Penilaian Risiko Keamanan *Enterprise Architecture* ITTelkom Surabaya Menggunakan Metode *Failure Mode and Effect Analysis* (FMEA) Berbasis ISO 27001

Tyrela Disya Arivani[*1)], Yupit Sudianto[2)], dan Aris Kusumawati[3)]
[1)]Sistem Informasi, Fakultas Teknologi Informasi dan Bisnis, Institut Teknologi Telkom Surabaya,
Jalan Ketintang No.156, Surabaya, 60243, Indonesia
tyreladisya@student.ittelkom-sby.ac.id

Abstrak

ITTelkom Surabaya telah menerapkan *Enterprise Architecture* (EA) berbasis *website* sebagai *blueprint* organisasi untuk menyelaraskan visi dan misi organisasi, serta proses bisnis dengan teknologi informasi dalam perspektif data, aplikasi, dan teknologi. Sejak EA dibangun belum pernah dilakukan penilaian risiko keamanan informasi sehingga rentan adanya risiko yang mengancam. Penelitian ini bertujuan untuk melakukan penilaian risiko keamanan informasi dengan standar ISO 27001:2013 sebagai pedoman dalam melakukan proses penilaian risiko dan menghasilkan identifikasi risiko yang terjadi. Hasil dari identifikasi risiko kemudian dilakukan analisis risiko menggunakan metode FMEA dan menghasilkan nilai *Risk Priority Number* (RPN) pada tiap risiko. Berdasarkan hasil analisis, diperoleh 25 risiko yang mengancam keamanan informasi pada EA ITTelkom Surabaya. Terdapat 7 risiko dengan level *low*, 4 risiko dengan level medium, 9 risiko dengan level *high*, dan 7 risiko dengan level *very high*. Selanjutnya didapatkan hasil rekomendasi mitigasi risiko berdasarkan ISO 27001:2013 dengan menggunakan 5 objektif kontrol dalam penanganan risiko.

Kata kunci: *EA, Keamanan Informasi, ISO 27001:2013, Penilaian Risiko, FMEA*

1. Pendahuluan (Introduction)

Peran Teknologi Informasi (TI) saat ini menjadi suatu kebutuhan dalam sebuah organisasi. Dengan adanya TI diharapkan mampu menunjang proses bisnis sehingga dapat mendukung dalam pencapaian visi, misi, dan tujuan organisasi. Hal ini penerapan TI tentu menjadi aset penting bagi keberlangsungan kehidupan di suatu organisasi dalam menjalankan strategi bisnisnya. Oleh karena itu dalam penerapan TI perlu adanya sebuah keamanan informasi agar terlindungi dari pihak yang tidak memiliki wewenang untuk mengetahui atau mengelolanya. Keamanan informasi memiliki tiga aspek utama diantaranya *confidentiality* (kerahasiaan) yaitu data dan informasi hanya dapat diakses oleh orang yang berhak, *integrity* (integritas) yaitu perlindungan terhadap keaslian data dan informasi, dan *availability* (ketersediaan) yaitu melindungi ketersediaan data dan informasi sehingga data dapat diakses pada saat dibutuhkan (Ramjanati, Wijaya and Muarie, 2021). *Enterprise Architecture* merupakan suatu pendokumentasian yang memuat elemen proses bisnis, teknologi, informasi data, dan aplikasi dengan sistem yang saling terintegrasi. Di dalam EA terdapat data atau informasi yang terpusat sehingga dapat membantu organisasi dalam menyelaraskan antara strategi bisnis dengan strategi TI agar lebih optimal. Institut Teknologi Telkom Surabaya (ITTelkom Surabaya) dengan beralamat di Jalan Ketintang No. 156, Surabaya yang baru berdiri pada tahun 2018 merupakan perguruan tinggi swasta dibawah naungan Yayasan Pendidikan Telkom (YPT) yang mempunyai visi menjadi perguruan tinggi berstandar internasional yang berbasis *Information and Communication Technology* (ICT). Hal tersebut menunjukkan bahwa EA sangat penting dalam menunjang dan mencapai strategi untuk kesuksesan terhadap visi institusi.

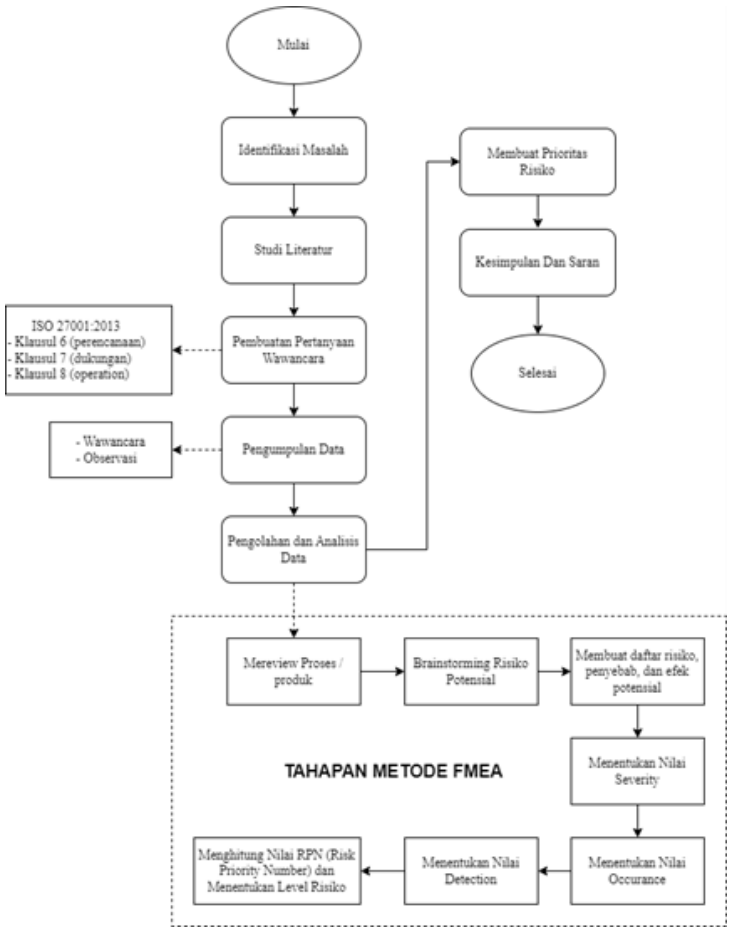
Didasari dengan EA yang merupakan penerapan dari TI tentu memiliki adanya ancaman dan risiko terhadap keamanan informasi. Dalam TI, risiko didefinisikan sebagai hasil dari kerentanan sistem

terhadap ancaman yang ditimbulkannya bagi organisasi (Tanaamah and Indira, 2021). Risiko keamanan informasi yang memungkinkan seperti modifikasi data secara ilegal, maupun kesalahan manusia (sumber daya manusia), dan sebagainya (Hanifah and S.Suroso, 2020). Berdasarkan hasil wawancara dengan informan Wakil Dekan FTIB selaku pengembang EA bahwa saat ini EA ITTelkom Surabaya digunakan sebagai *blueprint* organisasi untuk menyelaraskan visi dan misi organisasi, serta proses bisnis. EA terbilang masih baru dan dalam pengembangannya masih dengan menggunakan kerangka kerja TOGAF – ADM kemudian di *generate* menjadi sebuah *HyperText Markup Language* (HTML) sehingga dapat berupa *website*. Namun saat ini data yang ada pada EA masih dapat terlihat secara keseluruhan tanpa adanya pembagian hak akses informasi. Menurut pernyataan informan lain selaku staf SPMP dan pengembang EA bahwa sejak dilakukan pengembangan EA belum pernah dilakukan penilaian risiko keamanan informasi. Ada banyak cara untuk melakukan manajemen risiko salah satunya adalah dengan berpedoman pada persyaratan Standar Manajemen Keamanan Informasi (SMKI) ISO 27001:2013. ISO 27001:2013 lebih menekankan pada persyaratan keamanan informasi yang dituangkan dalam 10 klausa umum dan detail 114 kendali (*control*) yang terbagi dalam 14 domain dan menggunakan pendekatan aset informasi (*Asset Approach*) dalam manajemen risikonya. Klausa umum yang digunakan pada ISO 27001:2013 terdiri dari klausul 6 (perencanaan) karena sesuai dengan persyaratan ISO 27001 adalah tentang perencanaan, dan khususnya perencanaan tindakan untuk mengatasi risiko dan peluang (Hanti, 2023). Klausul 7 (dukungan) sesuai dengan persyaratan ISO 27001 untuk menyediakan sumber daya yang cukup untuk penerapan, pemeliharaan, penetapan, dan peningkatan berkelanjutan dari sistem manajemen keamanan informasi (Hanti, 2023). Klausul 8 (operasi) sesuai dengan persyaratan ISO 27001:2013 untuk meminta organisasi melakukan perencanaan, penerapan dan pengendalian proses yang diperlukan untuk memenuhi persyaratan untuk menerapkan tindakan yang ditentukan dalam klausul 6 (Hanti, 2023). Dalam melakukan analisis risiko terdapat banyak metode yang dapat digunakan sebagai acuan, salah satunya adalah metode *Failure Mode and Effect Analysis* (FMEA). FMEA merupakan proses yang terorganisasi untuk meningkatkan perlindungan terhadap aset informasi dalam mencegah terjadinya mode kegagalan, dampak, dan efek potensial yang dihasilkan dengan menganalisis dan mengelompokkan potensi risiko (Matondang, Isnainiyah and Muliawatic, 2018). FMEA memiliki perhitungan terkait *Risk Priority Number* (RPN) berdasarkan nilai *Severity* (keparahan), *Occurance* (kemungkinan), dan *Detection* (tingkat deteksi) kemudian dari hasil perhitungan dikelompokkan berdasarkan level risiko sehingga dari hal tersebut dapat diketahui potensi risiko paling tinggi dan memudahkan dalam pengambilan keputusan apakah perlu dimitigasi atau tidak (Ramayani, 2022). Adanya potensi risiko terhadap keamanan informasi yang ada pada EA, hal ini menjadi latar belakang menggunakan standar sistem yang salah satunya adalah ISO/IEC 27001:2013 dan melakukan analisis menggunakan metode FMEA. Dari hasil analisis juga dilakukan rencana penanganan / rekomendasi berdasarkan kontrol annex A ISO 27001:2013 yang nantinya disesuaikan dengan hasil risiko beserta penyebab potensial nya. Diharapkan nantinya dapat berguna sebagai bahan perbaikan pada pengembangan EA ITTelkom Surabaya kedepannya berdasarkan dari hasil penilaian risiko sehingga dapat meminimalisir adanya risiko ancaman, serta EA ITTelkom Surabaya dapat terimplementasikan sesuai dengan standar ISO 27001:2013.

2. Metode Penelitian (Methods)

Pengumpulan data dilakukan dengan melakukan wawancara kepada beberapa informan yang telah ditentukan sesuai dengan kualifikasi informan yang berkaitan dengan EA ITTelkom Surabaya. Informan yang digunakan yaitu unit bagian Satuan Penjaminan Mutu dan Perencanaan (SPMP), Wakil Dekan FTIB, dan unit bagian Pusat Teknologi Informasi (PUTI) untuk mengidentifikasi masalah pada *enterprise architecture* ITTelkom Surabaya dari hasil pengembangannya dan mengetahui bagaimana kondisi eksisting organisasi terkait sistem keamanan informasi, dan proses bisnis pada EA ITTelkom Surabaya. Selain itu pengumpulan data juga dilakukan observasi terhadap objek secara langsung guna

melihat proses maupun fenomena yang terjadi. Dalam melakukan wawancara, ISO 27001:2013 digunakan sebagai panduan dalam menyusun daftar pertanyaan guna nantinya menghasilkan temuan – temuan masalah yang terjadi pada EA ITTelkom Surabaya terkait dengan persyaratan yang telah pada klausul ISO 27001:2013 yaitu klausul 6 (perencanaan), klausul 7 (dukungan), dan klausul 8 (operasi). Selain itu juga dilakukan proses penilaian risiko yang terletak pada klausul 6 (perencanaan) ISO 27001:2013. Pengumpulan data juga dilakukan dengan cara studi *literatur* dengan sumber data yang digunakan yaitu jurnal, tesis, buku, dan internet. Metode yang digunakan adalah FMEA untuk melakukan analisis risiko sehingga didukung dengan menggunakan data kuantitatif dari hasil perhitungan RPN yang didapatkan berdasarkan hasil penilaian pada tingkat *Severity*, tingkat *Occurance*, tingkat *Detection* pada tiap risiko dengan langkah – langkah yang ditunjukkan pada Gambar 1.



Gambar 1 Alur Prosedur Penelitian

Tahap yang dilakukan dalam Gambar 1 adalah sebagai berikut :

1. ***Mereview* proses / cara kerja**
   Langkah pertama yang dilakukan pada tahap ini yaitu dengan menjabarkan proses bisnis / produk pada EA ITTelkom Surabaya.
2. ***Brainstorming* Risiko Potensial**
   Langkah ini dilakukan untuk menganalisis risiko potensial (*failure mode*) berdasarkan klausul 6, 7, dan 8 pada ISO 27001:2013 yang meliputi 4 kategori aset yaitu pada *software, hardware, people*, dan data yang didapatkan dari hasil wawancara kepada informan dengan tujuan untuk mengetahui kegagalan yang dapat terjadi.
3. **Membuat daftar risiko, penyebab, dan efek potensial**
   Langkah ini yaitu membuat daftar risiko dari hasil identifikasi risiko, penyebab, dan dampak / efek yang dihasilkan dari adanya risiko potensial.

4. **Menentukan Nilai *Severity* (S)**
   Langkah ini yaitu suatu penilaian tingkat keparahan dari keseriusan efek yang ditimbulkan dari mode-mode kegagalan (*failure mode*). Dan menghitung seberapa besar dampak / intensitas kejadian mempengaruhi output proses, maupun proses – proses selanjutnya. Hasil penilaian tingkat *Severity* (S) dari masing – masing risiko yang nantinya akan digunakan dalam menghitung RPN. Kriteria penilaian yaitu bersumber dari FMEA dengan menggunakan skala penilaian 1 – 10 pada tingkat *severity* (Hanifah and S.Suroso, 2020).
5. **Menentukan Nilai *Occurance* (O)**
   Langkah ini yaitu suatu penilaian mengenai probabilitas frekuensi penyebab mekanisme kegagalan yang akan terjadi, sehingga dapat menghasilkan bentuk/mode kegagalan yang memberikan akibat tertentu selama masa operasional EA. Hasil penilaian tingkat *Occurance* dari masing – masing risiko yang nantinya akan digunakan dalam menghitung RPN. Kriteria penilaian yaitu bersumber dari FMEA dengan menggunakan skala penilaian 1 – 10 pada tingkat *occurance* (Hanifah and S.Suroso, 2020).
6. **Menentukan Nilai *Detection* (D)**
   Langkah ini yaitu pengukuran terhadap tingkat efektivitas metode atau kemampuan untuk mendeteksi terjadinya suatu risiko. Deteksi dilakukan untuk melihat bagaimana cara mendeteksi peristiwa yang memiliki risiko secara tepat, agar organisasi mampu membuat tindakan terhadap risiko yang terdeteksi secara cepat. Hasil penilaian tingkat *Detection* (D) dari masing – masing risiko yang nantinya akan digunakan dalam menghitung RPN. Kriteria penilaian yaitu bersumber dari FMEA dengan menggunakan skala penilaian 1 – 10 pada tingkat *detection* (Hanifah and S.Suroso, 2020).
7. **Menghitung Nilai *Risk Priority Number* (RPN) dan Level Risiko**
   Tahap ini merupakan perhitungan *Risk Priority Number* (RPN). Perhitungan ini dilakukan dengan cara pengkalian dari nilai *Severity* (S), *Occurance* (O), *dan Detection* (D). Dari proses penilaian tersebut akan dibobotkan sehingga didapatkan RPN yang merupakan skor potensi dari risiko yang telah di identifikasi.

   Berikut adalah rumus perhitungan RPN :

   $$RPN = S \times O \times D \qquad (1)$$

   Selanjutnya dari nilai perhitungan nilai RPN tersebut diklasifikasikan berdasarkan tingkatan level risiko seperti pada **Error! Reference source not found.**Tabel 1.

Tabel 1 Kriteria Level Risiko

Level	Skala Nilai RPN
Very low (sangat rendah)	$x < 20$
Low (rendah)	$20 \leq x < 80$
Medium	$80 \leq x < 120$
High (tinggi)	$120 \leq x < 200$
Very High (sangat tinggi)	$x > 200$

Sumber : FMEA, 2023

8. **Menentukan Prioritas Risiko**
   Berdasarkan hasil penilaian RPN dan pengkategorian level risiko, maka dapat diketahui risiko yang memiliki nilai RPN tinggi masuk pada kategori *very high* sehingga dapat dijadikan prioritas dalam menentukan tindakan perbaikan terhadap risiko yang memiliki tingkatan paling tinggi, Tahap ini

dilakukan susunan urutan prioritas risiko mulai dari risiko yang tertinggi sampai risiko yang terendah (WARDHANU, 2020).

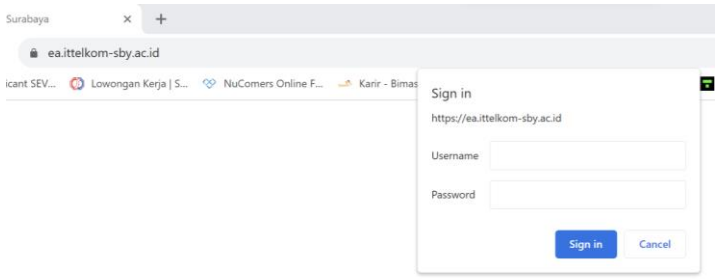
3. Hasil dan Pembahasan (*Results and Discussions*)

Analisis risiko menggunakan FMEA yang merupakan salah satu metode terstruktur dalam menganalisa, melakukan identifikasi, serta mencegah proses mode kegagalan dari penyebab serta memberikan penilaian terhadap risiko yang ada (WARDHANU, 2020). Berdasarkan hasil pengamatan yang telah dilakukan selama proses pengumpulan data berikut merupakan hasil analisis dan potensi kegagalan :

1. Analisis Cara Kerja / Produk

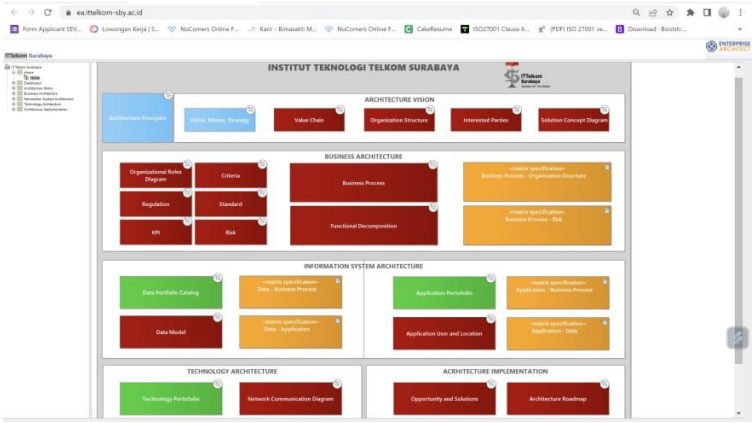
EA ITTelkom Surabaya dikembangkan menggunakan *software sparx systems enterprise architect* dengan *framework* TOGAF-ADM. Dalam *software* tersebut berisi data atau informasi yang kemudian di *generate* menjadi sebuah html sehingga berbasis *website*. EA saat ini juga telah menggunakan *domain* ittelkom-sby.ac.id sebagai web server sehingga dapat diakses secara *online* dan secara *public*. Dalam mengakses EA ini hanya dapat menggunakan komputer / PC, dan *google chrome* maupun sejenis nya yang digunakan sebagai web *browser*. Berikut dilakukan analisis dari cara kerja, dan fitur pada EA yang tersedia saat ini, antara lain:

a. *User* dapat mengunjungi halaman url https://ea.ittelkom-sby.ac.id/ kemudian melakukan *login* dengan menggunakan *username* dan *password*. Jika *username* dan *password* yang dimasukkan sesuai maka berhasil *login*, dan halaman utama (*home*) akan tampil. Jika *username* dan *password* yang dimasukkan tidak sesuai maka akan kembali ke halaman *login* seperti pada Gambar 2.



Gambar 2 Halaman *Login*

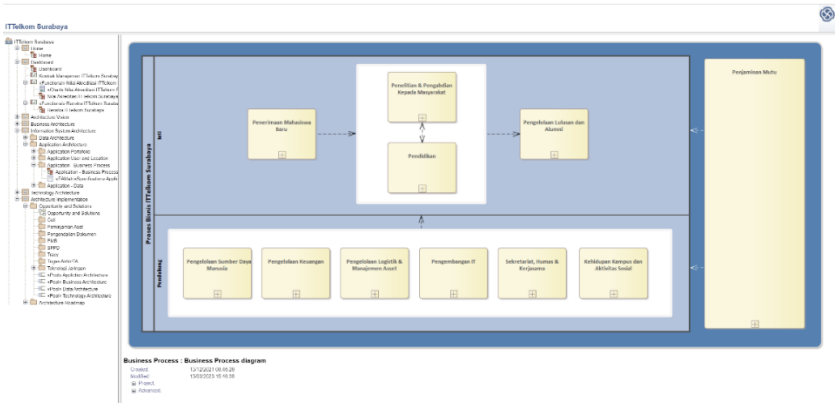
b. *User* mampu melihat seluruh data utama secara *general* pada halaman *home* yang telah di *generate* dari *software sparx systems enterprise* seperti pada Gambar 3. Data yang ada di EA juga dikelompokkan menjadi 5 bagian diantaranya yaitu *architecture vision, business architecture, information system architecture, technology architecture, dan architecture implementation.*



Gambar 3 Halaman *Home*

Terdapat beberapa warna yang digunakan dan memiliki arti diantaranya warna merah berupa diagram, oranye berupa *matrix*, hijau berupa *catalog*, dan biru berupa *text*.

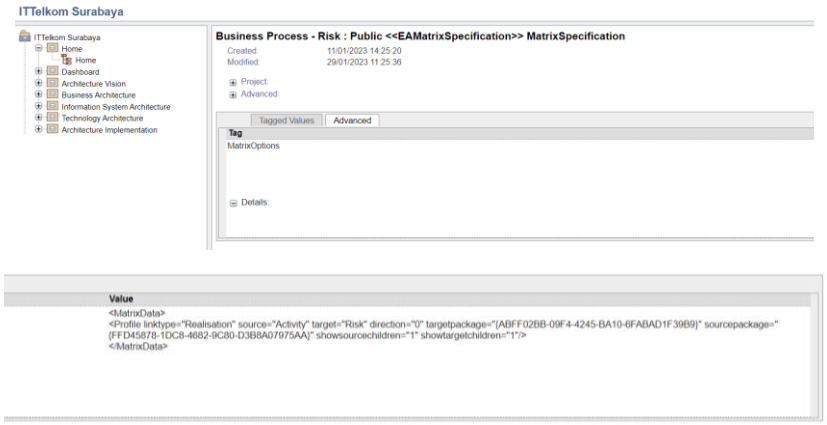
c. *User* juga dapat melihat data lain dengan lebih *detail* seperti yang ditunjukkan pada Gambar 4 dengan cara mengklik pada bagian kotak yang berwarna yang ada pada halaman *home* seperti pada Gambar 3 sesuai dengan data yang ingin dilihat.



Gambar 4 Halaman *Business Process*

Halaman proses bisnis ITTelkom Surabaya yang dijabarkan dalam bentuk diagram. Dalam proses bisnis tersebut terbagi menjadi 2 proses bisnis yaitu inti dan pendukung. Untuk proses bisnis inti terdiri dari 4 bagian, dan proses bisnis pendukung terdiri dari 6 bagian.

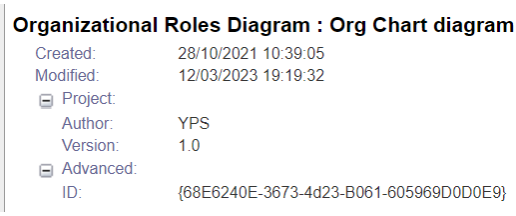
d. Terdapat data yang tidak dapat di *generate* ke html dari *software sparx systems enterprise* sehingga data tidak dapat ditampilkan pada EA. Salah satu data yang tidak dapat ditampilkan yaitu bagian data *matrix spesification* yang ditunjukkan pada Gambar 5.



Gambar 5 Halaman Data *Matrix Spesification*

Halaman data *matrix specification* berikut pada bagian *business process – risk.* Sehingga data yang ditampilkan pada EA masih hanya berupa *print text source code.*

e. *User* mampu melihat *history author* dan *version* perubahan dengan cara mengklik tanda + *project* yang ada dibagian bawah pada halaman yang dilihat, selain itu juga dapat melihat tanggal kapan data tersebut dibuat dan yang melakukan perubahan data pada EA seperti pada Gambar *6*.



Gambar 6 Tampilan *History* Perubahan Data

Dalam *history* perubahan diketahui tanggal *created,* dan *modified* serta jam nya dan *author project* nya.

2. Identifikasi Aset

Daftar aset diperoleh dari hasil wawancara yang telah dilakukan dengan bagian (SPMP) ITTelkom Surabaya, Wakil Dekan FTIB yang merupakan pengembang dari EA ITTelkom Surabaya, serta (PUTI) ITTelkom Surabaya yang merupakan pengelola dan pendukung operasional EA ITTelkom Surabaya. Berikut ini adalah daftar dari aset kritis yang dikategorisasikan berdasarkan *hardware, software, people,* dan data disajikan pada Tabel 2.

Tabel 2 Daftar Aset

Kategori Aset	Nama Aset
Software	*Website* EA
	Sparx systems enterprise architect
	Firewall
Hardware	Server DT YPT
	Perangkat Jaringan Internet (*router, access point)*
People	Kepala Bagian SPMP
	Staf Bagian SPMP
	Wakil Dekan FTIB (pengembang EA)
	Kepala Bagian PUTI
	Kepala Urusan Aplikasi (PUTI)
Data	*Architecture Vision*
	Business Architecture
	Information System Architecture
	Technology Architecture
	Architecture Implementation

3. Hasil Analisis Klausul ISO 27001:2013

Berdasarkan hasil wawancara dengan informan dengan berpedoman pada klausul 6, 7, dan 8 ISO 27001:2013 didapatkan hasil temuan sebagai berikut yang nantinya akan menghasilkan hasil identifikasi risiko :

Tabel 3 Hasil Temuan Pada Klausul ISO 27001:2013

No.	Klausul dalam ISO 27001:2013	Temuan
1.	Klausul 6: perencanaan	Belum adanya program kesadaran untuk memahami peran dan tanggung jawab dalam menjaga keamanan informasi
		Belum adanya program pelatihan / *training* kepada pihak yang diberikan wewenang untuk mengoperasionalkan EA / pengguna baru

No.	Klausul dalam ISO 27001:2013	Temuan
		Belum adanya pengujian dan evaluasi secara berkala terkait kontrol keamanan informasi pada EA.
		Untuk pemantauan saat ini dilakukan dengan melalui sistem notifikasi telegram ke pihak PUTI
2.	Klausul 7 : Dukungan	Belum adanya kebijakan yang terdokumentasi terkait *control access* informasi
		Belum adanya pembagian peran dan tanggung jawab yang jelas dan terdokumentasi terkait yang diperbolehkan mengoperasional EA.
		Untuk saat ini SDM yang terlibat dalam bertanggung jawab mengoperasionalkan EA memiliki kompetensi yang sesuai dan paham dengan EA namun terbatas
		Untuk saat ini yang dapat mengakses hanya pihak tertentu yang memiliki kepentingan namun masih belum adanya pembagian hak akses informasi
		Belum adanya prosedur / SOP yang terdokumentasi untuk pengguna baru
		Belum adanya SOP yang terdokumentasi untuk yang memiliki hak akses ubah data
		Saat ini jika terjadi adanya insiden keamanan informasi dengan melaporkan kepada pihak PUTI dan pemulihan dengan cara melakukan pemulihan data melalui github
3.	Klausul 8 : Operasi	Belum adanya perjanjian hukum yang tertulis dan terdokumentasi tentang penerapan kebijakan keamanan informasi kepada pihak yang diberikan akses informasi pada EA
		Untuk prosedur pemberian hak akses informasi / akses ke EA hanya melalui perijinan kepada pihak SPMP terlebih dahulu
		Adanya penggunaan *firewall* dan anti virus pada sisi server DT YPT
		Saat ini data belum di enkripsi
		Tidak adanya prosedur *backup* yang terdokumentasi, namun *backup* data dilakukan pada github dan berupa *print text*
		Server EA yang berupa hosting dan dijadikan satu dengan domain ittelkomsurabaya yang lain dan ditempatkan pada YPT di daerah lembong agar lebih terjaga 24 jam
		Saat ini untuk pengendalian akses yang tidak sah dilakukan oleh PUTI hanya menggunakan *tool* web *vulnerability* yaitu Nessus dan *Accunetix*
		Sudah terdapat halaman *login* biasa dan pemberian *Username* dan *Password* pada EA yang masih secara *default* serta hanya ada satu akses *login.*
		Ruangan server hanya diperbolehkan untuk orang tertentu saja yang boleh masuk
		Menggunakan jaringan VPN untuk akses data ke server dan hanya bisa digunakan / terhubung pada 1 laptop
		Belum adanya kontrol keamanan pada url yaitu belum menerapkan *expired time*
		Belum menerapkan limitasi gagal *login*

No.	Klausul dalam ISO 27001:2013	Temuan
		Belum adanya persyaratan yang terdokumentasi untuk pihak ketiga yang memiliki akses ke informasi rahasia atau penting karna untuk saat ini EA masih dapat diakses secara umum
		Saat ini belum adanya penerapan log aktivitas pada sisi web dan tidak adanya pemantauan secara berkala / setiap hari
		Tidak pernah dilakukan pemantauan / pengecekan kembali pada EA
		Belum adanya prosedur yang ditetapkan secara terdokumentasi, dan penanganan hanya baru dilakukan ketika terjadi masalah dan hanya dilakukan pemantauan melalui log web server

4. *Brainstorming* Risiko Potensial

Pada tahap ini dilakukan *brainstorming* risiko potensial dengan tujuan untuk mengetahui kegagalan yang dapat terjadi. Adapun identifikasi risiko potensial didapatkan berdasarkan hasil analisis temuan yang memenuhi persyaratan maupun tidak memenuhi persyaratan pada klausul ISO 27001:2013 yang telah dijabarkan pada **Error! Reference source not found.**Output yang dihasilkan pada tahap ini adalah daftar risiko kegagalan (*failure mode)* disertai penyebab potensial (*cause failure)*, dan efek potensial (*effect failure)* pada tiap kategori aset (Ramayani, 2022). Berikut hasil dari *brainstorming* risiko dan dikategorikan berdasarkan aset *software* (SFW), *hardware* (HDW), *people* (PEO), data (DAT) yang dijabarkan pada Tabel 4.

Tabel 4 *Brainstorming* Risiko

Kode Risiko	Identifikasi Risiko		
	Cause failure	*Failure Mode*	*Effect Failure*
SFW – 01	*Username* dan *Password* yang digunakan terlalu mudah untuk ditebak	Serangan *hacker* berupa peretasan *Username* dan *Password* akses *login*	Mendapatkan akses *illegal* ke EA untuk melihat informasi penting / rahasia oleh pihak yang tidak berhak.
	Tidak adanya pergantian *Password* secara berkala		
SFW – 02	Tidak adanya batasan ketika *user* gagal melakukan *login* pada EA	Adanya gangguan layanan pada akses *login (brute force)*	Membuat server *down* sehingga *user* yang memiliki hak akses terkendala mengakses informasi pada EA ketika dibutuhkan.
SFW – 03	Tidak adanya sistem deteksi untuk aktivitas yang mencurigakan / tidak sah (contoh : log aktivitas *login*) pada sisi web EA	*Illegal* akses	Pihak yang tidak memiliki akses / wewenang dapat mengakses seluruh data pada EA tanpa diketahui maksud dan tujuannya
SFW – 04	Adanya penggunaan *firewall* pada sisi server DT YPT	Adanya serangan *Denial of Service* (DDoS)	Pihak yang tidak berwenang dapat mengakses EA dan mempengaruhi ketersediaan layanan yang berakibat *server* menjadi lemah sehingga EA tidak dapat diakses
SFW – 05	Adanya serangan *malware*/virus melalui jaringan VPN yang digunakan	Perusakan data	Informasi / data pada EA tidak dapat diakses sehingga *user*

Kode Risiko	Identifikasi Risiko		
	Cause failure	*Failure Mode*	*Effect Failure*
			kesulitan ketika membutuhkan informasi melalui EA
SFW – 06	Tidak adanya *login expired session* pada EA ketika EA sudah tidak digunakan dalam jangka waktu lama.	Url *website* EA masih dapat diakses tanpa *login*.	EA masih dapat diakses dan kemungkinan dapat disalahgunakan untuk kepentingan yang tidak seharusnya oleh pihak yang tidak berkepentingan
HDW – 01	Terlalu banyak yang mengakses server secara bersamaan karena server EA yang berupa hosting dan dijadikan satu dengan domain ittelkomsurabaya yang lain.	Server *down*	EA tidak dapat diakses sehingga *user* tidak dapat mengakses informasi pada EA ketika dibutuhkan.
HDW – 02	Adanya *maintenance* yang tak terduga pada penyedia layanan yang dipakai dan server DT YPT	Gangguan jaringan untuk mengakses EA	IP local tidak dapat mengakses EA sehingga data / informasi pada EA tidak dapat di proses
HDW – 03	Penggunaan anti virus pada server DT YPT sebagai proteksi	Adanya serangan *malware* pada server DT YPT	Tidak dapat mengakses EA karena data yang ada di server hilang
HDW – 04	Kurangnya kontrol pemeliharaan/maintenance terhadap server.	Kerusakan fisik pada perangkat keras server DT YPT.	Mengakibatkan kerugiaan khususnya secara materi yang dapat menganggu jalannya proses bisnis untuk pemulihan data
	Bencana alam meliputi banjir, gempa, reruntuhan.		Menghambat pemrosesan *read and write* data pada EA dan akses ke EA menjadi lambat / lemot.
HDW – 05	*Space memory* yang tersedia melewati dari batas maksimal karena kelalaian monitoring dari internal institusi.	*Hard disk* pada server DT YPT penuh.	Data / informasi yang bersifat penting dan rahasia dapat disalahgunakan untuk kepentingan yang tidak seharusnya
PEO – 01	Tidak adanya kebijakan dan prosedur yang terdokumentasi terkait dengan *control* akses informasi.	Penyalahgunaan hak aksesinformasi.	
	Tidak adanya kontrol keamanan tambahan untuk autentikasi ketika melakukan *login* / akses data.		Seluruh data masih dapat dilihat oleh orang yang tidak sesuai jabatan untuk akses informasi tersebut
PEO – 02	Tidak adanya pembatasan hak akses informasi pada setiap *user* karena hanya ada 1	Penyebaran data *sensitive* / informasi rahasia.	Tidak dapat melakukan *login* ke *dashboard* sehingga tidak dapat mengakses informasi pada EA. Dan *user* kesulitan dalam

Kode Risiko	Identifikasi Risiko		
	Cause failure	*Failure Mode*	*Effect Failure*
	Username dan *Password* untuk akses *login* setiap *user*.		mendapatkan informasi melalui EA
PEO – 03	Tidak terdapat pesan / notif yang ditampilkan pada halaman *login* apabila terjadi kesalahan *input*.	Kesalahan dalam *input Username* dan *Password* pada halaman *login*	*User* masih kurang paham dengan cara kerja menggunakan EA sehingga rentan terjadi kesalahan dalam melaksanakan tugas dan mempengaruhi kerahasiaan data
PEO – 04	Belum adanya pelatihan dan masih hanya berupa sosialisasi.	*Human error*	Adanya kesalahan dalam konfigurasi dan input data / informasi pada *sparx systems enterprise architect* sehingga mengganggu produktivitas dan ketersediaan data, serta *integrity* data pada EA.
	Tidak adanya dokumentasi penggunaan EA dan tidak ada pendefinisian terkait peran / tanggung jawab.		
	Minimnya SDM yang paham tentang EA		Data dapat diakses oleh pihak yang tidak berkepentingan / tidak memiliki wewenang tanpa harus melakukan *login* ulang sehingga menimbulkan potensi adanya pencurian data
PEO – 05	Tidak dapat melakukan *logout* pada website EA karena tidak adanya fitur *logout*.	Penyalahgunaan akun	Adanya salinan data dan penyebaran informasi rahasia tidak sesuai aslinya kepada pihak yang tidak berhak / pihak luar.
PEO – 06	Tidak adanya kebijakan/regulasi yang terdokumentasi terkait penggandaan data / penyalinan informasi.	Duplikat data tanpa ijin	Tidak memiliki panduan yang jelas tentang bagaimana mengelola dan menjaga keamanan informasi pada akses informasi yang diberikan
PEO – 07	Belum adanya perjanjian hukum yang tertulis dan terdokumentasi tentang penerapan kebijakan keamanan informasi kepada pihak yang diberikan akses informasi pada EA	Adanya pelanggaran kebijakan / aturan yang berlaku.	Data yang dibutuhkan pada EA tidak tersedia / tidak dapat diakses
DAT – 01	Kerusakan pada server di pusat DT YPT.	Kehilangan data.	Data yang dibutuhkan pada EA bagian data matrix tidak tersedia / tidak dapat diakses
DAT – 02	Lisensi pada *sparx systems enterprise architect* yang terbatas.	Data *matrix specification* tidak dapat di *generate* ke html.	Data yang tersedia tidak akurat dan tidak dapat dipastikan kebenarannya sehingga mengancam *integrity* data yang tersedia.

Kode Risiko	Identifikasi Risiko		
	Cause failure	*Failure Mode*	*Effect Failure*
DAT – 03	Lamanya proses pengajuan untuk melakukan validasi kepada unit terkait.	Sebagian data pada EA belum tervalidasi.	Data / informasi yang bersifat penting dan rahasia dapat di salahgunakan untuk kepentingan yang tidak seharusnya.
DAT – 04	Tidak adanya enkripsi data untuk perlindungan data yang bersifat krusial.	Kebocoran data.	Tidak dapat melakukan pembaharuan data dan tidak tersedianya data yang dibutuhkan pada EA
DAT – 05	Data tidak ter *back-up* pada github	Data gagal dipulihkan / di *update.*	Tidak memiliki *backup* data ketika data mengalami kerusakan atau kehilangan
DAT – 06	Jaringan di pusat mati / mengalami kendala.	Data gagal di *back-up*	Kehilangan kerahasiaan data yang dapat mengancam turunnya reputasi organisasi / institusi karena data dapat disalahgunakan
DAT – 07	Tidak adanya kontrol keamanan tambahan pada website EA terkait screen picture / print out informasi melalui komputer / PC	Pencurian data secara *illegal*.	

5. Menentukan Nilai *Severity (S), Occurance (O), Detection (D)*

Langkah ini yaitu suatu penilaian tingkat keparahan (*severity)* dari keseriusan efek yang ditimbulkan dari mode kegagalan (*failure mode*). Penilaian mengenai probabilitas frekuensi penyebab mekanisme kegagalan yang akan terjadi (*occurance).* Serta pengukuran terhadap tingkat efektivitas metode atau kemampuan untuk mendeteksi terjadinya suatu risiko (*detection)*. Penilaian yang didapatkan seluruh informan mengacu pada skala penilaian 1 – 10 yang bersumber dari FMEA tingkat *Severity* dengan melakukan wawancara (Munaroh, Amrozi and Nurdian, 2020).

Tabel 5 Nilai Kategori *Software*

Kode Risiko	Identifikasi Risiko		Nilai FMEA		
	Cause failure	*Failure Mode*	S	O	D
SFW – 01	*Username* dan *Password* yang digunakan terlalu mudah untuk ditebak	Serangan *hacker* berupa peretasan *username* dan *password* akses *login*	8	4	4
	Tidak adanya pergantian *Password* secara berkala				
SFW – 02	Tidak adanya batasan ketika *user* gagal melakukan *login* pada EA	Adanya gangguan layanan pada akses *login (brute force)*	6	7	2
SFW – 03	Tidak adanya sistem deteksi untuk aktivitas yang mencurigakan / tidak sah (contoh : log aktivitas *login*) pada sisi web EA	*Illegal* akses	6	4	3
SFW – 04	Adanya penggunaan *firewall* pada sisi server DT YPT	Adanya serangan *Denial of Service* (DDoS)	5	4	1

Kode Risiko	Identifikasi Risiko		Nilai FMEA		
	Cause failure	*Failure Mode*	S	O	D
SFW – 05	Adanya serangan *malware* / virus melalui jaringan VPN yang digunakan	Perusakan data	8	4	2
SFW – 06	Tidak adanya *login expired session* pada EA ketika EA sudah tidak digunakan dalam jangka waktu lama.	Url *website* EA masih dapat diakses tanpa *login*.	6	4	3

Berdasarkan nilai *severity* pada Tabel 5 menunjukkan bahwa tingkat keparahan paling tinggi pada kategori software adalah serangan *hacker* berupa peretasan *username* dan *password* akses *login* dan adanya perusakan data. Pada nilai *occurance* paling tinggi adalah adanya gangguan layanan pada akses *login (brute force)*. Pada nilai *detection* semakin kecil nilai nya maka semakin cepat dapat dideteksi dan dikendalikan yang ditunjukkan padaTabel 5 yaitu serangan *Denial of Service* (DDoS).

Tabel 6 Nilai Kategori *Hardware*

Kode Risiko	Identifikasi Risiko		Nilai FMEA		
	Cause failure	*Failure Mode*	S	O	D
HDW – 01	Terlalu banyak yang mengakses server secara bersamaan karena server EA yang berupa hosting dan dijadikan satu dengan domain ittelkomsurabaya yang lain.	Server *down*	5	4	3
HDW – 02	Adanya *maintenance* yang tak terduga pada penyedia layanan yang dipakai dan *maintenance* pada server DT YPT	Gangguan jaringan untuk mengakses EA	4	5	5
HDW – 03	Penggunaan anti-virus pada server DT YPT sebagai proteksi	Adanya serangan *malware* pada server DT YPT	7	4	5
HDW – 04	Kurangnya kontrol pemeliharaan / *maintenance* terhadap server karena internal PUTI hanya dapat melakukan monitoring *online* pada server	Kerusakan fisik pada perangkat keras server DT YPT.	9	1	5
HDW – 05	*Space memory* yang tersedia melewati dari batas maksimal karena kelalaian monitoring dari internal institusi.	*Hard disk* pada server DT YPT penuh.	5	3	2

Berdasarkan nilai *severity* pada Tabel 6 menunjukkan bahwa tingkat keparahan paling tinggi pada kategori *hardware* adalah kerusakan fisik pada perangkat keras server DT YPT. Pada nilai *occurance* paling tinggi adalah Gangguan jaringan untuk mengakses EA. Pada nilai *detection* semakin kecil nilai nya maka semakin cepat dapat dideteksi dan dikendalikan yang ditunjukkan pada Tabel 6 yaitu *Hard disk* pada server DT YPT penuh.

Tabel 7 Nilai Tingkat *Severity* Kategori *People*

Kode Risiko	Identifikasi Risiko		Nilai FMEA		
	Cause failure	*Failure Mode*	S	O	D
PEO – 01	Tidak adanya kebijakan dan prosedur yang terdokumentasi terkait dengan *control* akses informasi.	Penyalahgunaan hak akses informasi.	8	4	7
	Tidak adanya kontrol keamanan tambahan untuk autentikasi ketika melakukan *login* / akses data.				
PEO – 02	Tidak adanya pembatasan hak akses informasi pada setiap *user* karena hanya ada 1 *username* dan *password* untuk akses *login* setiap *user*.	Penyebaran data *sensitive* / informasi rahasia.	9	7	7
PEO – 03	Tidak terdapat pesan / notif yang ditampilkan pada halaman *login* apabila terjadi kesalahan *input*.	Kesalahan dalam *input username* dan *password* pada halaman *login*	5	6	6
PEO – 04	Belum adanya pelatihan dan masih hanya berupa sosialisasi.	*Human error*	7	4	5
	Tidak adanya dokumentasi penggunaan EA dan tidak ada pendefinisian terkait peran / tanggung jawab.		6	4	7
	Minimnya SDM yang paham tentang EA		8	3	8
PEO – 05	Tidak dapat melakukan *logout* pada website EA karena tidak adanya fitur *logout*.	Penyalahgunaan akun	9	7	8
PEO – 06	Tidak adanya kebijakan / regulasi yang terdokumentasi terkait penggandaan data / penyalinan informasi.	Duplikat data tanpa ijin	9	5	7
PEO – 07	Belum adanya perjanjian hukum yang tertulis dan terdokumentasi tentang penerapan kebijakan keamanan informasi kepada pihak yang diberikan akses informasi pada EA	Adanya pelanggaran kebijakan / aturan yang berlaku.	6	3	7

Berdasarkan nilai *severity* pada Tabel 7 menunjukkan bahwa tingkat keparahan paling tinggi pada penyebaran data sensitive / informasi rahasia, penyalahgunaan akun, duplikat data tanpa ijin. Pada nilai *occurance* paling tinggi adalah penyalahgunaan akun. Pada nilai *detection* semakin kecil nilai nya maka semakin cepat dapat dideteksi dan dikendalikan yang ditunjukkan pada Tabel 7 adalah *human error* - belum adanya pelatihan dan masih hanya berupa sosialisasi.

Tabel 8 Nilai Tingkat *Severity* Kategori Data

Kode Risiko	Identifikasi Risiko		Nilai FMEA		
	Cause failure	*Failure Mode*	S	O	D
DAT – 01	Kerusakan pada server di pusat DT YPT	Kehilangan/kerusakan data.	6	2	6

Kode Risiko	Identifikasi Risiko		Nilai FMEA		
	Cause failure	*Failure Mode*	S	O	D
DAT – 02	Lisensi pada *sparx systems enterprise architect* yang terbatas	Data *matrix spesification* tidak dapat di-*generate* ke html.	7	8	6
DAT – 03	Lamanya proses pengajuan untuk melakukan validasi kepada unit terkait	Sebagian data pada EA belum tervalidasi.	7	5	5
DAT – 04	Tidak adanya enkripsi data untuk perlindungan data yang bersifat krusial.	Kebocoran data.	9	5	6
DAT – 05	Data tidak ter *back-up* pada github	Data gagal dipulihkan / di *update*.	6	4	6
DAT – 06	Jaringan di pusat mati / mengalami kendala.	Data gagal di *back-up*	6	4	6
DAT – 07	Tidak adanya kontrol keamanan tambahan pada EA terkait *screen picture* / *print out* informasi melalui PC.	Pencurian data secara *illegal*.	9	5	5

Berdasarkan nilai *severity* pada Tabel 8 menunjukkan bahwa tingkat keparahan paling tinggi pada kebocoran data, dan pencurian data secara *illegal*. Pada nilai *occurance* paling tinggi adalah Data *matrix spesification* tidak dapat di-*generate* ke html. Pada nilai *detection* semakin kecil nilai nya maka semakin cepat dapat dideteksi dan dikendalikan yang ditunjukkan pada Tabel 8 adalah sebagian data pada EA belum tervalidasi, dan pencurian data secara *illegal*.

6. Menghitung Nilai RPN, Level Risiko, dan Prioritas Risiko

Tahap ini merupakan perhitungan RPN yang dilakukan dengan cara pengkalian dari nilai (S), (O), dan (D). Selanjutnya dari hasil perhitungan nilai RPN tersebut diklasifikasikan berdasarkan tingkatan level risiko pada tiap kategori aset yang ditunjukkan pada Tabel 1. Kemudian berdasarkan hasil penilaian RPN dan pengkategorian level risiko, maka dapat diketahui risiko yang memiliki nilai RPN tinggi termasuk pada kategori *very high* sehingga dapat dijadikan prioritas dalam menentukan tindakan perbaikan terhadap risiko. Prioritas risiko diurutkan dari yang memiliki nilai RPN tertinggi sampai yang memiliki nilai RPN terendah (WARDHANU, 2020).

Tabel 9 Perhitungan Nilai RPN

Kode Risiko	*Cause failure*	*Failure Mode*	RPN	Level	*Rank*
PEO – 05	Tidak dapat melakukan *logout* pada website EA karena tidak adanya fitur *logout*.	Penyalahgunaan akun	504	*Very High*	1
PEO – 02	Tidak adanya pembatasan hak akses informasi pada setiap *user* karena hanya ada 1 *Username* dan *Password* untuk akses *login* setiap *user*.	Penyebaran data *sensitive* / informasi rahasia.	441	*Very High*	2

Kode Risiko	*Cause failure*	*Failure Mode*	RPN	Level	*Rank*
DAT – 02	Lisensi pada *sparx systems enterprise architect* yang terbatas	Data *matrix spesification* tidak dapat di-*generate* ke html.	336	*Very High*	3
PEO – 06	Tidak adanya kebijakan / regulasi yang terdokumentasi terkait penggandaan data / penyalinan informasi.	Duplikat data tanpa ijin	315	*Very High*	4
DAT – 04	Tidak adanya enkripsi data untuk perlindungan data yang bersifat krusial.	Kebocoran data.	270	*Very High*	5
DAT – 07	Tidak adanya kontrol keamanan tambahan pada EA terkait *screen picture* / *print out* informasi melalui komputer / PC	Pencurian data secara *illegal*.	225	*Very High*	6
PEO – 01	Tidak adanya kebijakan dan prosedur yang terdokumentasi terkait dengan *control* akses informasi.	Penyalahgunaan hak aksesinformasi.	224	*Very High*	7
	Tidak adanya kontrol keamanan tambahan untuk autentikasi ketika melakukan *login* / akses data.				
PEO - 04	Minimnya SDM yang paham tentang EA	*Human error*	192	*High*	8
PEO – 03	Tidak terdapat pesan / notif yang ditampilkan pada halaman *login* apabila terjadi kesalahan *input*.	Kesalahan dalam *input Username* dan *Password* pada halaman *login*	180	*High*	9
PEO – 04	Tidak adanya dokumentasi penggunaan EA dan tidak ada pendefinisian terkait peran / tanggung jawab.	*Human error*	168	*High*	10
DAT – 03	Lamanya proses pengajuan untuk melakukan validasi kepada unit terkait	Sebagian data pada EA belum tervalidasi.	175	*High*	11
DAT – 05	Data tidak ter *back-up* pada github	Data gagal dipulihkan / di update.	144	*High*	12
DAT – 06	Jaringan di pusat mati / mengalami kendala.	Data gagal di *back-up*	144	*High*	13
HDW – 03	Penggunaan anti-virus pada server DT YPT sebagai proteksi	Adanya serangan *malware* pada server DT YPT	140	*High*	14
PEO – 04	Belum adanya pelatihan dan masih hanya berupa sosialisasi.	*Human error*	140	*High*	15

Kode Risiko	*Cause failure*	*Failure Mode*	RPN	Level	*Rank*
PEO – 07	Belum adanya perjanjian hukum yang tertulis dan terdokumentasi tentang penerapan kebijakan keamanan informasi kepada pihak yang diberikan akses informasi pada EA	Adanya pelanggaran kebijakan / aturan yang berlaku.	126	*High*	16
HDW – 02	Adanya *maintenance* yang tak terduga pada penyedia layanan yang dipakai dan *maintenance* pada server DT YPT	Gangguan jaringan untuk mengakses EA	100	Medium	17
SFW – 01	*Username* dan *Password* yang digunakan terlalu mudah untuk ditebak Tidak adanya pergantian *Password* secara berkala	Serangan *hacker* berupa peretasan *Username* dan *Password* akses *login*	96	Medium	18
SFW – 02	Tidak adanya batasan ketika *user* gagal melakukan *login* pada EA	Adanya gangguan layanan pada akses *login (brute force)*	84	Medium	19
DAT – 01	Kerusakan pada server di pusat DT YPT	Kehilangan data.	72	Medium	20
SFW – 03	Tidak adanya sistem deteksi untuk aktivitas yang mencurigakan / tidak sah (contoh : log aktivitas *login*) pada sisi web EA	*Illegal* akses	72	*Low*	21
SFW – 06	Tidak adanya *login expired session* pada EA ketika EA sudah tidak digunakan dalam jangka waktu lama.	Url *website* EA masih dapat diakses tanpa *login*.	72	*Low*	22
SFW – 05	Adanya serangan *malware* / virus melalui jaringan VPN yang digunakan	Perusakan data	64	*Low*	23
HDW – 01	Terlalu banyak yang mengakses server secara bersamaan karena server EA yang berupa hosting dan dijadikan satu dengan domain ittelkomsurabaya yang lain.	Server *down*	60	*Low*	24
HDW – 04	Kurangnya kontrol pemeliharaan / *maintenance* terhadap server karena internal PUTI hanya dapat melakukan monitoring *online* pada server	Kerusakan fisik pada perangkat keras server DT YPT.	45	*Low*	25
HDW – 05	*Space memory* yang tersedia melewati dari batas maksimal karena kelalaian monitoring dari internal PUTI.	*Hard disk* pada server DT YPT penuh.	30	*Low*	26

Kode Risiko	*Cause failure*	*Failure Mode*	RPN	Level	*Rank*
SFW – 04	Adanya penggunaan *firewall* pada sisi server DT YPT	Adanya serangan *Denial of Service* (DDoS)	20	*Low*	27

7. Rekomendasi Mitigasi Risiko

Hasil pemeringkatan prioritas risiko yang didapatkan akan diberikan rekomendasi untuk dilakukan perbaikan kedepannya guna mengurangi dampak dari risiko yang ditimbulkan berdasarkan yang memiliki nilai RPN paling tinggi dengan kategori level risiko *very high* yang ditunjukkan pada Tabel 9. Rekomendasi perbaikan dilakukan dengan mengacu berdasarkan kontrol annex ISO 27001:2013. Berikut didapatkan 7 rekomendasi perbaikan berdasarkan klausul ISO 27001:2013 dan upaya mitigasi untuk mengatasi pada risiko. Berikut mode kegagalan yang harus mendapat mitigasi prioritas yaitu pada kode risiko PEO – 05 penyalahgunaan akun karena tidak dapat melakukan *logout* pada *website* EA karena tidak adanya fitur *logout* dengan nilai RPN 504 dan rekomendasi mitigasi sesuai objektif kontrol ISO 27001:2013 yaitu A.9 *Access Control* (Kontrol Akses dan Pengaturan Akses Pengguna) dengan kontrol ISO 27001:2013 yaitu A.9.4.1 Pengendalian Akses ke Sistem dan Layanan. Kode risiko PEO – 02 adanya penyebaran data sensitive / informasi rahasia karena Tidak adanya pembatasan hak akses informasi pada setiap *user* karena hanya ada 1 *Username* dan *Password* untuk akses *login* setiap *user* dengan nilai RPN 441 dan rekomendasi mitigasi sesuai objektif kontrol ISO 27001:2013 yaitu A.9 *Access Control* (Kontrol Akses dan Pengaturan Akses Pengguna) dengan kontrol ISO 27001:2013 yaitu A.9.2.3 Manajemen hak akses istimewa. Kode risiko DAT – 02 data *matrix specification* tidak dapat di generate ke html karena lisensi pada *sparx systems enterprise architect* yang terbatas dengan nilai RPN 336 dan rekomendasi mitigasi sesuai objektif kontrol ISO 27001:2013 yaitu A.8 Manajemen Aset dengan kontrol ISO 27001:2013 yaitu A.8.1.1 Inventaris Aset. Kode risiko PEO – 06 Duplikat data tanpa ijin karena tidak adanya kebijakan/regulasi yang terdokumentasi terkait penggandaan data/penyalinan informasi dengan nilai RPN 315 dan rekomendasi mitigasi sesuai objektif kontrol ISO 27001:2013 yaitu A.13 Keamanan Komunikasi dengan kontrol ISO 27001:2013 yaitu A.13.2.1 Prosedur dan kebijakan perpindahan informasi. Kode risiko DAT – 04 kebocoran data karena tidak adanya enkripsi data untuk perlindungan data yang bersifat krusial dengan nilai RPN 270 dan rekomendasi mitigasi sesuai objektif kontrol ISO 27001:2013 yaitu A.10 Kriptografi dengan kontrol ISO 27001:2013 yaitu A.10.1.2 Manajemen Kunci. Kode risiko DAT – 07 adanya pencurian data secara *illegal* karena tidak adanya kontrol keamanan tambahan pada EA terkait *screen picture* / *print out* informasi melalui PC dengan nilai RPN 225 dan rekomendasi mitigasi sesuai objektif kontrol ISO 27001:2013 yaitu A.12 Keamanan Operasi dengan kontrol ISO 27001:2013 yaitu A.12.1.1 Prosedur operasional yang didokumentasikan. Kode risiko PEO – 01 Penyalahgunaan hak akses informasi karena Tidak adanya kebijakan dan prosedur yang terdokumentasi terkait dengan *control* akses informasi dan Tidak adanya kontrol keamanan tambahan untuk autentikasi ketika melakukan *login* / akses data dengan nilai RPN 224 dan rekomendasi mitigasi sesuai objektif kontrol ISO 27001:2013 yaitu A.9 *Access Control* (Kontrol Akses dan Pengaturan Akses Pengguna) dengan kontrol ISO 27001:2013 yaitu A.9.4.2 Prosedur *log-on* yang aman.

Kesimpulan (Conclusion)

Berdasarkan dari hasil pembahasan penelitian pada EA ITTelkom Surabaya terdapat risiko dari 7 dari kategori *people* diantaranya yaitu PEO – 01 penyalahgunaan hak akses, PEO – 02 penyebaran data *sensitive* / informasi rahasia, PEO – 03 kesalahan dalam *input username* dan *password* pada halaman *login*, PEO – 04 *Human error*, PEO – 05 penyalahgunaan akun, PEO – 06 duplikat data tanpa ijin, PEO – 07 adanya pelanggaran kebijakan / aturan yang berlaku. Terdapat 7 risiko dari kategori data yaitu DAT – 01 kehilangan data, DAT – 02 data *matrix specification* tidak dapat di – *generate* ke html, DAT – 03

sebagian data pada EA belum tervalidasi, DAT – 04 kebocoran data, DAT – 05 data gagal dipulihkan / di-*update*, DAT – 06 data gagal di *back-up*, DAT – 07 : pencurian data secara *illegal*. Terdapat 6 risiko dari kategori *software* yaitu SFW – 01 serangan *hacker* berupa peretasan *username* dan *password* akses *login*, SFW – 02 adanya gangguan layanan pada akses *login* (*brute force*), SFW – 03 *illegal* akses, SFW – 04 adanya serangan *Denial of Service (DDoS)*, SFW – 05 perusakan data, SFW – 06 url *website* EA masih dapat diakses tanpa *login*. Terdapat 5 risiko dari kategori *hardware* yaitu HDW – 01 : server *down*, HDW – 02 : gangguan jaringan untuk mengakses EA, HDW – 03 : adanya serangan *malware* pada server DT YPT, HDW – 04 : kerusakan fisik pada perangkat keras server DT YPT, HDW – 05 : *hard disk* pada server DT YPT penuh.

Berdasarkan hasil penilaian risiko pada EA ITTelkom Surabaya dengan menggunakan metode FMEA berbasis ISO 27001:2013 dengan melakukan perhitungan RPN dan di kategorikan berdasarkan kriteria level risiko pada FMEA kategori level risiko *very high* (sangat tinggi), *high* (tinggi), medium, *low* (rendah), *very low* (sangat rendah) sehingga pada penelitian didapatkan 7 risiko dengan nilai RPN di kategori level risiko *very high*, 9 risiko dengan nilai RPN di kategori level risiko *high*, 4 risiko dengan nilai RPN di kategori level risiko medium, dan 7 risiko dengan nilai RPN di kategori level risiko *low*.

Didapatkan 7 rekomendasi perbaikan berdasarkan klausul ISO 27001:2013 dan upaya mitigasi untuk mengatasi pada risiko. Adapun yang diberikan rekomendasi adalah 7 risiko yang memiliki nilai risiko paling tinggi (*very high)* sehingga bisa dijadikan rekomendasi untuk dilakukan penanganan terlebih dahulu. Berikut mode kegagalan yang harus mendapat mitigasi prioritas yaitu berdasarkan kategori *very high* (sangat tinggi) yaitu pada kode risiko PEO – 05 penyalahgunaan akun karena tidak dapat melakukan *logout* pada *website* EA karena tidak adanya fitur *logout*. Kode risiko PEO – 02 adanya penyebaran data sensitive / informasi rahasia karena Tidak adanya pembatasan hak akses informasi pada setiap *user* karena hanya ada 1 *Username* dan *Password* untuk akses *login* setiap *user*. Kode risiko DAT – 02 data *matrix specification* tidak dapat di *generate* ke html karena lisensi pada *sparx systems enterprise architect* yang terbatas. Kode risiko PEO – 06 Duplikat data tanpa ijin karena tidak adanya kebijakan/regulasi yang terdokumentasi terkait penggandaan data/penyalinan informasi. Kode risiko DAT – 04 kebocoran data karena tidak adanya enkripsi data untuk perlindungan data yang bersifat krusial. Kode risiko DAT – 07 adanya pencurian data secara *illegal* karena tidak adanya kontrol keamanan tambahan pada EA terkait *screen picture* / *print out* informasi melalui komputer / PC dengan. Kode risiko PEO – 01 Penyalahgunaan hak akses informasi karena Tidak adanya kebijakan dan prosedur yang terdokumentasi terkait dengan *control* akses informasi dan Tidak adanya kontrol keamanan tambahan untuk autentikasi ketika melakukan *login* / akses data. Adapun terdapat 5 kontrol objektif ISO 27001:2013 yang digunakan sebagai rekomendasi mitigasi yaitu A.9 *Access Control* (Kontrol Akses dan Pengaturan Akses Pengguna), A.8 Manajemen Aset, A.13 Keamanan Komunikasi, A.10 Kriptografi, A.12 Keamanan Operasi.

Ucapan Terima Kasih (Acknowledgement)

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada berbagai pihak yang terlibat pada penelitian ini, yakni perwakilan Fakultas Teknologi Informasi dan Bisnis (FTIB), unit bagian Satuan Penjaminan Mutu dan Perencanaan (SPMP), dan unit bagian Pusat Teknologi Informasi (PUTI) ITTelkom Surabaya yang telah bersedia sebagai informan dalam proses penggalian data pada penelitian ini terkait dengan penilaian risiko pada *enterprise architecture* ITTelkom Surabaya. Sehingga penulis mampu menyelesaikan penelitian ini dengan baik dan sesuai dengan tujuan.

Daftar Pustaka

Hanifah, P. and S.Suroso, J. (2020) 'Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA', *Jurnal Komputer Terapan*, 6(Vol. 6 No. 2 (2020)), pp. 210–221. Available at: https://doi.org/10.35143/jkt.v6i2.3728.

Hanti, C. (2023) *KLAUSUL PADA ISO 27001 : 2013*. Available at: https://indosbu.com/blog/klausul-pada-iso-27001-2013#:~:text=Klausul 6 dari persyaratan ISO 27001 adalah tentang,ISO 27001 sehingga penting untuk memenuhi persyaratan mereka.

Matondang, N., Isnainiyah, I.N. and Muliawatic, A. (2018) 'Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)', *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 2(1), pp. 282–287. Available at: https://doi.org/10.29207/resti.v2i1.96.

Munaroh, L., Amrozi, Y. and Nurdian, R.A. (2020) 'Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013', *Technomedia Journal*, 5(2), pp. 167–181. Available at: https://doi.org/10.33050/tmj.v5i2.1377.

Ramayani, Y. (2022) 'Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)', *INOVTEK Polbeng - Seri Informatika*, 7(2), p. 289. Available at: https://doi.org/10.35314/isi.v7i2.2631.

Ramjanati, P., Wijaya, F.K. and Muarie, M.S. (2021) 'Penilaian Risiko Keamanan Informasi Menggunakan Octave Allegro: Studi Kasus pada Perguruan Tinggi', *JUSIFO (Jurnal Sistem Informasi)*, 7(1), pp. 10–20. Available at: https://doi.org/10.19109/jusifo.v7i1.5870.

Tanaamah, A.R. and Indira, F.J. (2021) 'Analysis of Information Technology Security Management UKSW SIASAT Using ISO/IEC 27001:2013', *IJITEE (International Journal of Information Technology and Electrical Engineering)*, 5(2), p. 68. Available at: https://doi.org/10.22146/ijitee.65670.

WARDHANU, E. (2020) *ANALISIS RISIKO SISTEM MANAJEMEN ASET BERBASIS ISO 27001 : 2013 MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS PADA PT. TIRTA INVESTAMA*. Available at: https://openlibrary.telkomuniversity.ac.id/pustaka/164455/analisis-risiko-sistem-manajemen-aset-berbasis-iso-27001-2013-menggunakan-metode-failure-mode-and-effects-analysis-pada-pt-tirta-investama.html.