Proses Review Jurnal Teknik Universitas Diponegoro

No	Uraian	Tanggal	Editor/Reviewer	Tanggapan Penulis	Ket
1	Submit	11-09-2017			Paper 1
2	Tanggapan dari reviewer	15-10-2017	▪ Bagian ini merupakan pernyataan dari peneliti lain atau bukan? Jika Bukan, maka argumentasinya harus didukung oleh penelitian lain yang relevan. Jika ini merupakan argumentasi penulis artikel ini, maka perlu justifikasi mengapa empat poin ini bisa muncul? ▪ Setidaknya dijelaskan jumlah responden yang disebut sebagai responden atau narasumber ▪ Posisi Tabel 5 seharusnya berada pada halaman selanjutnya dan perlu disesuaikan formatnya dengan standar Jurnal TEKNIK ▪ Singkatan perlu disebutkan karena di kalimat ikutan di bagian ini yang disebut Singkatannya	▪ Penambahan Referensi dari Dohanputro, 2008 ▪ Responden penelitian sebanyak 3 orang ▪ Format table telah diperbaiki ▪ Telah ditambahkan singkatan pada paragraph awal	Paper 2 dan Paper 3
3	Accept Submission	23-02-2019			Paper 4

TEKNIK

p-ISSN: 0852-1697
e-ISSN: 2460-9919

Jurnal Ilmiah Bidang Ilmu Kerekayasaan
Available online at: http://ejournal.undip.ac.id/index.php/teknik

#15918 Summary

Submission

Authors	Naniek Utami Handayani, Mochammad Agung Wibowo, Diana Puspita Sari, Yoga Satria, Akbar Romadhona Gifari
Title	Risk Assessment of Information System of Faculty of Engineering University Diponegoro Using Failure Mode Effect and Analysis Method based on F
Original file	15918-38536-1-SM.doc (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/38536/1) 11-09-2017
Supp. files	None
Submitter	Dr. Naniek Utami Utami Handayani (https://ejournal.undip.ac.id/index.php/teknik/user/email?to%5B%5D=Dr.%20Naniek%20Utami%20Utami%20Handayani%20%3Cnaniekh%40live.undip.ac.id%3E&redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Fir
Date submitted	September 11, 2017 - 10:49 AM
Section	Artikel
Editor	Editorial Jurnal Teknik (https://ejournal.undip.ac.id/index.php/teknik/user/email?to%5B%5D=Editorial%20Jurnal%20Teknik%20%3Cjteknik%40live.undip.ac.id%3E&redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2
Abstract Views	0

Status

Status	##mpgundip.submissions.published## Vol 39, No. 2 (2018): Desember 2018
Initiated	14-03-2019
Last modified	17-04-2020

Submission Metadata

Authors

Name	Naniek Utami Handayani (https://ejournal.undip.ac.id/index.php/teknik/user/email?redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2Fauthor%2Fsubmission%2F15918&to%5B%5D=Naniek%20Utami%20Handayani%
ORCID iD	http://orcid.org/0000-0001-7057-6126 (http://orcid.org/0000-0001-7057-6126)
Scopus ID	55292902200 (http://www.scopus.com/authid/detail.uri?authorId=55292902200)
URL	https://scholar.google.com/citations?user=wJT5zuEAAAAJ&hl=en (https://scholar.google.com/citations?user=wJT5zuEAAAAJ&hl=en)
Affiliation	Department of Industrial Engineering, Faculty of Engineering, Diponegoro University
Country	Indonesia
Bio Statement	–

Principal contact for editorial correspondence.

Name	Mochammad Agung Wibowo (https://ejournal.undip.ac.id/index.php/teknik/user/email?redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2Fauthor%2Fsubmission%2F15918&to%5B%5D=Mochammad%20Agung%20Wibow
Affiliation	Department of Civil Engineering, Faculty of Engineering, Diponegoro University
Country	Indonesia
Bio Statement	–

Name	Diana Puspita Sari (https://ejournal.undip.ac.id/index.php/teknik/user/email?redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2Fauthor%2Fsubmission%2F15918&to%5B%5D=Diana%20Puspita%20Sari%20%3(
Affiliation	Department of Industrial Engineering, Faculty of Engineering, Diponegoro University
Country	Indonesia
Bio Statement	–

Name	Yoga Satria (https://ejournal.undip.ac.id/index.php/teknik/user/email?redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2Fauthor%2Fsubmission%2F15918&to%5B%5D=Yoga%20Satria%20%3Cnaniekh%4
Affiliation	Department of Industrial Engineering, Faculty of Engineering, Diponegoro University
Country	Indonesia
Bio Statement	–

Name	Akbar Romadhona Gifari (https://ejournal.undip.ac.id/index.php/teknik/user/email?redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2Fauthor%2Fsubmission%2F15918&to%5B%5D=Akbar%20Romadhona%20Gifari%3
Affiliation	Department of Industrial Engineering, Faculty of Engineering, Diponegoro University

About This Journal

Focus and Scope (/index.php/teknik/about/editorialPolicies#focusAndScope)
Publication ethics (/index.php/teknik/about/editorialPolicies#custom-1)
Indexing (/index.php/teknik/about/editorialPolicies#custom-3)
p-ISSN: 0852-1697 (http://issn.pdii.lipi.go.id/issn.cgi?daftar&1180434000&1&&)
e-ISSN: 2460-9919 (http://u.lipi.go.id/1442566899)

For Authors

Author guidelines (/index.php/teknik/about/submissions#authorGuidelines)
How to submit (/index.php/teknik/about/submissions#onlineSubmissions)
Manuscript template (https://drive.google.com/file/d/170G8qvXShqScyASM0bVxE52Ls_KZ9k23/view?usp=sharing) (DOC)
Manuscript template (https://drive.google.com/file/d/1PVWWt0HUlkmIcAwdL-KfiKoHeAvoeyEfi/view?usp=sharing) (PDF)
Copyright Transfer (https://drive.google.com/file/d/1xM-zgidjlN3WAFkhaultZP6ZwlDeyZZJ/view?usp=sharing) (DOC)
Copyright Transfer (https://drive.google.com/file/d/1He5TERdM3CA-5AcB6PebuWyrQqOq_EgV/view?usp=sharing) (DOCX)
Copyright Transfer (https://drive.google.com/file/d/1_fkSdQMeY1W7KCgTA9Ij9Bo4a3Bpt96z/view?usp=sharing) (PDF)

Download articles

Vol 42 No 2 2021 (/index.php/teknik/issue/view/3056)
Vol 42 No 1 2021 (/index.php/teknik/issue/view/2975)
Vol 41 No 3 2020 (/index.php/teknik/issue/view/2913)
Vol 41 No 2 2020 (/index.php/teknik/issue/view/2876)
Vol 41 No 1 2020 (/index.php/teknik/issue/view/2798)

Faculty of Engineering

Diponegoro University

Jln. Prof. Soedarto, SH, Kampus UNDIP Tembalang, Semarang, Jawa Tengah, Indonesia. Postal Code: 50275; Ph. (024) 7460056, Fax: (024) 7460055, E-mail: jteknik@live.undip.ac.id

Country	Indonesia
Bio Statement	–

Title and 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
Abstract	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.
Notice	–
Original DOI	–

Indexing

Keywords	Information System; Risk assessment; ISO 27001 Framework; risk agent; FMEA; RPN
Language	id

Supporting Agencies / Funders

Agencies/Funders	–
Agencies/Funders Doi	–

References

References

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

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

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

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

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

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

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

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

TEKNIK(p-ISSN: 0852-1697;e-ISSN: 2460-9919),
is a scientific journal published by Fakultas Teknik, Universitas Diponegoro, Jln. Prof. Soedarto, SH, UNDIP Tembalang Campus, Semarang, Central Java, ZIP: 50275; Telp. (024)7460056, Fax: (024)7460055, E-mail: jteknik@live.undip.ac.id

TEKNIK

p-ISSN: 0852-1697
e-ISSN: 2460-9919

Jurnal Ilmiah Bidang Ilmu Kerekayasaan
Available online at: http://ejournal.undip.ac.id/index.php/teknik

#15918 Review

Summary (https://ejournal.undip.ac.id/index.php/teknik/author/submission/15918)
Review (https://ejournal.undip.ac.id/index.php/teknik/author/submissionReview/15918)
Editing (https://ejournal.undip.ac.id/index.php/teknik/author/submissionEditing/15918)

Submission

Authors	Naniek Utami Handayani, Mochammad Agung Wibowo, Diana Puspita Sari, Yoga Satria, Akbar Romadhona Gifari (https://ejournal.undip.ac.id/index.php redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2Fauthor%2FsubmissionReview%2F15918&to%5B%5D=%22Naniek%20Utami%20Har
Title	Risk Assessment of Information System of Faculty of Engineering University Diponegoro Using Failure Mode Effect and Analysis Method based on Fra
Section	Artikel
Editor	Editorial Jurnal Teknik (https://ejournal.undip.ac.id/index.php/teknik/user/email?redirectUrl=https%3A%2F%2Fejournal.undip.ac.id%2Findex.php%2Fteknik%2

Peer Review

Round 1

Review Version	15918-38545-2-RV.doc (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/38545/2) 13-09-2017
Initiated	13-09-2017
Last modified	17-10-2017
Uploaded file	Reviewer A 15918-39414-1-RV.doc (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/39414/1) 15-10-2017

Editor Decision

Decision	Accept Submission 23-02-2019
Notify Editor	(https://ejournal.undip.ac.id/index.php/teknik/author/emailEditorDecisionComment?articleId=15918) Editor/Author Email Record (javascript:openComments('https://ejournal.undip.ac.id/index.php/teknik/author/viewEditorDecisionComments/15918#7581');) 23-02-2019
Editor Version	15918-38597-1-ED.doc (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/38597/1) 13-09-2017 15918-38597-2-ED.doc (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/38597/2) 07-11-2017 15918-38597-3-ED.doc (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/38597/3) 25-02-2019
Author Version	15918-40036-1-ED.doc (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/40036/1) 06-11-2017 15918-40036-2-ED.docx (https://ejournal.undip.ac.id/index.php/teknik/author/downloadFile/15918/40036/2) 06-11-2017
Upload Author Version	Choose File No file chosen Upload

About This Journal

Focus and Scope (/index.php/teknik/about/editorialPolicies#fo
Publication ethics (/index.php/teknik/about/editorialPolicies#cu 1)
Indexing (/index.php/teknik/about/editorialPolicies#cu 3)
p-ISSN: 0852-1697 (http://issn.pdii.lipi.go.id/issn.cgi?daftar&1180434000&1&&)
e-ISSN: 2460-9919 (http://u.lipi.go.id/1442566899)

For Authors

Author guidelines (/index.php/teknik/about/submissions#authorGuidelines)
How to submit (/index.php/teknik/about/submissions#onlineSubmissions)
Manuscript template (https://drive.google.com/file/d/170G8qvXShoScvASM0bVxE52Ls_KZ9k23/view?usp=sharing) (DOC)
Manuscript template (https://drive.google.com/file/d/1PVWWt0HUlKmKVWpl-KfiKoHeAvoeyEfi/view?usp=sharing) (PDF)
Copyright Transfer (https://drive.google.com/file/d/1xM-zgidjlN3WAFkhaultZP6ZwlDeyZZJ/view?usp=sharing) (DOC)
Copyright Transfer (https://drive.google.com/file/d/1He5TERdM3CA-5AcB6PebuWyrQqOq_EgV/view?usp=sharing) (DOCX)
Copyright Transfer (https://drive.google.com/file/d/1_fkSdQMeY1W7RCgI47j9Bo4a3Bpt96z/view?usp=sharing) (PDF)

Download articles

Vol 42 No 2 2021 (/index.php/teknik/issue/view/3056)
Vol 42 No 1 2021 (/index.php/teknik/issue/view/2975)
Vol 41 No 3 2020 (/index.php/teknik/issue/view/2913)
Vol 41 No 2 2020 (/index.php/teknik/issue/view/2876)
Vol 41 No 1 2020 (/index.php/teknik/issue/view/2798)

Faculty of Engineering

Diponegoro University

Jln. Prof. Soedarto, SH, Kampus UNDIP Tembalang, Semarang, Jawa Tengah, Indonesia. Postal Code: 50275; Ph. (024) 7460056, Fax: (024) 7460055, E-mail: jteknik@live.undip.ac.id

(https://app.grammarly.com/)

Notifications

- View
  (https://ejournal.undip.ac.id/index.php/teknik/notification)
  (18 new)
- Manage
  (https://ejournal.undip.ac.id/index.php/teknik/notification/settings)

Journal Content

Search

Search Scope

All

Search

Browse

- By Issue
  (https://ejournal.undip.ac.id/index.php/teknik/issue/archive)
- By Author
  (https://ejournal.undip.ac.id/index.php/teknik/search/authors)
- By Title
  (https://ejournal.undip.ac.id/index.php/teknik/search/titles)
- Other Journals
  (https://ejournal.undip.ac.id/index.php/index/search)
- Categories
  (https://ejournal.undip.ac.id/index.php/index/search/categories)

Language (EN)

Select Language

ıttps://ejournal.undip.ac.id/index.php/teknik/user/setLocale/id_ID?
e=%2Findex.php%2Fteknik%2Fauthor%2FsubmissionReview%2F15918)

TEKNIK(p-ISSN: 0852-1697;e-ISSN: 2460-9919),
is a scientific journal published by Fakultas Teknik, Universitas Diponegoro, Jln. Prof. Soedarto, SH, UNDIP Tembalang Campus, Semarang, Central Java, ZIP: 50275; Telp. (024)7460056, Fax: (024)7460055, E-mail: jteknik@live.undip.ac.id

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

Teknik, 35 (1), 2014, 1-10

PENILAIAN RISIKO SISTEM INFORMASI FAKULTAS TEKNIK UNIVERSITAS DIPONEGORO MENGGUNAKAN *FRAMEWORK* ISO 27001

Naniek Utami Handayani[1*)], Mochammad Agung Wibowo[2], Diana Puspita Sari[1], Yoga Satria[1] dan 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

Sistem Informasi Fakultas Teknik merupakan asset penting dalam pengelolaan akademik maupun pendukung layanan akademik. Keamanan data/informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas teknologi informasi. Perlindungan terhadap keamanan sistem informasi di Fakultas Teknik Universitas Diponegoro masih perlu ditingkatkan. Hal ini ditunjukkan dengan pernah terjadinya kebocoran data mahasiswa yang berakibat penyalahgunaan informasi oleh pihak yang tidak berkepentingan. Tujuan penelitian ini adalah mengidentifikasi risiko, menganalisis manajemen keamanan sistem informasi, dan menentukan prioritas risiko yang disulkan kepada pengelola SIFT Universitas Diponegoro. Penelitian ini berbasis pada framework ISO 27001. Adapun metode yang digunakan adalah Failure Mode Effect and Analysis (FMEA). Berdasarkan hasil analisis yang dilakukan terdapat 25 risk agent yang dikategorikan menjadi empat jenis asset. Risiko tertinggi adalah risiko ketergantungan terhadap karyawan dengan nilai RPN sebesar 80 dan memiliki kategori High Level Risk..

Kata kunci*: Sistem Informasi, Keamanan, Kerangka ISO 27001, FMEA*

Abstract

[Risk Assessment of Information System of Faculty of Engineering University Diponegoro Using Framework ISO 27001] *The Information Systems of Faculty of Engineering is an important asset in academic management as well as supporting academic services. The security of information and electronic data becomes very important for companies using information technology facilities. The protection of security of information system in the Faculty of Engineering Diponegoro University is still need to be improve. This is shown the occurrence of leakage of student data resulting in misuse of information by unauthorized parties. The research aim is to identify risks, analyze security of information system management, and determine risk priority. This research is based on ISO 27001 framework. The research method is Failure Mode Effect and Analysis (FMEA). Based on the results of the analysis there are 25 risk agents are categorized into four types of assets. The highest risk is the risk of dependence on employees with an RPN value of 80 and has a High Level Risk category.*

Keywords*: Infromation System, Security, ISO 27001 Framework, FMEA*

[*] Naniek Utami Handayani
E-mail: naniekh@ft.undip.ac.id

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

Teknik, 35 (1), 2014, 1-10

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 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.

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 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. Metodologi 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:

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 industry Iebih efisien dan efktif. 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 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 practise” 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).

***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 dan pengambilan data sekunder. Data yang diperlukan pada penelitian ini adalah berbagai asset dan juga informasi dari pihak SIFT.

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).

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.

Tabel 2 Jenis Asset SIFT

Asset	Jenis	Keterangan
Information	Website Fakultas Teknik	Berbagai situs yang dikelola oleh SIFT
	Data pegawai Fakultas Teknik	Berisikan tentang informasi pegawai seperti data diri pegawai, kontak, dan informasi penting lainya.
	Data dokumentasi Fakultas Teknik	Memuat tentang surat-surat yang masuk ke Fakultas Teknik
	Data mahasiswa	Informasi data diri mahasiswa, nilai, kontak, dan informasi penting lainya.
	Informasi organisasi	Berisikan berbagai informasi yang berkaitan dengan Fakultas Teknik seperti struktur organisasi
	Data beasiswa	Informasi beasiswa yang diterima oleh mahasiswa Fakultas Teknik.
	Data pengabdian dan penelitian	Berbagai penelitian yang dilakukan oleh civitas akademi Fakultas Teknik Universitas Diponegoro
	Data alumni Fakultas Teknik	Informasi data diri alumni, kontak, dll
	Data monitoring Kegiatan	Hasil monitoring berjalanya kegiatan di Fakultas Teknik
	Data Monitoring Inventaris	Informasi tentang inventaris Fakultas Teknik
	Data informasi perpustakaan	Berbagai data di perpustakaan Fakultas Teknik 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 Fakultas Teknik	Mengelola operasional SIFT
	Teknisi	Mengelola permasalahan mengenai SIFT
	Developer	Pengembangan SIFT

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.

Tabel 3 Penilaian Dampak Ancaman Terhadap Asset

Kategori Asset	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 terback up	2	4	2	3	2,4	2	Low
	Modifikasi data tanpa izin	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 pada komputer server	2	3	3	4	2,6	3	Medium
	tidak berfungsinya komputer operasional	2	2	2	3	2,2	2	Low
	fiber optik tersambar petir	3	2	2	4	2,8	3	Medium
	server mati karena listrik padam	2	2	2	3	2,2	2	Low
	Performa hardware menurun karena usia	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
	Komputer Server berdebu	2	2	2	2	2,0	2	Low
	kebakaran karena overheating komponen sistem	2	3	3	3	2,4	2	Low
Network	miskonfigurasi 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	2	2	3	2,2	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
	miskomunikasi antar karyawan	3	2	3	2	2,6	3	Medium

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.

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 di pahami
		Akses Kontrol
		Kemanan *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

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.

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

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.

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

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

- 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.

- 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.

4. Kesimpulan

Berdasarkan analisis, kesimpulan yang dapat diambil dari penelitian ini sebagai berikut. Sistem Informasi Fakultas Teknik Universitas Diponegoro merupakan bagian dari Fakultas Teknik Universitas Diponegoro yang bertugas mengelola berbagai Sistem Informasi yang beroperasi di Fakultas Teknik UNDIP. SIFT bertanggung jawab dalam mengelola server baik untuk keperluan akademis hingga kepegawaian dari bagian internal fakultas hinggal eksternal fakultas. SIFT sebagai pengelola Sistem Informasi berpotensi mengalami berbagai macam ancaman yang mengganggu kegiatan operasional Sistem Informasi. Berpijak dari hasil identifikasi risiko dengan menggunakan kerangka ISO 27001 dan metode *Failure Mode Effect Analysis* dapat diketahui bahwa prioritas risiko pada SIFT adalah

ketergantungan kepada karyawan dalam kelangsungan operasional Sistem Informasi, fiber optic tersambar petir, misconfiguration ISP, modifikasi data tanpa ijin, dan kerusakan computer server. Mitigasi risiko yang dapat dilakukan antara lain sebagai berikut. Untuk kategori asset people dapat dilakukan pelatihan terkait software-software yang dikembangkan agar karyawan tidak bergantung terhadap developer software jika terjadi kendala di dalam implementasi SI. Untuk kategori asset hardware dan network dapat dilakukan dengan adanya program *maintenance* secara berkala. Sementara itu, untuk kategori asset informasi dapat dilakukan dengan perubahan kode sandi (*password*) secara berkala dan pengembangan sistem keamanan yang lebih solid.

Daftar Pustaka

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

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

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

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

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

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: PT. Bumi Aksara.

Russomanno, D.J., Bonnell, R.D. dan 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 & Teknologi Informasi. Surabaya: ITS Press

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

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

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

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

Teknik, 35 (1), 2014, 1-10

PENILAIAN RISIKO SISTEM INFORMASI FAKULTAS TEKNIK UNIVERSITAS DIPONEGORO MENGGUNAKAN *FRAMEWORK* ISO 27001

Abstrak

Sistem Informasi Fakultas Teknik merupakan asset penting dalam pengelolaan akademik maupun pendukung layanan akademik. Keamanan data/informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas teknologi informasi. Perlindungan terhadap keamanan sistem informasi di Fakultas Teknik Universitas Diponegoro masih perlu ditingkatkan. Hal ini ditunjukkan dengan pernah terjadinya kebocoran data mahasiswa yang berakibat penyalahgunaan informasi oleh pihak yang tidak berkepentingan. Tujuan penelitian ini adalah mengidentifikasi risiko, menganalisis manajemen keamanan sistem informasi, dan menentukan prioritas risiko yang disulkan kepada pengelola SIFT Universitas Diponegoro. Penelitian ini berbasis pada framework ISO 27001. Adapun metode yang digunakan adalah Failure Mode Effect and Analysis (FMEA). Berdasarkan hasil analisis yang dilakukan terdapat 25 risk agent yang dikategorikan menjadi empat jenis asset. Risiko tertinggi adalah risiko ketergantungan terhadap karyawan dengan nilai RPN sebesar 80 dan memiliki kategori High Level Risk..

Kata kunci: *Sistem Informasi, Keamanan, Kerangka ISO 27001, FMEA*

Abstract

[Risk Assessment of Information System of Faculty of Engineering University Diponegoro Using Framework ISO 27001] *The Information Systems of Faculty of Engineering is an important asset in academic management as well as supporting academic services. The security of information and electronic data becomes very important for companies using information technology facilities. The protection of security of information system in the Faculty of Engineering Diponegoro University is still need to be improve. This is shown the occurrence of leakage of student data resulting in misuse of information by unauthorized parties. The research aim is to identify risks, analyze security of information system management, and determine risk priority. This research is based on ISO 27001 framework. The research method is Failure Mode Effect and Analysis (FMEA). Based on the results of the analysis there are 25 risk agents are categorized into four types of assets. The highest risk is the risk of dependence on employees with an RPN value of 80 and has a High Level Risk category.*

Keywords: *Infromation System, Security, ISO 27001 Framework, FMEA*

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 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.

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 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. Metodologi 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:

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 industry Iebih efisien dan efktif. 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 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 practise" 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).

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.

Commented [fh1]: Bagian ini merupakan pernyataan dari peneliti lain atau bukan? Jika Bukan, maka argumentasinya harus didukung oleh penelitian lain yang relevan. Jika ini merupakan argumentasi penulis artikel ini, maka perlu justifikasi mengapa empat poin ini bisa muncul?

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 dan pengambilan data sekunder. Data yang diperlukan pada penelitian ini adalah berbagai asset dan juga informasi dari pihak SIFT.

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).

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.

Tabel 2 Jenis Asset SIFT

Asset	Jenis	Keterangan
Information	Website Fakultas Teknik	Berbagai situs yang dikelola oleh SIFT
	Data pegawai Fakultas Teknik	Berisikan tentang informasi pegawai seperti data diri pegawai, kontak, dan informasi penting lainya.
	Data dokumentasi Fakultas Teknik	Memuat tentang surat-surat yang masuk ke Fakultas Teknik
	Data mahasiswa	Informasi data diri mahasiswa, nilai, kontak, dan informasi penting lainya.
	Informasi organisasi	Berisikan berbagai informasi yang berkaitan dengan Fakultas Teknik seperti struktur organisasi
	Data beasiswa	Informasi beasiswa yang diterima oleh mahasiswa Fakultas Teknik.
	Data pengabdian dan penelitian	Berbagai penelitian yang dilakukan oleh civitas akademi Fakultas Teknik Universitas Diponegoro
	Data alumni Fakultas Teknik	Informasi data diri alumni, kontak, dll
	Data monitoring Kegiatan	Hasil monitoring berjalanya kegiatan di Fakultas Teknik
	Data Monitoring Inventaris	Informasi tentang inventaris Fakultas Teknik
	Data informasi perpustakaan	Berbagai data di perpustakaan Fakultas Teknik 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 Fakultas Teknik	Mengelola operasional SIFT
	Teknisi	Mengelola permasalahan mengenai SIFT
	Developer	Pengembangan SIFT

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.

Commented [fh2]: Setidaknya dijelaskan jumlah responden yang disebut sebagai responden atau narasumber

Tabel 3 Penilaian Dampak Ancaman Terhadap Asset

Kategori Asset	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 terback up	2	4	2	3	2,4	2	Low
	Modifikasi data tanpa izin	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 pada komputer server	2	3	3	4	2,6	3	Medium
	tidak berfungsinya komputer operasional	2	2	2	3	2,2	2	Low
	fiber optik tersambar petir	3	2	2	4	2,8	3	Medium
	server mati karena listrik padam	2	2	2	3	2,2	2	Low
	Performa hardware menurun karena usia	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
	Komputer Server berdebu	2	2	2	2	2,0	2	Low
	kebakaran karena overheating komponen sistem	2	3	3	3	2,4	2	Low
Network	miskonfigurasi 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	2	2	3	2,2	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
	miskomunikasi antar karyawan	3	2	3	2	2,6	3	Medium

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.

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 di pahami
		Akses Kontrol
		Kemanan *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

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.

Tabel 5 Penilaian FMEA

Commented [fh3]: Posisi Tabel 5 seharusnya berada pada halaman selanjutnya dan perlu disesuaikan formatnya dengan standar Jurnal TEKNIK

Commented [fh4R3]:

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

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.

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

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

- 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.

- 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.

4. Kesimpulan

Berdasarkan analisis, kesimpulan yang dapat diambil dari penelitian ini sebagai berikut. Sistem Informasi Fakultas Teknik Universitas Diponegoro merupakan bagian dari Fakultas Teknik Universitas Diponegoro yang bertugas mengelola berbagai Sistem Informasi yang beroperasi di Fakultas Teknik UNDIP. SIFT bertanggung jawab dalam mengelola server baik untuk keperluan akademis hingga kepegawaian dari bagian internal fakultas hinggal eksternal fakultas. SIFT sebagai pengelola Sistem Informasi berpotensi mengalami berbagai macam ancaman yang mengganggu kegiatan operasional Sistem Informasi. Berpijak dari hasil identifikasi risiko dengan menggunakan kerangka ISO 27001 dan metode *Failure Mode Effect Analysis* dapat diketahui bahwa prioritas risiko pada SIFT adalah ketergantungan kepada karyawan dalam kelangsungan operasional Sistem Informasi, fiber optic tersambar petir, misconfiguration ISP, modifikasi data tanpa ijin, dan kerusakan computer server. Mitigasi risiko yang dapat dilakukan antara lain sebagai berikut. Untuk kategori asset people dapat dilakukan pelatihan terkait software-software yang dikembangkan agar karyawan tidak bergantung terhadap developer software jika terjadi kendala di dalam implementasi SI. Untuk kategori asset hardware dan network dapat dilakukan dengan adanya program *maintenance* secara berkala. Sementara itu, untuk kategori asset informasi dapat dilakukan dengan perubahan kode sandi (*password*) secara berkala dan pengembangan sistem keamanan yang lebih solid.

Daftar Pustaka

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

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

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

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

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

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: PT. Bumi Aksara.

Russomanno, D.J., Bonnell, R.D. dan Bowles, J.B. (1993) Functional Reasoning in a Failure Modes and Effects Analysis (FMEA) Expert-System. Proceedings of the Annual Reliability and

Commented [fh5]: Singkatan perlu disebutkan karena di kalimat ikutan di bagian ini yang disebut Singkatannya

Commented [fh6R5]:

Maintainability Symposium, Atlanta, 26-28 January 1993, 339-347.

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

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

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

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

1. Manuskrip/Artikel yang sudah direvisi dalam MS Word
2. Jawaban-jawaban atas komentar dari Reviewer dalam file terpisah, jelaskan juga letaknya dimana perbaikannya (halaman, kolom, baris).
3.

No	Pertanyaan	Jawaban	Letak
1	Bagian ini merupakan pernyataan dari peneliti lain atau bukan? Jika Bukan, maka argumentasinya harus didukung oleh penelitian lain yang relevan. Jika ini merupakan argumentasi penulis artikel ini, maka perlu justifikasi mengapa empat poin ini bisa muncul?	Telah ditambahkan referensi Djohanputro, 2008 Program manajemen risiko akan lebih efektif jika menjalankan empat langkah di dalam proses manajemen risiko (**Djohanputro, 2008**):	Hal 2 paragraf 4
2	Setidaknya dijelaskan jumlah responden yang disebut sebagai responden atau narasumber	Pengumpulan data dilakukan dengan cara *indepth interview* pada penanggung jawab dan pelaksana SIFT dengan total responden adalah **3 orang**.	Hal 3 paragraf 1
3	Posisi Tabel 5 seharusnya berada pada halaman selanjutnya dan perlu disesuaikan formatnya dengan standar Jurnal TEKNIK	Seluruh format table telah diperbaiki sesuai template jurnal teknik Tabel 1 s.d. table 6	
	Singkatan perlu disebutkan karena di kalimat ikutan di bagian ini yang disebut Singkatannya	Telah ditambahkan singkatan pada paragraph awal	Hal 6, bagian kesimpulan, paragraph 1

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

Teknik, 35 (1), 2014, 1-10

PENILAIAN RISIKO SISTEM INFORMASI FAKULTAS TEKNIK UNIVERSITAS DIPONEGORO MENGGUNAKAN *FRAMEWORK* ISO 27001

Abstrak

Sistem Informasi Fakultas Teknik merupakan asset penting dalam pengelolaan akademik maupun pendukung layanan akademik. Keamanan data/informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas teknologi informasi. Perlindungan terhadap keamanan sistem informasi di Fakultas Teknik Universitas Diponegoro masih perlu ditingkatkan. Hal ini ditunjukkan dengan pernah terjadinya kebocoran data mahasiswa yang berakibat penyalahgunaan informasi oleh pihak yang tidak berkepentingan. Tujuan penelitian ini adalah mengidentifikasi risiko, menganalisis manajemen keamanan sistem informasi, dan menentukan prioritas risiko yang disulkan kepada pengelola SIFT Universitas Diponegoro. Penelitian ini berbasis pada framework ISO 27001. Adapun metode yang digunakan adalah Failure Mode Effect and Analysis (FMEA). Berdasarkan hasil analisis yang dilakukan terdapat 25 risk agent yang dikategorikan menjadi empat jenis asset. Risiko tertinggi adalah risiko ketergantungan terhadap karyawan dengan nilai RPN sebesar 80 dan memiliki kategori High Level Risk..

Kata kunci: *Sistem Informasi, Keamanan, Kerangka ISO 27001, FMEA*

Abstract

[Risk Assessment of Information System of Faculty of Engineering University Diponegoro Using Framework ISO 27001] *The Information Systems of Faculty of Engineering is an important asset in academic management as well as supporting academic services. The security of information and electronic data becomes very important for companies using information technology facilities. The protection of security of information system in the Faculty of Engineering Diponegoro University is still need to be improve. This is shown the occurrence of leakage of student data resulting in misuse of information by unauthorized parties. The research aim is to identify risks, analyze security of information system management, and determine risk priority. This research is based on ISO 27001 framework. The research method is Failure Mode Effect and Analysis (FMEA). Based on the results of the analysis there are 25 risk agents are categorized into four types of assets. The highest risk is the risk of dependence on employees with an RPN value of 80 and has a High Level Risk category.*

Keywords: *Infromation System, Security, ISO 27001 Framework, FMEA*

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 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.

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. Metodologi 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 industry Iebih efisien dan efktif. 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 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 practise" 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).

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

Commented [fh1]: Bagian ini merupakan pernyataan dari peneliti lain atau bukan? Jika Bukan, maka argumentasinya harus didukung oleh penelitian lain yang relevan. Jika ini merupakan argumentasi penulis artikel ini, maka perlu justifikasi mengapa empat poin ini bisa muncul?

Commented [t2R1]: Penambahan Referensi dari Dohanputro, 2008

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 adalah 3 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).

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.

Tabel 2 Jenis Asset SIFT

Asset	Jenis	Keterangan
Informasi	Website Fakultas Teknik	Berbagai situs yang dikelola oleh SIFT
	Data pegawai Fakultas Teknik	Berisikan tentang informasi pegawai seperti data diri pegawai, kontak, dan informasi penting lainya.
	Data dokumentasi Fakultas Teknik	Memuat tentang surat-surat yang masuk ke Fakultas Teknik
	Data mahasiswa	Informasi data diri mahasiswa, nilai, kontak, dan informasi penting lainya.
	Informasi organisasi	Berisikan berbagai informasi yang berkaitan dengan Fakultas Teknik seperti struktur organisasi
	Data beasiswa	Informasi beasiswa yang diterima oleh mahasiswa Fakultas Teknik.
	Data pengabdian dan penelitian	Berbagai penelitian yang dilakukan oleh civitas akademi Fakultas Teknik Universitas Diponegoro
	Data alumni Fakultas Teknik	Informasi data diri alumni, kontak, dll
	Data monitoring Kegiatan	Hasil monitoring berjalanya kegiatan di Fakultas Teknik
	Data Monitoring Inventaris	Informasi tentang inventaris Fakultas Teknik
	Data informasi perpustakaan	Berbagai data di perpustakaan Fakultas Teknik 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 Fakultas Teknik	Mengelola operasional SIFT
	Teknisi	Mengelola permasalahan mengenai SIFT
	Developer	Pengembangan SIFT

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

Commented [fh3]: Setidaknya dijelaskan jumlah responden yang disebut sebagai responden atau narasumber

Commented [t4R3]: Responden penelitian sebanyak 3 orang

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.

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	3	2	3	2	2,6	3	Medium

	antar karyawan

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 di pahami Akses Kontrol Kemanan *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

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

Commented [fh5]: Posisi Tabel 5 seharusnya berada pada halaman selanjutnya dan perlu disesuaikan formatnya dengan standar Jurnal TEKNIK

Commented [fh6R5]:

Commented [t7R5]: Format table telah diperbaiki

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.

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

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

- 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.

- 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.

4. Kesimpulan

Berdasarkan analisis, kesimpulan yang dapat diambil dari penelitian ini sebagai berikut. Sistem Informasi Fakultas Teknik (SIFT) Universitas Diponegoro merupakan bagian dari Fakultas Teknik Universitas Diponegoro yang bertugas mengelola berbagai Sistem Informasi yang beroperasi di Fakultas Teknik UNDIP. SIFT bertanggung jawab dalam mengelola server baik untuk keperluan akademis hingga kepegawaian dari bagian internal fakultas hinggal eksternal fakultas. SIFT sebagai pengelola Sistem Informasi berpotensi mengalami berbagai macam ancaman yang mengganggu kegiatan operasional Sistem Informasi. Berpijak dari hasil identifikasi risiko dengan menggunakan kerangka ISO 27001 dan metode *Failure Mode Effect Analysis* dapat diketahui bahwa prioritas

Commented [fh8]: Singkatan perlu disebutkan karena di kalimat ikutan di bagian ini yang disebut Singkatannya

Commented [fh9R8]:

Commented [t10R8]: Telah ditambahkan singkatan pada paragraph awal

risiko pada SIFT adalah ketergantungan kepada karyawan dalam kelangsungan operasional Sistem Informasi, fiber optic tersambar petir, misconfiguration ISP, modifikasi data tanpa ijin, dan kerusakan computer server. Mitigasi risiko yang dapat dilakukan antara lain sebagai berikut. Untuk kategori asset people dapat dilakukan pelatihan terkait software-software yang dikembangkan agar karyawan tidak bergantung terhadap developer software jika terjadi kendala di dalam implementasi SI. Untuk kategori asset hardware dan network dapat dilakukan dengan adanya program *maintenance* secara berkala. Sementara itu, untuk kategori asset informasi dapat dilakukan dengan perubahan kode sandi (*password*) secara berkala dan pengembangan sistem keamanan yang lebih solid.

Daftar Pustaka

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

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

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

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

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

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: PT. Bumi Aksara.

Russomanno, D.J., Bonnell, R.D. dan 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 & Teknologi Informasi. Surabaya: ITS Press

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

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

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

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

TEKNIK, 39 (2), 2018, App. 1-5

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 & Mattord, 2010).

Keamanan data/informasi secara langsung maupun tidak langsung dapat mempertahankan kelangsungan proses bisnis, mengurangi risiko, dan bahkan mendorong meningkatnya peluang bisnis. Ancaman dan risiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data/informasi menjadi alasan disusunnya standard sistem manajemen

doi: 10.14710/teknik.v39n1.xxxxxx

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.

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. Metodologi 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 & 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 industry Iebih efisien dan efktif. 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 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 & Iffano, 2009).

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, Bonnel, & Bowles, 1993; Chen, 1996; Huang, Nie & Mak, 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/

doi: 10.14710/teknik.v39n2.15918

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).

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

doi: 10.14710/teknik.v39n2.15918

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.

- 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.

doi: 10.14710/teknik.v39n2.15918

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

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

doi: 10.14710/teknik.v39n2.15918

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 di pahami; Akses Kontrol; Kemanan *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

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.

doi: 10.14710/teknik.v39n2.15918

Daftar Pustaka

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

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

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

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

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

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

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

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

doi: 10.14710/teknik.v39n2.15918

Re: [TEKNIK] Copyediting Review Request

Naniek Utami Handayani <naniekh@yahoo.com> 7 November 2017 pukul 13.43
Kepada: Editorial Jurnal Teknik <jteknik@live.undip.ac.id>

Ysh. Editor Jurnal Teknik

Assalamu'alaikum wr wb

Mohon info, paper tersebut untuk terbitan tahun berapa nggih? Kok diatas tertulis Nopember 2016? Bukannya 2017 ya?
Terima kasih

Wassalamu'alaikum wr wb

2017-11-07 10:41 GMT+07:00 Editorial Jurnal Teknik <jteknik@live.undip.ac.id>:

> Dr. Naniek Utami Handayani:
>
> Your submission "PENILAIAN RISIKO SISTEM INFORMASI FAKULTAS TEKNIK UNIVERSITAS DIPONEGORO MENGGUNAKAN FRAMEWORK ISO 27001" for Teknik has been through the first step of copyediting, and is available for you to review by following these steps.
>
> 1. Click on the Submission URL below.
> 2. Log into the journal and click on the File that appears in Step 1.
> 3. Open the downloaded submission.
> 4. Review the text, including copyediting proposals and Author Queries.
> 5. Make any copyediting changes that would further improve the text.
> 6. When completed, upload the file in Step 2.
> 7. Click on METADATA to check indexing information for completeness and accuracy.
> 8. Send the COMPLETE email to the editor and copyeditor.
>
> Submission URL:
> http://ejournal.undip.ac.id/index.php/teknik/author/submissionEditing/15918
> Username: naniekh
>
> This is the last opportunity to make substantial copyediting changes to the submission. The proofreading stage, that follows the preparation of the galleys, is restricted to correcting typographical and layout errors.
>
> If you are unable to undertake this work at this time or have any questions, please contact me. Thank you for your contribution to this journal.
>
> Editorial Jurnal Teknik
> Editorial Office Jurnal Teknik, Fakultas Teknik, Universitas Diponegoro
> jteknik@live.undip.ac.id
>
> _____
> TEKNIK
> http://ejournal.undip.ac.id/index.php/teknik
> http://jteknik.undip.ac.id