MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI MENGGUNAKAN METODE FMEA DAN ISO 27001 PADA ORGANISASI XYZ

Raden Budiarto

Sistem Informasi STMIK Jakarta STI&K
Jl.BRI Radio Dalam, Kebayoran Baru, Jakarta 12140
raden@jak-stik.ac.id

***Abstrak* — Sekalipun sudah populer di bidang teknik industri, metode Failure Mode & Effect Analysis FMEA masih sangat jarang dilaporkan penelitiannya terhadap objek sistem informasi. Hal ini menarik untuk dieksplorasi lebih lanjut pemanfaatannya pada sistem informasi. Variabel yang diukur pada penelitian ini adalah occurrence (frekuensi kejadian), severity (dampak) dan detection (pencegahan). Data penelitian diambil terutama berdasarkan dari hasil pengamatan langsung. Penelitian ini mencakup perlindungan terhadap aset informasi di lingkungan Organisasi XYZ dengan melakukan penilaian risiko keamanan informasi. Penilaian tersebut dilakukan dengan menggunakan metode (FMEA). Pada penelitian ini juga menggunakan kerangka kerja ISO 27001 untuk melengkapi daftar rekomendasi aksi penanggulangan mode kegagalan. Hasil dari penelitian ini yaitu berupa laporan hasil pengelolaan manajemen risiko yang berisikan daftar prioritas analisis risiko yang disertai akar sebab permasalahan dan pengendalian risiko sesuai dengan standar ISO 27001. Hasil dari studi kasus telah membuktikan penerapan standar ISO 27001 berimbas terhadap penurunan tingkat kerawanan sebesar 30%.**

***Keywords* — FMEA, ISO 27001, keamanan informasi, manajemen risiko**

I. PENDAHULUAN

A. *Latar Belakang*

Penerapan tata kelola sistem informasi (SI) sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik dalam upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola SI faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola SI akan terganggu jika informasi sebagai salah satu objek utama dari tata kelola tersebut mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

Organisasi XYZ merupakan salah satu organisasi yang memiliki tugas pokok dan fungsi dalam bidang keamanan dan keselamatan di wilayah yurisdiksi laut NKRI. Dalam menjalankan tugas pokok dan fungsinya, secara umum organisasi XYZ memiliki sistem pengoperasian deteksi dini berbasis sistem teknologi informasi dalam upaya mencegah terjadinya pelanggaran-pelanggaran di wilayah kelautan NKRI yang dapat menyebabkan terganggunya stabilitas keamanan.

Untuk mengetahui tingkat kematangan teknologi informasi yang dimiliki oleh organisasi XYZ dalam upayanya menjaga keamanan dan keselamatan laut Indonesia, organisasi XYZ telah mengikuti *Desktop Assessment* pada tahun 2014 yang menggunakan indeks KAMI versi 2.3 berbasis SNI ISO/IEC 27001:2009 [1]. Berdasarkan hasil yang ada, organisasi XYZ berada pada tingkat kematangan I dari V tingkat kematangan. Sedangkan, menurut hasil evaluasi tingkat kesiapan dan capaian dari standar ISO tersebut, peran TI yang ada pada organisasi XYZ berada dalam status kesiapan dengan nilai 73 dari 588 pada kategori sedang. Hasil lainnya pada pemeringkatan indeks KAMI di tahun 2015 dengan menggunakan versi 3.1 berbasis SNI ISO/IEC 27001, hasil penilaian berupa kelengkapan penerapan standar tersebut terhadap sistem elektronik yang dimiliki oleh organisasi XYZ adalah 85 dari 645 untuk kategori dengan kerawanan tinggi.

Berdasarkan hasil penilaian tersebut, dapat disimpulkan bahwa kontrol pengamanan sistem elektronik dan teknik informasi yang dimiliki oleh organisasi XYZ masih belum memadai dan membutuhkan peningkatan di banyak aspek sesuai dengan kebutuhan kontrol yang termasuk dalam kategori tinggi. Terkait permasalahan tersebut, sebagai institusi pemerintahan yang bersinggungan dengan pelanggaran-pelanggaran berupa kejahatan yang dapat mengganggu stabilitas keamanan laut dan perekonomian negara, keamanan perangkat sistem elektronik dan teknologi informasi yang dimiliki oleh organisasi XYZ menjadi hal penting yang perlu diperhatikan dalam penelitian ini.

Untuk mengatasi berbagai permasalahan tersebut, diperlukan suatu metode yang tepat untuk mencari akar dari dari berbagai jenis penyebab yang berpotensi menimbulkan kerawanan sistem dan membuat analisis untuk perbaikan dengan

menggunakan *Failure Mode and Effect Analysis* (FMEA). FMEA merupakan teknik yang digunakan untuk mendefinisikan, mengidentifikasi, memprioritaskan dan menghilangkan permasalahan kegagalan sistem, baik permasalahan yang telah diketahui maupun yang potensial terjadi pada sistem. Metode FMEA dipilih karena metode ini mudah digunakan dan sudah populer digunakan pada bidang teknik industri. Bagaimana pun untuk penerapan di bidang sistem informasi masih sangat jarang dilaporkan. Dengan demikian tulisan ini ingin mengeksplorasi lebih jauh penggunaan metode FMEA di bidang sistem informasi.

B. *Perumusan Masalah*

Berdasarkan latar belakang yang telah dijabarkan di atas, maka dapat dirumuskan permasalahan penelitian sebagai berikut:

- Bagaimana kondisi tingkat perawan dan risiko keamanan pada sistem informasi organisasi XYZ saat ini?
- Apa saja yang menjadi akar permasalahan yang potensi menimbulkan kerawanan atau kegagalan sistem informasi organisasi XYZ?
- Bagaimanakah model manajemen risiko keamanan informasi yang seharusnya diterapkan dalam upaya meningkatkan keamanan dan kehandalan sistem informasi di lingkungan organisasi XYZ?

C. *Tujuan Penelitian*

Tujuan yang ingin dicapai dari penelitian ini yaitu mengidentifikasi potensi gangguan dan permasalahan yang ada pada sistem teknologi keamanan informasi di organisasi XYZ kemudian memberikan rekomendasi kontrol yang perlu diterapkan untuk manajemen risiko keamanan informasi yang lebih baik. Pada akhirnya yang diharapkan output dari penelitian ini adalah sistem informasi organisasi XYZ yang lebih aman dan dapat diandalkan.

II. LANDASAN TEORI

Sekilas Tentang FMEA

Dasar FMEA pertama kali diambil dari standar prosedur untuk FMECA (*Failure mode, Effect, Critical Analysis*) yang digambarkan dalam Angkatan Bersenjata AS pada dokumen militer MIL-P-1629 (tahun 1949) kemudian direvisi pada tahun 1980 sebagai MIL-STD-1629A [2]. Pada awal 1960-an, kontraktor untuk *National Aeronautics and Space Administration* (NASA) menggunakan variasi dari FMECA yang dikenal sebagai nama FMEA. Beberapa program NASA yang telah menggunakan prosedur FMEA di antaranya Apollo, Viking, Galileo, dan Skylab. FMEA kemudian banyak diadopsi oleh industri penerbangan sipil, dimulai dari *Society for Automotive Engineers* (SAE) penerbitan ARP926 pada tahun 1967. Selama tahun 1970-an, penggunaan FMEA menyebar ke industri lainnya. Pada tahun 1971 NASA menyiapkan laporan untuk Survei Geologi AS merekomendasikan penggunaan FMEA dalam penilaian eksplorasi minyak lepas pantai. Pada tahun 1973 laporan *Environmental Protection Agency* Amerika Serikat juga telah menjelaskan penerapan FMEA untuk instalasi pengolahan air limbah. Industri otomotif mulai menggunakan FMEA pada pertengahan 1970-an. Ford Motor Company memperkenalkan FMEA untuk industri otomotif untuk keperluan keselamatan pengguna setelah terjadi beberapa insiden yang melibatkan keselamatan pengguna mobil Ford. Ford menerapkan pendekatan yang sama untuk proses (PFMEA) untuk mempertimbangkan proses potensial yang disebabkan kegagalan sebelum meluncurkan produksi. Pada tahun 1993 Industri *Otomotif Action Group* (AIAG) pertama kali menerbitkan standar FMEA untuk industri otomotif.

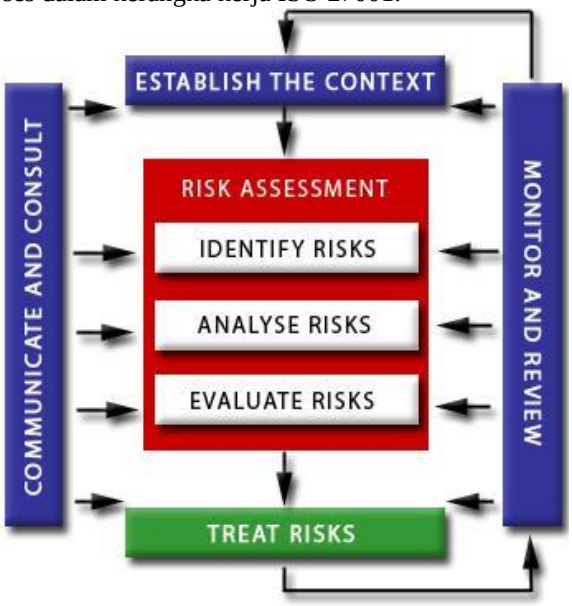
FMEA merupakan metode yang sangat masuk akal dan efektif jika dilaksanakan dengan teliti. Lebih lanjut menurut Gunjan & Himanshu Joshi [3] keuntungan menggunakan FMEA antara lain:

1. Mengurangi kemungkinan kegagalan serupa di masa
2. Meminimalkan biaya akibat kegagalan
3. Meminimalkan perubahan dramatis (*last minutes change*)
4. Meningkatkan produk / kualitas proses serta kehandalan & keselamatan
5. Peningkatan kepuasan pengguna
6. Berfokus pada pencegahan

Pada sisi lain FMEA juga memiliki berbagai kekurangan di antaranya FMEA saja tidak akan menghilangkan modus kegagalan. Tindakan tambahan yang mungkin berada di luar FMEA sangat dibutuhkan untuk itu. Selain itu FMEA hanya dapat mengidentifikasi mode kegagalan-kegagalan utama yang terdapat dalam sistem tanpa merambah ke cabang-cabang kegagalan yang lebih kecil. Untuk hal masalah tersebut *Failure Tree Analysis* (FTA) cenderung lebih cocok digunakan untuk "*top-down*" analisis [4]. Selain itu, peringkat berdasarkan *severity, occurrence & detection* dapat memunculkan peringkat yang tidak sesuai dengan kenyataan, di mana mode kegagalan kurang parah justru mendapatkan nilai RPN yang lebih tinggi dari mode kegagalan yang lebih parah. Peringkat skala ordinal pada nilai RPN hanya menunjukkan bahwa satu peringkat lebih baik atau lebih buruk dari peringkat yang lain, tapi tidak seberapa banyak. Sebagai contoh peringkat 4 bukan berarti 4 kali lebih buruk dari peringkat 1. Kelemahan dari penggunaan FMEA adalah sifatnya yang cenderung reaktif dan beradaptasi dari kegagalan ketimbang mencegahnya terlebih dahulu.

Kerangka Kerja ISO 27001

Keamanan data/informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur penting. Sebab data/informasi adalah aset bagi perusahaan tersebut. Ancaman dan risiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data/informasi menjadi alasan disusunnya standar sistem manajemen keamanan informasi yang salah satunya adalah ISO 27001:2013. Dalam ISO ini dikenal standar penganan risiko (*risk assessment*) yang melibatkan proses identifikasi risiko di mana setiap risiko yang ada harus dapat dikenal dengan baik, kemudian risiko dianalisis dampaknya dan dievaluasi cara-cara untuk menanggulangi risiko tersebut. Kerangka kerja ISO 27001 melibatkan proses komunikasi dan konsultasi serta pemantauan dan peninjauan untuk proses manajemen risiko. Proses penanganan risiko itu sendiri dijalan dalam empat tahapan proses secara berurutan yakni identifikasi, analisis, evaluasi dan penanganan risiko. Gbr. 1 mengilustrasikan proses-proses dalam kerangka kerja ISO 27001.



Gbr. 1 Proses manajemen risiko dalam kerangka kerja ISO 27001 (Sumber: BSI Standards Publication)

Penyusunan standar ini berawal pada tahun 1995, di mana sekelompok perusahaan besar yang terdiri dari Board of Certification, British Telecom, Marks & Spencer, Midland Bank, Nationwide Building Society, Shell dan Unilever bekerja sama untuk membuat suatu standar yang dinamakan British Standard 7799 (BS 7799) kemudian berkembang menjadi The International Standards Organization yang merupakan lembaga independen yang mengeluarkan standar operasional prosedur (SOP) terhadap kualitas suatu layanan. ISO memperkenalkan ISO 27001:2013 yang berisi standar mengenai manajemen informasi yang terakhir kali diperbarui pada tahun Oktober 2013 .

Penelitian-Penelitian Sebelumnya

Terdapat berbagai laporan terkait dengan penelitian yang menggunakan metode FMEA. Objek penelitian sebelumnya yang ada pada penelitian-penelitian terkait penggunaan metode FMEA sudah cukup bervariasi. Penggunaan FMEA telah menyebar ke berbagai industri lainnya seperti industri tekstil [5], kerajinan tangan [6] dan pengolahan limbah [7]. Bagaimana pun terdapat sebuah kecenderungan penelitian-penelitian yang ada yang terpusat pada industri manufaktur atau perusahaan yang memiliki produk berwujud fisik.

Penelitian ini mencoba untuk mengeksplorasi lebih jauh pemanfaatan metode FMEA pada bidang teknologi informasi khususnya sistem informasi. Sistem informasi di sini cukup menarik dibahas karena tidak berwujud fisik dan keamanannya dapat bernilai sangat penting. Keamanan informasi dapat didefinisikan sebagai perlindungan dari dari akses yang tidak wewenang baik dalam bentuk pemanfaatan, perusakan atau perubahan terhadap data dan sistem informasi [8]. Saat ini peran keamanan informasi telah menjadi lebih penting karena telah banyak orang, bisnis dan lembaga pemerintah menyimpan data dalam bentuk digital dengan menggunakan berbagai jenis teknologi.

TABEL I
PENELITIAN-PENELITIAN TERKAIT

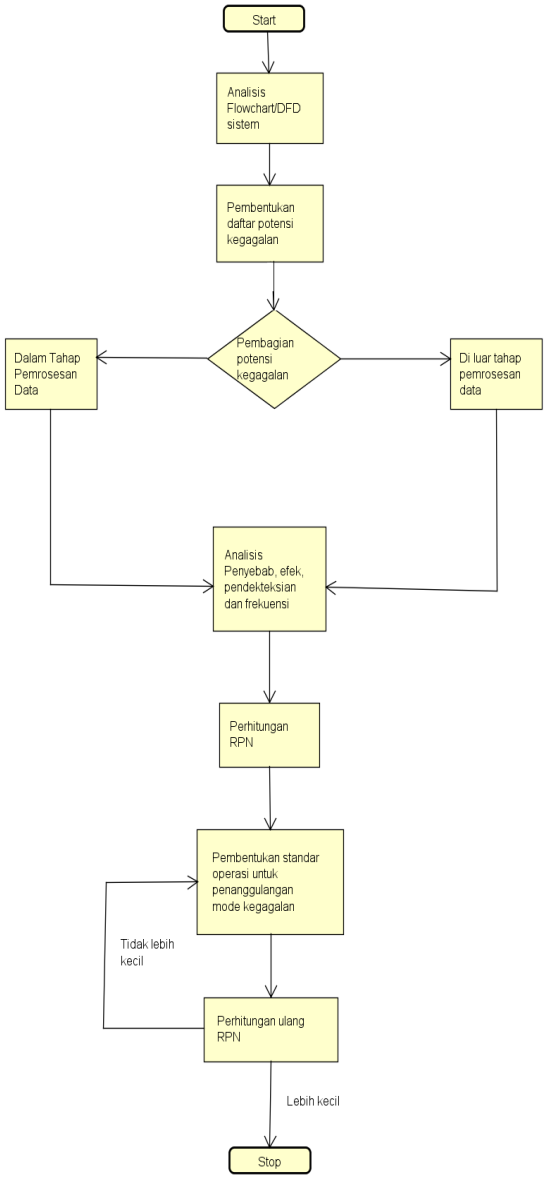
Peneliti	Objek	Metode	Hasil
Richma Yulinda, dkk [9]	Industri manufaktur	FMEA, FTA	Penggunaan metode FMEA untuk menentukan nilai (RPN) selanjutnya digunakan menentukan *potential cause* dengan *Fault Tree Analysis* (FTA).
Awni Itradat [10]	Sistem Informasi Pendidikan	ISO 27001	Menerapkan penilaian kerentanan dan penetrasi kemanankemudian disusun menjadi rencana pengendalian risiko.
Wahyu Oktri Widyarto, dkk [11]	Industri manufaktur	FMEA, six sixma	Penggunaan metode FMEA untuk menentukan nilai (RPN) selanjutnya digunakan metode Six sixma untuk perbaikan kualitas produk
Innike Desy, dkk [12]	Perbankan	FMEA	Daftar analisis risiko
Balqis Lembah dkk, [13]	Sistem Informasi	Octave	identifikasi risiko yang dapat terjadi

III. METODE PENELITIAN

A. Alur Penelitian

Alur penelitian ini menunjukkan langkah demi langkah yang dilalui saat proses penelitian. Alur penelitian dimulai dari analisis aliran data dan proses yang ada dengan meninjau diagram *flowchart* dan data *flow* diagram sistem informasi Organisasi XYZ. Dari diagram tersebut diambil proses-proses yang ada mulai dari data mentah menjadi informasi. Selanjutnya dari setiap proses yang ada dianalisis dengan bantuan tim ahli sistem informasi untuk menganalisis setiap daftar potensi kegagalan yang mungkin terjadi. Untuk memudahkan mendaftar semua kemungkinan potensi kegagalan pada sistem maka daftar potensi kegagalan tersebut dipilah menjadi dua kategori yakni kategori pertama berisi semua potensi kegagalan selama proses pengolahan data mentah menjadi informasi dan kategori kedua berisi semua potensi kegagalan di luar proses pengolahan.

Pada tahap berikutnya penulis melakukan analisis penyebab, deteksi, dampak dan frekuensi dari semua daftar potensi kegagalan. Kesemua deteksi, dampak dan frekuensi diubah ke dalam bentuk skala ordinal kemudian dilakukan perhitungan RPN (*Risk Priority Number*). Salah tahap paling penting dalam penelitian ini yang juga merupakan output utama adalah membuat prosedur penanggulangan mode kegagalan dari hasil analisis RPN beserta penyebab dan dampak kegagalan. Setelah prosedur ini dirancang dan diterapkan maka akan dilakukan perhitungan RPN ulang untuk melihat apakah risiko kegagalan sudah berkurang atau belum. Diharapkan dengan menetapkan standar prosedur baru mode kegagalan akan berkurang secara signifikan. Detail alur penelitian ini dapat dilihat pada Gbr. 2



Gbr. 2 Alur Penelitian

B. Objek Penelitian

Objek penelitian pada penelitian ini adalah sistem informasi portal organisasi XYZ. Luasnya wilayah perairan dan perkembangan teknologi saat ini mendorong munculnya sebuah metode pengamanan laut memerlukan harus melibatkan peralatan dan operasi multifungsi berbasis teknologi informasi. Pada sisi lain menimbang perlunya sistem informasi *monitoring* wilayah laut Indonesia untuk mendukung penegakan hukum di bidang kelautan NKRI.

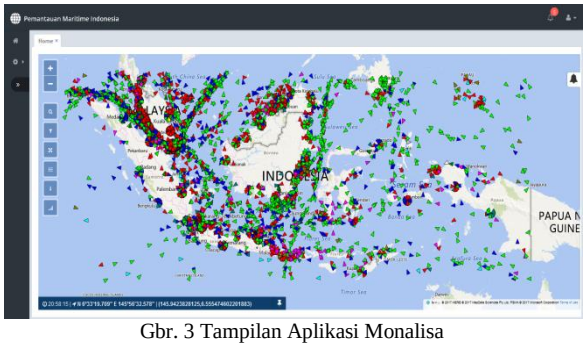
Bagaimana pun belum terintegrasinya peralatan dan teknologi informasi *monitoring* dan pengamanan di laut yang ada di organisasi XYZ menyebabkan sulit kontrol *monitoring* keamanan dan membuka celah kerawanan yang sulit terdeteksi. Melihat dari hasil tersebut dapat disimpulkan bahwa kontrol pengamanan sistem elektronik dan teknik informasi yang dimiliki oleh organisasi XYZ masih belum memadai dan membutuhkan peningkatan di berbagai

aspek terutama aspek keamanan. Salah satu upaya yang dilakukan adalah mengembangkan sistem baru yang lebih terintegrasi dan lebih aman. Hal sudah dilakukan organisasi XYZ sejak akhir tahun 2016 dengan membangun sistem informasi berupa portal organisasi XYZ yang terdiri dari 3 aplikasi utama yakni:

1. BIIS (*Integrated Information System*)
2. Monalisa (Monitoring & Analisa)
3. DashBoard (Pelaporan)

Aplikasi *dashboard* (Pelaporan Keamanan dan Keselamatan Laut) memiliki fitur berupa tampilan grafik dan diagram yang berfungsi sebagai bahan pelaporan kejadian yang terkait dengan berbagai jenis pelanggaran keamanan laut. Kejadian tersebut termasuk penyelundupan BBM, pencurian ikan, ilegal *mining*, kecelakaan, pembajakan, penyelundupan miras narkoba dan sebagainya. Aplikasi lebih ditujukan untuk pelaporan bagi eksekutif jajaran organisasi XYZ sehingga mereka mendapatkan rincian gambaran berbagai kejadian terkait keamanan dan keselamatan laut serta aplikasi berguna untuk mengambil keputusan strategis.

Aplikasi Monalisa (Pemantauan Maritim Indonesia) memiliki fitur tampilan berupa seluruh kapal/perahu laut yang terdeteksi oleh satelit (AIS) dan radar yang berada pada wilayah maritim negara kesatuan republik Indonesia. Aplikasi mendapatkan data yang diolah berdasarkan *Automatic Identification System* (AIS) merupakan sebuah sistem pelacakan otomatis yang digunakan pada kapal dengan pelayanan lalu lintas kapal untuk mengidentifikasi dan menemukan kapal dengan cara pertukaran data elektronik melalui kapal lain di dekatnya, BTS dan atau satelit. Informasi yang disediakan oleh peralatan AIS, seperti identifikasi yang unik, posisi, arah dan kecepatan.



Gbr. 3 Tampilan Aplikasi Monalisa

Aplikasi BIIS (*Integrated Information System*) digunakan untuk menampilkan kejadian dan informasi iklim/cuaca di wilayah maritim Indonesia. Kejadian yang ditampilkan mencakup tabrakan, pencurian, pembajakan, kecelakaan, penyelundupan, ilegal *fishing* dan sebagainya. Hasil dari kejadian ini akan dilaporkan secara berkala pada aplikasi *dashboard*. Pada aplikasi BIIS juga terdapat laporan cuaca, temperatur, arah angin yang diperbarui secara *real time*. Selain itu terdapat berbagai informasi demografi seperti informasi terkait demografi penduduk, ekonomi, wabah penyakit yang ditampilkan secara GIS (*Geographic Information Systems*).

C. Pengumpulan Data

Data yang digunakan pada penelitian ini adalah data primer yang diambil langsung dari hasil pengamatan terhadap objek yang diteliti. Pengumpulan data dilakukan selama 2 bulan, yaitu dari tanggal 6 Januari sampai dengan 6 Maret 2017. Pengambilan data dilakukan dengan berbagai metode di antaranya dengan metode pengamatan. Metode ini ditempuh dengan mengamati sistem informasi portal organisasi XYZ. Kemudian metode pengumpulan data. Metode ini dilaksanakan dengan mengumpulkan data dari *checksheet* hasil inspeksi harian. Lalu metode menganalisis dan mengklasifikasi data yang dijalani dengan wawancarai pihak terkait serta metode memperoleh data historis.

Dalam menyelesaikan penelitian ini, tentunya dibutuhkan data-data untuk diolah sesuai dengan kebutuhannya. Sebuah sistem informasi yang dalam hal ini merupakan objek penelitian mengambil input berupa data-data yang nantinya akan diolah menjadi Informasi. Berikut ini adalah data-data yang dibutuhkan dalam penelitian ini:

1. Diagram alir data (Data Flow Diagram)
2. Bagan Alir (FlowCharts)
3. Data penyebab kegagalan sistem
4. Data frekuensi kegagalan sistem
5. Data dampak dari kegagalan sistem
6. Data akses ke administrasi sistem

Ketika melakukan penelitian, tahap pengumpulan data merupakan salah satu tahap yang penting. Dalam melakukan proses pengumpulan data ini, setiap data yang dibutuhkan harus dapat didefinisikan dengan baik, sehingga proses pengambilan data pun tidak dilakukan dengan sia-sia dan data yang didapatkan memang benar-benar data yang dibutuhkan untuk menyelesaikan penelitian ini dengan baik. Adapun teknik pengumpulan data yang dilakukan dalam penelitian ini terdiri dari 4 macam, yaitu: studi literatur, wawancara dan tanya jawab, pengamatan langsung dan pengumpulan data historis

D. Pengolahan Data

Langkah berikutnya untuk analisis data adalah menetapkan satuan untuk variabel *occurrence*, *severity* dan *detection*. Secara umum karena metode FMEA lebih sering digunakan pada ranah teknik industri semua variabel tersebut diukur per satuan produksi namun di sini karena objek yang diteliti adalah sebuah sistem informasi maka satuan yang digunakan adalah setiap kali menyinkron data. Besaran variabel *occurrence*, *severity* dan *detection* adalah nilai skala ordinal dari 1 sampai 10. Berikut satuan masing-masing ukuran skala dalam bentuk tabel:

TABEL 2
SKALA PENILAIAN SEVERITY

Skala	Keterangan
1	*Negligible severity* (Pengaruh buruk yang dapat diabaikan). Kita tidak perlu memikirkan bahwa akibat ini akan berdampak pada kualitas produk. User mungkin tidak akan memperhatikan kecacatan ini.
2,3	*Mild severity* (Pengaruh buruk yang ringan). Akibat yang ditimbulkan akan bersifat ringan, user tidak akan merasakan penurunan kualitas.
4,5,6	*Moderate severity* (Pengaruh buruk yang sedang). User akan merasakan penurunan kualitas, namun masih dalam batas toleransi.
7.8	*High severity* (Pengaruh buruk yang tinggi). User akan merasakan penurunan kualitas yang berada diluar batas toleransi.
9,10	*Potential severity* (Pengaruh buruk yang sangat tinggi). Akibat yang ditimbulkan sangat berpengaruh terhadap kualitas lain, User tidak akan menerimanya.

TABEL 3
SKALA PENILAIAN OCCURRENCE

Degree	Frekuensi	Skala
Remote	< 0,01 per 1000 fetch	1
Low	0,1 per 1000 fetch 0,5 per 1000 fetch	2 3
Moderate	1 per 1000 fetch 2 per 1000 fetch 5 per 1000 fetch	4 5 6
High	10 per 1000 fetch 20 per 1000 fetch	7 8
Very High	50 per 1000 fetch 100 per 1000 fetch >	9 10

TABEL 4
SKALA PENILAIAN DETECTION

1	Metode deteksi dan pencegahan sangat efektif. Hampir tidak ada kesempatan penyebab gagal mungkin muncul.	< 0,01 per 1000 fetch
2 3	Kemungkinan penyebab terjadi sangat rendah.	0,1 per 1000 fetch 0,5 per 1000 fetch
4 5 6	Kemungkinan penyebab terjadi bersifat moderat. Metode pencegahan kadang memungkinkan penyebab itu terjadi.	1 per 1000 fetch 2 per 1000 fetch 5 per 1000 fetch
7 8	Kemungkinan penyebab terjadi masih tinggi. Metode pencegahan kurang efektif. Penyebab masih berulang kembali.	10 per 1000 fetch 20 per 1000 fetch
9 10	Kemungkinan penyebab terjadi masih sangat tinggi. Metode deteksi dan pencegahan sangat tidak efektif. Penyebab masih berulang kembali.	50 per 1000 fetch 100 per 1000 fetch >

Pada penelitian ini diagram Pareto digunakan untuk mengidentifikasi permasalahan yang menjadi prioritas utama. Karena dalam penelitian ini melibat 3 variabel yakni *severity, occorrence* dan *detection* maka akan dibuat 3 diagram Pareto berdasarkan masing-masing variabel. Dari masing-masing variabel tersebut akan dipilih mode kegagalan sebagai prioritas utama menggunakan prinsip Pareto menyatakan bahwa sekitar 80% dari efek berasal dari 20% dari penyebab [14].

Setelah memilih prioritas penanganan masalah dengan menggunakan prinsip Pareto, maka langkah selanjutnya yang dilakukan adalah menentukan penyebab-penyebab mode kegagalan. Identifikasi ini dilakukan dengan menggunakan *Fishbone* Diagram. Diagram ini dibuat dengan melakukan *brainstorming* dengan para ahli teknologi informasi dengan developer. Hasil *Fishbone* diagram kemudian digunakan untuk membuat FMEA untuk menganalisa penyebab-penyebab dari masing-masing mode kegagalan yang terpilih

IV. HASIL DAN PEMBAHASAN

A. *Hasil Analisis Mode Kegagalan*

Berdasarkan hasil pengamatan yang telah dilakukan selama proses pengumpulan data, dikumpulkan berbagai hasil mode kegagalan yang terjadi pada sistem informasi organisasi XYZ. Selain penganan langsung terhadap objek yang diteliti, dalam tahap ini peneliti juga melakukan studi pustaka merujuk pada literatur-literatur manajemen risiko dan keamanan sistem informasi untuk menggali lebih banyak daftar potensi kegagalan yang mungkin terjadi. Berikut ini merupakan hasil analisis daftar potensi kegagalan:

1. Sistem tidak dapat diakses

Terdapat beberapa hal yang menyebabkan sistem informasi berbasis web tidak bisa diakses. Untuk mengetahui penyebab masalahnya dapat melihat pesan-pesan eror seperti "404 Not Found", "403 Forbidden", "500 Internal Server Error" dan lain sebagainya muncul di layar *browser*. Kesalahan penulisan pada file .htacces juga dapat menyebabkan *website* menjadi tidak bisa diakses dengan memunculkan eror 500 Internal Server Error.

2. Sistem tidak tersedia

Sistem tidak tersedia (*offline*) dapat disebabkan oleh beberapa hal seperti koneksi internet, Power *failure*, *server maintenance* dan sebagainya. Dalam perjanjian tingkat layanan, umumnya menyebutkan nilai persentase (per bulan atau per tahun) yang dihitung dengan membagi jumlah semua *downtime* dengan total waktu dari rentang waktu referensi (misalnya satu bulan). 0% *downtime* berarti bahwa *server* yang tersedia sepanjang waktu. Untuk *server* Internet *downtime* di atas 1% per tahun dapat dianggap sebagai tidak dapat diterima karena ini berarti *downtime* lebih dari 3 hari per tahun.

3. *Hardware failure*

Hardware failure merupakan kerusakan dalam sirkuit elektronik atau komponen-komponen fisik dari sistem komputer. Pemulihan dari kegagalan perangkat keras membutuhkan perbaikan atau penggantian pada bagaikan yang bermasalah. Pada sistem informasi Organisasi XYZ *hardware failure* kemungkinan terjadi pada *server* tempat menampung seluruh file dan database sistem.

4. Software Failure

Merupakan bentuk kegagalan pada sistem terjadi ketika layanan yang diberikan oleh sistem tidak lagi sesuai dengan spesifikasi. Kegagalan ini disebabkan oleh adanya *bug* atau eror pada kode program sehingga mengganggu fungsi sistem secara keseluruhan. *Software failure* dapat diminimalkan dengan pengujian perangkat lunak dan jaminan kualitas perangkat lunak.

5. Network Failure

Merupakan bentuk kegagalan dari jaringan karena kerusakan atau bencana alam atau yang disebabkan manusia. Beberapa bentuk dari *Networks failure* yang umum terjadi adalah *download time* dan *slow connection*. Efek dari *network failure* dapat menyebabkan gangguan pada fungsi sistem sampai sistem tidak dapat diakses.

6. Power Failure

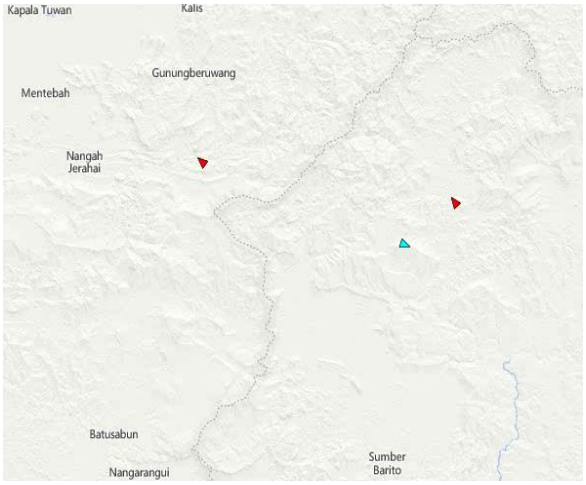
Power falure merupakan bentuk kegagalan yang disebabkan sumber tenaga listrik yang padam dan dapat terjadi pada sisi *server* maupun *client*. *Power failure* dapat menyebabkan kelumpuhan total pada sistem.

7. Informasi cuaca tidak akurat

Salah fitur yang ditampilkan pada sistem informasi organisasi XYZ adalah keberadaan informasi cuaca seperti perkiraan temperatur, arah angin dan hujan. Keberadaan informasi ini juga memungkinkan mode kegagalan di mana informasi yang ditampilkan tidak akurat atau tidak sesuai dengan keadaan sebenarnya.

8. Lokasi kapal tidak akurat / delay

Sistem informasi organisasi XYZ menggunakan data satelit AIS untuk melacak keberadaan kapal di wilayah perairan Indonesia. Bagaimana pun berdasarkan pengamatan langsung pada sistem masih berbagai kesalahan penunjukan lokasi kapal seperti ada beberapa kapal yang ditemui berada di daratan. Berdasarkan pengamatan langsung terdapat beberapa kapal yang memiliki jeda waktu hingga beberapa hari sejak lokasi terakhir. Seharusnya *delay* lokasi kapal yang dapat ditoleriri maksimal selama 6 jam.



Gbr.4 Lokasi Kapal yang berada di daratan

9. Peta/Kapal tidak tampil

Baik peta maupun lokasi kapal menggunakan aplikasi dari pihak ketiga untuk dapat tampil dalam sistem informasi organisasi XYZ. Menggunakan aplikasi pihak ketiga dapat menjadi salah satu penghalang untuk semua tampil bersamaan seperti ketika terjadi *crash* atau eror pada salah satu pihak tersebut yang akhirnya dapat menyebabkan peta atau kapal tidak tampil

10. Waktu *loading* terlalu lama

Lama waktu *loading* sebuah *website* dapat dipengaruhi beberapa hal di antaranya: Performa dari *hosting server*, *internet service provider* dan juga konten yang dimuat pada *website*. Sistem informasi organisasi XYZ sudah memiliki *hosting server* IIX di lokasi pulau Bitung yang memiliki performa cukup baik. Bagaimana pun waktu *loading* yang lama masih mungkin terjadi dari kecepatan akses internet pengguna dan aplikasi penyedia konten pihak ketiga seperti data satelit dan peta.

11. Pelaporan (*report*) tidak tampil

Salah satu komponen dalam sistem informasi organisasi XYZ adalah pelaporan keamanan dan keselamatan laut yang ditujukan untuk kepentingan manajerial. Berdasarkan peninjauan langsung pada sistem, bagian pelaporan ini masih menggunakan aplikasi dari pihak ketiga yang berpotensi cukup rawan baik dalam hal privasi data laporan dan ketersediaan laporan.

12. Informasi *past tracking* kapal tidak tampil

Salah fitur yang terdapat pada sistem informasi organisasi XYZ adalah informasi pas Trading kapal. Keberadaan atau jalur sebuah kapal sampai dengan seminggu lalu. Bagaimana pun berdasarkan pengamatan langsung informasi *past tracking* ini sering kali mendapat kendala sehingga tidak tampil sama sekali.

13. Notifikasi tidak muncul

Notifikasi pada sistem informasi organisasi XYZ digunakan untuk memberikan berbagai macam peringatan seperi notifikasi keadaan kapal yang mencurigakan, kapal yang sedang dalam ancaman

bahaya termasuk notifikasi internal antar *user* dalam sistem. Sayangnya fitur notifikasi ini masih dalam tahapan pengembangan sehingga belum dapat berfungsi secara normal.

B. *Hasil Pehitungan RPN*

Setelah daftar potensi kegagalan dibentuk, langkah berikutnya adalah mengumpulkan data frekuensi kejadian (*occurence*) dari masing-masing daftar potensi kegagalan berdasarkan hasil pengamatan langsung. Pada saat bersamaan juga dilakukan *brainstorming* untuk menentukan tingkat keparahan (*severity*) serta mengidentifikasi penyebab dan pencegahan dini dari masing-masing mode kegagalan. Nantinya baik tingkat keparahan maupun frekuensi kejadian akan dijadikan sebagai tolak ukur untuk menentukan prioritas. Nilai RPN merupakan hasil kali dari variabel *severity*, *occcurrance* dan *detection*. Hasil dari perhitungan RPN dapat dilihat pada tabel 5.

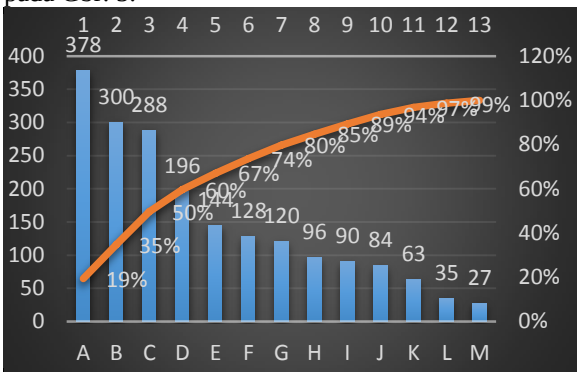
TABEL 5
Hasil perhitungan RPN

Mode Kegagalan	Occ.	Sev.	Det.	RPN
Sistem tidak dapat diakses	1	9	7	63
Sistem tidak tersedia	5	10	6	300
Hardware Failure	2	9	7	128
Software Failure	2	8	6	96
Network Failure	6	8	6	288
Power Failure	1	9	3	27
Informasi cuaca tidak akurat	7	4	7	196
Lokasi kapal tidak akurat / *delay*	9	6	7	378
Kapal/peta tidak tampil	3	8	6	144
Waktu *loading* terlalu lama	6	4	5	120
Pelaporan tidak tampil	1	5	7	35
Informasi *past tracking* kapal tidak tampil	3	5	6	90
Notifikasi tidak muncul	7	4	3	84

Berdasarkan hasil pengamatan tingkat frekuensi kejadian yang paling tinggi adalah *delay* atau jeda waktu tampilan dari lokasi kapal. Hal ini sulit untuk diantisipasi sebelumnya karena informasi yang ditampilkan berdasarkan data satelit yang disewa oleh organisasi XYZ. Informasi lokasi ini murni dari pihak ketiga tanpa bisa diolah lebih lanjut. Menurut draf sewa satelit, informasi lokasi kapal dapat ditampilkan dengan *delay* (jeda waktu) paling lambat selama 6 jam akan tetapi berdasarkan pengamatan langsung terdapat beberapa kapal yang memiliki jeda waktu lebih dari 6 jam sejak lokasi terakhir.

C. *Hasil Analisis Prioritas Kegagalan*

Untuk melakukan analisis prioritas penulis menggunakan diagram Pareto yang dapat menentukan prioritas permasalahan yang akan diselesaikan. Permasalahan yang paling banyak dan sering terjadi adalah prioritas utama untuk melakukan tindakan. Dari masing-masing variabel tersebut akan dipilih mode kegagalan sebagai prioritas utama menggunakan prinsip Pareto menyatakan bahwa sekitar 80% dari efek berasal dari 20% dari penyebab. Diagram pareto mode kegagalan disajikan pada Gbr. 5.



Gbr. 5 Diagram pareto mode kegagalan

Hasil dari diagram Pareto menunjukkan terdapat tiga prioritas mode kegagalan yakni:

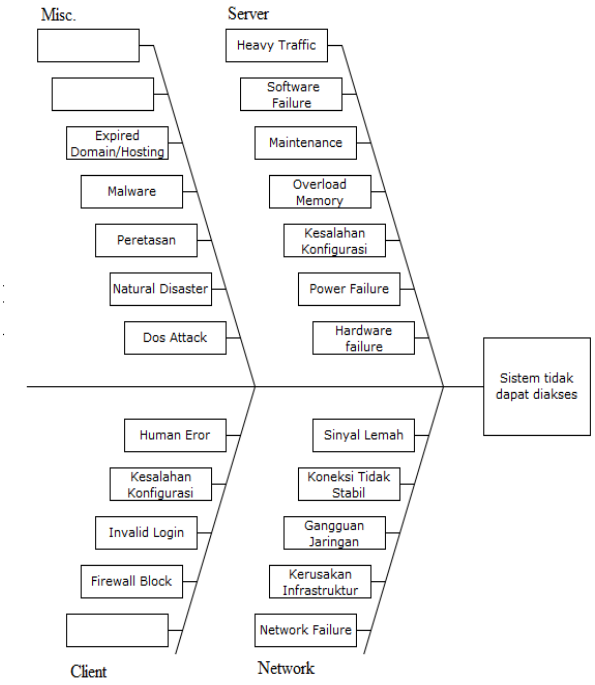
1. Tampilan informasi kapal terlambat
2. Sistem tidak tersedia
3. Lokasi kapal tidak akurat

Ketiga mode kegagalan tersebut mempunyai dampak yang cukup signifikan terhadap fungsional sistem secara keseluruhan. Bagaimanapun bentuk tidak tersedianya sistem tidak hanya berimbas pada tidak berfungsinya sistem secara keseluruhan namun juga dapat menimbulkan efek psikologis. Prioritas pertama ada pada masalah tampilan informasi atau lokasi kapal yang terlambat. Selama masa pengumpulan data mode kegagalan ini merupakan bentuk mode kegagalan yang paling sering terjadi.

D. *HASIL ANALISIS PENYEBAB KEGAGALAN*

Langkah berikutnya setelah membuat diagram Pareto adalah membuat diagram Ishikawa atau dikenal juga sebagai diagram *fishbone* (tulang ikan). Diagram ini dibuat dengan melakukan studi pustaka dan *brainstorming* dengan para developer. Salah satu tujuan yang ingin dicapai dari penelitian ini yaitu mengidentifikasi potensi gangguan dan memberikan rekomendasi kontrol yang perlu diterapkan, maka untuk mencapai hal tersebut mutlak diperlukan analisis penyebab kegagalan sehingga dapat memberikan solusi yang tepat untuk mengurangi potensi kegagalan. Diharapkan dengan hasil penyebab yang telah ditemukan dapat mempermudah untuk menyelidiki lebih lanjut rekomendasi tindakan

untuk penanganan mode kegagalan yang berpotensi terjadi. Berikut salah satu contoh dari diagram *fishbone* untuk mode kegagalan sistem tidak dapat diakses.



Gbr. 6 Fishbone diagram sistem tidak dapat diakses

E. *Hasil Perhitungan Ulang RPN*

Sebelum dilakukan perhitungan ulang RPN, terdapat berbagai perubahan yang terjadi pada sistem informasi organisasi XYZ. Perubahan-perubahan merupakan wujud dari hasil rekomendasi daftar aksi yang telah dirumuskan sebelumnya. Beberapa perubahan yang ada di sini diselaraskan dengan kerangka kerja ISO 27001 dan ditetapkan dengan tahapan dengan rekonsiliasi para developer sistem untuk hasil yang lebih optimal. Diharapkan setelah sistem diperbarui berdampak pada meminimalkan nilai RPN serta mengurangi tingkat kerawanan sistem secara keseluruhan. Adapun perubahan-perubahan yang dimaksud adalah:

1. Saat ini sistem informasi organisasi XYZ telah dilengkapi *firewall* yang membatasi hak akses berdasarkan IP *Address* sehingga akses oleh pengguna yang tidak berwenang dapat dicegah.
2. *Login form* saat telah menggunakan enkripsi AES 256 bit
3. Informasi sensitif seperti *user*, *password* sekarang dikirim melalui SSL (*Secure Socket Layer*), hal ini berguna untuk mencegah penyadapan data
4. Terdapat manajemen *user* seperti untuk *recoverypassword*, hapus *user* dan tambah *user*.
5. Terdapat produser kriteria penggunaan *password* minimal yang dapat dipakai
6. Peta yang digunakan beralih ke *OpenStreetMap*, peta dunia berbasis *open source* yang lebih ringan digunakan sehingga mempercepat waktu *loading*.
7. Penghapusan fitur-fitur yang dianggap tidak terlalu penting, seperti *user messaging*. Dengan meminimalkan fitur yang tidak penting juga diharapkan dapat meminimalkan celah keamanan.
8. *Hosting server* yang ditempati kini telah dilengkapi dengan fasilitas anti virus dan anti *spamming*. *Backup* data dilakukan secara otomatis oleh *server* secara periodik.
9. Algoritma pencarian kapal telah diperbarui sehingga dapat menemukan posisi kapal secara *real time* lebih cepat dan akurat.

Di samping perubahan-perubahan yang telah dilakukan seperti yang disebutkan pada poin-poin di atas, terdapat juga berbagai perubahan yang saat ini masih sedang dalam tahapan pengerjaan. Hal ini termasuk pengerjaan sistem log pencatatan aktivitas-aktivitas penting, pemisahan antara *modul control dan view* dan sistem notifikasi kerawanan. Karena keterbatasan waktu pengerjaannya masih tertunda saat penulisan ini dikerjakan.

Setelah berbagai modifikasi sistem dilakukan, penulis kembali melakukan perhitungan ulang RPN. Perhitungan ini dilakukan untuk konfirmasi hasil modifikasi sistem agar dapat terukur secara objektif sejauh mana dampaknya terhadap penurunan kegagalan sistem. Perhitungan ini masih tetap menggunakan teknik yang sama seperti perhitungan RPN sebelumnya. Tabel 6 menunjukkan hasil perhitungan ulang RPN.

TABEL 6
Hasil Perhitungan Ulang RPN

Mode Kegagalan	Occ.	Sev.	Det.	RPN	RPN (*before*)
Sistem tidak dapat diakses	1	9	7	63	63
Sistem tidak tersedia	2	0	6	120	300
Hardware Failure	1	9	7	63	128
Software Failure	1	8	6	48	96
Network Failure	3	8	6	144	288
Power Failure	1	9	3	27	27
Informasi cuaca tidak akurat	4	4	7	112	196
Lokasi kapal tidak akurat / *delay*	5	6	7	210	378
Kapal/peta tidak tampil	3	8	6	144	144
Waktu *loading* terlalu lama	6	5	6	300	120
Pelaporan tidak tampil	1	5	7	35	35
Informasi *past tracking* kapal tidak tampil	3	5	6	90	90
Notifikasi tidak muncul	1	4	3	12	84
Total				1368	1949

Hasil perhitungan ulang RPN menunjukkan terjadi beberapa perubahan yang cukup signifikan. Beberapa mode kegagalan menunjukkan kecenderungan nilai RPN yang berkurang semakin kecil seperti sistem tidak tersedia, *network*, *hardware* dan *softwarefailure*. Beberapa di antaranya masih tetap seperti nilai sebelumnya dan terdapat satu nilai RPN yang cenderung meningkat yakni waktu *loading* yang terlalu lama. Waktu yang yang terlalu lama ini menurut hasil analisis diakibatkan oleh peralihan peta yang digunakan. Jika sebelumnya menggunakan peta dari Microsoft Bing kini menggunakan peta *OpenStreet Map*, peta dunia berbasis *open source.* Dampak dari peralihan ini justru memberikan imbas negatif pada waktu *loading* sistem. Adapun beberapa nilai RPN yang berhasil diturunkan, menurut hasil analisis ini adalah hasil nyata dari upaya yang telah diwujudkan seperti pada poin-poin perubahan sistem yang telah dijabarkan sebelumnya.

Bagaimana pun hasil perubahan RPN yang disampaikan pada penulisan ini masih dinilai kurang optimal. Hal ini dikarenakan perhitungan RPN dilakukan saat beberapa perubahan masih dalam proses pengerjaan dan terdapat berbagai kendala untuk mewujudkan perubahan seperti sistem log untuk pencatatan aktivitas petis, pemisahan komponen *logic* dan *view*, *refactoring* kode program, optimalisasi notifikasi sistem. Karena keterbatasan waktu pengerjaan tugas-tugas tersebut masih terhambat.

KESIMPULAN

Penelitian ini telah berhasil membuktikan secara empiris melalui serangkaian hasil percobaan menunjukkan bahwa metode FMEA merupakan salah upaya nyata yang dapat dilakukan untuk mengetahui keadaan tingkat kerawanan dari sistem informasi, mengidentifikasi penyebab potensial dari berbagai bentuk kegagalan serta mengurutkan prioritas kegagalan berdasarkan nilai RPN.

Penelitian ini telah berhasil melalukan audit keamanan informasi pada sistem informasi organisasi XYZ. Berdasarkan hasil analisis terdapat berbagai celah keamanan yang telah dijabarkan dalam penelitian ini. Di samping itu hasil penelitian ini menunjukkan tingkat kerawanan yang tinggi dengan nilai *Risk priority number* (RPN) dalam rentang 30-40%. Berbagai tindakan rekomendasi berdasarkan standar ISO 27001 telah dilakukan untuk mengurangi tingkat kerawanan dan telah menunjukkan hasil positif dengan penurunan nilai RPN sebesar 30%. Dengan demikian tujuan dari penelitian ini telah tercapai dengan dijabarkannya daftar rekomendasi tindakan dari data yang telah olah dan telah diuji. Penelitian ini telah memberikan kontribusi teori terhadap pengukuran skala pada variabel *severity* dan *occurrance* pada pengukuran RPN sehingga dapat diterapkan pada objek sistem informasi.

Terlepas dari berbagai keunggulan metode FMEA, terdapat sisi negatif dari penggunaan metode FMEA adalah sifatnya yang reaktif terhadap risiko kegagalan ketimbang pencegahan terhadap risiko. Hal ini dikarenakan FMEA menganalisis risiko dari data sejarah kejadian berbagai mode kegagalan kemudian melakukan tindakan reaktif untuk penanggulangan atau pencegahan di kemudian hari. Pada penerapannya di bidang sistem informasi sekali terjadi mode kegagalan seperti peretasan dapat berdampak signifikan baik bagi sistem itu sendiri maupun perusahaan yang menjalankannya. Untuk melengkapi pengelolaan manajemen risiko yang lebih baik maka diperlukan metode tambahan yang lebih bersifat preventif terhadap risiko kegagalan..

Untuk pengembangan sistem informasi yang lebih lanjut, dari hasil penelitian ini penulis juga menyarankan untuk menyelesaikan pengerjaan sistem *log* pencatatan aktivitas-aktivitas penting, pemisahan antara komponen *control* dan *view* dan sistem notifikasi kerawanan. Selain itu diperlukan juga *refactoring* kode program untuk mengatasi masalah terkait waktu *loading* sistem. Hal-hal tersebut merupakan bagian dari prioritas keamanan dan diharapkan dapat mengurangi kerawanan secara signifikan.

REFERENSI

[1] Anom, "organisasi XYZ Desktop Asessment Report," KAMI, Jakarta, 2014.

[2] R. Budiarto, "Penerapan Metode FMEA Untuk Keamanan Sistem Informasi (Studi Kasus Website POLRI)," dalam *Seminar Nasional IPTEK Terapan*, Tegal, 2017.

[3] G. Joshi dan H. Joshi, "FMEA and Alternatives versus Enhanced Risk Assessment Mechanism," *International Journal of Computer Applications*, vol. 93, no. 14, p. 2, 2014.

[4] N. B. Puspitasari dan A. Martanto, "Penggunaan FMEA dalam Mengidentifikasi Resiko Kegagalan Proses Produksi Sarung Atm," *JaTI Undip*, vol. IX, no. 2, pp. 93-95, 2014.

[5] D. F. Mayangsari, H. Adianto Dan Y. Yuniati, "Usulan Pengendalian Kualitas Produk Isolator dengan Metode Failure Mode And Effect Analysis (FMEA) dan Fault Tree Analysis (FTA)," *Jurnal Online Institut Teknologi Nasional*, vol. III, no. 2, pp. 81-91, 2015.

[6] R. Y. Hanif, H. S. Rukmi Dan S. Susanty, "Perbaikan Kualitas Produk Keraton Luxury Di Pt. X dengan Menggunakan Metode (FMEA) dan (FTA)," *Jurnal Online Institut Teknologi Nasional*, vol. III, no. 3, pp. 137-147, 2015.

[7] Anisa, "Evaluasi Dan Analisis Waste Pada Proses Produksi Kemasan dengan Menggunakan Methode FMEA," *Jurnal Fakultas Teknik Industri Universitas Indonesia*, pp. 50-62, 2010.

[8] T. Neubauer dan M. Pehn, "Workshop-based Security Safeguard Selection," *International Journal on Advances in Security*, vol. III, no. 3, pp. 123-134, 2010.

[9] R. Hanif dan H. S. Rukmi, "Perbaikan Kualitas Produk Keraton Luxury di Pt. X dengan Menggunakan Metode Failure Mode And Effect Analysis dan Fault Tree Analysis," *Jurnal Online Institut Teknologi Nasional*, vol. III, no. 3, pp. 137-147, 2015.

[10] A. Itradat, S. Sultan, M. Al-Junaidi dan R. Qaffaf, "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study," *Jordan Journal of Mechanical and Industrial Engineering*, vol. VII, no. 2, pp. 102-118, 2014.

[11] W. O. Widyarto, G. A. Dwiputra dan Y. Kristiantoro, "Penerapan Konsep Fmea dalam Pengendalian Kualitas Produk dengan Menggunakan Metode Six Sigma," *Jurnal Rekayasa dan Teknik Inovasi Industri*, vol. III, no. 1, pp. 13-23, 2015.

[12] I. Desy, B. C. Hidayanto dan H. Maria Astuti, "Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis di Divisi TI Pt. Bank Xyz Surabaya," dalam *Seminar Nasional Sistem Informasi Indonesia*, Surabaya, 2014.

[13] B. L. Mahersmi, F. A. Muqtadiroh dan B. C. Hidayanto, "Analisis Risiko Keamanan Informasi dengan Menggunakan Metode Octave dan Kontrol Iso 27001 Pada Dishubkominfo Kabupaten Tulungagung," dalam *Seminar Nasional Sistem Informasi Indonesia*, Surabaya, 2016.

[14] K. Ankunda, "The Application Of The Pareto Principle In Software Engineering," pp. 1-12, 2011.