PENILAIAN RISIKO ASET TEKNOLOGI INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI XYZ

Tugas Akhir

Diajukan untuk memenuhi persyaratan mencapai derajat Sarjana Sistem Informasi

Chycillia

16 17 09005

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2021

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

PENILAIAN RISIKO ASET TEKNOLOGI INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI XYZ

yang disusun oleh

CHYCILLIA

161709005

dinyatakan telah memenuhi syarat pada tanggal 10 Februari 2021

		Keterangan
Dosen Pembimbing 1	: Samiaji Sarosa, S.E., M.Info.Sys., Ph.D.	Telah menyetujui
Dosen Pembimbing 2	: Samiaji Sarosa, S.E., M.Info.Sys., Ph.D.	Telah menyetujui
Tim Penguji		
Penguji 1	: Samiaji Sarosa, S.E., M.Info.Sys., Ph.D.	Telah menyetujui
Penguji 2	: Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng.	Telah menyetujui
Penguji 3	: Putri Nastiti, S.Kom., M.Eng	Telah menyetujui

Yogyakarta, 10 Februari 2021

Universitas Atma Jaya Yogyakarta

Fakultas Teknologi Industri

Dekan ttd

Dr. A. Teguh Siswantoro, M.Sc

LEMBAR PERNYATAAN
Orisinalitas & Publikasi Ilmiah

Saya yang bertanda tangan di bawah ini:

Nama Lengkap : Chycillia

NPM : 161709005

Program Studi : Sistem Informasi

Judul Penelitian : Penilaian Risiko Aset Teknologi Informasi Pada Dinas Komunikasi dan Informatika Provinsi XYZ

Menyatakan dengan ini:

1. Skripsi ini adalah benar merupakan hasil karya saya sendiri tidak merupakan salinan sebagian atau keseluruhan dari karya orang lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta, berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, mendistribusikan, serta menampilkan untuk kepentingan akademis, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum yang mengikuti atas pelanggaran Hak Cipta dalam pembuatan skripsi ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 10-01-2021

Yang menyatakan,

Chycillia

161709005

HALAMAN PERSEMBAHAN

“Barangsiapa setia dalam perkara-perkara kecil, ia setia juga dalam perkara-perkara besar. Dan barangsiapa tidak benar dalam perkara-perkara kecil, ia tidak benar juga dalam perkara-perkara besar ”

Lukas 16 : 10

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa, karena atas rahmat dan berkah-Nya, penulis dapat menyelesaikan laporan tugas akhir dengan baik. Laporan tugas akhir ini ditulis dengan tujuan untuk memenuhi syarat dalam memperoleh gelar sarjana Sistem Informasi dari Program Studi Sistem Informasi, Fakultas Teknologi Industri di Universitas Atma Jaya Yogyakarta. Penulis menyadari dalam pengerjaan tugas akhir penulis telah mendapat banyak bimbingan, bantuan, dan dorongan dari banyak pihak, oleh karena itu penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yesus Kristus atas berkat dan kasih karunia-Nya.
2. Seluruh pegawai di Dinas Kominfo atas izin yang diberikan dan bersedia untuk diwawancarai dalam proses penelitian.
3. Bapak Samiaji Sarosa, S.E., M.Info.Sys., Ph.D., selaku pembimbing yang bersedia meluangkan waktunya dan membimbing dalam penyusunan Laporan Tugas Akhir.
4. Bapak Aloysius Bagas Pradipta Irianto S.Kom., M.Eng selaku pembimbing akademik yang telah memberi motivasi kepada penulis untuk menyelesaikan tugas akhir.
5. Ibu Flourensia Sapty Rahayu S.T., M.Kom., yang bersedia meluangkan waktunya untuk membimbing dan memberi masukan dalam proses penelitian.
6. Papa, Mama, Chyntia, Shella, Titan, Koko dan semua keluarga yang mendukung penulis selama berkuliah di Universitas Atma Jaya Yogyakarta.
7. Ci Oktri yang bersedia menemani penulis dalam proses penggumpulan data.
8. Koko Rinaldi, Carolina dan Yossi yang selalu memberikan semangat, masukan dan menjadi tempat curhat.
9. Risco, Alwi, Gia, Ricky, Ardo sebagai team magang yang membantu dalam proses pra penelitian.
10. Lao shi sekolah minggu yang selalu memberikan semangat, keceriaan, dukungan dan doa di tengah penyusunan skripsi
11. Teman seperjuangan Windy, Enjel dan Ulfa yang menjadi penyemangat untuk melalukan revisi setiap minggunya .

Serta seluruh pihak yang telah membantu dan yang tidak disebutkan namanya namun telah memberi warna dalam pengerjaan tugas akhir. Penulis menyadari bahwa Laporan tugas akhir ini masih jauh dari kesempurnaan. Kritik dan saran yang membangun sangat diharapkan untuk memajukan penelitian yang lebih baik lagi kedepannya. Semoga Laporan Tugas Akhir ini memberikan manfaat yang sebesar-besarnya bagi perusahaan dan pihak yang membaca.

Yogyakarta, 10-01-2021

Chycillia

Penulis

ABSTRAK

Perkembangan teknologi informasi menjadikan teknologi informasi menjadi faktor utama dalam bisnis. Berkembangnya teknologi informasi diiringi dengan pertumbuhan permasalahan yang timbul pada teknologi, manajemen dan keamanan informasi. Oleh karena itu dibutuhkan panduan Manajemen Risiko untuk menghindari risiko yang mungkin terjadi pada aset teknologi informasi. ISO 27005 merupakan sebuah standar Manajemen Risiko. Dinas Komunikasi dan Informatika (Diskominfo) Provinsi XYZ sedang dalam tahap persiapan untuk menuju sertifikasi ISO 27001. Untuk mencapai hal tersebut, Diskominfo melakukan penilaian tingkat kematangan menggunakan Indeks KAMI dan didapatkan bahwa Diskominfo kurang matang dalam melakukan Manajemen Risiko Keamanan Informasi dan mendapatkan rekomendasi untuk membuat dokumen pengelolaan risiko. Oleh karena itu dilakukan penilaian risiko pada aset Diskominfo mencakup kegiatan identifikasi, analisis dan evaluasi risiko sesuai dengan standar ISO 27005. Berdasarkan hasil penilaian terdapat sebanyak 91 skenario risiko dengan 32 risiko pada level tinggi, 41 risiko level sedang dan 18 risiko level rendah. Berdasarkan risiko tersebut terdapat rekomendasi untuk meminimalkan risiko di Diskominfo Provinsi XYZ.
.

Kata kunci: Keamanan Informasi ; ISO 27001 ; ISO 27005 ; Manajemen Risiko; Indeks KAMI

DAFTAR ISI

HALAMAN PENGESAHAN ii
LEMBAR PERNYATAAN iii
HALAMAN PERSEMBAHAN iv
KATA PENGANTAR v
ABSTRAK vii
DAFTAR ISI viii
DAFTAR GAMBAR x
DAFTAR TABEL xi
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Perumusan Masalah 3
1.3. Pertanyaan Penelitian 3
1.4. Batasan Masalah 4
1.5. Tujuan Penelitian 4
1.6. Manfaat Penelitian 4
1.7. Bagan Penelitian 4
BAB II MANAJEMEN RISIKO 5
2.1. Studi Sebelumnya 5
2.2. Dasar Teori 9
2.2.1 Risiko 9
2.2.2 Manajemen Risiko 10
2.2.3 ISO 27005 10
BAB III METODOLOGI PENELITIAN 13
3.1. Tahapan Pelaksanaan Proses Penelitian 13
BAB IV HASIL DAN PEMBAHASAN 17
4.1. Identifikasi Risiko 17
4.1.1. Identifikasi Aset 17
4.1.2. Identifikasi Ancaman, Kerentanan, Dampak dan Kontrol 20
4.2. Analisis Risiko 31
4.3. Evaluasi Risiko 43
BAB V KESIMPULAN DAN SARAN 50
5.1. Kesimpulan 50

5.2. Saran 51
DAFTAR PUSTAKA 52
LAMPIRAN 54
Dokumen Klasifikasi Ancaman 54
Dokumen Klasifikasi Kerentanan 56
Dokumen Klasifikasi Dampak 59
Contoh Kuesioner 60
Risk Register Perangkat Keras 61

DAFTAR GAMBAR

Gambar 2.1. Tahapan Manajemen Risiko 10
Gambar 2.2. Matriks Nilai Aset, Ancaman Dan Kerawanan..... 11
Gambar 2.3. Matriks Skenario Insiden 12
Gambar 2.4. *Risk Register* 12

DAFTAR TABEL

Tabel 2.1.1. Perbandingan Penelitian Terdahulu 7
Tabel 4.1.1. Daftar Aset Perangkat Keras 18
Tabel 4.1.2. Identifikasi Ancaman, Kerentanan, Dampak Dan Kontrol..... 21
Tabel 4.1.3. Jenis Ancaman 31
Tabel 4.1.4. Jenis Kerentanan 31

serviens in lumine veritatis

BAB I PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi bukan lagi menjadi faktor pendukung bagi suatu organisasi melainkan sudah menjadi faktor utama dalam menjalankan bisnis. Seiring perkembangannya, perkembangan teknologi informasi didampingi dengan pertumbuhan permasalahan yang muncul baik dari sisi teknologi, manajemen maupun keamanan. Permasalahan yang timbul tersebut dapat memberikan dampak bagi organisasi seperti menurunnya kinerja teknologi informasi bahkan dapat menimbulkan kerugian finansial dan operasional. Informasi merupakan aset yang sangat berharga karena dapat meningkatkan nilai bisnis suatu organisasi dan merupakan sumber daya strategis [1].

Pada tahun 2020, kejahatan *cyber* menyerang sebuah *e-commerce* dengan mengambil sebanyak 91 juta data pengguna serta 7 juta akun *merchant* yang berisikan User ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor ponsel dan kata sandi. Data tersebut kemudian dijual pada sebuah *Dark Web* [2]. Dampak secara finansial dari bocornya data ini *e-commerce* digugat sebesar 100 M. Selain itu *e-commerce* mengalami kesulitan dalam mencari pelanggan baru dan terdapat biaya ekstra bagi karyawan yang lembur untuk menyelesaikan permasalahan ini. Karyawan teknologi informasi dikerahkan untuk menangani masalah ini, sehingga menghambat proses operasional di organisasi [3].

Insiden kehilangan informasi terjadi pada Gedung Inspektorat Pemerintahan. Hal ini terjadi pada januari 2020. Gedung Inspektorat mengalami kebakaran sehingga menghanguskan beberapa peralatan kantor dan membakar beberapa dokumen kantor. Hal ini terjadi karena adanya korsleting listrik pada gedung kantor [4].

Maraknya permasalahan keamanan informasi belum menjadi fokus utama bagi pemilik maupun pengelola informasi. Hal ini dikarenakan pengadaan anggaran bagi penanganan risiko dianggap tidak berdampak memberikan laba bagi organisasi. Oleh karena itu dibutuhkan suatu panduan manajemen risiko teknologi informasi yang berfungsi untuk menghindari kegagalan penerapan teknologi informasi dan risiko yang mungkin terjadi pada aset teknologi informasi. Pembentukan manajemen risiko teknologi informasi harus sesuai

dengan manajemen risiko pada organisasi dan diketahui oleh pemilik dan pengelola teknologi informasi pada organisasi [5] .

ISO 27005 merupakan sebuah standar pedoman Manajemen Risiko Keamanan Informasi bagi organisasi. Penggunaan ISO 27005 guna mendukung persyaratan Sistem Manajememn Keamanan Informasi (SMKI) sesuai dengan standar ISO 27001. ISO 27005 memiliki 6 tahapan dalam melakukan manajemen risiko yaitu *Context Establishment, Risk Assesment, Risk Treatment, Risk Acceptance, Communication and Consultation, Monitoring and Review* [6].

Dinas Komunikasi dan Informatika (Diskominfo) Provinsi XYZ merupakan sebuah organisasi perangkat daerah Provinsi yang bertanggung jawab secara langsung dibawah naungan Gubernur. Tugas dan tanggung jawab dari adalah membantu Gubernur dalam melaksanakan tugas pemerintahan bidang komunikasi dan informatika, persandian dan statistik [7] [8].

Diskominfo Provinsi XYZ memiliki 9 bagian dalam struktur organisasinya yaitu Kepala Dinas, Sekretariat, Bidang Informasi dan Komunikasi Publik, Bidang Statistik, Bidang Teknologi Informasi dan Komunikasi, Bidang *E-Government*, Bidang Persandian dan Keamanan Informasi, UPT Dinas dan Kelompok Jabatan Fungsional. Setiap bagian tersebut memiliki seksi dengan tugas pokok. Salah satu tugas pokok dari Seksi Pengamanan dan Persandian Informasi Bidang Persandian dan Keamanan Informasi yaitu menyiapkan bahan pengamanan kegiatan, aset, fasilitas, instalasi serta informasi dan mengukur tingkat kerawanan dan keamanan informasi [9].

Kegiatan Pengamanan Informasi tentang Sistem Manajemen Pengamanan Informasi yang diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor 4 tahun 2016 pasal 7 ayat 1 dan 2 bahwa Sistem Elektronik strategis dan tinggi harus menerapkan standar SNI ISO 27001 sedangkan Sistem Elektronik rendah harus menerapkan pedoman Indeks Kemanan Informasi. Sistem Elektronik merupakan rangkaian perangkat dan prosedur elektronik yang memiliki fungsi mempersiapkan, menampilkan, mengelola, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan menyebarkan Informasi Elektronik [10].

Saat ini Diskominfo melakukan penilaian dengan menggunakan Indeks Keamanan Informasi (Indeks KAMI). Indeks KAMI merupakan alat evaluasi yang berfungsi untuk menganalisis tingkat kesiapan keamanan informasi pada organisasi. Alat ini digunakan untuk menggambarkan kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada pimpinan organisasi. Indeks KAMI yang digunakan oleh Diskominfo adalah Indeks KAMI versi 4.0. Adapun area yang dinilai yaitu Kategori Sistem Elektronik, Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi serta Suplemen. Berdasarkan penilaian tersebut Diskominfo Provinsi XYZ pada kategori Manajemen Risiko Keamanan Informasi berada pada tingkat kematangan I+ [11]. Berdasarkan hasil tersebut diketahui bahwa Diskominfo berada pada tahap awal dalam melakukan Manajemen Risiko Keamanan Informasi. Tahapan yang telah dilakukan oleh Diskominfo yaitu dengan membuat dokumen Kebijakan dan Prosedur Manajemen Risiko SMKI. Untuk berada pada tingkat kematangan III dengan tingkat kematangan teridentifikasi dan konsisten, Diskominfo harus melakukan Manajemen Risiko pada seluruh aset yang yang dimiliki.

1.2. Perumusan Masalah

Saat ini Diskominfo Provinsi XYZ sedang menghadapi permasalahan dalam menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yaitu melakukan penilaian risiko pada aset yang terkait informasi. Diskominfo Provinsi XYZ telah melakukan SMKI pada tahap awal yaitu dengan membuat dokumen Kebijakan dan Prosedur Manajemen Risiko. Tahap selanjutnya dalam menerapkan SMKI yaitu penilaian risiko pada aset. Hal ini penting dilakukan untuk mengetahui kondisi riil dilapangan. Jika penilaian risiko aset tidak dilakukan maka pemerintah tidak siap dalam mengelola risiko pada aset sehingga dapat berdampak bagi kinerja dan reputasi pelayanan pemerintahan.

1.3. Pertanyaan Penelitian

Berdasarkan rumusan masalah yang telah dijabarkan di atas, dapat dirumuskan sebagai berikut :

1) Bagaimana penilaian risiko aset yang terkait informasi pada Diskominfo Provinsi XYZ ?

1.4. Batasan Masalah

Batasan masalah dalam penelitian ini berupa :

1. Penelitian dilakukan pada aset perangkat keras yang tercatat dalam Dokumen Aset Diskominfo Provinsi XYZ tahun 2019
2. *Best-practice* yang digunakan adalah ISO 27005 : 2008 hal ini karena keterbatasan referensi dan sumber pendukung pada ISO 27005 : 2013
3. Tahapan ISO 27005 : 2008 yang diterapkan berfokus pada penilaian risiko
4. Parameter yang digunakan adalah dokumen Kebijakan dan Prosedur Manajemen Risiko Diskominfo Provinsi XYZ

1.5. Tujuan Penelitian

1. Penilaian risiko pada aset perangkat keras pada Diskominfo Provinsi XYZ dengan menilai aset, ancaman, kerawan serta dampak
2. Membuat rekomendasi prioritas penanganan berdasarkan tingkat risiko

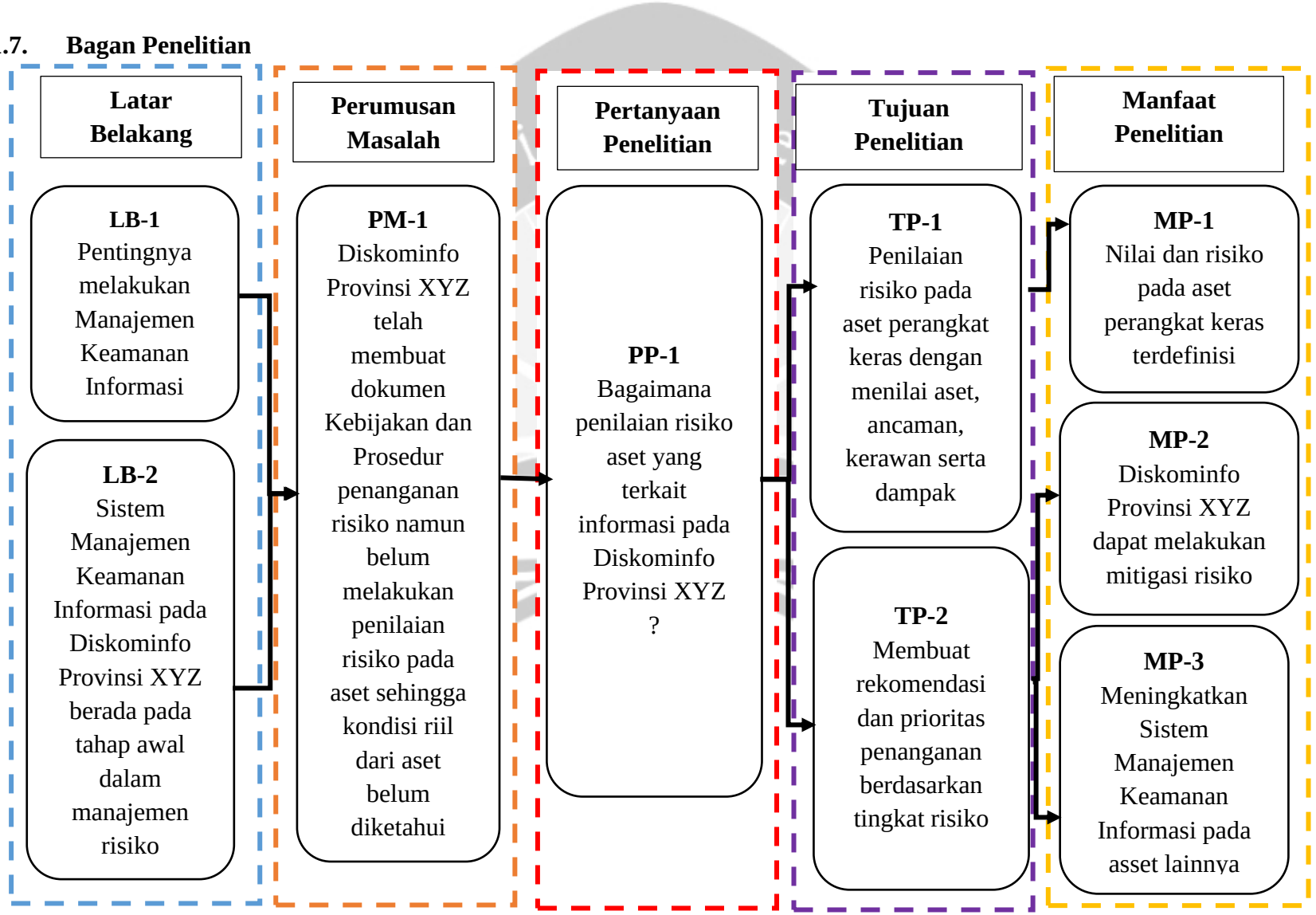
1.6. Manfaat Penelitian

Adapun manfaat dalam penelitian ini yaitu :

1. Nilai dan risiko pada setiap asset perangkat keras dapat di diketahui
2. Diskominfo Provinsi XYZ dapat melakukan mitigasi risiko berdasarkan hasil analisis
3. Diskominfo Provinsi XYZ dapat meningkatkan Sistem Manajemen Keamanan Informasi pada aset lainnya

serviens in lumine veritatis

1.7. Bagan Penelitian



BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan

Tahapan dalam penilaian risiko pada aset perangkat keras Diskominfo Provinsi XYZ dilakukan dengan menggunakan standar ISO 27005 : 2008. Adapun tahapannya yaitu identifikasi aset yang kemudian dilanjutkan dengan tahap analisis dan evaluasi risiko. Pada tahap identifikasi aset, didapatkan sebanyak lima belas aset perangkat keras yang berada di kantor maupun ruang Data *Center* Diskominfo Provinsi XYZ. Tahap selanjutnya dilakukan identifikasi terhadap ancaman, kerentanan, kontrol dan dampak. Berdasarkan hasil identifikasi diketahui terdapat sebanyak enam ancaman, lima belas kerentanan dan dampak yang dapat mempengaruhi baik secara langsung maupun tidak langsung.

Pada tahap analisis dilakukan penilaian terhadap aset, ancaman, kerentanan dan dampak. Diketahui bahwa terdapat sebanyak lima aset dengan nilai tinggi dan sepuluh aset dengan nilai sangat tinggi. Adapun hasil dari analisis risiko terdapat 91 skenario ancaman yang mungkin terjadi yang berada pada skala rendah sampai tinggi. Berdasarkan hasil evaluasi risiko terdapat tiga puluh dua risiko di level tinggi, empat puluh satu risiko di level sedang dan delapan belas di level rendah. Prioritas di buat berdasarkan skala risiko dari yang tertinggi hingga yang terendah.

Adapun ancaman yang sering muncul yaitu kerusakan pada peralatan, hilangnya pasokan listrik serta debu dan korosi. Kerentanan yang sering muncul yaitu karena kurangnya pemeliharaan/kesalahan instalasi, kerentanan terhadap variasi voltase, kerentanan terhadap kelembapan, debu dan kotoran. Selain itu kerentanan lainnya yaitu penyimpanan yang tidak dilindungi, kerentanan terhadap suhu yang bervariasi dan sambungan kabel yang buruk. Oleh karena itu, prioritas rekomendasi yang perlu dilakukan yaitu membuat jadwal pemeliharaan aset secara berkala, memaksimalkan penggunaan UPS, menyediakan media penyimpanan aset, menggunakan kabel dengan kualitas yang baik dan menambahkan pelindung khusus kabel.

5.2. Saran

Berikut ini saran yang dapat dilakukan pada penelitian selanjutnya :

1. Melakukan manajemen risiko lanjutan untuk dapat dilakukan penanganan, pemantauan dan peninjauan risiko
2. Melakukan manajemen risiko pada aset lain seperti perangkat lunak

DAFTAR PUSTAKA

[1] P. R. E. Indrajit, "ISO 17799 Kerangka Standar Keamanan Informasi," *id-SIRTII*, 2018.

[2] Roy. (2020, May 4). Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia. Available : https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia/1

[3] Iskandar. (2020, Januari 4). Tokopedia Diserang Hacker, Ini Dampak Bagi Karyawan dan Pelanggan. Available : https://www.liputan6.com/tekno/read/4244527/tokopedia-diserang-hacker-ini-dampak-bagi-karyawan-dan-pelanggan

[4] M.Haryanto.(2020, Januari 4). Kantor Inspektorat Terbakar, Dokumen Lama Hangus [Jawa Post Radar Semarang]. Available : https://radarsemarang.jawapos.com/berita/semarang/2020/01/04/kantor-inspektorat-terbakar-dokumen-lama-hangus/?amp

[5] ISACA, "The Risk IT Framework. Rolling Meadows," *USA : ISACA*, vol. II, 2009.

[6] I. S. Organization, "ISO/IEC 27005 Information Technology - Security Techniques - Information Security Risk Management," 2018.

[7] Peraturan Pemerintah, tentang Pemerintah Daerah, Nomor 23, 2014.

[8] Peraturan Pemerintah, tentang “Perangkat Daerah”, Nomor 18, 2016.

[9] Peraturan Gubernur, tentang “Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika”, Nomor 70, 2016.

[10] Peraturan Menteri Komunikasi dan Informatika Republik Indonesia, tentang “Sistem Manajemen Pengamanan Informasi”, Nomor 18, 2016

[11] P. P. T. Sinergi, "Laporan Akhir Penilaian Sistem Manajemen Pengamanan Informasi Berbasis Indeks KAMI Versi 4.0," 2019.

[12] S. Prasetyo and G. Sucahyo, "Information Security Risk Management Planning : A Case Study at Application Module of State Assest Directorate general on State Asset Ministry of Finance," *ICAICS*, 2014.

[13] F. I. S. Yudha and R. E. Gunadhi, "Risk Assesment Pada Manajemen Risiko Keamanan Informasi Mengacu Pada British Standard ISO/IEC 27005 Risk Management," *Jurnal Algoritma*, vol. 13 No 1, no. ISSN : 2302-7339, 2016.

[14] Asriyanik and Prajoko, "Manajemen Risiko Keamanan Informais Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas

Muhammadiyah Sukabumi (UMMI)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 4, no. p-ISSN : 244-2210 e-ISSN : 2443-2229, 2018.

[15] Voughan.E.J and Curtis M.Elliot, “Fundamentals of Risk and Insurance”, Toronto : John Wiley & Sons Inc, 1978.

[16] Australian/New Zeland Standard, “Risk Management Standard”, AS/NZS 4360, 2004.

[17] F. Mahardika, “Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasis:STMIK Sumedang),” vol. 02, no.02, pp. 1-8,2017.

[18] S. Salahuddin, A. Ambarwati, and M.N. Al Azam, “Identifikasi Risiko Keamanan Informasi Menggunakan ISO 27005 pada Sebuah Perguruan Tinggi Swata di Surabaya,” *Semin. Nas. Sist. Inf.*, pp. 990-996, 2018.

LAMPIRAN

Dokumen Klasifikasi Ancaman

Jenis	Kode	Ancaman	Kode	Ancaman
Kerusakan Fisik	T1	Api	T44	Hacker
	T2	Kerusakan karena air	T45	Kriminal Komputer
	T3	Polusi	T46	Teroris
	T4	Kecelakaan Besar	T47	Spionase Industri (Kecerdasan, Perusahaan, Pemerintah Asing, Kepentingan pemerintah lainnya)
	T5	Perusakan pada peralatan atau media		
	T6	Debu, korosi, pembekuan		
Peristiwa Alam	T7	Fenomena Iklim		
	T8	Fenomena Gempa Bumi		
	T9	Fenomena Vulkanik	T48	Orang Dalam (Karyawan yang kurang terlatih, tidak puas, berbahaya, lalai, tidak jujur atau dipecat)
	T10	Fenomena Meteorologi		
	T11	Banjir		
Kehilangan layanan yang penting	T12	Kegagalan AC atau sistem pasokan air		
	T13	Hilangnya pasokan listrik		
	T14	Kegagalan Peralatan telekomunikasi		
Gangguan akibat radiasi	T15	Radiasi Elektromagnetik		
	T16	Radiasi Panas		
	T17	Pulsa Elektromagnetik		
Kompromi akan informasi	T18	Intersepsi mengorbankan sinyal interfensi		
	T19	Memata-matai dari jauh		
	T20	Menguping		
	T21	Pencarian media atau dokumen		
	T22	Pencurian Peralatan		
	T23	Retrieval media di daur ulang atau dibuang		
	T24	Penyingkapan		
	T25	Data dari sumber yang tidak dapat dipercaya		
	T26	Gangguan perangkat keras		
	T27	Gangguan Perangkat Lunak		
	T28	Pendeteksi posisi		
	T29	Kegagalan peralatan		

Kegagalan teknis	T30	Kerusakan peralatan		
	T31	Kejenuhan sistem informasi		
	T32	Kerusakan perangkat lunak		
	T33	Pelanggaran pemeliharaan sistem informasi		
Tindakan yang tidak sah	T34	Penggunaan peralatan yang tidak sah		
	T35	Menyalin perangkat lunak palsu		
	T36	Penggunaan perangkat lunak palsu		
	T37	Korupsi data		
	T38	Pengolahan data illegal		
Kompromi terhadap fungsi	T39	Kesalahan penggunaan		
	T40	Penyalahgunaan hak		
	T41	Penempatan hak		
	T42	Penyangkalan pada tindakan		
	T43	Pelanggaran ketersediaan personel		

Dokumen Klasifikasi Kerentanan

Jenis	Kode	Kerentanan
Perangkat Keras	V1	Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan
	V2	Kurangnya skema pergantian berkala
	V3	Kerentanan terhadap kelembaban, debu, kotoran
	V4	Kurangnya kontrol perubahan konfigurasi yang efisien
	V5	Kerentanan terhadap voltase yang bervariasi
	V6	Kerentanan terhadap suhu yang bervariasi
	V7	Penyimpanan yang tidak dilindungi
	V8	Kurangnya perawatan di pembuangan
	V9	Penyalinan yang tidak terkendali
Perangkat Lunak	V10	Tidak ada atau tidak cukup pengujian perangkat lunak
	V11	Kekurangan yang telah diketahui pada perangkat lunak
	V12	Tidak 'logout' ketika meninggalkan komputer
	V13	Pembuangan atau pemakaian ulang media penyimpanan tanpa penghapusan yang tepat
	V14	Kurangnya audit trail
	V15	Kesalahan penempatan hak akses
	V16	Perangkat lunak yang didistribusikan secara luas
	V17	Menerapkan program aplikasi untuk data yang salah dalam hal waktu
	V18	Antar muka yang rumit
	V19	Kurangnya dokumentasi
	V20	Kesalahan pengaturan parameter
	V21	Kesalahan tanggal
	V22	Kurangnya mekanisme identifikasi dan otentikasi seperti otentikasi pengguna
	V23	Tabel password yang tidak dilindungi
	V24	Manajemen password yang buruk
	V25	Layanan yang tidak perlu diaktifkan
	V26	Perangkat lunak baru atau belum matang
	V27	Spesifikasi pengembangan yang tidak jelas atau tidak lengkap
	V28	Kurangnya kontrol perubahan yang efektif
	V29	Pengunduhan dan penggunaan perangkat lunak yang tidak terkontrol
	V30	Kurangnya salinan back-up
	V31	Kurangnya perlindungan fisik pada gedung, pintu, dan jendela
	V32	Kesalahan pembuatan laporan manajemen
Jaringan	V33	Kurangnya bukti pengiriman dan penerimaan pesan
	V34	Jalur komunikasi yang tidak dilindungi
	V35	Lalu lintas sensitif yang tidak dilindungi
	V36	Sambungan kabel yang buruk
	V37	Titik tunggal kegagalan
	V38	Kurangnya identifikasi dan otentikasi pada pengirim dan penerima

	V39	Arsitektur jaringan yang tidak aman
	V40	Transfer password dengan jelas
	V41	Manajemen jaringan yang tidak cukup (ketahanan routing)
	V42	Koneksi jaringan publik yang tidak dilindungi
Personel	V43	Ketidakhadiran personel
	V44	Prosedur rekrutmen yang tidak cukup
	V45	Pelatihan keamanan yang tidak cukup
	V46	Kesalahan penggunaan atas perangkat lunak dan perangkat keras
	V47	Kurangnya kesadaran akan keamanan
	V48	Kurangnya mekanisme pemantauan
	V49	Bekerja tanpa pengawasan oleh orang luar atau karyawan pembersih
	V50	Kurangnya kebijakan untuk penggunaan yang benar atas media telekomunikasi dan pesan
Situs	V51	Penggunaan yang tidak memadai atau ceroboh atas kontrol akses fisik ke bangunan dan ruangan-ruangan
	V52	Lokasi pada daerah yang rentan banjir
	V53	Jaringan listrik yang tidak stabil
	V54	Kurangnya perlindungan fisik terhadap gedung, pintu, dan jendela
Organisasi	V55	Kurangnya prosedur formal untuk pendaftaran dan penghapusan pengguna
	V56	Kurangnya proses formal untuk meninjau hak akses (pengawasan)
	V57	Kurangnya ketentuan yang memadai (mengenai keamanan) dalam kontrak dengan pelanggan dan/atau pihak ketiga
	V58	Kurangnya prosedur pemantauan fasilitas pengolah informasi
	V59	Kurangnya audit berkala (pengawasan)
	V60	Kurangnya prosedur identifikasi dan penilaian risiko
	V61	Kurangnya laporan kesalahan yang tercatat dalam administrator dan pengelola log
	V62	Respon pemeliharaan layanan yang tidak memadai
	V63	Kurang atau tidak cukup Service Level Agreement
	V64	Kurangnya prosedur kontrol perubahan
	V65	Kurangnya prosedur formal untuk pengendalian dokumen SMKI
	V66	Kurangnya prosedur formal untuk rekaman pengawasan SMKI
	V67	Kurangnya proses formal untuk otorisasi informasi yang tersedia untuk publik
	V68	Kurangnya alokasi yang tepat atas tanggung jawab keamanan informasi
	V69	Kurangnya rencana berkesinambungan
	V70	Kurangnya kebijakan penggunaan surat elektronik

	V71	Kurangnya prosedur untuk memperkenalkan perangkat lunak ke dalam sistem operasional
	V72	Kurangnya catatan di administrator dan pengelola log
	V73	Kurangnya prosedur untuk menangani informasi rahasia
	V74	Kurangnya tanggung jawab keamanan informasi dalam deskripsi pekerjaan
	V75	Kurangnya atau tidak memadainya ketentuan (mengenai keamanan informasi) dalam kontrak dengan karyawan
	V76	Kurangnya proses disipliner yang ditetapkan dalam kasus insiden keamanan informasi
	V77	Kurangnya kebijakan formal pada penggunaan ponsel
	V78	Kurangnya penguasaan aset lokal
	V79	Kurangnya atau tidak cukup kebijakan meja bersih dan layar bersih
	V80	Kurangnya otorisasi fasilitas pengolahan informasi
	V81	Kurangnya mekanisme pemantauan yang ditetapkan untuk pelanggaran keamanan
	V82	Kurangnya tinjauan manajemen rutin
	V83	Kurangnya prosedur pelaporan kelemahan keamanan
	V84	Kurangnya prosedur ketentuan sesuai dengan hak intelektual

Dokumen Klasifikasi Dampak

Jenis	Kode	Dampak
Langsung	I1	Nilai Penggantian keuangan atas kehilangan (bagian dari) aser
	I2	Biaya akuisisi, konfigurasi dan instalasi asset baru atau back up
	I3	Biaya operasi yang ditangguhkan akibat insiden tersebut sampai layanan yang disediakan oleh asset dikembalikan
	I4	Dampak yang menghasilkan pelanggaran keamanan informasi
Tidak Langsung	I5	Biaya peluang (sumber daya keuangan yang diperlukan untuk mengganti atau memperbaiki asset akan telah digunakan di tempat lain)
	I6	Biaya operasi yang terganggu
	I7	Penyalahgunaan potensi informasi yang diperoleh melalui pelanggaran keamanan
	I8	Pelanggaran kewajiban hukum atau peraturan
	I9	Pelanggaran kode etik

Contoh Kuesioner

Penilaian Risiko Ruangan

Bidang Informasi dan Komunikasi Publik

Kategori	Kode Aset	Aset	Kategori Utama / Pendukung	** Nilai	Ancaman	*Nilai Ancaman	Kerentanan	*Nilai Kerentanan	Dampak	*Nilai Dampak	Keterangan
Hard ware	A1	Kamera/Video Recorder									
	A2	PC (Multimedia)									
	A3	Laptop (Grafis, Multimedia ROG)									
	A4	Server									
	A5	HP									
	A6	HT									
	A7	Multimedia Workstation (Laptop)									
	A8	CPU									
	A9	Printer									
	A10	Scanner									
	A11	Harddisk									
	A12	UPS									
	A13	Flash									
	A14	Tripod									
	A15	Voice Recorder									
	A16	Lensa									
	A17	Batery									
	A18	Drone									
	A19	Versatile									
	A20	Tablet Controller									
	A21	Conference System									

Petunjuk Pengisian :

- * : Diisi dengan Rendah (R), Sedang (S), Tinggi(T)
- ** : Diisi dengan angka 0,1,2,3,4 (0 : Sangat Rendah, 1 : Rendah, 2: Sedang, 3:Tinggi, 4:Sangat Tinggi)

***Risk Register* Perangkat Keras**

Aset	Identifikasi Risiko			Kontrol	Analisa Risiko			Rekomendasi
	Ancaman	Kerentanan	Dampak		Nilai Dampak	Nilai *Likelihood*	Nilai Risiko	
A1 (Kamera, Video dan Voice Recorder)	Kecelakaan (T1)	- Penyimpanan yang tidak dilindungi (V7)	Biaya perbaikan dan pengganti an aset	- Setiap aset memiliki tali pengikat untuk pengguna sehingga memudahkan dalam memegang aset - Aset disimpan dalam *Dry Box*	S	5	S	- Menyediakan media penyimpanan aset di tempat terbuka - Membuat dokumen panduan mengoperasikan aset (manual book) - Melakukan pelatihan penggunaan asset - Membuat dokumen inventarisasi asset - Membuat jadwal pemeliharaan aset secara berkala - Melakukan penilaian terhadap
		- Kesalahan penggunaan atas perangkat keras (V4)				4	S	
	Kerusakan pada peralatan (T6)	- Kurangnya skema pergantian secara berkala (V2)				6	T	
		- Kesalahan penggunaan atas perangkat keras (V4)				5	S	
	Debu dan Korosi (T3)	- Kurangnya pemeliharaan/kesalaha n instalasi media penyimpanan (V1)				5	S	

		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				5	S	kondisi aset secara berkala
		- Kerentanan terhadap suhu yang bervariasi (V6)				5	S	
		- Penyimpanan yang tidak dilindungi (V7)				5	S	
A2 (Personal Computer)	Debu dan Korosi (T3)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)	Biaya perbaikan, biaya instalasi aset baru, kinerja terganggu	- Dilakukan pelatihan terhadap pegawai tentang keamanan informasi - Setiap *Personal Computer (*PC) terhubung dengan UPS	T	4	S	- Membuat dokumen panduan mengoperasikan aset (*Manual Book)* - Melakukan penyuluhan dan pelatihan aset secara rutin tentang cara mengoperasikan aset dan keamanan informasi yang disimpan dalam asset
		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				4	S	
	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)				6	T	
		- Kurangnya pemeliharaan/kesalaha				6	T	

	Kerusakan Perangkat Lunak (T5)	n instalasi media penyimpanan (V1)						- Membuat jadwal pemeliharaan aset secara berkala - Melakukan penilaian aset secara berkala - Memaksimalkan penggunaan UPS - Instalasi dan pemeliharaan dilakukan oleh penanggungjawab asset - Melakukan pembaharuan secara berkala pada perangkat lunak - Menyediakan lisensi asli dalam menggunakan perangkat lunak - Membatasi hak akses dan memblokir situs - situs yang berbahaya
		- Pengunduhan dan penggunaan perangkat lunak yang tidak terkontrol (V13)				7	T	
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				4	S	
		- Kesalahan penggunaan atas perangkat keras (V4)				4	S	
		- Kerentanan terhadap variasi voltase (V3)				5	S	
	Menyalin dan menggunakan perangkat	- Pengunduhan dan penggunaan perangkat lunak yang tidak terkontrol (V13)				8	T	

	lunak palsu (T2)	- Kurangnya kesadaran akan keamanan (V10)				7	T	
		- Kurangnya mekanisme pemantauan (V11)				7	T	
		- Pelatihan keamanan yang tidak cukup (V12)				7	T	
A3 (Laptop)	Debu dan Korosi (T3)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)	Biaya perbaikan, biaya instalasi aset baru, kinerja terganggu	- Belum terdapat kontrol pada aset	S	4	S	- Membuat dokumen panduan mengoperasikan aset (Manual Book) - Melakukan penyuluhan dan pelatihan aset secara rutin tentang cara mengoperasikan aset dan keamanan informasi yang disimpan dalam asset
		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				4	S	
	Kerusakan Perangkat Lunak (T5)	- Pengunduhan dan penggunaan perangkat lunak yang tidak terkontrol (V13)				6	T	
		- Kurangnya pemeliharaan/kesalaha				4	S	

	Kerusakan Peralatan (T6)	n instalasi media penyimpanan (V1)						- Membuat jadwal pemeliharaan aset secara berkala - Melakukan penilaian aset secara berkala - Membatasi hak akses dan memblokir situs - situs yang berbahaya
		- Kerentanan terhadap variasi voltase (V3)				4	S	
	Menyalin dan menggunakan perangkat lunak palsu (T2)	- Pengunduhan dan penggunaan perangkat lunak yang tidak terkontrol (V13)				6	T	
		- Kurangnya kesadaran akan keamanan (V10)				6	T	
		- Kurangnya mekanisme pemantauan (V11)				6	T	
		- Pelatihan keamanan yang tidak cukup (V12)				6	T	
A4 (Server)		- Kurangnya pemeliharaan/kesalaha	Biaya perbaikan	- Menggunakan	T	4	S	

	Kerusakan Perangkat Lunak (T5)	n instalasi media penyimpanan (V1)	, biaya pengganti an, terhambat nya proses bisnis, penyalah gunaan potensi informasi	Honeypot untuk merekam setiap serangan yang masuk - Tersambung dengan UPS - Terdapat sensor suhu ruangan - Pembatasan hak akses dalam menggunakan server				
		- Kurangnya skema pergantian secara berkala (V2)				4	S	- Membuat standar kondisi ruangan server - Membuat jadwal pemeliharaan aset secara berkala - Instalasi dan pemeliharaan dilakukan oleh ahli - Memaksimalkan penggunaan UPS - Menggunakan *Air Purifier* dan sensor suhu pada ruangan server - Membatasi hak akses ruangan
	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)				6	T	
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalaha n instalasi media penyimpanan (V1)				4	S	
		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				4	S	
		- Kerentanan terhadap suhu yang bervariasi (V6)				4	S	
		- Kerentanan terhadap variasi voltase (V3)				4	S	

A5 (Smartphone dan HT)	Kecelakaan (T1)	- Penyimpanan yang tidak dilindungi (V7)	Biaya perbaikan dan pengganti an aset	- Aset disimpan dalam *Dry Box*	R	3	S	- Menyediakan media penyimpanan aset di tempat terbuka - Membatasi hak akses dan memblokir situs-situs yang berbahaya - Membuat jadwal pemeliharaan aset secara berkala - Instalasi dan pemeliharaan dilakukan oleh penanggungjawab
		- Kesalahan penggunaan atas perangkat keras (V4)				3	S	
	Kerusakan pada peralatan (T6)	- Kurangnya skema pergantian secara berkala (V2)				3	S	
		- Kesalahan penggunaan atas perangkat keras (V4)				3	S	
A6 (Printer, Scanner, Mesin Penghancur Kertas)	Debu dan Korosi (T3)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)	Biaya perbaikan dan pengganti an aset, melangga r keamana	- Panduan dalam menggunakan aset - Dilakukan pemeliharaan setiap 1 minggu 1x	S	3	S	- Membuat panduan mengoperasikan aset (*Manual Book)* - Menghubungkan pada UPS - Membuat jadwal pemeliharaan
		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				3	S	

	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)	n informasi, melanggar kewajiban hukum	- Terhubung dengan UPS		5	S	aset secara berkala - Membatasi hak akses
	Kerusakan Peralatan (T6)	- Kurangnya skema pergantian secara berkala (V14)				5	S	
		- Penyalinan yang tidak terkendali (V15)				6	T	
		- Kesalahan penggunaan atas perangkat keras (V4)				6	T	
A7 (Harddisk)	Kecelakaan (T1)	- Penyimpanan yang tidak dilindungi (V7)	Biaya pengganti an aset, menggan ggu kinerja, penyalah gunaan potensi informasi	- Belum terdapat kontrol pada aset	S	5	S	- Membuat panduan mengoperasikan aset (*Manual Book)* - Instalasi dan pemeliharaan dilakukan oleh penanggungjawab - Membuat jadwal pemeliharaan secara berkala
		- Kesalahan penggunaan atas perangkat keras (V4)				6	T	
	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)				6	T	
		- Pengunduhan dan penggunaan perangkat				6	T	

	Kerusakan Perangkat Lunak (T5)	lunak yang tidak terkontrol (V13)						- Membatasi hak akses - Perangkat tambahan terhubung dengan UPS
		- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				6	T	
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				5	S	
		- Kerentanan terhadap suhu yang bervariasi (V6)				6	T	
A8 (UPS)	Debu dan Korosi (T3)	- Kerentanan terhadap kelembapan, debu, kotoran (V5)	Biaya instalasi aset baru, mengham bat kinerja	- Belum terdapat kontrol pada aset	T	4	S	- Membuat jadwal pemeliharaan aset secara berkala - Instalasi dan pemeliharaan dilakukan oleh
		- Kerentanan terhadap suhu yang bervariasi (V6)				4	S	

		- Penyimpanan yang tidak dilindungi (V7)	aset yang terkait			4	S	penanggungjawab
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				4	S	
		- Kerentanan terhadap variasi voltase (V3)				4	S	
A9 (TV)	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)	Biaya perbaikan dan pengganti an aset	- Belum terdapat kontrol pada aset	R	3	S	- Menghubungkan pada *stabilizer* - Membuat jadwal pemeliharaan aset secara berkala - Menggunakan kabel dengan kualitas baik - Membuat dokumen inventarisasi aset
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				4	S	
		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				5	S	

		- Sambungan kabel yang buruk (V8)				3	S	
A10 (CCTV)	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)	Biaya perbaikan dan pengganti an, pelanggar an kode etik dan hukum	- Belum terdapat kontrol pada aset	S	6	T	- Menghubungkan pada UPS - Membuat jadwal pemeliharaan aset secara berkala - Menggunakan kabel dengan kualitas yang baik dan menambahkan pelindung khusus untuk kabel
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalaha n instalasi media penyimpanan (V1)				4	S	
		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				4	S	
		- Sambungan kabel yang buruk (V8)				4	S	
A11 (Router)	Debu dan Korosi (T3)	- Kerentanan terhadap kelembapan, debu, kotoran (V5)	Biaya perbaikan , biaya pengganti an, terhambat nya	- Pembagian jaringan publik dan privat - Pemeliharaan dengan reset IP secara rutin	S	4	S	- Membuat standar kondisi ruangan - Membuat jadwal pemeliharaan aset secara berkala - Instalasi dan pemeliharaan
		- Kerentanan terhadap suhu yang bervariasi (V6)				4	S	

		- Penyimpanan yang tidak dilindungi (V7)	proses bisnis, penyalah gunaan potensi informasi	- Pembatasan hak akses terhadap aset		5	S	dilakukan oleh ahli - Memaksimalkan penggunaan UPS - Menggunakan kabel dengan kualitas yang baik - Melakukan manajemen jaringan secara efektif
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				5	S	
		- Kerentanan terhadap variasi voltase (V3)				5	S	
	Hilangnya Pasokan Listrik (T4)	- Sambungan kabel buruk (V8)				5	S	
		- Manajemen jaringan yang tidak cukup (V9)				4	S	
A12 (Switch)	Debu dan Korosi (T3)	- Kerentanan terhadap kelembapan, debu, kotoran (V5)	Biaya perbaikan, biaya pengganti an, terhambat nya	- Terdapat sensor suhu ruangan - Menggunakan grounding	S	4	S	- Membuat standar kondisi ruangan - Membuat jadwal pemeliharaan aset secara berkala - Instalasi dan pemeliharaan
		- Kerentanan terhadap suhu yang bervariasi (V6)				4	S	

		- Penyimpanan yang tidak dilindungi (V7)	proses bisnis, penyalah gunaan potensi informasi			5	S	dilakukan oleh ahli - Memaksimalkan penggunaan UPS - Menggunakan kabel dengan kualitas yang baik - Melakukan manajemen jaringan secara efektif
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				5	S	
		- Kerentanan terhadap variasi voltase (V3)				5	S	
	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)				5	S	
		- Sambungan kabel buruk (V8)				5	S	
		- Manajemen jaringan yang tidak cukup (V9)				4	S	
A13 (Mesin Presensi)	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)	Biaya perbaikan dan	- Belum terdapat	R	5	S	- Menghubungkan pada UPS

	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)	pengganti an, pelanggar an kode etik	kontrol pada aset		5	S	- Membuat jadwal pemeliharaan aset secara berkala - Menggunakan kabel dengan kualitas yang baik dan menambahkan pelindung khusus untuk kabel
		- Kerentanan terhadap kelembapan, debu, kotoran (V5)				5	S	
		- Sambungan kabel yang buruk (V8)				5	S	
A14 (Mixer Video, Lampu Shooting, Video Streaming, Mixer Audio)	Hilangnya Pasokan Listrik (T4)	- Kerentanan terhadap variasi voltase (V3)	Biaya perbaikan dan pengganti an aset	- Disimpan dalam kotak khusus penyimpanan aset dengan bahan fiber - Menggunakan stabilisator ketika digunakan	R	4	S	- Menggunakan *stabilizer* - Menggunakan kabel dengan kualitas yang baik dan menambahkan pelindung khusus untuk kabel
	Kerusakan Peralatan (T6)	- Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan (V1)				4	S	
		- Sambungan kabel yang buruk (V8)				4	S	
A15 (Flash, Tripod,		- Kurangnya pemeliharaan/kesalaha	Biaya perbaikan		R	3	S	- Menyediakan media

Lensa, Baterai)	Kerusakan Peralatan (T6)	n instalasi media penyimpanan (V1)	dan pengganti an aset	- Disimpan dalam *Dry Box*				penyimpanan aset di tempat terbuka
		- Kerentanan terhadap suhu yang bervariasi (V6)				3	S	- Membuat jadwal pemeliharaan aset secara berkala
		- Penyimpanan yang tidak dilindungi (V7)				3	S	- Membuat dokumen inventarisasi aset

REVISI

No	Revisi	Halaman
1.	Penambahan batasan masalah mengenai penggunaan ISO 27005:2008 karena keterbatasan referensi ISO 27005:2013	Halaman 3 pada bagian batasan masalah poin ke 2
2.	Latar belakang pentingnya melakukan manajemen risiko	Halaman 1 pada bagian Latar Belakang paragraf ke 2 dan 3
3.	Rekomendasi dari penilaian risiko	Halaman 37 dan Lampiran *Risk Register* pada kolom rekomendasi
4.	Format penulisan laporan	Font, Typo, No Halaman, abstrak