E-ISSN: 2528 - 6544
P-ISSN: 2620 - 3383
Vol.5 No.2 Februari 2021

Technomedia Journal

iLearning Journal Center (iJC)

TMJ (Technomedia Journal)
Vol.5 No.2 Edisi Februari 2021
E-ISSN: 2528 – 6544
P-ISSN: 2620 – 3383

Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013

Lailatul Munaroh[1]
Yusuf Amrozi[2]
Risky Agung Nurdian[3]

Universitas Islam Negeri Sunan Ampel Surabaya
Surabaya, Jawa Timur
E-mail: lailaniro@gmail.com[1], yusuf.amrozi@gmail.com[2], riskyagungnurdian@gmail.com[3]

ABSTRAK

Teknologi informasi saat ini menjadi prioritas utama karena keefektifan dan keefisienannya. Namun dengan kemudahan dan keefektifannya teknologi menjadi hal yang rawan akan keamanannya. Untuk itu manajemen keamanan juga hal yang menjadi prioritas setelah adanya teknologi informasi/sistem informasi. Penelitian ini bertujuan untuk mengukur dan mengidentifikasi risiko dengan menggunakan metode FMEA dan standar ISO/IEC 27001:2013. Hasil analisis menunjukkan terdapat terdapat 22 cause failure yang akan menyebabkan terjadinya risiko pada keamanan aset TI di Bidang Perdagangan Dalam Negeri (PDN) Dinas Perdagangan dan Perindustrian Pemerintah Provinsi XYZ. Terdapat 11 cause failure yang memiliki level tinggi dengan rentan nilai 400 – 175.

***Kata Kunci**: Aset Teknologi Informasi, FMEA, ISO/IEC 27001:2013, RPN*

ABSTRACT

Information technology is now a top priority because of its effectiveness and efficiency. However, with the ease and effectiveness of technology that is vulnerable to its security. For this reason, security management is also a priority after the existence of information technology / information systems. This study aims to measure and identify risks using the FMEA method and ISO / IEC 27001: 2013 standard. The analysis shows that there are 22 cause failures that will cause a risk to the security of IT assets in the Domestic Trade (PDN) Department of Trade and Industry of the XYZ Provincial Government. There are 11 cause failures that have a high level with a vulnerable value of 400 - 175.

***Keywords**: Information Technology Assets, FMEA, ISO/IEC 27001:2013, RPN*

PENDAHULUAN

Teknologi informasi saat ini menjadi prioritas utama karena keefektifan dan keefisienannya. Dengan adanya teknologi informasi/sistem informasi dapat memudahkan akses dan *sharing* data, dengan kapasitas penyimpanan yang besar. Namun dengan kemudahan dan keefektifannya teknologi menjadi hal yang rawan akan keamanannya. Untuk itu manajemen keamanan juga hal yang menjadi prioritas setelah adanya teknologi

informasi/sistem informasi. Dinas Perindustrian dan Perdagangan adalah salah satu dinas yang memiliki tugas untuk membantu Gubernur dalam melaksanakan urusan pemerintahan. Fungsi dari dinas adalah perumusan kebijakan di bidang perindustrian dan perdagangan, pelaksana kebijakan di bidang perindustrian dan perdagangan, pelaksana evaluasi dan pelaporan di bidang perindustrian dan perdagangan, pelaksana administrasi dinas di bidang perindustrian dan perdagangan dan pelaksana fungsi lain yang diberikan oleh gubernur terkait dengan tugas dan fungsinya. Dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang sistem manajemen pengamanan informasi pasal 1 ayat 5 berbunyi sistem manajemen pengamanan informasi adalah peraturan keajiban bagi penyelenggara sistem elektronik dalam penerapan manajemen pengamanan informasi berdasarkan asas risiko. Pada ayat 6 berbunyi Keamanan informasi adalah terjaganya kerahasiaan, keutuhan dan ketersediaan. Berdasarkan peraturan menteri yang ada diwajibkan bagi instansi pemerintahan untuk menerapkan keamanan informasi dan manajemen risiko. Namun dalam wawancara yang dilakukan pada staf bagian pengadaan barang yaitu Bapak X mengatakan belum ada standar dalam pengelolaan keamanan TI/SI dan belum ada pedoman dalam melakukan manajemen risiko. Manajemen risiko adalah pendekatan atau metodologi dalam mengelola ketidakpastian yang berkaitan dengan potensi terjadinya sesuatu yang merugikan. Dengan adanya manajemen terhadap risiko maka ada aktivitas dan kontrol organisasi untuk menangani risiko. Risiko adalah sesuatu yang dapat diukur dengan melihat dari tingkat dampak dan kemungkinan risiko tersebut terjadi. Dalam mengatasi risiko keamanan membutuhkan keahlian dalam pengelolaan manajemen risiko keamanan [9]. Banyak kerangkakerja/standar/metode yang dapat menjadi acuan dalam pengukuran tingkat risiko salah satunya adalah metode FMEA. FMEA adalah teknik rekayasa yang digunakan sebagai penetapan, identifikasi dan menghilangkan kegagalan yang telah diketahui, permasalahan, *error* dan sejenis dari sistem, desain, proses dan jasa sebelum mencapai konsumen [1]. Pada FMEA ada 4 penilaian yaitu *severity, occurence, detection,* dan *RPN (Risk Priority Number). Severity* adalah Penilaian berhubungan dengan seberapa besar kemungkinan terjadi impact yang mengakibatkan terjadinya kegagalan. *Occurence* adalah penilaian pada seberapa sering kemungkinan terjadinya suatu risiko. *Detection* bertujuan mengetauhi seberapa bersar kemungkinan terjadinya risiko dapat dideteksi secara maksimal. Dan terakhir adalah RPN yaitu perkalian nilai dari *severity, occurence* dan *detection.* Metode FMEA digunakan untuk mengambil data angka dan penentuan Failure Mode mana yang diprioritaskan. Ancaman dan risiko dapat menimbulkan dampak pada kegiatan dalam pengelolaan dan pemeliharaan data/informasi, hal ini menjadi latar belakang disusunnya standar sistem yang salah satunya adalah ISO/IEC 27001:2013 [2]. Pada standart ISO/IEC 27001:2013 ini dikenal sebagai penanganan risiko dimana risiko yang ada harus dapat dikelola dengan baik, dianalisis dan dievaluasi cara untuk pengendalian risiko tersebut. Standar ISO/IEC 27001:2013 merupakan kontrol yang digunakan dalam tahap mitigasi atau penanganan risiko [2]. Mitigasi risiko adalah fase penanganan risiko, fase dimana agen risiko terpilih dari fase pertama dinilai dengan tindakan penanganan [10]. Pengelolaan atau manajemen terhadap keamanan sistem informasi diperlukan guna mengantisipasi dan meminimalisir ancaman yang mungkin terjadi [8].

PERMASALAHAN

Berdasarkan latar belakang diatas, maka rumusan masalah yang dibahas adalah

bagaimana tingkat manajemen risiko keamanan teknologi informasi pada Dinas Perindustrian dan Perdagangan Provinsi XYZ di Bidang Perdagangan Dalam Negeri?

METODE PENELITIAN

Metode penelitian ini menggunakan metode penelitian kualitatif, untuk mengukur dan mengevaluasi sejauhmana tingkat risiko keamanan aset teknologi informasi. Metode pengumpulan data yang digunakan dalam penelitian ini yaitu *study literature* digunakan sebagai rujukan atau acuan dalam penelitian. Sumber data yang digunakan untuk *study literature* dalam penelitian ini yaitu jurnal, tesis, buku, internet dan dokumen terkait. *Interview* dengan melakukan tanya jawab atau wawancara. Wawancara dilakukan secara langsung dengan staf bagian pengadaan barang yaitu Bapak X. Observasi dimana peneliti melakukan pengamatan secara langsung terhadap objek yang akan diteliti. Dalam penelitian ini pengamatan dilakukan di Dinas Perdagangan dan Perindustrian Pemerintah Provinsi XYZ. Beberapa penelitian terkait terdahulu, misalnya oleh Raden Budiarto (2017) dengan judul "Manajemen Risiko Sistem Informasi Menggunakan Metode FMEA dan ISO 27001 Pada Organisasi XYZ". Hasil penelitian menunjukkan penerapan standar ISO 27001 berimbas terhadap penurunan tingkat kerawanan sebesar 30%. Merujuk pada penelitian yang dilakukan oleh Anindhita Firdani, Suprapto, dan Andi Reza Perdana Kusuma (2019) dengan judul "Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 Menggunakan Indeks KAMI Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Rembang". Hasil penelitian terdapat 15 prioritas risiko dengan nilai RPN tertinggi sebesar 126. Gunawan Setyadi dan Yupie Kusumawati melakukan penelitian dengan judul "Mitigasi Risiko Aset dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja OCTAVE dan FMEA Pada Universitas Dian Nuswantoro". Hasil penelitian terdapat 50 risiko dengan prioritas risiko sebanyak 14. Berdasarkan penelitian yang dilakukan oleh Irawan Afrianto, Taryana Suryana dan Sufa'atin (2015) dengan judul "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI-SNI ISO/IEC 27001:2009 Studi Kasus Perguruan Tinggi X". Hasil penelitian menunjukkan bahwa tingkat kematangan informasi PT.X pada level I+ s/d II+, dimana untuk mendapatkan sertifikasi ISO/IEC 27001:2009 level keamanan informasi minimal III. Secara umum titik perbedaan dari penelitian sebelumnya terletak pada sasaran penelitian. Penelitian ini dilakukan di bidang industri perdagangan dalam negeri pemerintah dinas perindustrian dan perdagangan pemerintah provinsi XYZ.

HASIL DAN PEMBAHASAN

Berdasarkan hasil pengamatan yang telah dilakukan selama proses pengumpulan data, terdapat berbagai hasil mode kegagalan yang terjadi. Berikut ini merupakan hasil analisis potensi kegagalan:

1. *Hardware failure*
   Kurangnya skema pergantian perangkat secara berkala, kurangnya pemeliharaan untuk

pemeliharaan yang rumit, kerentanan terhadap kelembapan, debu dan kotoran, kerentanan terhadap nilai informasi yang tersimpan pada PC, kerentanan terhadadap voltase yang bervariasi hubungan arus pendek pada panel listrik, supply listrik yang tidak stabil, beban kerja server tinggi, dan pertambahan memori yang cepat dalam pemrosesan.

2. Data
   Data terlalu sering di *update,* data tidak ter *update*, kurangnya salinan *back-up,* jaringan internet kurang optimal, kesalahan penempatan hak akses, dan terlalu banyak data yang di input.
3. Layanan teknologi informasi
   Kurangnya dokumentasi *user* manual untuk aplikasi, kurangnya mekanisme identifikasi dan otentifikasi pengguna aplikasi, karyawan kurang memperhatikan pentingnya antivirus, dan kekurangan yang telah diketahui pada perangkat lunak.
4. *Network failure*
   Jaluk komunikasi yang tidak dilindungi, arsitektur jaringan yang tidak aman, manajemen jaringan yang tidak cukup, sambungan kabel yang buruk, kualitas jaringan yang kurang baik, bencana alam dan kejadian yang tidak terduga, SDM yang tidak kompeten, peletakan kabel sembarangan, dan tidak ada perlindungan kabel.

Dari hasil identifikasi kegagalan maka tahap selanjutnya adalah identifikasi risiko. Berikut Tabel 1 adalah hasil identifikasi risiko.

Tabel 1. Identifikasi risiko

Aset	Cause Failure	Risiko
Hardware: - Komputer - Server - Mesin Fotocopy - Printer	Maintenance yang tidak teratur	Hardware failure
	Kerusakan fisik pada server	
	Kurangnya pengamanan organisasi	Pencurian media atau informasi penting
	Korsleting listrik	Kebakaran
	Pemandaman listrik	Power failure
	Server overheat	Hardware failure

	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)	Memori penuh
Data: - Data pengadaan barang - Data informasi kegiatan dinas	Kesalahan dalam penginputan dan penghapusan data	Human error
	Organisasi tidak melakukan prosedur back up	Backup failure
	Speed Koneksi internet yang lemah dan tidak stabil	Network failure
	Tidak ada penggunaan hak akses	Penyalahgunaan hak akses
	Server down	Backup failure
Layanan Teknologi informasi: - SISKAPERBAPO - SIPAP	Kurangnya dokumentasi (user manual) untuk karyawan baru	Human error
	Password tidak pernah diganti	Penyalahgunaan hak akses
	PC terserang virus	Human reeoe
	Staf mengetauhi kelemahan pada aplikasi	Modifikasi dan pencurian data
Perangakat jaringan (network)	Lemahnya keamanan di sistem internal TI	Serangan hacker
	Kurangnya mekanisme pemantauan terhadap jaringan	Network failure
	Ganguan jaringan pada provider	
	Kerusakan pada infrastruktur jaringan	
	Kesalahan dalam melakukan konfigurasi access point	
	Kabel digigit oleh hewan	Hardware Failure

Setelah melakukan daftar potensi kegagalan dan indentifikasi risiko, langkah selanjutnya adalah mengumpulkan data frekuensi kejadian (*occurrence*) dari masing-masing

daftar potensi kegagalan berdasarkan hasil pengamatan yang telah dilakukan secara langsung. Pada saat yang bersamaan juga menentukan tingkat keparahan (*severity*) serta mengidentifikasi penyebab dan pencegahan dini. Tingkat keparahan dan frekuensi kejadian akan dijadikan sebagai nilai tolak ukur untuk menentukan prioritas. Nilai RPN merupakan hasil kali dari *severity*, *occurrence,* dan *detection.* Tabel 2 merupakan hasil perhitungan RPN.

Tabel 2. Perhitungan RPN

Aset	No Cause Failure	Cause Failure	Sev	Occ	Dec	RPN
Hardware: - Komputer - Server - Mesin Fotocopy - Printer - AC	1	Maintenance yang tidak teratur	8	3	5	120
	2	Kerusakan fisik pada server	8	8	3	192
	3	Kurangnya pengamanan organisasi	1	3	3	9
	4	Korsleting listrik	8	8	5	320
	5	Pemandaman listrik	8	5	5	200
	6	Server overheat	5	8	10	400
	7	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)	5	8	5	200
Data: Data vendor, data pengadaan barang, data informasi kegiatan dinas	8	Kesalahan dalam penginputan dan penghapusan data	1	8	5	40
	9	Organisasi tidak melakukan prosedur back up	7	8	3	168
	10	Speed Koneksi internet yang lemah dan tidak stabil	6	5	5	150
	11	Tidak ada penggunaan hak akses	7	5	5	175

	12	Server down	7	8	3	168
Layanan Teknologi Informas - SISKAPERBAPO - SIPAP	13	Kurangnya dokumentasi (user manual) untuk karyawan baru	7	8	3	200
	14	Password tidak pernah diganti	8	5	5	200
	15	PC terserang virus	7	5	5	175
Perangkat Jaringan (*nerwork):*	16	Staf mengetauhi kelemahan pada aplikasi	6	5	5	150
	17	Lemahnya keamanan di sistem internal TI	6	5	5	150
	18	Kurangnya mekanisme pemantauan terhadap jaringan	7	5	5	175
	19	Ganguan jaringan pada provider	6	8	3	144
	20	Kerusakan pada infrastruktur jaringan	8	5	3	120
	21	Kesalahan dalam melakukan konfigurasi access point	8	5	3	120
	22	Kabel digigit oleh hewan	8	5	6	240

Setelah dilakukan perhitungan RPN maka data pada Tabel 2 disorting berdasarkan kolom RPN mulai dari nilai terbesar sampai terkecil diketauhi cause failure mana yang diprioritaskan, yaitu pada cause failure nomor 6, 4, 22, 5, 7, 13, 14, 2, 11, 15 dan 18. Sebagaimana pada Tabel 3 berikut:

Tabel 3. Hasil sorting nilai RPN

No Cause Failure	Cause Failure	RPN
6	Server overheat	400
4	Korsleting listrik	320
22	Kabel digigit oleh hewan	240
5	Pemandaman listrik	200
7	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)	200
13	Kurangnya dokumentasi (user manual) untuk	200

	karyawan baru	
14	Password tidak pernah diganti	200
2	Kerusakan fisik pada server	192
11	Tidak ada penggunaan hak akses	175
15	PC terserang virus	175
18	Kurangnya mekanisme pemantauan terhadap jaringan	175
9	Organisasi tidak melakukan prosedur back up	168
12	Server down	168
10	Speed Koneksi internet yang lemah dan tidak stabil	150
16	Staf mengetauhi kelemahan pada aplikasi	150
17	Lemahnya keamanan di sistem internal TI	150
19	Ganguan jaringan pada provider	144
1	Maintenance yang tidak teratur	120
20	Kerusakan pada infrastruktur jaringan	120
21	Kesalahan dalam melakukan konfigurasi access point	120
8	Kesalahan dalam penginputan dan penghapusan data	40
3	Kurangnya pengamanan organisasi	9

Setelah dilakukan perhitungan RPN maka dilakukan penentuan level yang digambarkan dalam bentuk matrik, hal ini bertujuan untuk menentukan daerah prioritas *cause failure* dengan mempertimbangkan nilai *severity* dan nilai *occurence* [3]. Peletakan Nomor *cause failure* berdasarkan nilai *severity* dan *occurence*, sebagai contoh *cause failure* Nomor 6 pada Tabel 2 memiliki nilai *severity* 5 dan nilai *occurence* 8, maka peletakan angka 2 ada pada sumbu *severtiy Low* dan sumbu *Occurence High* atau didaerah kolom merah, begitu juga dengan *cause failure* yang lain. Berikut adalah matrik level pada Tabel 4.

Tabel 4. Matrik level

SEVERITY/ DAMPAK						
	Very High					
	High	**1**	**5, 11, 14, 15, 18,**		**2, 4, 9. 12**	

			20, 21, 22			
	Moderate		**10, 16, 17,**		**19**	
	Low				**6,7, 13,**	
	Very Low	**3**			**8**	
		Very Low	**Low**	**Moderate**	**High**	**Very High**
		***OCCURENCE*/KEMUNGKINAN**				

Dari hasil pemetaan matrik diatas dapat diketauhi bahwa *cause failure* yang memerlukan penanganan adalah *cause failure* yang berada di kolom merah dan kuning yaitu *cause failure* nomor 2, 4, 9, 12, 19, 6, 7, dan 13. Dari hasil perhitungan RPN dan Matrik dapat dipetakan lagi dalam bentuk tabel untuk melihat kesesuaian dan memilih *cause failure* mana yang akan di prioritaskan dalam proses mitigasi atau ditangani untuk meminimalisir terjadinya risiko. Berikut Tabel 5 adalah pemetaan kesesuaian hasil RPN dan Matrik.

Tabel 5. Kesesuaian Hasil RPN dan Matrik

No Cause Failure	Cause Failure	RPN	Matrik
6	Server overheat	√	√
4	Korsleting listrik	√	√
22	Kabel digigit oleh hewan	√	-
5	Pemandaman listrik	√	-
7	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)	√	√
13	Kurangnya dokumentasi (user manual) untuk karyawan baru	√	√
14	Password tidak pernah diganti	√	-
2	Kerusakan fisik pada server	√	√
11	Tidak ada penggunaan hak akses	√	-
15	PC terserang virus	√	-
18	Kurangnya mekanisme pemantauan terhadap jaringan	√	-
9	Organisasi tidak melakukan prosedur backup	-	√
19	Gangguan jaringan provider	-	√
12	Kurangnya dokumentasi (user manual) untuk karyawan baru	-	√

Berdasarkan hasil pemetaan pada Tabel 5 maka *cause failure* yang akan di mitigasi adalah risiko nomor 2, 4, 9, 12, 19, 6, 7 dan 13 karena memiliki tingkat yang tinggi. Mitigasi adalah langkah terakhir untuk memberikan penanganan pada yang memiliki tingkat tinggi, hal ini bertujuan untuk meminimalisir terjadinya risiko dan saran yang diberikan dapat dilakukan jika risiko terjadi. Berdasarkan hasil pemetaan pada Tabel 4 diketauhi bahwa ada 8 *cause failure* yang di mitigasi yaitu *cause failure* nomor 2, 4, 9, 12, 19, 6, 7 dan 13. Pada Tabel 6 merupakan mitigasi yang dilakukan berdasarkan standar ISO/IEC 27001:2013.

Tabel 6. Mitigasi *cause failure*

Aset	No. Cause Failure	Cause Failure	Tindakan Mitigasi berdasarkan ISO/IEC 27001:2013		
			Klausul	Kontrol	Tindakan
Hard ware Server	2	Kerusakan fisik pada Hardware	A.11 *Physical and environmental security* (A.11.1.2, A.11.1.3, A.11.1.4)	- Mencegah akses fisik yang tidak sah, kerusakan dan gangguan pada informasi dan fasilitas pemrosesan informasi organisasi. - Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa personel resmi diizinkan mengakses - Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan - Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang dan diterapkan	- Melakukan kontrol yang rutin terhadap penyimpanan server dalam waktu 1 bulan sekali - Pengecekan suhu ruangan server
Hard ware	4	Korsleting listrik	Berdasarkan Penelitian Terdahulu yang dilakukan	Korsleting listrik dan generator terbakar memiliki dampak tidak dapat mengoperasionalkan	Perlindungan keamanan pengkabelan dari kerusakan dan melakukan

			oleh Mahersmi, Artowini, & Hidayanto pada tahun 2016.	semua perangkat yang membutuhkan daya listrik [4].	monitoring berkala [4].
Data	9	Organisasi tidak melakukan prosedur back up	A.12 *operation security* (A.12.3 *Backup*)	Salinan cadangan informasi, perangkat lunak, dan gambar yang disimpan pada sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati	- membuat salinan data pada semua software - mengadakan server cadangan yang ditempatkan diluar dinas.
Hard ware - Server	12	Server Down	*Performance evaluation*	- Menjaga kualitas hardware diperlukan diperulukan evaluasi performa - Prosedur monitoring terhadap aset teknologi informasi yang dimiliki organisasi	-Dinas menetapkan kebijakan mengenai monitoring aset teknologi informasi - Monitoring dilakukan secara berkala dan memastikan
Jaring an	19	Ganguan jaringan pada provider	Klausul 13, Sub A.13.1 *Network security management.*	- Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi - mekanisme keamanan, tingkat layanan, dan persyaratan pengelolaan semua layanan jaringan harus diidentifikasi termasuk dalam perjanjian layanan jaringan, apakah	Andanya monitoring secara intens terhadap jaringan.

				layanan ini disediakan di rumah atau di-outsourcing. - Kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan	
Hard ware	6	Server overheat	A.11 *Physical and environmental security (* A.11.1.3)	- Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan	- Melakukan kontrol yang rutin terhadap penyimpanan server dalam waktu 1 bulan sekali - Pengecekan suhu ruangan server - Pastikan server disimpan di rak pendingin untuk memungkinkan aliran udara yang tepat melalui server - Memasang sensor suhu dan kelembapan dan memantau setiap kenaikan suhu di sekitar server dan peralatan jaringan
Hard ware	7	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)	A.12 *operation security* (A.12.3 *Backup*)	Salinan cadangan informasi, perangkat lunak, dan gambar yang disimpan pada sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan	- membuat salinan data pada semua software - mengadakan server cadangan yang ditempatkan diluar dinas.

				yang disepakati	
	13	Kurangnya dokumentasi (user manual) untuk karyawan baru	A.12 *operation security* (A.12.1 *Operational prosedures and responsibilities, A.12.1.1 Documented operating procedure)*	- Prosedur operasi harus didokumentasikan dan disediakan untuk semua pengguna yang membutuhkannya.	- Membuat manual *book* pada semua sistem/aplikasi yang ada agar dapat memudahkan karyawan baru dalam mempelajari dan menggunakan sistem/aplikasi

KESIMPULAN

Dari hasil pengukuran pada pembahasan diatas dapat disimpulkan bahwa terdapat 22 *cause failure* yang akan menyebabkan terjadinya risiko pada keamanan aset TI di Bidang Perdagangan Dalam Negeri (PDN). Terdapat 11 *cause failure* yang memiliki level tinggi dengan rentan nilai 400 – 175 yaitu *cause failure* nomor 6 server overheat, 4 (korsleting listrik), 22 (kabel digigit oleh hewan), 5 (pemadaman listrik), 7 (kapasitas memori server sudah tidak memenui kebutuhan), 13 (kurangnya dokumentasi (user manual) untuk karyawan baru), 14 (password tidak diganti), 2 (kerusakan fisik pada server), 11 (tidak ada penggunaan hak akses), 15 (PC terserang virus) dan 18 (kurangnya mekanisme pemantauan terhadap jaringan). Sedangkan pada pemetaan matrik pada Tabel 3 ada 8 *cause failure* yang berada pada kolom merah yang berarti kritis yaitu kerusakan fisik pada server (2), korsleting listrik (4), Organisasi tidak melakukan prosedur back up (9), server down (12), gangguan jaringan pada provider (19), server overheat (6), Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full) (7) dan Kurangnya dokumentasi (user manual) untuk karyawan baru (13). Berdasarkan hasil pemetaan akhir untuk melihat kesesuaian nilai RPN dan matrik (Tabel 4) didapatkan 8 *cause failure* yang sesuai dan yang akan dilakukan mitigasi. 8 *cause failure* tersebut diantaranya adalah kerusakan fisik pada server (2), korsleting listrik (4), Organisasi tidak melakukan prosedur back up (9), server down (12), gangguan jaringan pada provider (19), server overheat (6), Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full) (7) dan Kurangnya dokumentasi (user manual) untuk karyawan baru (13). Mitigasi atau penanganan terhadap 8 *cause failure* menggunakan standart ISO/IEC 27001:2013 sebagaimana terdapat pada Tabel 5.

SARAN

Hasil identifikasi manajemen aset pada dinas sudah baik berdasarkan ISO/IEC 27001:2013, saran yang diberikan yaitu diharapkan untuk dilakukan update data aset secara rutin pada aplikasi yang sudah ada, melakukan identifikasi sebelum pengadaan barang dan memberi perlindungan pada media yang mengandung informasi, seperti memberi password pengaman pada printer. Sedangkan hasil dari pengukuran risiko dan mitigasi dapat menjadi panduan bagi dinas dalam pengelolaan dan pemeliharaan aset teknologi informasi yang ada. Untuk meminimalisir terjadinya risiko dan mengetauhi tindakan yang dilakukan saat risiko itu terjadi. Sesuai dengan peraturan menteri komunikasi dan informatika republik indonesia nomor 4 tahun 2016 tentang manajemen pengamanan informasi pada pasal 7 diharapkan pada dinas untuk menerapkan standar SNI ISO/IEC 27001. Pengukuran risiko ini dapat dilanjutkan dengan metode dan standar yang lain untuk menghasilkan solusi yang lebih baik dan lebih detail.

DAFTAR PUSTAKA

[1] Hanif, R. Y., Rukmi, H. S., & Susanty, S. (2015). *PERBAIKAN KUALITAS PRODUK KERATON LUXURY DI PT. X DENGAN MENGGUNAKAN METODE FAILURE MODE and EFFECT ANALYSIS (FMEA) dan FAULT TREE ANALYSIS (FTA)*. 11.

[2] Budiarto, R. (2017). *MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI MENGGUNAKAN METODE FMEA DAN ISO 27001 PADA ORGANISASI XYZ*. *2*(2), 11.

[3] Nanda, L., Hartanti, L. P. S., & Runtuk, J. K. (2014). *Analisis Risiko Kualitas Produk dalam Proses Produksi Miniatur Bis dengan Metode Failure Mode and Effect Analysis pada Usaha Kecil Menengah Niki Kayoe*. *3*(2), 12.

[4] Mahersmi, B. L., Muqtadiroh, F. A., & Hidayanto, B. C. (2016). *ANALISIS RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DISHUBKOMINFO KABUPATEN TULUNGAGUNG*. 14.

[5] Afrianto, I., Suryana, T., & Sufa'atin, S. (2015). Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009. *Jurnal ULTIMA InfoSys*, *6*(1), 43–49. https://doi.org/10.31937/si.v6i1.278

[6] Firdani, A. (2019). *Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 menggunakan Indeks KAMI Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang*. 7.

[7] Setyadi, G., & Kusumawati, Y. (n.d.). *Mitigasi Risiko Aset Dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja OCTAVE Dan FMEA Pada Universitas Dian Nuswantoro*. 10.

[8] Chazar, C. (2015). *STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005*. 10.

[9] Sakinah, F., Setiawan, B., & Hakim, J. A. R. (2014). *Indeks Penilaian Kematangan (Maturity) Manajemen Keamanan Layanan TI*. *3*(2), 6.

[10] Kristanto, B. R. (2014). APLIKASI MODEL HOUSE OF RISK (HOR) UNTUK MITIGASI RISIKO PADA SUPPLY CHAIN BAHAN BAKU KULIT. *Jurnal Ilmiah Teknik Industri*, *13*(2), 9.