Penerapan Metode FMEA Untuk Keamanan Sistem Informasi (Studi Kasus Website POLRI)

Raden Budiarto

Jurusan Sistem Informasi STMIK Jakarta STI&K
Jl Radio Dalam Jakarta Selatan
E-mail : raden@jak-stik.ac.id

Abstrak

Penelitian ini menjabarkan pemecahan persoalan keamanan data dan jaringan serta manajemen risiko dengan menggunakan metode FMEA. Sekalipun sudah populer di bidang teknik industri, metode FMEA belum pernah dilaporkan penelitiannya terhadap objek sistem informasi. Hal ini menarik untuk dieksplorasi lebih lanjut untuk meneliti menelusuri lebih jauh pemanfaatan metode FMEA pada keamanan data dan jaringan. Sebagai objek penelitian dilakukan pada website Polri yang selama ini dilaporkan rawan terjadi peretasan. Variabel yang diukur pada penelitian ini adalah occurence (frekuensi kejadian), severity (dampak) dan detection (deteksi atau pencegahan) dari masing-masing mode kegagalan. Data penelitian diambil sebagian besar berdasarkan dari hasil pengamatan langsung. Hasil pengolahan data menunjukkan adanya tingkat kerawanan yang tinggi. Selama periode pengumpulan data setidaknya terdapat 5 celah keamanan yang berpotensi menimbulkan setidaknya 7 potensi kegagalan sistem informasi. Fokus prioritas keamanan tertinggi ada pada ketersediaan sistem dan konsistensi tampilan sistem dengan nilai risk priority number 576 dan 400. Beberapa saran keamanan untuk juga telah dijabarkan pada penelitian ini..

Kata Kunci : Keamanan data, keamanan jaringan, manajemen risiko, FMEA, keamanan sistem informasi, kegagalan sistem

Pendahuluan

Kebutuhan akan teknologi informasi (TI) dewasa ini memiliki peningkatan peminatan yang semakin tinggi. Hal tersebut dapat dilihat dari pemanfaatan TI yang digunakan untuk menjalankan aktivitas-aktivitas penting. Tetapi demi tercapainya hal tersebut perlu ditunjang dengan adanya pengelolaan TI yang memadai supaya keberadaan infrastruktur TI mampu menyokong kesuksesan perusahaan atau organisasi dalam mencapai tujuannya Tentunya segala bentuk pemanfaatan dan pengolahan TI ini tidak bisa terlepas dari ancaman terhadap bentuk integritas data dan keamanan jaringan.

Segala bentuk organisasi, baik profit maupun non-profit, baik pemerintah maupun swasta, organisasi besar ataupun kecil, pasti akan menghadapi segala bentuk permasalahan internal dan eksternal dalam usaha untuk mencapai tujuan serta visi dan misi organisasi. Adapun bentuk-bentuk permasalahan tersebut dapat menimbulkan suatu ketidakpastian yang dapat mempengaruhi tujuan organisasi tersebut. Ketidakpastian tersebut dikenal dengan istilah risiko. David Vose mengatakan bahwa risiko merupakan efek negatif dari kemungkinan terjadinya suatu kejadian yang tidak terprediksi terhadap pencapaian suatu tujuan organisasi [1]. Untuk meminimalkan efek dari risiko tersebut dapat diterapkan sebuah manajemen risiko. Menurut Emmet Vaughan dan Therese Vaughan, manajemen risiko adalah pendekatan secara ilmiah yang bertujuan untuk mengatasi segala risiko dengan mengantisipasi kerugian-kerugian yang terjadi dan mengimplementasikan prosedur yang mampu untuk meminimalkan terjadinya kerugian [2].

Terdapat berbagai macam metode dan alat bantu untuk analisis manajemen risiko salah satu yang cukup populer digunakan adalah FMEA (Failure Mode & Effect Analysis). FMEA merupakan suatu metode yang terstruktur yang dapat digunakan untuk mengidentifikasi, memprioritaskan mode kegagalan (fail-

ure mode) kemudian mencegahnya sebanyak mungkin. FMEA dapat digunakan untuk menelusuri sumber-sumber yang penyebab dari suatu kegagalan dan masalah kualitas [3]. Bentuk dari mode kegagalan yang dimaksud di sini adalah segala sesuatu yang termasuk pada kategori kecacatan, seperti cacat pada proses dalam desain, kondisi di luar batas persyaratan spesifikasi yang telah ditetapkan, atau segala hal yang dapat menyebabkan produk yang dihasilkan tidak berfungsi atau berfungsi namun tidak tepat.

Penelitian ini berusaha untuk mengeksplorasi penggunaan metode FMEA pada objek sistem informasi. Pemilihan objek sistem informasi pada penelitian ini dirasakan cukup menarik karena masalah keamanan dan manajemen risiko pada sistem informasi sering kali tidak diprioritaskan. Masalah yang sering kali dijumpai adalah kesulitan untuk mengajak pemilik atau manajer sistem informasi melakukan investasi pada bidang keamanan. Majalah Information week [4] pada tahun 1997 mengumumkan sebuah hasil survei terhadap 1271 manajer sistem informasi di Amerika Serikat. Berdasarkan hasil survei tersebut hanya terdapat 22% yang memberikan opini bahwa masalah keamanan sistem informasi merupakan masalah yang sangat vital. Sebagian besar dari mereka cenderung lebih mengutamakan mengurangi biaya dan meningkatkan persaingan ketimbang masalah pada sektor keamanan, meskipun sebenarnya biaya dari perbaikan sistem informasi setelah diretas dapat menghabiskan biaya yang jauh lebih banyak. Meskipun masalah keamanan sering kali dilihat sebagai sesuatu yang tidak dapat langsung diukur dengan mata uang (intangible), namun masalah celah keamanan sebuah sistem informasi sebetulnya dapat diukur secara real (tangible) misalkan kerugian akibat dari sebuah sistem informasi yang offline dan tidak bekerja selama beberapa jam.

Alasan utama mengapa memilih untuk menggunakan FMEA pada analisis manajemen risiko di antaranya FMEA dapat sangat berguna untuk mengidentifikasi kegagalan. FMEA digunakan untuk menangkap potensi kegagalan, risiko & dampak dan memprioritaskan mereka dengan nomor prioritas disebut risk priority number (RPN) yang berkisar antara 1 sampai 1000. RPN diperoleh dengan mengalikan Severity, Occurrence & Detection. Masing-masing dari nilai tersebut diidentifikasi pada skala 1 sampai 10 sehingga nilai maksimal RPN hingga 1000. Nilai RPN ini mudah dan realistis [5].

Objek penelitian dipilih website Polri karena website ini termasuk rentan terhadap peretasan. Tugas utama polisi yang menertibkan masyarakat sangat berpotensi mengundang stigma negatif di masyarakat dan menjadikan website Polri sebagai sasaran peretasan. Permasalahan yang pernah ada di pada website resmi POLRI saat ini berkaitan dengan celah kerawanan keamanan informasi. Beberapa kejadian yang pernah tercatat di antaranya website tidak dapat diakses, akses data oleh yang tidak berwenang dan deface (perubahan tampilan) pada website. Jika permasalahan ini tidak dapat diperbaiki secara berkelanjutan, alhasil akan memberikan dampak ataupun risiko kepada keberlangsungan sistem ini juga citra polisi di masyarakat. Berbagai upaya telah dilakukan pihak POLRI untuk melibatkan anggotanya berpartisipasi demi keamanan website. Seperti mengadakan pelatihan workshop komputer untuk anggota polisi yang ditugaskan untuk mengelola website namun hal ini dianggap masih belum dapat memenuhi target keamanan website secara keseluruhan.

Tujuan yang ingin dicapai dari penelitian ini yaitu untuk mengeksplorasi penggunaan metode FMEA pada sistem informasi serta mengidentifikasi potensi gangguan dan permasalahan yang ada pada sistem informasi website Polri. Output dari penelitian ini diharapkan dapat memberikan rekomendasi kontrol yang perlu diterapkan untuk manajemen risiko keamanan informasi, kebijakan keamanan dan standar operasional Prosedurnya. Agar pembahasan pada penelitian ini tidak terlalu luas, maka penulis akan membatasi pembahasan penelitian yakni evaluasi terhadap analisis manajemen risiko keamanan informasi dilakukan pada website Polri (www.polri.go.id) dengan metode analisis menggunakan FMEA.

Tinjauan Pustaka

FMEA merupakan metode yang sangat masuk akal dan efektif jika dilaksanakan dengan teliti. Lebih lanjut menurut Gunjan & Himanshu Joshi [6] keuntungan menggunakan FMEA antara lain:

1. Mengurangi kemungkinan kegagalan

serupa di masa depan

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. Selain itu, peringkat berdasarkan *severity*, *occurrence & detectio*n 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 3 bukan berarti 3 kali lebih buruk dari peringkat 1. Kelemahan dari penggunaan FMEA adalah sifatnya yang cenderung reaktif dan beradaptasi dari kegagalan ketimbang mencegahnya terlebih dahulu.

Jika melihat ke belakang sejak awal awal sejarah FMEA sudah banyak diterapkan pada dunia industri. 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). Pada awal tahun 1960 kontraktor untuk National Aeronautics and Space Administration (NASA) menggunakan variasi dari FMECA yang dikenal sebagai nama FMEA. Program NASA menggunakan prosedur FMEA termasuk Apollo, Viking, Voyager, dan Skylab. FMEA kemudian banyak diadopsi oleh industri penerbangan sipil, dimulai dari *Society for Automotive Engineers* (SAE) penerbitan ARP926 pada tahun 1967. Setelah melalui tahapan dua kali revisi, ARP926 digantikan dengan ARP4761, yang saat ini telah digunakan secara luas pada bidang penerbangan sipil. Selama tahun 1970-an, mulai digunakan secara luas pada berbagai bidang.

Objek penelitian sebelumnya yang ada pada penelitian-penelitian terkait penggunaan metode FMEA sudah cukup bervariasi. penggunaan FMEA menyebar ke berbagai industri lainnya seperti industri tekstil [7], kerajinan tangan [8] dan pengolahan limbah [9]. Bagaimana pun terdapat sebuah kecenderungan penelitian-penelitian yang ada yang terpusat pada industri manufaktur atau perusahaan yang memiliki produk berwujud fisik.

Tabel 1: Penelitian-Penelitian Terkait

Peneliti	Objek	Metode	Hasil
Diana Fitria dkk [10]	Industri manufaktur	FMEA, FTA	Penggunaan metode FMEA untuk menentukan nilai (RPN) selanjutnya digunakan menentukan potential cause dengan Fault Tree Analysis (FTA).
Richma Yulinda, dkk [11]	Industri manufaktur	FMEA, FTA	idem
Wahyu Oktri Widyarto, dkk [12]	Industri manufaktur	FMEA, six sixma	Penggunaan metode FMEA untuk menentukan nilai (RPN) selanjutnya digunakan metode Six sixma untuk perbaikan kualitas produk
Innike Desy, dkk [13]	Perbankan	FMEA	Daftar analisis risiko
Balqis Lembah dkk, [14]	Sistem Informasi	Octave	identifikasi risiko yang dapat terjadi

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 [15]. 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.

Metode Penelitian

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 dua 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 website Polri. Metode dilaksanakan dengan mengumpulkan data dari checksheet hasil inspeksi harian. Langkah berikutnya dilakukan metode menganalisis dan mengklasifikasi data yang dijalani dengan wawancarai pihak terkait serta metode memperoleh data historis. Data yang telah dikumpulkan dianalisis menggunakan alat bantu Microsoft Excel 2013. Setelah melakukan pengamatan dan wawancara terhadap developer sistem untuk menentukan apakah data dan prosedur yang dilakukan sudah valid penulis melakukan pengolahan data.

Adapun teknik pengumpulan data yang dilakukan dalam penelitian ini terdiri dari 4 macam, yaitu:

1. Studi literatur Tahap pertama yang dilakukan adalah mempelajari tentang teori dan topik yang akan dibahas. Dalam proses ini, semua teori yang berhubungan dengan topik "Keamanan sistem informasi" dikumpulkan dari berbagai sumber; buku, jurnal, internet, dan sebagainya.

2. Pengamatan secara langsung Pengamatan secara langsung terhadap sistem bertujuan untuk mempelajari bagaimana proses aliran data menjadi informasi dalam *website* Polri. Selanjutnya adalah melihat contoh kegagalan atau ketidaksesuaian yang terjadi beserta jenis-jenis dan penyebabnya.

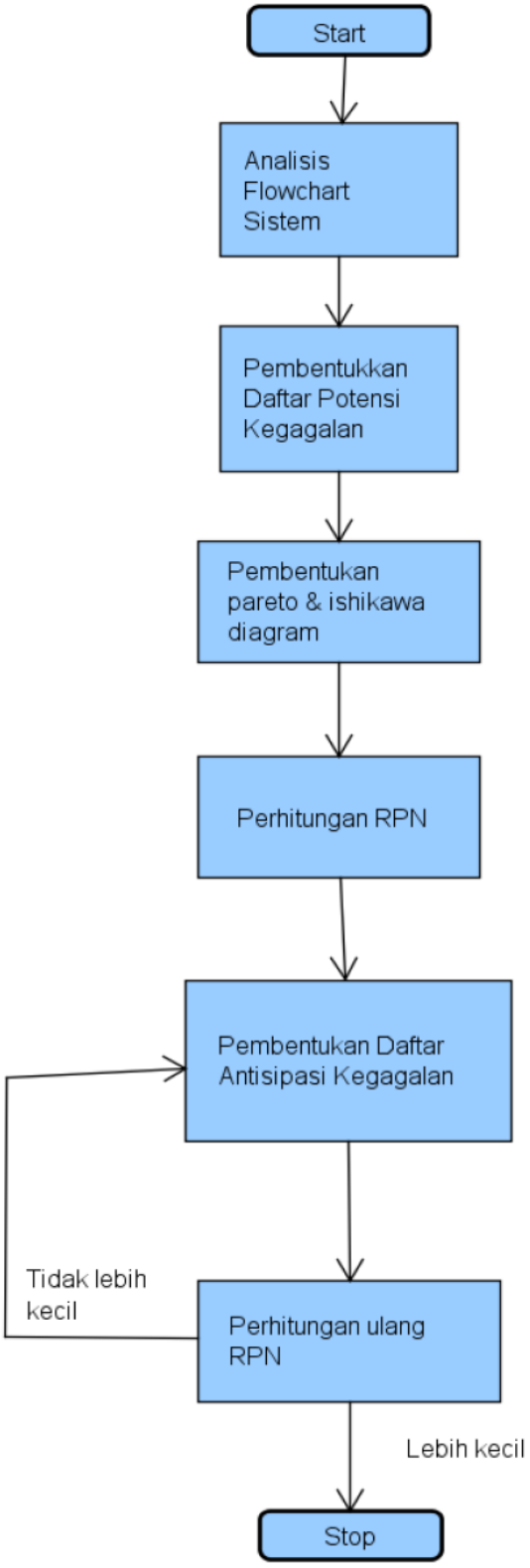
3. Pengumpulan data historis Tahap pengumpulan data historis merupakan tahap yang paling penting dalam penelitian ini, karena dari data historis itulah diketahui jenis-jenis ketidaksesuaian, sumber prosesnya, jumlah serta spesifikasinya, hingga akibat ketidaksesuaian pada kegagalan tersebut yang merupakan salah satu data yang penting untuk dianalisis.

4. Wawancara dan Tanya jawab Wawancara dan Tanya jawab ini dilakukan dengan berbagai pihak yang berhubungan dengan sistem informasi *website* Polri. Peneliti sudah mewawancarai berbagai pihak yang terkait di antaranya pengembang sistem (*developer)*, sistem analisis, dan pengguna sistem untuk mengumpulkan semua data-data yang diperlukan dalam penelitian ini. Hal ini bertujuan untuk mendapatkan gambaran atau uraian tentang kuantitas atau jenis-jenis kegagalan yang pernah terjadi, sumber dan penyebabnya berdasarkan pengetahuan masing-masing orang.

Tahapan Penelitian

Alur penelitian ini dapat dilihat pada gambar 1. Alur penelitian ini menunjukkan langkah demi langkah dari awal sampai akhir yang dilalui saat proses penelitian. Alur penelitian dimulai dari analisis proses yang ada dengan meninjau diagram flowchart sistem informasi pada objek yang diteliti. Hasil dari analisis flowchart di sini diharapkan dapat membantu mengenali celah-celah keamanan yang terdapat pada sistem. Pada tahap ini teknik wawancara dengan nara sumber terkait akan dilakukan untuk mengumpulkan data.

Selanjutnya data yang dikumpulkan dari setiap proses yang ada pada flowchart sistem akan dianalisis untuk pembentukan daftar potensi kegagalan yang mungkin terjadi. Dalam tahap ini peneliti akan melakukan studi pustaka merujuk pada literatur-literatur manajemen risiko dan keamanan sistem informasi untuk menggali lebih banyak daftar potensi kegagalan yang mungkin terjadi.



Gambar 1: Alur Penelitian

Setelah daftar potensi kegagalan dibentuk, langkah berikutnya adalah mengumpulkan data frekuensi kejadian dari masing-masing daftar potensi kegagalan berdasarkan hasil pengamatan langsung. Frekuensi daftar kejadian ini nantinya akan dijadikan rujukkan untuk membuat Pareto diagram. Pareto diagram berguna untuk mengambil prioritas dalam daftar potensi kegagalan di mana prioritas tertinggi adalah kegagalan yang paling kerap kali muncul selama selang waktu pengumpulan data. Setelah Pareto diagram dibuat, tahap selanjutnya adalah membuat diagram Ishikawa atau lebih dikenal dengan diagram tulang ikan. Diagram ini digunakan untuk mencari sebab-sebab dari daftar potensi kegagalan yang mungkin terjadi. Pada tahap ini dilakukan studi pustaka dan penelusuran literatur untuk menghimpun daftar penyebab dari potensi kegagalan yang mungkin terjadi.

Tahap berikutnya dalam alur penelitian setelah membuat diagram Ishikawa adalah melakukan perhitungan RPN (*Risk Priority Number*). RPN merupakan hasil kali dari nilai *severity, occurrance, detection* [16]. Nilai RPN berada pada rentang 1 sampai 1000, di mana semakin tinggi nilai RPN maka semakin tinggi pula risiko kegagalan terjadi. Setelah nilai RPN dikalkulasi, langkah berikutnya adalah membentukkan daftar rekomendasi aksi. Daftar ini mencakup segala macam cara yang dapat mengurangi nilai RPN seperti pencegahan, pendeteksian maupun penanggulangan potensi kegagalan. Setelah itu tahap pengumpulan data frekuensi potensi kegagalan kembali dilakukan untuk menghitung ulang nilai RPN. Setelah daftar rekomendasi aksi dilakukan diharapkan ada penurunan nilai RPN yang signifikan yang secara keseluruhan juga berarti sistem informasi yang lebih aman, stabil dan dapat diandalkan.

Variabel Penelitian

Penelitian mengguna sebuah variabel dependen yakni RPN (*Risk Priority Number*) dan tiga variabel Independent yakni *occurrence, severity* dan *detection.* Nilai RPN merupakan hasil kali besaran 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 akan disesuaikan. Penulis merumuskan besaran skala variabel baru terutama untuk *severity* dan *occurrance* agar lebih sesuai dengan konteks sistem informasi. Besaran variabel *occurrence,*

severity dan *detection* adalah nilai skala ordinal dari 1 sampai 10. Berikut satuan masing-masing ukuran skala yang telah disesuaikan dapat dilihat pada tabe 2 dan 3.

Tabel 2: Skala Penilaian Variabel *Severity*

Skala	Severity	Keterangan
10	System Crash	Seluruh sistem crash, sistem operasi harus di-restart
9	Program Crash	Program aplikasi crash, hang, force close.
8	Non-Functioning	Fitur program tidak berfungsi sama sekali dan berdampak langsung pada output informasi yang dihasilkan
7	Non-Functioning	Fitur program tidak berfungsi sama sekali
6	Incorrectly functioning	Fitur program berfungsi namun tidak valid atau akurat
5	Incorrectly functioning with workaround	Fitur program berfungsi namun tidak sesuai dengan aturan penggunaan atau spesifikasi
4	Performance cost	Dampak penurunan kinerja program
3	Efficiency cost	Program tidak efisien terhadap penggunaan CPU, memori, jaringan atau power
2	Cosmetic damage	Berdampak pada tampilan, user interface pada back-end sistem dan front-end sistem
1	Cosmetic damage	Berdampak pada tampilan, user interface pada back-end sistem

Tabel 3: Skala Penilaian Variabel *Occurrance*

Skala	Kategori	Keterangan
10	Extreme High	Kejadian lebih dari 5% waktu uptime sistem berjalan
9	Very High	Kejadian lebih dari 4,5% waktu uptime sistem berjalan
8	High	Kejadian lebih dari 4% waktu uptime sistem berjalan
7	Medium High	Kejadian lebih dari 3% waktu uptime sistem berjalan
6	Medium	Kejadian antara 2,5%-3% waktu uptime sistem berjalan
5	Medium	Kejadian antara 2% sampai 2,4% waktu uptime sistem berjalan
4	Medium Low	Kejadian kurang dari 2% waktu uptime sistem berjalan
3	Low	Kejadian kurang dari 1% waktu uptime sistem berjalan
2	Very low	Kejadian kurang dari 0,5% waktu uptime sistem berjalan
1	Remote	Kejadian kurang dari 0,1% waktu uptime sistem berjalan

Hasil dan Pembahasan

Daftar Potensi Kegagalan

Setelah melakukan analisis terhadap sistem informasi website Polri menggunakan melihat ke sistem secara langsung, mengamati *flowchart* dan dokumen-dokumen terkait maka penulis merumuskan daftar potensi kegagalan yang mungkin terjadi. Dalam tahap ini penulis juga sempat melakukan wawancara terkait data histori website Polri untuk menggali lebih banyak daftar potensi kegagalan yang mungkin terjadi. Berikut ini merupakan hasil analisis daftar potensi kegagalan:

1. Administrasi sistem tidak dapat diakses
2. Sistem tidak tersedia
3. Artikel tidak muncul setelah diinput
4. Tampilan berubah/tidak berkesesuaian
5. Menu layanan tidak dapat diakses
6. Gagal koneksi ke *database*
7. Waktu *loading* terlalu lama

Berdasarkan hasil analisis website yang berjalan saat diteliti memiliki beberapa celah kerawanan di antaranya:

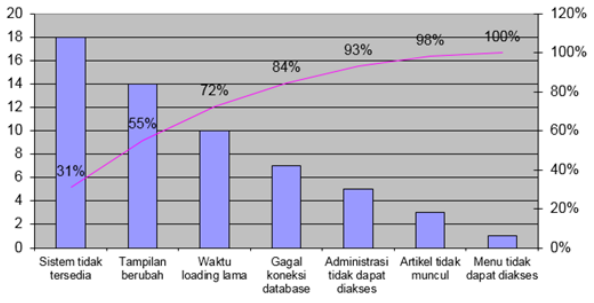
1. Terdapat *add-ons* pihak ketiga yang tidak pernah di-update dan berpotensi menjadi celah keamanan
2. Terlalu banyak fungsi layanan yang diberikan. Terdapat layanan SIM, STNK, SKCK, penerimaan POLRI, Pengadaan Barang/Jasa, dan juga fasilitas Internal Polri. Kesemua hal ini tidak hanya menjadikan beban akses server yang lama tetapi juga menjadikan *website* sulit untuk di-*maintenance*.
3. Informasi yang diekspos ke publik terlalu detail. Hal ini tidak bermanfaat bagi pengguna biasa namun dapat bermanfaat bagi peretas.
4. Banyak duplikasi kode antar menu dan *database* sehingga terdapat hubungan *coupling* yang tinggi antar kelas dengan demikian *website* akan sulit di-*maintenance* dan berpotensi menjadi lubang keamanan

5. Data input pada form tidak terlebih dahulu diamankan (*data sanitization*). Hal ini membuat *website* sangat rentan terhadap serangan kode injeksi.

Diagram Pareto & Ishikawa

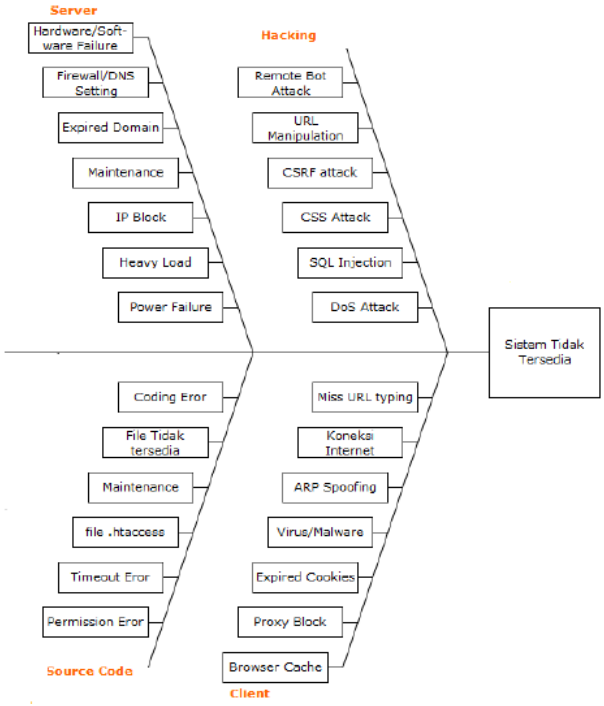
Diagram Pareto atau dikenal juga sebagai diagram Ishikawa merupakan salah satu alat bantu yang dapat digunakan mengidentifikasikan prioritas permasalahan yang harus terlebih dahulu diselesaikan. Permasalahan yang paling banyak dan sering terjadi adalah prioritas utama untuk melakukan tindakan. Pada penelitian ini diagram Pareto akan digunakan untuk mengidentifikasi permasalahan yang menjadi prioritas utama. Diagram pareto digambarkan dalam bentuk diagram batang yang menunjukkan kejadian yang diurutkan berdasarkan banyaknya jumlah frekuensi kejadian. Urutannya dimulai dari bentuk permasalahan yang frekuensinya paling sering terjadi sampai yang paling sedikit terjadi.

Diagram pareto ini dibuat berdasarkan data hasil penganan terhadap frekuensi kemunculan mode kegagalan. 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 [17]. Pada gambar 2 menunjukkan diagram Pareto dari frekuensi kegagalan.



Gambar 2: Diagram fishbone sistem tidak tersedia

Langkah berikutnya setelah membuat diagram Pareto adalah membuat diagram Ishikawa. Diagram ini dibuat dengan melakukan studi pustaka dan brainstorming dengan para developer. Hasil Fishbone diagram kemudian digunakan untuk membuat FMEA untuk menganalisa penyebab-penyebab dari masing-masing mode kegagalan yang terpilih. Penyebab kegagalan dikelompokkan ke dalam kategori masing-masing dan digambarkan seperti tulang ikan sedangkan garis di tengah merupakan mode kegagalan. Pada gambar 3 adalah hasil dari diagram Ishikawa.



Gambar 3: Diagram fishbone sistem tidak tersedia

Perhitungan RPN

Setelah menentukan prioritas menggunakan diagram Pareto dan menentukan daftar penyebab melalui diagram Ishikawa langkah pengujian berikutnya adalah menghitung nilai Risk Priority Number (RPN). Nilai RPN merupakan hasil kali dari variabel *severity, occcurance* dan *detection*. Terdapat dua prioritas mode kegagalan dalam diagram Pareto yakni sistem tidak tersedia dan tampilan berubah. Baik sistem tidak tersedia mapan tampilan yang berubahan keduanya mempunyai dampak yang sangat fatal terhadap fungsional sistem. Bagaimanapun bentuk tampilan website yang berubah tidak hanya berimbas pada tidak berfungsinya sistem secara keseluruhan namun juga dapat menimbulkan efek psikologis. Kedua mode kegagalan ini juga sulit dideteksi pada sistem yang berjalan saat ini karena tidak ada fasilitas log.

Hasil perhitungan RPN dapat dilihat secara detail pada tabel 4. Hasil perhitungan RPN menunjukkan bahwa mode kegagalan sistem tidak tersedia memiliki nilai RPN 576 dan mode kegagalan tampilan berubah memiliki RPN 400. Nilai RPN ini berada pada rentang 1-1000 di mana semakin tinggi nilai RPN maka semakin besar pula risiko yang berpotensi terjadi. Setelah melalukan perhitungan RPN hasil pengujian ini juga membuat daftar Recomended Action yang berisi segala jenis tindakan yang berpotensi untuk mengurangi nilai RPN baik dengan cara meminimalkan dampak dan frekuensi kejadian atau upaya pendeteksian dini dan pencegahan mode kegagalan. Diharapkan setelah melakukan aksi yang direkomendasikan ini nilai RPN dapat berkurang secara signifikan.

Tabel 4: *:* Hasil Perhitungan RPN

Potensi Kegagalan	**Dampak**	**S**	**O**	**D**	**RPN**	**Recomended Actions**
Sistem tidak tersedia	Kegagalan sistem secara total	9	8	8	576	- Membagi sistem ke beberapa aplikasi terpisah (SIM, SKCK, Penerimaan) - Gunakan *cloud server* untuk meminimalkan waktu *downtime* - Gunakan *firewall*, untuk mencegahkan serangan Dos - Gunakan koneksi SSL/HTTPS pada informasi yang bersifat sensitif
Tampilan berubah/ tidak beraturan	Kegagalan sistem secara total dan dampak psikologis	10	5	8	400	Melakukan sanitasi data, sehingga data yang diinput melalui *form* dan URL tidak berbahaya - Menyediakan log file yang mencacat aktivitas penting, terkait, *user*, waktu dan *update*/perubahan yang dilakukan - Pesan kesalahan tidak perlu ditampilkan secara detail - Manajemen hak akses harus dibatasi, diawasi dan dikelola dengan baik

Penutup

Penelitian ini telah berhasil melalukan audit keamanan sistem informasi pada website Polri. 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 40 sampai 60% dan berbagai tindakan rekomendasi telah dijabarkan untuk mengurangi tingkat kerawanan. 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. Bagaimana pun terdapat keterbatasan pada penelitian ini dikarenakan tidak dapat menguji ulang nilai RPN setelah daftar rekomendasi tindakan diberikan. Penghitungan ulang RPN ini diperlukan untuk konfirmasi apakah tingkat kerawanan dari mode kegagalan telah berkurang atau belum. Implikasi dari penelitian ini adalah penerapan metode FMEA pada objek sistem informasi dan diharapkan ke depan para peneliti lainnya mengeksplorasi lebih jauh perhitungan variabel *occurrance* dan *detection* dengan skala yang lebih objektif.

Daftar Pustaka

[1] D. Vose, Risk Analysis: A Quantitative Guide, 3rd ed., New Jersey: Wiley, 2008.

[2] E. Vaughan and T. Vaughan, Fundamentals of Risk and Insurance, New Jersey: Wiley, 2013.

[3] L. S. Lipol, "Risk Analysis Method: FMEA in the Organizations," *International Journal of Basic & Applied Sciences IJBAS*, vol. XI, no. 5, pp. 49-57, 2011.

[4] C. Dikmen, Information Week, San Francisco: UBM Tech, 1997.

[5] D. May, "The Return of Innovation," *Cambrige Journal*, pp. 11-17, 2015.

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

[7] 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.

[8] R. Hanif and 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.

[9] Anisa, "Evaluasi dan analisis waste pada proses produksi kemasan dengan menggunakan methode FMEA," Jurnal Fakultas Teknik Industri Universitas Indonesia, pp. 50-62, 2010.

[10] 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.

[11] 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.

[12] 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.

[13] 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," in *Seminar Nasional Sistem Informasi Indonesia,* Surabaya, 2014.

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

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

[16] H. Martin and L. Priscila, "The World technological capacity to store, communicate and compute information," *Science,* vol. 332, no. 6025, pp. 60-65, April 2011.

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