Tersedia online di: http://ejournal.undip.ac.id/index.php/teknik

TEKNIK, 39 (2), 2018, 78-85

Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis *Framework* ISO 27001

Naniek Utami Handayani[1*], Mochammad Agung Wibowo[2], Diana Puspita Sari[1], Yoga Satria[1], Akbar Romadhona Gifari[1]

[1]Departemen Teknik Industri, Fakultas Teknik, Universitas Diponegoro
[2]Departemen Teknik Sipil, Fakultas Teknik, Universitas Diponegoro
Jl. Prof. Soedarto, SH, Kampus Undip Tembalang, Semarang, Indonesia 50275

Abstrak

Kebocoran data dan penyalahgunaan informasi oleh pihak yang tidak berkepentingan yang pernah terjadi mengharuskan perlindungan terhadap keamanan Sistem Informasi di Fakultas Teknik Universitas Diponegoro (SIFT UNDIP) untuk terus ditingkatkan. Penelitian ini bertujuan untuk mengidentifikasi risiko, menganalisis manajemen keamanan sistem informasi, dan menentukan prioritas risiko pada SIFT UNDIP. Penelitian dilakukan menggunakan metode Failure Mode Effect and Analysis berbasis framework ISO 27001. Hasil analisis menunjukkan terdapat 25 risk agent pada SIFT UNDIP yang dikategorikan menjadi empat jenis asset. Risiko tertinggi pada kategori High Level Risk adalah risiko ketergantungan terhadap karyawan dengan nilai Risk Priority Number sebesar 80.

Kata kunci*: Sistem Informasi; Penilaian risiko; Framework ISO 27001; risk agent; FMEA; RPN*

Abstract

[Title: Risk Assessment of Information System of Faculty of Engineering University Diponegoro Using Failure Mode Effect and Analysis Method based on Framework ISO 27001]
The data leakage and misuse of information by unauthorized parties that had happened forces the protection of security of information system in the Faculty of Engineering Diponegoro University (SIFT UNDIP) to be improved. This research aims to identify the risks, to analyze security of information system management, and to determine risk priority in SIFT UNDIP. This research is conducted using Failure Mode Effect and Analysis method based on ISO 27001 framework. Analysis results show that there are 25 risk agents in SIFT UNDIP which are categorized into four types of assets. The highest risk in High Level Risk category is the risk of dependence on employees which has Risk Priority Number value of 80.

Keywords*: Information System; Risk assessment; ISO 27001 Framework; risk agent; FMEA; RPN*

1. Pendahuluan

Keamanan informasi merupakan salah satu aspek penting yang harus diperhatikan oleh organisasi dan perusahaan. Informasi baik berupa teks, gambar, audio, maupun video yang menyimpan asset penting bagi perusahaan, wajib dilindungi dengan sistem manajemen keamanan informasi. Kebocoran, kerusakan atau hilangnya suatu informasi dapat menimbulkan kerugian baik secara finansial maupun produktivitas bagi organisasi dan perusahaan (Mufadhol, 2009). Pada awalnya, keamanan informasi berpijak pada 3 prinsip yaitu: *confidentiality*, *integrity*, dan *availability*. Tetapi seiring perkembangan teknologi informasi, prinsip itu menjadi CIA+, yaitu *confidentiality*, *integrity*, *availability*, *privasi*, *identification*, *authentification*, *authorization*, dan *accountability* (Whitman dan Mattord, 2010).

Keamanan data/informasi secara langsung maupun tidak langsung dapat mempertahankan kelangsungan proses bisnis, mengurangi risiko, dan

*) Penulis Korespondensi.
E-mail: naniekh@ft.undip.ac.id

doi: 10.14710/teknik.v39n2.15918

bahkan mendorong meningkatnya peluang bisnis. Ancaman dan risiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data/informasi menjadi alasan disusunnya standard sistem manajemen keamanan informasi yang diantaranya adalah ISO 27001. ISO/IEC 27001 adalah sebuah kerangka khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional dan digunakan dalam mengidentifikasi risiko yang ada dengan mengetahui asset serta berbagai ancaman dan kelemahan sistem yang ada (Sarno, 2009; Sarno dan Iffano, 2009).

Penelitian terdahulu terkait manajemen risiko sistem informasi diantaranya adalah ontology draft ISO 27001:2013 (Milicevic dan Goeken, 2010), tata cara implementasi ISO 27001 pada Sistem Informasi Manajemen (Stephanus, 2014), analisis risiko pada sistem informasi akademik di perguruan tinggi dengan menggunakan metode OCTAVE Allegro (Jakaria, dkk, 2013); evaluasi ISO 27001 pada sistem informasi pemerintahan (Astikasari dan Chandra, 2018; Maingak, dkk, 2018), dan evaluasi ISO 27001 pada layanan pelanggan (Fajar, dkk, 2018). Berbeda dengan penelitian sebelumnya, penelitian ini mengevaluasi kesiapan implementasi ISO/IEC 27001:2013 *Information Security Management Systems standard* pada Sistem Informasi Fakultas Teknik UNDIP dengan menggunakan metode *Failure Mode Effect and Analysis* (FMEA).

Informasi merupakan aset yang sangat penting bagi keberlangsungan suatu organisasi, pertahanan keamanan, keutuhan negara, kepercayaan publik. Kemampuan untuk menyediakan informasi secara akurat dan cepat menjadi hal yang penting bagi suatu organisasi. Sistem informasi digunakan untuk mendukung berbagai kegiatan dalam perusahaan, bahkan untuk memperoleh keuntungan dan memenangkan persaingan (Chazar, 2015). Risiko keamanan sistem informasi dapat dikurangi dengan dukungan tata kelola yang optimal terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) dari suatu informasi.

Setiap intansi baik besar, menengah, maupun kecil membutuhkan manajemen yang baik dalam hal pengolahan data, sehingga kinerja suatu instansi dalam pelayanan kepada *stakeholders* dapat ditingkatkan. Fakultas Teknik Universitas Diponegoro sebagai institusi pendidikan terus berupaya untuk mengembangkan sistem informasi yang terintegrasi dibawah manajemen Sistem Informasi Fakultas Teknik (SIFT) UNDIP. Sistem informasi berbasis web yang dikelola oleh SIFT antara lain Sistem Informasi Akademik, Sistem Infromasi Keuangan, Sistem Informasi Barang Milik Negara, dan lain-lain. Keamanan data/informasi elektronik menjadi hal yang sangat penting bagi Fakultas Teknik UNDIP yang menggunakan fasilitas teknologi informasi dan menempatkannya sebagai infrastruktur penting. Hal ini disebabkan data/informasi adalah asset bagi keberlangsungan dan kecepatan layanan pada Fakultas Teknik UNDIP.

Berpijak dari pentingnya perlindungan terhadap keamanan informasi yang dimiliki oleh Fakultas Teknik UNDIP, maka penelitian ini bertujuan untuk melakukan penilaian risiko mengenai keamanan Sistem Informasi yang ada di Fakultas Teknik UNDIP.

2. Metode Penelitian

Manajemen Risiko

Manajemen risiko diartikan sebagai kemampuan seorang manajer untuk menata kemungkinan variabilitas pendapatan dengan menekan sekecil mungkin tingkat kerugian yang diakibatkan oleh keputusan yang diambil dalam menggarap situasi yang tidak pasti. Konsep dasar manajemen risiko yang dapat dipahami oleh pihak manajemen perusahaan adalah manajemen risiko hanya sebuah pendekatan, tetapi manajemen risiko merupakan strategi fleksibel yang dapat diterapkan untuk berbagai skala industri (Darmawi, 2005; Muslich, 2007; Djohanputro, 2008; Kountur, 2008).

Program manajemen risiko akan lebih efektif jika menjalankan empat langkah di dalam proses manajemen risiko (Djohanputro, 2008):

1. Mengenal pasti potensi kerugian
2. Mengevaluasi potensi kerugian
3. Memilih teknik tepat, atau mengkombinasikan beberapa teknik manangani ancaman kerugian
4. Menerapkan program penanganan kerugian yang mengancam.

Manajemen Resiko Keamanan Sistem Informasi ISO 27001

ISO/IEC 27001 adalah standar keamanan informasi (*information security*) yang diterbitkan pada Oktober 2005 oleh *International Organization for Standarization dan International Electrotechnical Commission* (IEC), standar ini menggantikan BS-77992:2002 (Sarno, 2009; Sarno dan Iffano, 2009). ISO (*International Organization for Standarzitation*) adalah pengembang terbesar di dunia standar international secara sukareIa. Standar international memberikan keamanan yang lebih spesifik, layanan yang baik, membantu industri Iebih efisien dan efektif. Dikembangkan melalui kesepakatan global, mereka membantu untuk mengatasi hambatan perdagangan internasional.

ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasionaI. Standar ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi atau *Information Security Management System*, biasa disebut ISMS, yang

doi: 10.14710/teknik.v39n2.15918

memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahan dalam usahanya untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi diperusahan berdasarkan "*best practice*" dalam pengamanan informasi.

Audit internal SMKI (internal ISMS audits) ISO 27001 adalah klausul 6 yang menjelaskan keharusan pelaksanaan internal audit secara berkala terhadap Objektif Kontrol, proses dan prosedur dari SMKI di dalam organisasi (Sarno, 2009; Sarno dan Iffano, 2009).

Sebagian besar organisasi menerapkan sertifikasi ISO 27001 agar mendapatkan nilai tambah bagi institusinya. Adopsi ISO 27001 dipengaruhi oleh peraturan nasional dan persyaratan organisasi (Ifinedo, 2014). Pengaruh budaya internal organisasi sangat dominan terhadap kinerja perlindungan keamanan sistem informasi. Hal ini disebabkan kepekaan staf bidang sistem informasi untuk melaksanakan tugas secara akurat tidak sama dalam satu organisasi (Ashenden dan Sasse, 2013). Selain itu, adopsi aturan dan regulasi ISO 27001 membutuhkan tingkat perubahan budaya organisasi (perilaku orang) dalam mendukung terlaksananya persyaratan keamanan sistem informasi secara berkelanjutan (Fomin dkk., 2008). Dampak budaya dan implementasi ISMS berbanding terbalik, di satu sisi, efek budaya bersifat *bottom-up* (Hui dan Triandis, 1985); sedangkan, implementasi ISMS bersifat *top-down*. Sebagai akibatnya, untuk mengubah perilaku staf / teknisi untuk memenuhi persyaratan keamanan sistem informasi organisasi menjadi sangat sulit (Ernest Chang dan Lin, 2007). Oleh karena itu, organisasi hendaknya mempertimbangkan kepraktisan aturan dan regulasi yang ditetapkan dengan budaya keamanan sistem informasi organisasi sebagai langkah penting dalam merancang ISO 27001 (Shojaie dkk., 2015), karena kerjasama antar pihak merupakan faktor penting untuk meningkatkan efisiensi ISO 27001 (Montesino dan Fenz, 2011).

Failure Mode Effect and Analysis (FMEA)

Menurut Stamatis (2003), FMEA merupakan sebuah metodologi yang digunakan untuk mengevaluasi kegagalan terjadi dalam sebuah sistem, desain, proses, atau pelayanan (*service*). Identifikasi kegagalan potensial dilakukan dengan cara pemberian nilai atau skor masing – masing moda kegagalan berdasarkan atas tingkat kejadian (*occurrence*), tingkat keparahan (*severity*), dan tingkat deteksi (*detection*) (Russomanno dkk., 1993; Chen, 1996; Huang dkk., 1999). Langkah-langkah dalam pembuatan FMEA adalah sebagai berikut:

1. Me-*review* proses.
2. *Brainstorming* risiko potensial.
3. Membuat daftar risiko, penyebab, dan efek potensial.
4. Menentukan tingkat *severity*, yaitu suatu penilaian tingkat keparahan dari keseriusan efek yang ditimbulkan dari mode-mode kegagalan (*failure mode*), menghitung seberapa besar dampak/ intensitas kejadian mempengaruhi output proses, maupun proses-proses selanjutnya.
5. Menentukan tingkat *occurrence*, yaitu suatu penilaian mengenai probabilitas frekuensi penyebab mekanisme kegagalan yang akan terjadi, sehingga dapat menghasilkan bentuk/mode kegagalan yang memberikan akibat tertentu selama masa penggunaan produk.
6. Menentukan tingkat *detection*, yaitu pengukuran terhadap kemampuan mengendalikan/ mengontrol kegagalan yang dapat terjadi.
7. Menghitung RPN (*Risk Priority Number*), yaitu hasil perkalian *severity* (S), *occurrence* (O), dan *detection* (D). Kriteria RPN ditunjukkan pada Tabel 1.

Tabel 1. Kriteria RPN

RPN	*Calculation Level*
0-25	Very Low
26-50	Low
51-75	Medium
76-100	High
>100	Very High

Pengumpulan dan Pengolahan Data

Pengumpulan data dilakukan dengan cara *indepth interview* pada penanggung jawab dan pelaksana SIFT dengan total responden tiga orang. Selain itu, pengambilan data sekunder juga dilakukan guna mendukung hasil wawancara. Data yang diperlukan pada penelitian ini adalah berbagai asset dan juga informasi terkait tugas, pokok, dan fungsi SIFT serta risiko dan kendala dalam pelaksanaan tupoksi.

Pengolahan data dilakukan menggunakan metode FMEA. Data-data dan informasi mengenai SIFT dihimpun menggunakan Kerangka ISO 27001 dan diidentifikasi berbagai macam asset dan informasi yang berhubungan dengan sistem informasi, kemudian di identifikasi tingkat Risiko yang kemungkinan dapat muncul sehingga dapat dianalisa menggunakan metode FMEA. Indeks penilaian pada asset berdasarkan ISO 27001 ada tiga jenis, yaitu *confidentially* (kerahasiaan), *integrity* (keamanan), dan *availability* (ketersediaan). Melalui pendekatan FMEA, risiko dinilai berdasarkan tiga hal, yaitu *severity* (keparahan yang ditimbulkan), *occurrence* (kemungkinan terjadi), dan *detection* (kesulitan dalam mendeteksi).

doi: 10.14710/teknik.v39n2.15918

3. Hasil dan Pembahasan

Identifikasi Asset

Asset adalah kekayaan (sumber daya) yang dimiliki oleh entitas bisnis yang bisa diukur secara jelas dapat berupa fisik maupun non fisik, asset disini adalah berbagai macam alat pendukung agar sistem informasi Fakultas Teknik dapat bekerja, seperti disajikan pada Tabel 2.

SIFT merupakan sebuah bagian dari Fakultas Teknik yang bertugas untuk mengelola berbagai macam Sistem informasi yang berada di Fakultas Teknik. Dari data hasil wawancara yang telah dilakukan pada bagian SIFT maka di identifikasilah asset yang mendukung kegiatan dari SIFT UNDIP agar tetap berjalan. Asset yang ada dibagi menjadi empat bagian, yaitu asset Informasi, Asset Hardware, asset Network, dan asset sumber daya manusia yang mendukung berjalanya Sistem informasi.

Penilaian ISO 27001

Berpijak dari Tabel 2, selanjutnya diidentifikasi berbagai macam risiko dan diklasifikasikan ke dalam beberapa golongan sesuai dengan hasil penilaian dampak pada asset SIFT. Hasil penilaian ancaman terhadap asset SIFT, disajikan pada Tabel 3.

Identifikasi Kerentanan Asset

Identifikasi kerentanan asset adalah identifikasi terhadap peluang kejadian-kejadian yang dapat menimbulkan munculnya ancaman terhadap asset sehingga mengganggu jalannya operasional Sistem Informasi. Kerentanan Asset SIFT dusajikan pada Tabel 4.

Analisis FMEA (Failure Mode Effect Analysis)

Tahapan selanjutnya setelah mengidentifikasi berbagai macam ancaman yang mengancam operasional segala asset pada SIFT, yaitu menganalisis dan mengetahui prioritas ancaman apa yang sebaiknya diutamakan. Selanjutnya, dapat diketahui bagaimana penanganan yang tepat dan pengambilan keputusan yang baik untuk mengatasi dan meminimalisir ancaman yang ada, tahapan ini menggunakan metode FMEA dengan menghitung RPN (*Risk Priority Number*). Penilaian FMEA disajikan pada Tabel 5.

Mitigasi Risiko

Setelah dilakukan penilaian dan prioritas ancaman yang muncul terhadap Sistem Informasi Fakultas Teknik Universitas Diponegoro menggunakan metode *Failure Mode Effect Analysis* dapat diketahui bahwa yang menjadi prioritas risiko, seperti disajikan pada Tabel 6.

Berdasarkan hasil penentuan prioritas risiko asset SIFT pada masing-masing kategori, mitigasi risiko yang diusulkan adalah sebagai berikut.

1. Ketergantungan terhadap karyawan

Hal ini memang menjadi perhatian dari pihak Sistem Informasi Fakultas Teknik, faktanya pengembang/*developer* dari Sistem Informasi Fakultas Teknik dipegang oleh beberapa orang tertentu. Tidak semua Pegawai di bagian Sistem Informasi Fakultas Teknik memiliki pengetahuan yang sama terhadap system, contohnya adalah pihak pelaksana SIFT adalah pihak yang mengelola operasional Sistem Informasi Fakultas Teknik sehari-hari, namun apabila ada problem pada sistem pihak pelaksana tidak dapat mengatasi secara langsung dikarenakan pelaksana SIFT bukan merupakan Pengembang dari system itu sendiri maka dari itu proses perbaikan sistem harus menunggu hingga *Developer* turun tangan untuk mengatasi masalah yang terjadi. Kejadian seperti ini dapat diminimalisir dengan adanya pelatihan-pelatihan atau *workshop* dan *brainstorming* terhadap berbagai pihak yang terkait dengan "Sistem Informasi Fakultas Teknik Universitas Diponegoro" sehingga tanpa pengembang, pelaksana masih dapat mengatasi problematika yang berhubungan langsung dengan sistem.

- *Fiber optic* tersambar petir

Fiber optic merupakan salah satu komponen yang menunjang berjalannya koneksi internet dari *Internet Service Provider* ke suatu jaringan lokal, dimusim penghujan risiko yang mengancam kegiatan operasional Sistem Informasi Fakultas Teknik adalah tersambar petirnya komponen Risiko ini dapat diantisipasi dengan membuat tiang-tiang penyangga petir di sekitar lokasi, atau dapat menggunakan jasa pemasangan oleh pihak ketiga yang sudah bersertifikasi untuk menginstalasi *Fiber Optic* sehingga lebih terjamin tidak akan terjadi masalah komponen terbakar.

- *Misconfiguration* jaringan ISP (*Internet Service Provider*)

Apabila terjadi miskonfigurasi antara ISP dan Sistem di SIFT makan akan menyebabkan koneksi internet tidak dapat terhubung ke jaringan, sehingga layanan SIFT akan terganggu dan tidak dapat digunakan. Ada beberapa alternatif untuk meminimalisir risiko ini, yaitu proses konfigurasi jaringan ISP didampingi dan dipantau secara langsung oleh pihak ISP sehingga proses instalasi jaringan dapat berjalan dengan baik dan tanpa mengalami kendala, selain itu pihak Fakultas Teknik juga dapat memperpanjang kontrak dengan ISP sehingga kegiatan konfigurasi hanya perlu dilakukan di awal dan tahun selanjutnya tidak perlu dilakukan perubahan.

doi: 10.14710/teknik.v39n2.15918

- Modifikasi data tanpa ijin

Risiko ini merupakan hal yang menjadi perhatian apabila berbicara tentang sistem informasi, yang terpenting didalam sebuah system adalah informasi yang akan digunakan oleh entitas-entitas yang berhubungan dengan sistem. Namun tidak ada sistem yang sempurna, akan ada celah yang dapat di eksploitasi untuk kepentingan oknum, maka dari itu risiko adanya data yang dimodifikasi tanpa izin akan selalu ada. Untuk meminimalisir risiko ini sebaiknya pihak SIFT selalu menyaring data yang akan dimasukan kedalam system, pastikan sesuai prosedur dan juga sudah mendapatkan izin dari pihak terkait. Selain itu perlu dilakukan. Untuk mencegah adanya oknum yang tidak bertanggung jawab untuk mengedit informasi dari dalam, perlu diadakanya Brainstorming dan juga penanaman sikap tanggung jawab oleh pegawai. Untuk mengantisipasi hal-hal yang tidak diinginkan dari luar sebaiknya pihak SIFT selalu memperketat keamanan yang ada di sistemnya sehingga tidak ada pihak luar yang dapat mengakses dan mengubah informasi tanpa izin.

- Kerusakan pada Komputer Server

Computer server yang rusak akan menyebabkan layanan sistem informasi tidak dapat digunakan. Untuk mengantisipasi risiko ini maka yang harus dilakukan adalah selalu melakukan maintenance rutin harian untuk pengecheckan performa dari komputer server, dan juga dilakukan pembersihan pada computer server tiap bulan hal ini akan membuat computer server akan terus bersih dan tidak ada debu yang merusak komponen, selain itu perlu dilakukan penggantian computer server 5 tahun sekali untuk menjaga agar performa dari server yang digunakan tetap maksimal.

- Mitigasi risiko

Mitigasi risiko yang dapat dilakukan untuk kategori asset people adalah berupa pelatihan terkait software-software yang dikembangkan. Ini bertujuan supaya karyawan tidak bergantung pada developer software ketika ada kendala di dalam implementasi SI. Mitigasi untuk kategori asset hardware dan network adalah dengan program *maintenance* secara berkala. Mitigasi untuk kategori asset informasi adalah dengan perubahan kode sandi (*password*) secara berkala dan pengembangan sistem keamanan yang lebih solid.

Tabel 2. Jenis Asset SIFT

Asset	Jenis	Keterangan
Information	Website FT	Berbagai situs yang dikelola oleh SIFT
	Data pegawai FT	Berisikan tentang informasi pegawai seperti data diri pegawai, kontak, dan informasi penting lainya.
	Data dokumentasi FT	Memuat tentang surat-surat yang masuk ke FT UNDIP
	Data mahasiswa	Informasi data diri mahasiswa, nilai, kontak, dan informasi penting lainya.
	Informasi organisasi	Berbagai informasi yang berkaitan dengan FT seperti struktur organisasi
	Data beasiswa	Informasi beasiswa yang diterima oleh mahasiswa FT UNDIP.
	Data pengabdian dan penelitian	Berbagai penelitian yang dilakukan oleh civitas akademi FT UNDIP
	Data alumni FT	Informasi data diri alumni, kontak, dll
	Data monitoring Kegiatan	Hasil monitoring berjalanya kegiatan di FT UNDIP
	Data Monitoring Inventaris	Informasi tentang inventaris FT UNDIP
	Data informasi perpustakaan	Berbagai data di perpustakaan FT UNDIP seperti buku, kumpulan skripsi, dll.
Hardware	Komputer Server	Server untuk sistem informasi
	CPU	Untuk operasional
	Networking & Communication Equipment	Hardware penunjang koneksi ke network
Network	Bandwith	Kapasitas Bandwith Internet server
	Jaringan Internet	Koneksi internet operasional Sistem Informasi
	Jaringan LAN	Jaringan LAN untuk akses data di Local Area
People	Pelaksana Sistem Informasi FT	Mengelola operasional SIFT
	Teknisi	Mengelola permasalahan mengenai SIFT
	Developer	Pengembangan SIFT

doi: 10.14710/teknik.v39n2.15918

Tabel 3. Penilaian Dampak Ancaman Terhadap Aset

Kategori Aset	Threat	Probabilitas Kejadian	Security Properties Loss Rate			Threat Score	Conversion Grade	Level
			Confidentiality	Integrity	Availability			
Informasi	Data mahasiswa tersebar	2	4	3	3	2,6	3	Medium
	Data karyawan tersebar	2	4	3	3	2,6	3	Medium
	Data tidak ter-back up	2	4	2	3	2,4	2	Low
	Modifikasi tanpa ijin	2	4	3	3	2,6	3	Medium
	Data corrupt	2	3	2	4	2,4	2	Low
	Penyalahgunaan informasi data	2	4	3	3	2,6	3	Medium
Hardware	Kerusakan computer server	2	3	3	4	2,6	3	Medium
	Tidak berfungsinya computer operasional	2	2	2	3	2,2	2	Low
	Fiber optic tersambar petir	3	2	2	4	2,8	3	Medium
	Server mati karena listrik padam	2	2	2	3	2,2	2	Low
	Performa hardwqre menurun karena usia / depresiasi	2	2	3	3	2,3	2	Low
	Storage data penuh	2	3	2	4	2,4	2	Low
	Pendingin server tidak berfungsi	2	2	2	2	2,0	2	Low
	Computer server berdebu	2	2	2	2	2,0	2	Low
	Kebakaran karena overheating komponen system	2	3	3	3	2,4	2	Low
Network	Misconfiguration jaringan dengan ISP	2	3	2	4	2,4	2	Low
	Serangan hacker	2	4	4	3	2,7	3	Medium
	Adanya gangguan gateway	3	2	2	3	2,6	3	Medium
	Gangguan pada data center SIFT	2	3	3	2	2,3	2	Low
	Bandwith melewati batas optimal	2	3	3	2	2,3	2	Low
People	Kebocoran informasi ke pihak luar	2	4	4	3	2,7	3	Medium
	Tidak loyal terhadap instansi	2	3	4	3	2,6	3	Medium
	Ketergantungan terhadap karyawan	3	4	3	3	3,2	3	Medium
	Maintenance terhambat	2	2	2	2	2,0	2	Low
	Miscommunication antar karyawan	3	2	3	2	2,6	3	Medium

Tabel 4. Kerentanan Asset

No	Kategori Kerentanan	Keterangan
1	Fisik	Pintu tidak terkunci / tanpa pengawasan; banyak barang mudah terbakar; ruangan dapat dilihat dari luar (kaca); ruangan dapat dimasuki siapapun
2	Hardware	*Outdated firmware;*sistem tidak terkonfigurasi dengan baik
3	Software	Antivirus tidak terupdate; aplikasi sulit dipahami; akses kontrol; keamanan *password*
4	Koneksi	tidak terenkripsi; terhubung ke berbagai *network;* tidak ada *filtering* tiap network segmen; protocol yang tidak perlu diizinkan terhubung
5	Manusia	Prosedur kurang jelas; informasi penting dapat diketahui; *maintenance* tidak rutin

doi: 10.14710/teknik.v39n2.15918

Tabel 5. Penilaian FMEA

Kategori Asset	Identifikasi Risiko	Severity	Occurrence	Detection	RPN	Level	Rank
People	ketergantungan terhadap karyawan	4	5	4	80.0	High	1
Hardware	fiber optik tersambar petir	4	3	5	60.0	Medium	2
Network	miskonfigurasi jaringan dengan ISP	5	3	4	60.0	Medium	3
Informasi	Modifikasi data tanpa izin	4	2	5	40.0	Low	4
Hardware	Kerusakan pada komputer server	5	2	4	40.0	Low	5
Informasi	Data corrupt	4	2	4	32.0	Low	6
Informasi	Penyalahgunaan informasi data	4	2	4	32.0	Low	7
Network	bandwith melewati batas optimal	3	5	2	30.0	Low	8
Network	gangguan pada data center SIFT	3	3	3	27.0	Low	9
People	miskomunikasi antar karyawan	3	3	3	27.0	Low	10
Network	serangan hacker	5	1	5	25.0	Very Low	11
People	kebocoran informasi ke pihak luar	5	1	5	25.0	Very Low	12
People	tidak loyal terhadap instansi	5	1	5	25.0	Very Low	13
Informasi	Data tidak terback up	4	2	3	24.0	Very Low	14
Hardware	Storage data penuh	4	2	3	24.0	Very Low	15
Informasi	Data mahasiswa tersebar	5	1	4	20.0	Very Low	16
Hardware	tidak berfungsinya komputer operasional	3	2	3	18.0	Very Low	17
Network	adanya gangguan gateway	3	2	3	18.0	Very Low	18
Hardware	server mati karena listrik padam	4	2	2	16.0	Very Low	19
Informasi	Data karyawan tersebar	5	1	3	15.0	Very Low	20
Hardware	kebakaran karena overheating komponen system	5	1	3	15.0	Very Low	21
Hardware	Performa hardware menurun karena usia	2	2	3	12.0	Very Low	22
Hardware	Pendingin server tidak berfungsi	3	2	2	12.0	Very Low	23
Hardware	Komputer Server berdebu	2	2	3	12.0	Very Low	24
People	maintenance terhambat	3	2	2	12.0	Very Low	25

Tabel 6. Prioritas Risiko

Kategori Asset	Identifikasi Risiko
People	ketergantungan terhadap karyawan
Hardware	fiber optik tersambar petir
Network	miskonfigurasi jaringan dengan ISP
Informasi	Modifikasi data tanpa izin
Hardware	Kerusakan pada komputer server

4. Kesimpulan

Hasil identifikasi risiko menggunakan metode *Failure Mode Effect Analysis* berbasis kerangka ISO 27001 menunjukkan bahwa lima prioritas risiko teratas pada SIFT UNDIP adalah ketergantungan kepada karyawan dalam kelangsungan operasional Sistem Informasi dengan nilai RPN = 80, fiber optic tersambar petir dengan nilai RPN = 60, misconfiguration ISP dengan nilai RPN = 60, modifikasi data tanpa ijin dengan nilai RPN = 40, dan kerusakan computer server dengan nilai RPN = 40.

Daftar Pustaka

Ashenden, D. and Sasse, A., (2013). CISOs and organisational culture: Their own worst enemy? Computers & Security, **39**, 396-405.

Astikasari, D.C., Chandra, S.E. (2018). Evaluation of Information Technology Governance with COBIT 5 in XYZ for ISO 27001:2013 Readiness. *International Journal of Engineering and Techniques*, **4**(4), 76-86.

Chazar, C. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO 27001:2005. *Jurnal Informasi*, **7**(2), 48-57.

Chen, H.C. (1996) *Failure Modes and Effects Analysis Training Manual*. Personal Communication, Hen Technology Inc., USA.

Ernest Chang, S. dan Lin, C.S., (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, **107**(3), 438-458.

Darmawi, H. (2005). *Manajemen Resiko*. Jakarta: Bumi Aksara.

Djohanputro, B. (2008). *Corporate Risks Management.* Jakarta: PPM.

Fajar, A.N., Christian, H., dan Girsang, A.S. (2018). Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. *IOP Conf. Series: Journal of Physics: Conf. Series 1090*. Fomin, V.V., Vries, H. dan Barlette, Y., (2008),

September. ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. In EUROMOT 2008 Conference, Nice, France.

Huang, G.Q., Nie, M., dan Mak, K.L. (1999) Web-Based Failure Mode and Effect Analysis. *Computers & Industrial Engineering*, **37**, 177-180.

Hui, C.H. dan Triandis, H.C., (1985). Measurement in cross-cultural psychology a review and comparison of strategies. Journal of cross-cultural psychology, **16**(2), 131-152.

Ifinedo, P., (2014). The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management*, **12**(2), 75.

Jakaria, D.A., Dirgahayu, R.T., Hendrik (2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. Yogyakarta. *Prosiding Seminar Nasional Aplikasi Teknologi Informasi* (SNATI) 2013, 15 Juni 2013.

Kountur, R. (2008). *Manajemen Resiko Operasional Perusahaan*. Jakarta: Pendidikan Pembinaan Manajemen.

Maingak, A.Z., Candiwan, Harsono, L.D. (2018). Information Security Assessment Using Iso/Iec 27001: 2013 Standard On Government Institution. *Trikonomika*, **17**(1), 28-37.

Milicevic, D. dan Goeken, M. (2010). Ontology-based Evaluation of ISO 27001. Conference Paper in IFIP Advances in Information and Communication Technology, November 2010.

Montesino, R. dan Fenz, S., (2011), August. Information security automation: how far can we go? In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on (pp. 280-285). IEEE.

Mufadhol (2009). Kerahasiaan dan Keutuhan Keamanan Data dalam Menjaga Integritas dan Keberadaan Informasi Data. *Jurnal Transformatika*, **6**(2), 80.

Muslich, M. (2007). *Manajemen Resiko Operasional*. Jakarta: Bumi Aksara.

Russomanno, D.J., Bonnell, R.D., Bowles, J.B. (1993) Functional Reasoning in a Failure Modes and Effects Analysis (FMEA) Expert-System. *Proceedings of the Annual Reliability and Maintainability Symposium*, Atlanta, 26-28 January 1993, 339-347.

Sarno, R. (2009). *Audit Sistem dan Teknologi Informasi*. Surabaya: ITS Press.

Sarno, R. dan Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*. Surabaya: ITS Press.

Shojaie, B., Federrath, H. and Saberi, I., (2015), The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. In Availability, Reliability and Security (ARES), 2015 10th International Conference on (pp. 159-167). IEEE.

Stamatis, D. H. (2003). Failure Mode and Effect Analysis: FMEA from Theory to Execution. Amer Society for Quality; 2 Rev Exp edition.

Stephanus (2014). Implementation Octave-S and ISO 27001 controls in Risk Management Information Systems. ComTech, **5**(2), 685-693.

Whitman, M.E. and Mattord, H. J. (2010). Management of Information Security. 3rd edition. Boston: Course Technology.

doi: 10.14710/teknik.v39n2.15918