BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dalam proses pengelolaan risiko, diawali dengan mengetahui narasumber yang tepat agar memperoleh data yang valid pada Diskominfo DIY. Penelitian dilanjutkan dengan melihat klausul kerangka kerja ISO 31000:2018 untuk mengukur efektivitas dan kematangan organisasi atau instansi dalam menerapkan manajemen risiko, yang kemudian lanjutkan dengan melakukan identifikasi aset aplikasi (perangkat lunak) dan aset aplikasi tersebut akan diklasifikasikan sesuai penelitian terdahulu yang merujuk pada dokumen standar ISO. Pada klasifikasi aset aplikasi (perangkat lunak) terdapat lima jenis pengkategorian, diantaranya: situs, sistem operasi pada *client*, perangkat lunak pelayanan; pemeliharaan; dan administrasi, aplikasi bisnis, serta perangkat lunak umum. Sesuai dengan klasifikasi aset tersebut, dilakukan proses identifikasi kemungkinan risiko dan kemungkinan dampak yang akan muncul.

Dari proses identifikasi, dilakukan proses pengukuran risiko yang dibedakan menjadi dua bagian dengan melihat pengklasifikasian aset aplikasi pada situs; perangkat lunak pelayanan; pemeliharaan; dan administrasi, aplikasi bisnis, dan perangkat lunak umum yang terdiri dari 2 risiko tingkat tinggi (*high*), 4 risiko tingkat sedang (*medium*), 11 risiko tingkat rendah (*low*), sedangkan pengklasifikasian aset aplikasi lainnya seperti sistem operasi pada *client* yang terdiri dari 3 risiko tingkat sedang (*medium*) dan 4 risiko tingkat rendah (*low*).

Sehingga, pada proses pengendalian risiko peneliti memberikan opsi, saran, atau rekomendasi berdasarkan tingkatan risiko dan klasifikasi terhadap aset aplikasi. Pengendalian risiko ini dapat berupa peraturan mengenai pengelolaan dan keamanan hak akses, pemantauan yang dilakukan secara berkala dan teratur, pengadaan pelatihan terhadap karyawan, dan penambahan infrastruktur dalam proses pengamanan aset. Pengendalian risiko ini dilakukan dengan studi literatur pada dokumen, jurnal, *e-book*, *proceeding*, dan prosedur yang relevan serta dapat diterapkan sesuai kondisi aset pada Diskominfo DIY.

5.2. Saran

Berdasarkan penelitian yang telah dilakukan, berikut merupakan saran dari peneliti, antara lain:

1. Dalam pengelolaan manajemen risiko, Diskominfo DIY perlu melakukan tindakan lanjutan untuk menentukan nilai risiko lain setelah tindakan pengendalian risiko sebelumnya.
2. Pada penelitian ini, dilakukan pengelolaan risiko terhadap aset aplikasi (perangkat lunak) menggunakan ISO 31000:2018. Untuk penelitian berikutnya, dapat menerapkan pengelolaan risiko terhadap aset perangkat keras, aset personil, ataupun aset fisik lainnya.
3. Melakukan kegiatan lanjutan berupa pemantauan dan peninjauan, serta pencatatan atau pelaporan terhadap standar ISO 31000:2018.

DAFTAR PUSTAKA

[1]. H. Nugroho, "Analisis Manajemen Resiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4.1," *Konf. Nas. ICT-M Politek. Telkom*, 2012.

[2]. A. Saharuddin, "Peran Teknologi Pembelajaran Islam dalam Organisasi Belajar," *J. Pend. Edumaspul*, vol. 1, no. 1, pp. 1-8, 2017, doi: https://doi.org/10.33487/edumaspul.v1i1.34.

[3]. M. Irawan Padli Nasution, "Strategi Pembelajaran Efektif Berbasis *Mobile Learning* pada Sekolah Dasar," *J. Iqra'*, vol. 1, no. 1, pp. 1-14, 2015.

[4]. I. Pangkey, and S. Pinatik, "Analisis Efektivitas dan Efisiensi Anggaran Belanja pada Dinas Kebudayaan dan Pariwisata Provinsi Sulawesi Utara," *J. EMBA*, vol. 3, no. 4, pp. 33-43, 2015, doi: https://doi.org/10.35794/emba.v3i4.10581.

[5]. Gabby E. M. S., Bonny F. S., and Robert J. M. M., "Manajemen Risiko Kesehatan dan Keselamatan Kerja (K3) (Studi Kasus pada Pembangunan Gedung SMA Eben Haezar)," *J. Ilm. Media Eng.*, vol. 4, no. 4, pp. 229-238, 2014.

[6]. J. Sleeman, T. Finin, and M. Halem, "Temporal Understanding of Cybersecurity Threats," no. May, pp. 115–121, 2020, doi: 10.1109/bigdatasecurity-hpsc-ids49724.2020.00030.

[7]. V. Gaftea, "Socio-economic Major Risks Related to the Information Technology," *Procedia Econ. Financ.*, vol. 8, no. 14, pp. 336–345, 2014, doi: 10.1016/s2212-5671(14)00099-9.

[8]. H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus: Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[9]. A. T. Ratnawati, "Analisis Faktor-Faktor yang Mempengaruhi Keberadaan Komite Manajemen Risiko (*Risk Management Committe*) (Studi Empiris pada Perusahaan Non PerbankanYang Listing di BEI)," *Media Ekon. dan Manaj.*, vol. 26, no. 2, pp. 66-78, 2012, doi: http://dx.doi.org /10.24856/mem.v26i2.196.

[10]. A. B. Setiawan, "Perencanaan Strategis Sistem Informasi pada Pusat Penanganan Insiden Keamanan Informasi Sektor Pemerintah," *J. Masy. Telemat. dan Inf.*, vol. 5, no. 1, pp. 1-24, 2014.

[11]. F. M. Ahmad., "Analisis Manajemen Risiko Dalam Mewujudkan *Good Governance* pada Pemerintah Kabupaten Bandung Barat," *Pros. Ind. Res. Work. and Natl. Semin*, vol. 10, no. 1, pp. 1182-1192, 2019, doi: https://doi.org/10.35313/irwns.v10i1.1470.

[12]. M. Indriani, A. R. Arafah, and F. N. Islamy, "Implementasi Peraturan Pemerintah Nomor 82 Tahun 2012 Sebagai Upaya Negara Mencegah Cybercrime Dalam Sistem Transaksi Elektronik," *J. Yuridika*, vol. 29, no. 3, pp. 331-345, 2014, doi: http://dx.doi.org/10.20473/ydk.v29i3.375.

[13]. W. Hermawan, "Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE)," *InComtech: J. Telekomun. dan Komput.*, vol. 9, no. 2, pp. 130-140, 2019, doi: 10.22441/incomtech.v9i2.6474.

[14]. International Organization for Standardization, "INTERNATIONAL STANDARD ISO/IEC Information technology - Security techniques - Information security management systems - Requirements," *Inf. Technol. - Secur. Tech. - Inf. Secur. Manag. Syst. - Requir.*, vol. 2014, no. ISO/IEC 27001:2013, p. 38, 2013.

[15]. A. Asriyanik and Prajoko, "Manajemen Keamanan Informasi pada Sistem Informasi Akademik Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 315–325, 2018, doi: 10.28932/jutisi.v4i2.792.

[16]. A. Ismiyanto, "Diskominfo DIY Catat 30.000 Serangan Hacker Sasar Server Pemda," 2019. [Online]. Available: https://jogja.tribunnews.com /2019/04/22/diskominfo-diy-catat-30000-hacker-serang-server-pemda.

[17]. S. Salahuddin, A. Ambarwati, and M. N. Al Azam, "Identifikasi Risiko Keamanan Informasi Menggunakan ISO 27005 pada Sebuah Serguruan Tinggi Swasta di Surabaya," *Semin. Nas. Sist. Inf.*, pp. 990–996, 2018.

[18]. F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," *J. Pengemb. IT*, vol. 02, no. 02, pp. 1–8, 2017.

[19]. A. N. Rilyani, Y. Firdaus, and D. D. Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus: i-Gracias Telkom University)," *e-Proceeding Eng.*, vol. 02, no. 02, pp. 1–8, 2015.

[20]. Zulkifli, "Mengukur Indeks Keamanan Informasi dengan Metode OCTAVE Berstandar ISO 27001 pada Universitas Almuslim-Bireuen," *J. TECHSI.*, vol. 8, no. 1, pp. 157-166, 2016.

[21]. O. B. Umum, "Direktorat Penelitian dan Pengaturan Perbankan," no. November, p. 2009, 2007.

[22]. International Organization for Standardization, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements," *Inf. Technol. — Secur. Tech. — Inf. Secur. Manag. Syst. — Requir.*, vol. 2014, no. ISO/IEC 27001:2013, p. 38, 2013.

[23]. P. Hopkin and I. of R. Management, Fundamentals of Risk Management, vol. 2nd Editio. 2010.

[24]. KBBI, "Definisi Risiko menurut Kamus Besar Bahasa Indonesia." [Online]. Available: https://kbbi.web.id/risiko.

[25]. Cardiff and Vale University Health Board, "Risk Assessment and Risk Register Procedure," no. January 2013, pp. 1–22, 2017.

[26]. B. L. Mahersmi, F. A. Muqtadiroh, and B. C. Hidayanto, "Analisis Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE dan Kontrol ISO 27001 pada DISHUBKOMINFO Kabupaten Tulungagung," *J. of Inf. Syst.*, vol. 5, no. 1, pp. 181-194, 2016.

[27]. I. Häring, "Risk Analysis and Management: Engineering Resilience," *Risk Anal. Manag. Eng. Resil.*, pp. 1–365, 2016, doi: 10.1007/978-981-10-0015-7.

[28]. A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi ITOP," *J. Sist. Inf. dan Tek.*, vol. 2, no.1, pp. 13-20, 2019, doi: 10.24176/sitech.v2i1.3122.

[29]. BSI Standards Publication, "ISO 31000:2018 Risk Management – Guidelines". 2nd ed. Switzerland : BSI Standards Limited, 2018.

[30]. ISO – The International Organization for Standardization, "ISO 31000:2009 Risk Management – Principles and Guidelines". 1st ed. Switzerland : The International Organization for Standardization, 2009.

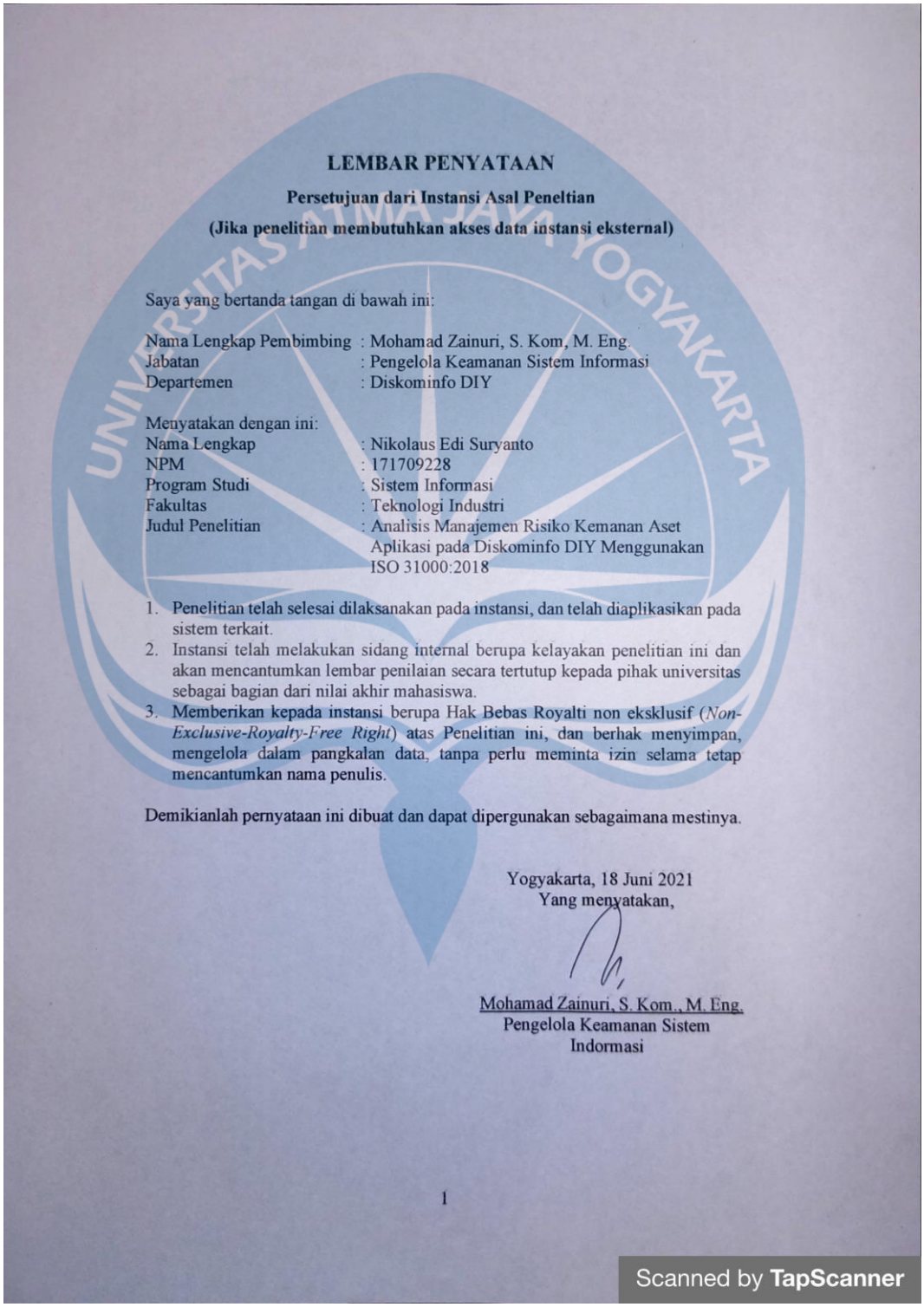
[31]. A. Fernando, "Analisis Manajemen Risiko Sistem Informasi *Automotive Management System* Menggunakan Metode ISO 31000", *Rep. UIN Suska Riau*, 2020.

[32]. K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000:2018 (Studi Kasus: CV. XY)", *J. SEBATIK*, vol. 23, no. 01, pp. 277-283. 2019. doi: 10.46984/sebatik.v23i1.572.

[33]. R. M. Candra, Y. N. Sari, I. Iskandar, and F. Yanto, "Sistem Manajamen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018", *J. CoreIT*, vol. 5, no. 1, pp. 19-28. 2019. doi: 10.24014/coreit.v5i1.8200.

LAMPIRAN

Lembar Pernyataan



LEMBAR PENYATAAN

Persetujuan dari Instansi Asal Peneltian

(Jika penelitian membutuhkan akses data instansi eksternal)

Saya yang bertanda tangan di bawah ini:

Nama Lengkap Pembimbing	: Mohamad Zainuri, S. Kom, M. Eng.
Jabatan	: Pengelola Keamanan Sistem Informasi
Departemen	: Diskominfo DIY

Menyatakan dengan ini:

Nama Lengkap	: Nikolaus Edi Suryanto
NPM	: 171709228
Program Studi	: Sistem Informasi
Fakultas	: Teknologi Industri
Judul Penelitian	: Analisis Manajemen Risiko Kemanan Aset Aplikasi pada Diskominfo DIY Menggunakan ISO 31000:2018

1. Penelitian telah selesai dilaksanakan pada instansi, dan telah diaplikasikan pada sistem terkait.
2. Instansi telah melakukan sidang internal berupa kelayakan penelitian ini dan akan mencantumkan lembar penilaian secara tertutup kepada pihak universitas sebagai bagian dari nilai akhir mahasiswa.
3. Memberikan kepada instansi berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas Penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 18 Juni 2021
Yang menyatakan,

Mohamad Zainuri, S. Kom., M. Eng.
Pengelola Keamanan Sistem
Indormasi

1

Contoh Kuesioner

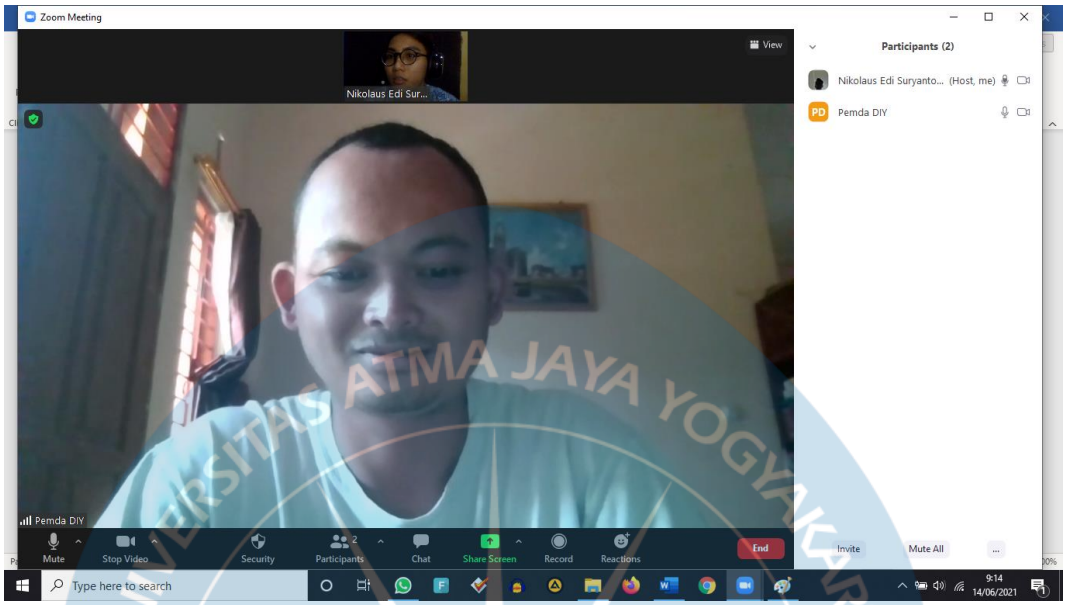
PERHATIAN! BERIKUT MERUPAKAN TATA CARA PENGERJAAN KUESIONER:
1. Responden cukup mengisi **Kolom KUNING (4 yaitu RISIKO dan 5 yaitu DAMPAK).**
2. Kolom 4, **RISIKO (pilih salah satu)** dengan mengisi angka skala 1 - 5 dengan frekuesi **PALING KECIL.**
3. Kolom 5, **DAMPAK (pilih salah satu)** dengan mengisi angka skala 1 - 5 dengan frekuesi **PALING RENDAH.**
4. **JIKA**, kemungkinan **RISIKO** tidak dapat terjadi, **MAKA** diisi dengan skala 0.
5. Mohon diisi sesuai dengan kondisi instansi Responden.

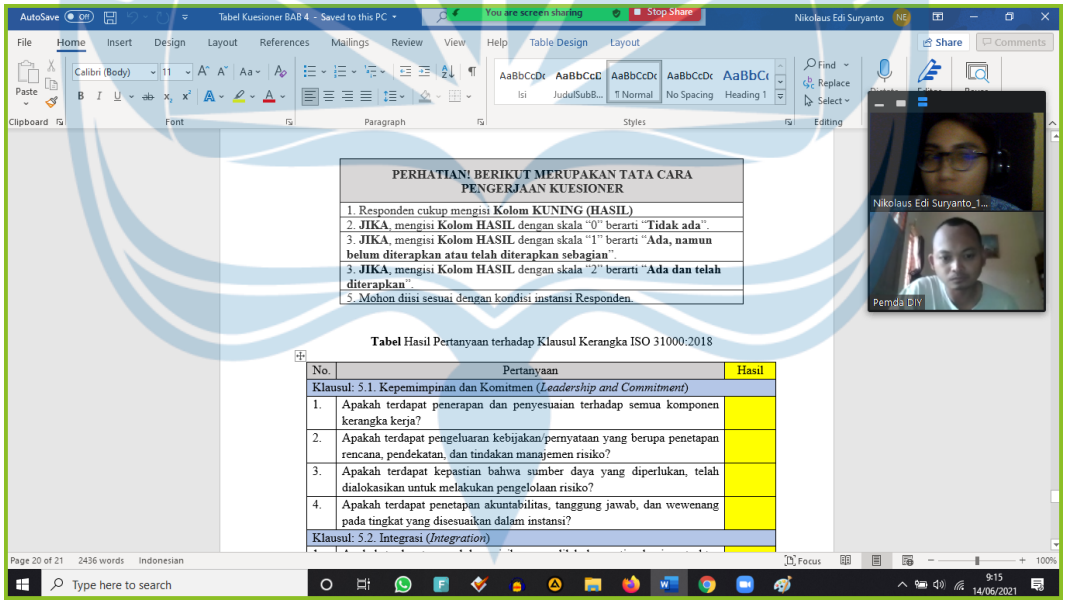
Tabel Pengukuran Risiko			
Index	**Singakatan**	**Probabilitas**	**Waktu**
5	SB	Sangat Besar	< 1 tahun
4	B	Besar	1 – 2 tahun
3	S	Sedang	2 – 4 tahun
2	K	Kecil	3 – 5 tahun
1	SK	Sangat Kecil	> 5 tahun

Tabel Pengukuran Dampak		
Index	**Singakatan**	**Probabilitas**
5	SB	Sangat Besar
4	B	Besar
3	S	Sedang
2	R	Rendah
1	SR	Sangat Rendah

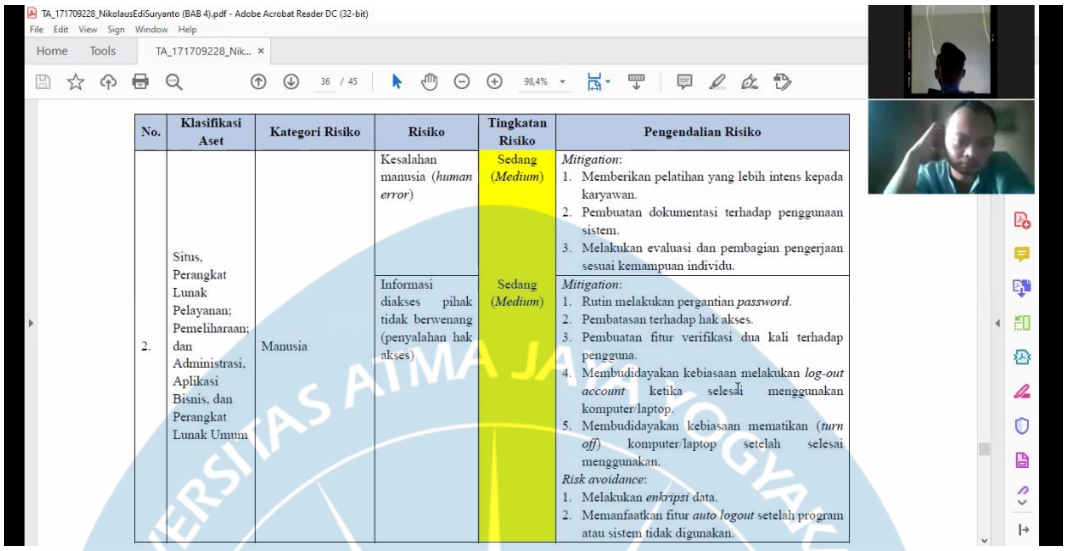
No.	Klasifikasi Aset	Aset	Kategori Risiko	Pengukuran				Skor *RPN*
				Risiko		Dampak		
0	1	2	3	Keterangan	4	Keterangan	5	6
1.	Situs	*Website* Diskominfo DIY	Manusia	Pencurian perangkat		Kerugian dari segi finansial, dan kehilangan data		
				Kesalahan manusia (*Human error*)		Proses kinerja menjadi lambat, dan kesalahan penginputan data		
				Informasi diakses pihak tidak berwenang (penyalahan hak akses)		Kehilangan data, terhambatnya aktivitas layanan instansi, dan kehilangan reputasi dengan pihak lain		
				Kebocoran data terhadap informasi internal		Kerugian finansial, dan kehilangan data atau informasi		
				Kerusakan akibat ulah manusia (vandalisme, terorisme, pembajakan, dan *cybercrime*)		Manipulasi data, kebocoran data, dan kerugian finansial		

Wawancara dan Pengerjaan Kuesioner





Proses Justifikasi



TA_171709228_NikolausEdiSuryanto (BAB 4).pdf - Adobe Acrobat Reader DC (32-bit)

No.	Klasifikasi Aset	Kategori Risiko	Risiko	Tingkatan Risiko	Pengendalian Risiko
2.	Situs, Perangkat Lunak Pelayanan; Pemeliharaan; dan Administrasi, Aplikasi Bisnis, dan Perangkat Lunak Umum	Manusia	Kesalahan manusia (*human error*)	Sedang (*Medium*)	*Mitigation*: 1. Memberikan pelatihan yang lebih intens kepada karyawan. 2. Pembuatan dokumentasi terhadap penggunaan sistem. 3. Melakukan evaluasi dan pembagian pengerjaan sesuai kemampuan individu.
			Informasi diakses pihak tidak berwenang (penyalahan hak akses)	Sedang (*Medium*)	*Mitigation*: 1. Rutin melakukan pergantian *password*. 2. Pembatasan terhadap hak akses. 3. Pembuatan fitur verifikasi dua kali terhadap pengguna. 4. Membudidayakan kebiasaan melakukan *log-out account* ketika selesai menggunakan komputer/laptop. 5. Membudidayakan kebiasaan mematikan (*turn off*) komputer/laptop setelah selesai menggunakan. *Risk avoidance*: 1. Melakukan *enkripsi* data. 2. Memanfaatkan fitur *auto logout* setelah program atau sistem tidak digunakan.

TABEL REVISI

No.	Revisi	Halaman Revisi
1.	Abstrak terlalu panjang, lebih dipersingkat lagi.	Bagian abstrak dilakukan perubahan dan lebih dirangkum kembali pada halaman vii dan viii.
2.	BAB I: perbaikan rumusan masalah pada bagan keterkaitan.	BAB I: melakukan perubahan rumusan masalah terhadap bagan keterkaitan pada halaman 5.
3.	BAB IV: perbaiki secara umum mitigasi risiko (*server down*).	BAB IV: melakukan penambahan pengendalian risiko atau mitigasi terhadap *server down* dan *overcapacity* pada halaman 66.
4.	BAB IV: pada bagian justifikasi, kata "sangat tepat" perlu dilakukan perubahan.	BAB IV: pada bagian justifikasi, kata "sangat tepat" telah diubah menjadi "sesuai' pada halaman 77.
5.	BAB IV: pada bagian justifikasi, perlu ditambahkan umpan balik atau *feedback* dari narasumber.	BAB IV: pada bagian justifikasi, dilakukan penambahan narasi umpan balik atau *feedback* dari narasumber pada halaman 77.