prosedur	*Restore data*	*Training and awarness*
Network Error	Kehilangan data	*Quality services*	*Backup network configuration*

2. Risiko yang mungkin terjadi risiko pada *Infrastructure* adalah :

a) *Hardware Failure* (Kegagalan Perangkat Keras)

Berdasarkan Tabel 10 dilakukan analisis risiko pada *Hardware Failur.* Risiko ini merupakan risiko yang memiliki kemungkinan terjadi kesalahan pada keseluruhan proses perekaman data yang berhubungan langsung dengan penggunaan aplikasi perekaman data, baik saat perekaman maupun penyimpanan data.

TABEL 10
Risiko pada *Hardware Failure*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Overheating	*Memory* penuh, *not responding*	*Task manager*	*Memori disk control usage*
Electrical Dischagrge	Kehilangan data, kesalahan prosedur	*Restored data*	*Network attach storage*
Human error	Kehilangan data	*Incident response plan*	*Network attach storage, training and awarness*

b) Power Outages (pemadaman Listrik*)*

Berdasarkan Tabel 11 dilakukan analisis pada risiko *Power Outages.* Risiko ini merupakan risiko yang memiliki kemungkinan terjadi kapanpun dan hal ini merupakan diluar kekuasaan. Hal ini hanya dapat ditangani dengan cara pembuatan sumber listrik alternatif ataupun penerapan *back up* data berkala. Sehingga data tetap dapat ditangani.

TABEL 11.
Risiko pada *Power Outages*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Power Cut/ Power Blackout/ Power Failure	Kehilangan data	*Regular back up, power generators*	Scheduling maintenance, *Emergency response plan*

3. Risiko yang memiliki kemungkinan terjadi risiko pada *People* adalah :

a. *Inappropriate Access* (melakukan akses yang tidak tepat)

Pada Tabel 12, terdapat analisis risiko *Inappropriate Access.* Risiko ini merupakan risiko yang memiliki kemungkinan terjadi diakibatkan pengguna / pemegang data lalai terhadap akses. Oleh karena itu diperlukan metode *recovery* berupa *incident response plan.*

TABEL 12.
Risiko pada *Inappropriate Access*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Unauthorized Access/	Pencurian data, manipulasi data	*Incident response plan*	*Access control policy*

b. *Abuse of Position* (Penyalahgunaan kedudukan)

Sesuai dengan Tabel 13, terdapat analisis risiko *Abuse of Position.* Risiko ini merupakan risiko yang memiliki kemungkinan terjadi yang diakibatkan pengguna / pemegang data lalai terhadap akses.

TABEL 13.
Risiko pada *Abuse of Position*

Threats	***Impact/ consequences***	***Recovery***	***Control***
Penyebaran data	Data yang harusnya privasi tersebar.	*Incident response plan*	*Security network*

*c. Lack of genogram technology (*kurangnya pengetahuan terhadap *genogram*)

Pada Tabel 14*,* dilakukan analisis *Abuse of Position* merupakan risiko yang memiliki kemungkinan terjadi yang diakibatkan pengguna / pemegang data lalai terhadap akses Tabel 13.

TABEL 14.
Risiko pada *Lack of* genogram technology

Threats	***Impact/ consequences***	***Recovery***	***Control***
Human error	*Tidak memahami penggunaan dan penerapan aplikasi*	*Incident response plan*	*Awareness and training*

4.2 Risk Assessment

Metode yang digunakan untuk melakukan *risk assessment* adalah analisis risiko dengan menerapkan perangkingan tingkat *likelihood* dan *impact* yang mungkin terjadi, kemudian evaluasi risiko dengan menerapkan treatment risiko. Berikut merupakan uraian proses risk assessment:

1. Risk analysis

Pada Tabel 15 dilakukan analisis risiko dengan inputan identifikas jenis risiko lalu memetakkan sesuai Tingkat *likelihood* dan *impact*.

TABEL 15.
Identifikasi nilai *likelihood* dan *impact*

No.	***Identifikasi Risiko***	***Likelihood***	***Impact***
1	*External Attacks*	*Rare*	*Moderate*
2	*Network Congestion*	*Possible*	*Moderate*
3	*System Crash*	*Rare*	*Minor*
4	*Database Failure*	*Rare*	*Moderate*
5	*Hardware Failure*	*Rare*	*Minor*
6	*Power Outages*	*Possible*	*Moderate*
7	*Inappropriate Access*	*Rare*	*Major*
8	*Abuse of Position*	*Rare*	*Major*
9	*Lack of genogram technology*	*Possible*	*Major*

Selanjutnya pada Tabel 16 merupakan penerjemahan hasil nilai identifikasi menjadi nilai angka sesuai dengan *range* nilai *likelihood* dan *Impact*.

TABEL 16.
Identifikasi nilai *likelihood* dan *impact*

No.	Identifikasi Risiko	*Likelihood*	*Impact*
1	*External Attacks*	1	3
2	*Network Congestion*	3	3
3	*System Crash*	1	2
4	*Database Failure*	1	3
5	*Hardware Failure*	1	2
6	*Power Outages*	3	3
7	*Inappropriate Access*	1	4
8	*Abuse of Position*	1	4
9	*Lack of genogram technology*	3	4

2. Risk Evaluation

Berdasarkan hasil dari analisis risiko maka, dapat diambil hasil evaluasi dengan melihat nilai sebaran risiko berdasarkan *likelihood* dan *impact.* Pada Tabel 17 didapatkan hasil pemeringkatan level risiko.

TABEL 17.
Pemetaan *likelihood* dan *impact*

No.	*Identifikasi Risiko*	*Likelihood*	*Impact*	*Risk Level*
1	*External Attacks*	1	3	*Low*
2	*Network Congestion*	3	3	*Medium*
3	*System Crash*	1	2	*Low*
4	*Database Failure*	1	3	*Low*
5	*Hardware Failure*	1	2	*Low*
6	*Power Outages*	3	3	*Medium*
7	*Inappropriate Access*	1	4	*High*
8	*Abuse of Position*	1	4	*High*
9	*Lack of genogram technology*	3	4	*High*

Untuk mengetahui treatment risiko yang dapat diterapkan sesuai dengan Tabel 18 dilakukan pemetaan lebih mendalam untuk mengetahui dengan adanya identifikasi risiko ancaman (threats) seperti apa yang mungkin terjadi dan penanganannya (*treatment*). Terdapat beberapa kondisi yaitu *low likelihood* tetapi Tingkat *impact high*, *low likelihood* tetapi *medium impact* dan medium *likelihood high impact.*

TABEL 18.
Usulan *risk treatment*

No.	*Risk identification*	*Threats*	*Risk Treatment*
1.	*Network Congestion*	*Slow Network Througput*	Mempersiapkan *link backup*
2	*Power Outages*	*Power Cut/ Power Blackout/ Power Failure*	Menerapkan *data center tier* dan mengajukan gardu khusus untuk keperluan operasional.
3	*Inappropriate Access*	*Unauthorized Access*	Menerapkn *Policy on Use of Network Services* seperti; hanya user dan *third parties* yang memeliki *user-id* yang dapat *log-on* kedalam sistem
4	*Abuse of Position*	Penyebaran informasi rahasia	Memastikan terdapat prosedur perlindungan dokumen organisasi.

V. Kesimpulan

Berdasarkan hasil penelitian tersebut didapatkan hasil analisis risiko yang mungkin terjadi dengan penggunaan *genogram tools* jika ditinjau berdasarkan COBIT *for IT Risk* , dapat dipetakkan sesuai empat (4) tipe risiko yang mungkin terjadi yaitu risiko aplikasi, risiko informasi, risiko sarana/prasaran dan risiko *people.*

Hasil dari analisis risiko sesuai dengan tipe risiko dari COBIT *for Risk IT* selanjutnya dipetakkan dengan melakukan identifikasi *threat* dan *impact/ consequence* sesuai dengan *Bow Tie Analysis*. Untuk mengetahui *impact* dan *consequence* dari sebuah analisis risiko maka, diterapkan identifikasi *Hazard* dan Top *Event* sehingga dapat dianalisis strategi mitigasi dan preventifnya sehingga risiko pemanfaatan *genogram tools* dapat berjalan dengan tepat.

Identifikasi *Hazard* pada penelitian ini adalah rendahnya kualitas pelayanan untuk analisis penyakit degenerative pada klinik. Hal ini menyebabkan adanya *Top Event* berupa pemanfaatan *genogram tools.* Selanjutnya berdasarkan kegiatan (as-is) dan (to-be) yang didapatkan dari pelayanan Kesehatan di klinik maka dilakukan identifikasi risiko TI sebagai berikut:

1) Hasil identifikasi risiko aplikasi adalah :
   a) *External Attack* (Serangan eksternal)
   b) *Network Congestion* (Kesalahan jaringan)
   c) *System Crash*
2) Hasil identifikasi risiko informasi:
   a) Database Failure
3) Hasil identifikasi risiko infrastruktur :
   a) Hardware failure
   b) Power Outages
4) Hasil identifikasi risiko *people*:
   a). Inappropriate access
   b) Abuse of Position
   c) Lack Of Genogram technology

Berdasarkan pemetaan analisis nilai *likelihood* kejadian dan *impact* risiko yang mungkin terjadi, terbentuk nilai evaluasi yang menunjukkan tingkat *impact* risiko yaitu *low, middle, dan high.* Risiko dengan nilai evaluasi *high* adalah *inappropriate access, abuse of position* dan *lack of genogram technology.* Sedangkan untuk risiko *middle* adalah *Network congestion, power outages.* Terakhir risiko dengan tingkatan *low likelihood* tapi high *impact* adalah *External attack, database failure,* dan *Hardware failure.* Oleh karena itu diperlukan adanya treatment untuk risiko yang dapat dimitigasi sesuai kemampuan organisasi.

REFERENCE

[1] M. Hammer and J. Champy, "Reengineering the corporation: A manifesto for business revolution," *Bus. Horiz.*, vol. 36, no. 5, pp. 90–91, 1993, doi: 10.1016/S0007-6813(05)80064-3.

[2] K. L. Karen Coffman, "Management of Change 2007 Innovation [online]." [Online]. Available: https://slideplayer.com/slide/7749547/ [september 2018]

[3] ISACA, *Risk Scenarios Using COBIT 5 for Risk*. 2014.

[4] D. Kernick, "Wanted — new methodologies for health service research . Is complexity theory the answer ?," no. March, pp. 385–390, 2006, doi: 10.1093/fampra/cml011.

[5] A. Hejazi, N. Abdolvand, and S. R. Harandi, "Assesing The organizational Readiness For Implementing BI System," vol. 6, no. 1, 2016, doi: 10.5121/ijitcs.2016.6102.

[6] N. H. Al-Moosa and N. Sharts-Hopko, "Using Change Management to Redesign Oman′s Health Professions Education Sector," *Heal. Prof. Educ.*, vol. 3, no. 2, pp. 108–112, 2017, doi: 10.1016/j.hpe.2016.09.001.

[7] ISACA, *Risk Scenario Using COBIT 5 for Risk*. Rolling Meadows, IL 60008 USA: ISACA, 2014.

[8] M. Alaeddini and M. Mir-Amini, *Integrating COBIT with a hybrid group decision-making approach for a business-aligned IT roadmap formulation*, vol. 21, no. 2. Springer US, 2020. doi: 10.1007/s10799-019-00305-0.

[9] R. Zulfitri, "Analisis Kebijakan Pelayanan Kesehatan Primer Dalam Manajemen Penatalaksanaan Penyakit Kronis Lansia," *J. Kesehat. Masy. Andalas*, vol. 10, no. 1, pp. 52–58, 2017, doi: 10.24893/jkma.v10i1.163.

[10] A. Stevenson, Oxford Dictionary of English, Oxford: Oxford University Press, 2010.

[11] Hubbard, Douglas (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons. p. 46.

[12] ISO/IEC, "International Standard ISO 31000," *61010-1 © Iec2001*, vol. 2009, p. 13, 2009.

[13] ISACA, *COBIT 5 for Risk*, no. For usage guidelinesFor usage guidelines. 2013.

[14] 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.

[15] Y. Sani, "Analisis Layanan Kesehatan Primer ' Andal ' Dengan Pendekatan Desain Layanan Pada Poliklinik," 2018, [Online].Available: https://repository.ub.ac.id/id/eprint/193432/1/Yasir Sani.pdf