JUSTIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989
DOI: 10.26418/justin.v10i4.48977
Vol. 10, No. 4, Oktober 2022

Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto

Moniq Kartika Sari [a1], Yudha Saintika[a2], Wahyu Adi Prabowo[b3]
[a]*Program Studi S1 Sistem Informasi, Fakultas Informatika, Institut Teknologi Telkom Purwokerto*
[b]*Program Studi S1 Teknik Informatika, Fakultas Informatika, Institut Teknologi Telkom Purwokerto*
Jl. DI Panjaitan No.128, Karangreja, Purwokerto Kidul, Jawa Tengah, Indonesia
[1]17103097@ittelkom-pwt.ac.id
[2]yudha@ittelkom-pwt.ac.id
[3]wahyuadi@ittelkom-pwt.ac.id

Abstrak

Perencanaan manajemen risiko keamanan informasi bagi suatu perusahaan sangatlah penting untuk mengukur tingkat kesiapan organisasi dalam menghadapi ancaman yang mungkin bisa terjadi. Perencanaan manajemen risiko keamanan informasi pada Kampus IT Telkom Purwokerto juga sangat penting, karena untuk mengetahui keamanan data dan informasi yang ada di kampus tersebut, baik data Dosen, karyawan ataupun mahasiswa. dalam menyusun perencanaan manajemen risiko di IT Telkom Purwokerto terkait Keamanan Informasi standar yang digunakan adalah Indeks Keamanan Informasi (KAMI) yang sesuai dengan standar ISO 27001 yang merupakan salah satu Standar Manajemen Keamanan Informasi (SMKI) untuk organisasi atau perusahaan. Kegunaan SMKI yaitu untuk melindungi dan menjaga Kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*) dan Ketersediaan (*Availability*) Informasi dan untuk mengendalikan dan mengelola risiko keamanan informasi. tahapan dalam menyusun manajeen risiko keamanan informasi yaitu Identifikasi Aset, Menghitung Nilai Aset, Identifikasi Ancamaan dan Kelemahan Aset, Menghitung Nilai Risiko, Analisa Dampak Bisnis (BIA), dan yang terakhir Menentukan Level Risiko dari aset. Hasil dari penelitian ini nantinya yaitu berupa Dokumen *Risk Profile* yang berisi Risiko yang ada di ITTP dan langkah-langkah penanganan dari Risiko tersebut.
Kata kunci: Keamanan Informasi (KAMI), Risk Profile, ISO 27001, Manajemen Risiko

Preparation of Information Security Risk Management with ISO 27001 Standard Case study Telkom Purwokerto Institute of Technology

Abstract

Information security risk management planning for a company is very important to measure the level of organizational readiness in dealing with threats that may occur. Information security risk management planning at the IT Telkom Purwokerto Campus is also very important, because it is to determine the security of data and information on the campus, whether data from lecturers, employees or students. In preparing risk management planning at IT Telkom Purwokerto related to Information Security the standard used is the Information Security Index (KAMI) which is in accordance with the ISO 27001 standard which is one of the Information Security Management standards for organizations or companies. The use of the ISMS is to protect and maintain the Confidentiality, Integrity and Availability of Information and to control and manage information security risks. the stages in compiling information security risk management are Asset Identification, Calculating Asset Value, Identification of Asset Threats and Weaknesses, Calculating Risk Value, Business Impact Analysis (BIA), and finally determining the Risk Level of the asset. The results of this research will be in the form of a Risk Profile Document that contains the Risks in ITTP and the steps for handling these risks.
Keywords: Information Security,Risk Profile, ISO 27001,Risk Management

I. PENDAHULUAN

Secara umum, Risiko adalah dampak positif atau negatif yang mungkin terjadi dari ketidakpastian dengan adanya tujuan. Artinya dalam mencapai suatu tujuan pasti terdapat resiko dan ketidakpastian yang mungkin terjadi. Terkadang tujuan itu berjalan sesuai dengan keinginkan namun tidak menutup kemungkinan juga dalam mencapai tujuan akan terdapat suatu ketidakpastian [1]. Manajemen Risiko adalah proses identifikasi, pengukuran, dan kontrol keuangan dari sebuah risiko yang mengancam aset dan

bisa mengakibatkan kerugian penghasilan dari sebuah perusahaan atau proyek *(Smith, 1990)*[2]. Penggunaan Teknologi Informasi baik *software* ataupun *hardware* untuk keperluan institusi di IT Telkom Purwokerto semakin meningkat. Data yang diperolehpun semakin banyak, baik data civitas akademika, data calon mahasiswa baru maupun data yang lainnya. Data yang didapatkan tersebut merupakan data privasi atau *sensitive* yang harus dijaga dengan aman. Dengan demikian Manajemen Risiko Keamanan Informasi sangat diperlukan bagi IT Telkom Purwokerto [3].

Namun dalam pengelolaan resiko keamanan informasi, IT Telkom Purwokerto belum mempunyai acun yang jelas terkait standar keamanan informasi hal tersebut dikatakan dalam dokuman IT Master Plan IT Telkom Purwokerto tahun 2019-2023. Dengan tidak adanya standar keamana informasi akan berdampak pada informasi atau data yang tidak terjaga kerahasiaannya (*Confidentially),* tidak utuh (*Integrity)* dan tidak selalu tersedia (*Availability)*[4]. Dalam penyusunan Manajemen risiko keamanan informasi ini menggunakan indeks Keamanan Informasi (KAMI) yang sesuai dengan ISO 27001. Selain itu juga terdapat indeks KAMI dimana Indeks KAMI ini merupakan sebuah aplikasi yang dapat membantu dalam melakukan proses *Assessment* dan juga proses Evaluasi terhadap keamanan informasi di suatu organisasi untuk mengukur tingkat kesiapan (kelengkapan dan kematangan) keamanan informasi yang akan diterapkan dengan berdasarkan pada kriteria SNI ISO/IEC 27001. Selain itu juga terdapat dukungan dari Pemerintah terkait Imeplementasi TI seperti misalnya Peraturan menteri Kominfo No.41 Tahun 2007 **:** Tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional[5]. Hasil *Assessment* di IT Telkom menunjukan nilai tidak layak yaitu pada nilai 144 [6].

Risiko juga merupakan kombinasi dari konsekuensi dan probabilitas dari adanya suatu peristiwa [1]. Ada beberapa kategori risiko yaitu Risiko Spekulatif adalah suatu keadaan yang dapat memberikan keuntungan dan kerugian bagi perusahaan yang menghadapinya. Dan Risiko Murni adalah sesuatu yang tidak mungin menguntungkan dan tidak terjadi apa-apa atau hanya dapat merugikan[10]. Perusahaan mengidentifikasi dan membedakan ancaman kecil atau besar dengan menggunakan teknik manajemen risiko dimana yang hasil akhirnya akan merekomendasikan keputusan untuk menghindari, mentransfer, memitigasi atau menerima risiko [11]. Dalam melakukan *assessment* dibantu dengan menggunakan alat yaitu Indek Keamanan Informasi (KAMI). Alat tersebut disusun oleh Badan Siber dan Sandi Negara (BSSN) untuk memudahkan pengguna dalam memahami standar ISO. Indeks Keamanan Informasi (KAMI) merupakan sebuah aplikasi yang dapat membantu dalam melakukan proses *Assessment* dan juga proses Evaluasi terhadap keamanan informasi di suatu organisasi untuk mengukur tingkat kesiapan (kelengkapan dan kematangan) keamanan informasi yang akan diterapkan dengan berdasarkan pada kriteria SNI ISO/IEC 27001 yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Aspek Teknologi dan Suplemen [6].

Manajemen Risiko meruapakan proses menghilangkan risiko yang tidak dapat diterima dengan mengidentifikasi, menganalisis, mengevaluasi, mengendalikan, menghindari dan meninimalkan risiko. langkah-langkah dalam manajemen risiko yaitu identifikasi aset, identifikasi risiko, identifikasi ancaman *(Threat),* identifikasi kerentanan *(Vulnerability),* identifikasi kemungkinan dari adanya ancaman dan kerentanan, Identifikasi level risiko, menentukan dampak bisnis. Banyak penelitian manajemen risiko yang sudah dilakukan dengan berbagai standard an *framework.* Penelitian [12] menggunakan indeks KAMI yang diikuti juga dengan standar ISO 27001 pada instansi pendidikan sebagai standar internasioal untuk memastika keamanan informasi di suatu organisasi sudah efektif. Penelitian [13] menggunakan standar ISO 27001 untuk menyusun kebijakan keamanan informasi di instansi pendidikan. Sedangkan dalam penelitian [14] menggunakan standar ISO 27001 dengan metode FMEA pada instansi pemerintahan. pada penelitian [15] standar yang digunakan yaitu ISO 27001 dengan metode FMEA yang diterapkan pada instansi pendidikan. Pada penelitian [16] standar yang digunakan yaitu OCTAVE dan ISO 27001 yang diterapkan pada instansi pemerintahan, digunakannya dua standar tersebut yaitu supaya mendapatkan proses manajemen risiko dan langkah mitigasi yang maksimal. Sedangkan pada penelitian [17] standar OCTAVE-S yang digunakan untuk melakukan evaluasi pada perguruaan tinggi berskala kecil dengan struktur hierarki yang sedikit dan ISO 27001 digunakan untuk mengrekomendasikan langkah-langkah mitigasi penanganan risiko yang diterapkan pada instansi pendidikan. Terdapat juga metode lain yang digunakan dalam manajemen risiko seperti penelitian ini [18] yang membahas mengenai *Disaster Recover Plan* (DRP) Metode yang digunakan yaitu NIST SP 800-34 Rev.1 dimana metode tersebut digunakan untuk mengetahui tingkat keberhasilan perencanaan dokuman pemulihan akibat bencana [18].

II. METODOLOGI

Dalam menyusun penelitian ini, metode yang digunakan yaitu Indeks Keamanan Informasi (KAMI) yang sesuai dengan standar ISO 27001 yang terdapat beberapa tahapan yaitu :

1) *Analisis business context* yang berisi analisis bisnin perusahaan yaitu analisis isu internal dan eksternal oranisasi dan penentuan ruang lingkup.

2) Identifikasi aset, Dikelompokan menjadi empat kategori yaitu aset hardware, software, people dan data/informasi.

3) *Analisis risiko,* yaitu melakukan identifikasi ancaman (*threat*) dan Kerentanan (*vulnerability*)

4) Pengelolaan risiko, melakuka perhitungan risiko dengan range nilai 1 – 5 yang terjadi pada masing-masing aset yang dilihat dari adanya ancaman dan kerentanan.

TABEL I
RANGE NILAI RISIKO [19]

Range Nilai		Keterangan	Pengelolaan risiko
5	20-25	Sangat Tinggi	Memindahkan risiko
4	16-19	Tinggi	Mengurangi akibat
3	12-15	Moderat	Mengurangi kemungkinan
2	6-11	Rendah	Menghindari aktivitas
1	1-5	Sangat Rendah	Menerima risiko

5) Penentuan level risiko, menentukan level risiko dari masing-masing risiko yang ada dengan mengkalikan nilai dampak dan kemungkinan,

TABEL II
RISK LEVEL [19]

Score	Risk Level
>= 13	Tinggi
7-12	Moderat
<=6	Rendah

6) Penanganan risiko, memilih penanganan risiko apakah risiko diterima (*acceptance*), mengurangi kelemahan (*mitigation*), mengalihkan (*transfer*) atau menghindari risiko (*avoidance*) .

7) Penentuan kontrol pengendalian risiko, Menentukan kontrol keamanan sistem sesuai ISO 27001.

III. HASIL DAN PEMBAHASAN

A. *Analisis Business Context*

Berdasarkan analisis data isu Eksternal dan internal maka didapatkan ruang lingkup SMKI di ITTP yaitu:

- Layanan Penanganan Komplain
- Layanan Pengembangan Aplikasi
- Layanan Datacenter Management

B. *Identiffikasi Aset*

Dalam melakukan identifikasi aset didapatkan aset *hardware, software, people* dan data / informasi seperti pada tabel 3.

TABEL III
DATA ASET

Kategori	Aset	Owner
Hardware	Server	Unit IT Support
	Akses poin	Unit IT Support
	Modem	Unit IT Support
	Router	Unit IT Support
	RFID	Unit IT Support
	Kamera CCTV	Unit IT Support
	Webcame	Unit IT Support
	PC	Unit IT Support
	Smart TV	Unit IT Support
	Keyboard	Unit IT Support
	Camtouch	Unit IT Support
	Kabel	Unit IT Support
	Harddisk	Unit IT Support
Software	Blog Mahasiswa	Unit IT Support
	Proxmox Virtual Environment 5.1-35	Unit IT Support
	Aplikasi ELERNING ITTP (LMS)	Unit IT Support
	Server Backup e-Learning	Unit IT Support
	Database e-Learning	Unit IT Support
	iGracias Development	Unit IT Support
	Suket ITTP	Unit Akademik
People	Dosen	Unit SDM
	TPA	Unit SDM
	Tenagaa Penunjang	Unit SDM
	Mahasiswa	Kemahasiswaan
	Outsourcing	Unit SDM
Data / Informasi	Data Identitas Mahasiswa	Kemahasiswaan
	Data Identitas Pegawai	Unit SDM
	Data Infrastruktur	Unit IT Support
	Data Keuangan	Unit Keuangan
	Data MOU	Unit Kerjasama

C. *Analisis Risiko*

Setelah data aset didapatkan selanjutnya melakukan analisi risiko pada masing-masing aset yang sudah diidentifikasi seperti pada tabel 4 berikut.

TABEL IV
IDENTIFIKASI RISIKO

Kategori	Aset	*Threat*	*Vulnerability*	Risiko
Hardware	Server	Kebakaran	Masih kurangnya pendeteksi dini kebakaran	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak
	Kabel	Kebakaran	Masih kurangnya pendeteksi dini kebakaran	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak
Software	Aplikasi ELERNING ITTP (LMS)	Loading time website	Terjadinya peningkatan trafik akses website	Sistem tidak dapat diakses
		Website down	Server mengalami peningkatan trafik	Aplikasi dan informasi tidak dapat diakses
People / SDM	Mahasiswa	Password Cracking	Password tidak sesuai standar	Bocornya data penting yang ada, Data / informasi tidak valid / tidak utuh karena sudah diubah-ubah, Data dihapus/dihilangkan oleh pihak yang tidak bertanggung jawab
Data / Informasi	Data identitas mahasiswa	Kehilangan data	Kurangnya backup data	Data/infromasi tidak dapat diakses, Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan

	Data identitas pegawai	Pencurian data	Keamanan informasi masih lemah	Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan, Data / informasi tidak valid /utuh karena sudah diacak-acak

D. Pengelolaan Risiko

Setelah risiko diidentifikasi selanjutnya yaitu identifikasi nilai kemungkinan dan dampak dengan menggunakan matriks 5x5 seperti pada table 5.

TABEL V
MATRIKS RISIKO [19]

Kemungkinan	Dampak / Akibat				
	1	2	3	4	5
1	Sangat rendah	Sangat rendah	Sangat rendah	Sangat rendah	Sangat rendah
2	Sangat rendah	Sangat rendah	Rendah	Rendah	Rendah
3	Sangat rendah	Rendah	Rendah	Moderat	Moderat
4	Sangat rendah	Rendah	Moderat	Tinggi	Sangat tinggi
5	Sangat rendah	Rendah	Moderat	Sangat tinggi	Sangat tinggi

E. Penentuan Level Risiko

Dalam analisis risiko yaitu melakukan penilaian risiko dengan memasukan kategori dampak dan kemungkinan dengan range nilai 1-5 [20] seperti pada tabel 6.

TABEL VI
HASIL PENILAIAN LEVEL RISIKO

Aset	Risiko	Dampak	*Likelihood*	*Matrik Score*	*Risk Level*
Server	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak	4	5	20	H
Kabel	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak	4	5	20	H
Aplikasi ELERNING ITTP (LMS)	Sistem tidak dapat diakses	5	4	20	H
	Aplikasi dan informasi tidak dapat diakses	4	4	16	H
Mahasiswa	Bocornya data penting yang ada, Data / informasi tidak valid / tidak utuh karena sudah diubah-ubah, Data dihapus/dihilangkan oleh pihak yang tidak bertanggung jawab	5	3	15	H
	pihak yang tidak bertanggung jawab				
Data identitas mahasiswa	Data/infromasi tidak dapat diakses, Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan	3	3	9	M
Data identitas pegawai	Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan, Data / informasi tidak valid /utuh karena sudah diacak-acak	3	4	12	M

F. Penanganan Risiko

Penanganan Risiko dilakukan untuk menentukan langkah penanganan risiko sesuai dengan kriteria-kriteria penanganan risiko yaitu, risiko diterima (*risk acceptance),* risiko direduksi (*risk reduction),* risiko ditolak *(risk avoidance)* dan risiko dialihkan *(risk transfer*). Untuk penanganan risiko dilihat dari level risiko risiko tidak dapat diterima ketika level risikonya berada pada level *high.* [11].

TABEL VII
PENANGANAAN RISIKO

Aset	Risiko	*Risk Level*	*Penanganan Risiko*
Server	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak	H	Risk Avoidance
Kabel	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak	H	Risk Avoidance
Aplikasi ELERNING ITTP (LMS)	Sistem tidak dapat diakses	H	Risk Avoidance
	Aplikasi dan informasi tidak dapat diakses	H	Risk Avoidance
Mahasiswa	Bocornya data penting yang ada, Data / informasi tidak valid / tidak utuh karena sudah diubah-ubah, Data dihapus/dihilangkan oleh pihak yang tidak bertanggung jawab	H	Risk Avoidance
Data identitas mahasiswa	Data/infromasi tidak dapat diakses, Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan	M	Risk Acceptance

Data identitas pegawai	Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan, Data / informasi tidak valid /utuh karena sudah diacak-acak	M	Risk Avoidance

G. Kontrol Pengendalian Risiko

Kontrol pengendalian risiko diambil sesuai dengan ISO 27001 Annex – 2013.

TABEL VIII
KONTROL PENGENDALIAN

Aset	*Threat*	Risiko	Kontrol Keamanan
Server	Kebakaran	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak	A.11.1.4 Protecting against external and environmental threats
Kabel	Kebakaran	Perangkat rusak atau tidak berfungsi, Perangkat berkurang karena rusak	A.11.1.4 Protecting against external and environmental threats
Aplikasi ELERNING ITTP (LMS)	Loading time website	Sistem tidak dapat diakses	A.12.1.3 Capacity management
	Website down	Aplikasi dan informasi tidak dapat diakses	A.12.1.3 Capacity management
Mahasiswa	Password Cracking	Bocornya data penting yang ada, Data / informasi tidak valid / tidak utuh karena sudah diubah-ubah, Data dihapus/dihilangkan oleh pihak yang tidak bertanggung jawab	A.9.4.3 Password management system
Data identitas mahasiswa	Kehilangan data	Data/infromasi tidak dapat diakses, Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan	A.12.3.1 Information backup
Data identitas pegawai	Pencurian data	Bocornya data penting perusahaan kepada pihak yang tidak berkepentingan, Data / informasi tidak valid /utuh karena sudah diacak-acak	

IV. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan maka dapat disimpulkan bahwa pada awal pemetaan identifikasi aset diperoleh beberapaa aset yaitu aset *hardware, software, people* dan data/informasi. Dari beberapa hasil temuan yang didapatkan pada dokumen *Risk Register* terdapat beberapa aset yang memiliki level risiko *high* antara lain Server, kabel memiliki risiko tinggi disebabkan adanya kebakaran hal tersebut terjadi karena masih kurangnya pendeteksi dini kebakaran. Sedangkan Aplikasi Elerning memiliki risiko tinggi karena adanya peningkatan trafik akses website. Pada aset yang memiliki risiko tinggi memerlukan mitigasi antara lain yaitu server perlu diadakannya CCTV disetiap ruangan dan juga Alat pemadam api ringan (APAR). Selaian mitigasi aset yang memiliki level risiko tinggi ditentukan juga kontrol keamanannya sesuai dengn Annex – 2013. Di ITTP SOP belum tersedia karena masih dalam proses penyusunan Manajemen Risiko Keamanan Informasi. Penggunaan ISO 27001 dapat menggunakan metode Disaster Recovery Planning NIST SP800-34 sehingga dalam dokumentasi pemetaan resiko lebih komprehensif.

DAFTAR PUSTAKA

[1] Suryanto, "PENGERTIAN RISK MANAGEMENT DARI BERBAGAI SUMBER," *March, 20 20172017*. [Online]. Available: https://kap-suryanto.id/2017/03/20/pengertian-risk-management-dari-berbagai-sumber/.

[2] Tommy, "Pengertian Manajemen Risiko Menurut Para Ahli." [Online]. Available: https://kotakpintar.com/pengertian-manajemen-risiko-menurut-para-ahli/. [Accessed: 18-Mar-2020].

[3] I. T. Master *et al.*, "IT Master Plan 2019-2023 Institut Teknologi Telkom Purwokerto," Purwokerto.

[4] Septafiansyah, "ISO 27001 adalah Ikon Standarisasi Manajemen Keamanan Informasi," 2019. [Online]. Available: https://itgid.org/iso-27001-adalah/. [Accessed: 15-Apr-2020].

[5] Adipurnomo, "Standar ISO 27001 ISMS," 2019. [Online]. Available: https://standarku.com/standar-iso-27001-isms/. [Accessed: 30-Jul-2020].

[6] BSSN, "INDEKS KEAMANAN INFORMASI (KAMI)," 2018. [Online]. Available: https://bssn.go.id/indeks-kami/. [Accessed: 24-Jun-2020].

[7] B. M. Susanto, "Mengukur keamanan informasi studi : Komparasi ISO 27002 dan NIST 800-55," *Semin. Nas. Teknol. Inf. dan Komun.*, no. Mengukur Keamanan Informasi, pp. 175–180, 2013.

[8] ISO, "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements," 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

[9] ISO, "ABOUT US ISO." [Online]. Available: https://www.iso.org/about-us.html#1.

[10] Wikipedia, "Manajemen Risiko," 2019. [Online]. Available: https://id.wikipedia.org/wiki/Manajemen_risiko. [Accessed: 18-Mar-2020].

[11] D. Gibson, *Managing Risk in Information Systems*. 2014.

[12] F. Basyarahil, H. Astuti, and B. Hidayanto, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya," *J. Tek. ITS*, vol. 6, no. 1, pp. 116–121, 2017.

[13] S. A. Sholikhatin, A. Setyanto, S. Si, E. T. Luthfi, and M. Kom, "Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus : Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto)," vol. 4, no. 1, pp. 1–9.

[14] R. Budiarto, "Manajemen Risiko Keamanan Sistem Informasi," vol. 2, no. 2, pp. 105–115, 2017.

[15] N. U. Handayani, M. A. Wibowo, D. P. Sari, and Y. Satria, "Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001," vol. 39, no. 2, pp. 78–85, 2018.

[16] F. A. Anshori and A. R. Perdanakusuma, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 1701–1707, 2019.

[17] R. R. Wijayanti, "Implementasi Octave-S Dan Standar

Pengendalian Iso," vol. 11, no. 2, pp. 221–233, 2018.
[18] Z. Rifai, A. Maydina, and A. A. Kurniawan, "Rancangan Dokumen Disaster Recover Plan Pada IS/IT di Dinas XYZ," *Comput. Eng. Sci. Syst. J.*, vol. 3, no. 2, p. 147, 2018.
[19] I. R. Sholihah, M. Basuki, and P. I. Santosa, "Penilaian Risiko Pekerjaan Bunker Untuk Mencegah Tumpahan Minyak Di Atas Kapal Sesuai Isgott Pada Km. Camara Nusantara I," *Pros. Semin. Teknol. ...*, no. August, pp. 11–18, 2020.
[20] W. A. Prabowo and R. D. Ramadhani, "Perancangan Contingency Planning Disaster Recovery Unit Teknologi Informasi Perguruan Tinggi (Design of Contingency Planning Disaster Recovery College Information Technology Unit)," *J. Inform.*