

ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI INLISLITE DI DINAS KEARSIPAN DAN PERPUSTAKAAN PROVINSI NUSA TENGGARA TIMUR

Gery Gerald Moleong, Andeka Rocky Tanaamah

Program Studi Sistem Informasi, Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana, Jl. Diponegoro No.52-60 Salatiga, Indonesia
682017039@student.uksw.edu

ABSTRAK

Aplikasi INLISLite digunakan oleh Dinas Kearsipan dan Perpustakaan provinsi Nusa Tenggara Timur, khususnya pada bagian perpustakaan untuk mengelola perpustakaan secara digital. Aktivitas digitalisasi perpustakaan ini tidak luput dari setiap risiko yang mengancam keamanan aplikasi, sehingga agar fungsi digitalisasi perpustakaan ini berjalan baik dibutuhkan analisis risiko untuk memetakan dengan jelas risiko apa saja yang ada, seperti apa analisisnya, bagaimana tingkat risiko teknologi informasi pada aplikasi INLISLite saat ini dan seperti apa sikap yang hendak diambil untuk memitigasi risiko – risiko yang ada. Analisis risiko menggunakan ISO 31000 yang terdiri dari 2 bagian besar yakni tahapan penilaian risiko (terdapat metode identifikasi, analisis, dan evaluasi risiko) dan perlakuan risiko. Hasil analisis risiko berupa dokumentasi daftar risiko, dampak dan kecenderungan munculnya risiko, tingkat keparahan, dan usulan perlakuan risiko. Produk penelitian ini dapat dipakai menjadi alternatif referensi untuk mencegah sampai meminimalisir risiko yang ada sehingga risiko – risiko tidak sampai membuat produktifitas instansi menjadi terhambat.

Kata kunci : Analisis Risiko, ISO 31000, INLISLite (*Integrated Library System*).

1. PENDAHULUAN

Teknologi telah berkembang sedemikian rupa dan dampak penggunaan teknologi secara nyata telah membantu manusia dalam pencapaian tujuan mereka. Besarnya pengaruh sumber daya teknologi bagi kepentingan manusia membuat pemerintahan di negara maju maupun negara berkembang terus mendorong pemanfaatan dari sumber daya tersebut untuk dimaksimalkan. Di Indonesia, Khususnya di wilayah NTT, salah satu lembaga instansi pemerintahan yang telah memanfaatkan sumber daya teknologi adalah Dinas Kearsipan & Perpustakaan Provinsi NTT.

Penelitian ini akan berfokus pada bagian perpustakaan dari dinas terkait. Khusus untuk bagian Perpustakaan, instansi menggunakan aplikasi dalam membantu kerja – kerja mengelola perpustakaan secara digital, yakni INLISLite. INLIS (*Integrated Library System*) Lite merupakan aplikasi opensource berbasis web (*webbased application software*) yang dibuat dan dikembangkan oleh Perpustakaan Nasional RI untuk menghimpun koleksi nasional dalam jaringan Perpustakaan Digital Nasional Indonesia, dan telah digunakan oleh Dinas Kearsipan dan Perpustakaan Provinsi NTT untuk membantu instansi mengembangkan pengolahan dan pelayanan perpustakaan berbasis IT.

Begitu vitalnya peran aplikasi INLISLite, maka penting sebagai pengguna aplikasi dalam hal ini instansi untuk selalu memonitor aplikasi selalu terkendali dan sebisa mungkin aman dari ancaman – ancaman terhadap aplikasi. Karena pada dasarnya, setiap aktivitas yang dilakukan punya risiko dan setiap risiko yang ada perlu diketahui dan diambil tindakan mitigasi agar tidak mengganggu keamanan aplikasi

INLISLite, yang secara langsung akan berdampak pada aktivitas pengelolaan perpustakaan.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Studi tentang manajemen resiko menggambarkan pentingnya kesadaran terhadap kebutuhan akan manajemen resiko yang menyeluruh demi kelangsungan organisasi. Terlihat dari hasil penelitian yang menemukan resiko tak terduga serta dampak dari penanganan-penanganan resiko temuan [1] - [3].

Penggunaan Metode kerja atau framework dalam manajemen resiko bervariasi. Salah satu framework yang dipakai dalam manajemen resiko ialah ISO 3100 yang diterbitkan oleh International Organization for Standardization. Studi tentang manajemen resiko berbasis ISO 31000 membuktikan ISO 31000 para peneliti ini dibantu membuat peta manajemen resiko dalam organisasi dengan melakukan tahapan - tahapan seperti identifikasi resiko, penilaian resiko, pengelompokkan resiko berdasarkan penilaian sebelumnya, evaluasi resiko berdasarkan matriks (*likelihood*) dan dampak (*impact*) resiko serta perlakuan resiko [4] - [6].

Mitigasi atau perlakuan resiko dalam manajemen resiko menjadi sangat krusial karena dampak dari mitigasi akan sangat mempengaruhi aktivitas bisnis yang sedang berjalan. Sehingga dibutuhkan analisis resiko yang mendalam serta komprehensif demi membuat mitigasi resiko yang efektif dan berkelanjutan. Hasil Studi dengan mitigasi risiko yang telah dilakukan menghasilkan daftar perlakuan terhadap resiko yang telah melewati tahapan proses analisis yang menyeluruh terhadap semua resiko temuan [7] - [8].

Berdasarkan penelitian terdahulu mengungkapkan adanya hubungan dengan penelitian yang penulis lakukan tentang kerangka dan prosedur mengidentifikasi aset-aset teknologi informasi, kemungkinan risiko, dampak yang bisa ditimbulkan, menilai dan mengevaluasi risiko, serta menyikapi risiko. Penulis melakukan sebuah penelitian yang bertujuan untuk memberikan usulan perlakuan risiko terhadap setiap kemungkinan risiko, baik risiko yang pernah dihadapi oleh instansi dan mengantisipasi kemungkinan risiko yang belum pernah ada tetapi mempunyai kemungkinan untuk muncul pada masa depan instansi.

2.2. Teknologi Informasi

Menurut Bodnar dan Hopwood (1995) Teknologi Informasi (TI) adalah semua cara yang terunifikasi digunakan untuk memperoleh, menggarap, dan menyampaikan data secara elektronik menjadi informasi dalam banyak bentuk yang bermanfaat bagi penggunaannya [9].

Selanjutnya Haag dan Keen (1996) mengartikan TI serupa alat bantu anda yang bekerja dengan informasi untuk mengerjakan tugas-tugas mengenai pemrosesan informasi tersebut [10].

2.3. Tata Kelola Teknologi Informasi

Weill dan Ross (2004) menyebut tata kelola TI sebagai hak pengambilan keputusan dan skema akuntabilitas untuk mengiatkan perilaku yang dikehendaki dalam pemanfaatan TI [11].

2.4. Risiko

Menurut Hanafi (2006), Risiko merupakan bahaya, akibat atau konsekuensi yang bisa terjadi akibat sebuah proses yang sedang berlangsung atau kejadian yang akan datang [12].

2.5. Manajemen Risiko

Menurut Djohanputro (2008) adalah proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan risiko, dan memonitor dan mengendalikan penanganan risiko [13].

2.6. Framework ISO 31000

Merupakan standar pengelolaan risiko yang dibuat oleh International Organization for Standardization (ISO). Standar ini dimaksudkan untuk memastikan bahwa produk dan layanan yang dihasilkan perusahaan aman, andal, dan berkualitas baik.

3. METODE PENELITIAN

Framework ISO 31000 merupakan standar pengelolaan risiko yang dibuat oleh International Organization for Standardization (ISO). Standar ini dimaksudkan untuk memastikan bahwa produk dan layanan yang dihasilkan perusahaan aman, andal, dan berkualitas baik. Terdapat 2 Bagian Utama. Bagian Pertama yakni Risk Assesment (Penilaian Resiko).

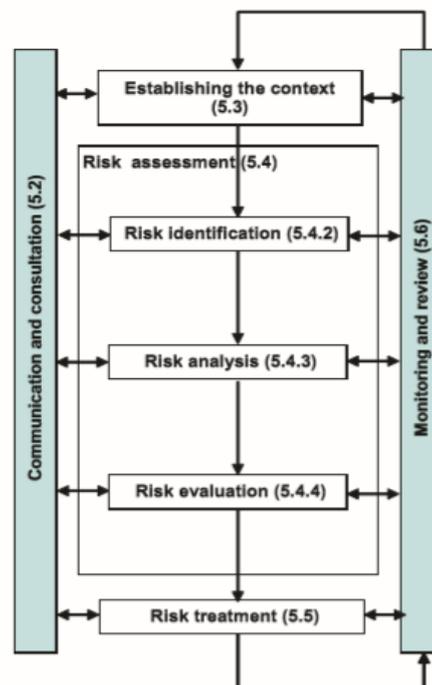
Terdapat 3 proses dalam Penilaian Risiko, yakni Identifikasi Risiko, Analisis Risiko, dan Evaluasi Risiko.

Identifikasi risiko adalah proses penentuan risiko yang berpotensi mempengaruhi organisasi dalam mencapai tujuannya.

Analisis risiko adalah upaya memahami risiko secara mendalam.

Kemudian Evaluasi risiko merupakan proses evaluasi terhadap tingkat kedaruratan setiap risiko lewat kriteria yang ada.

Bagian Kedua yakni Risk Treatment (Perlakuan Risiko), merupakan upaya pemberian usulan antisipatif dan penangulangan terhadap setiap risiko.



Gambar 1. Risk Management Principles and Guidelines

Penulis menggunakan metode Kualitatif - Studi kasus yang berfokus pada sebuah kasus atau peristiwa dan mengambil sample pada sebuah kelompok. Sehingga penulis dapat memperoleh data yang memadai terhadap obyek penelitian.

Data primer digunakan dalam penelitian ini, berupa wawancara dan dokumen terkait dari narasumber.

Peneliti mengumpulkan data lewat wawancara dan kuisioner dengan petugas layanan otomatis informasi dan maintenance hardware-software instansi serta petugas Data entry.

4. HASIL DAN PEMBAHASAN

4.1. Penilaian Risiko (Risk Assesment)

Terdapat 3 tahapan dalam proses menilai risiko, dimulai dengan Risk Identification (Identifikasi Risiko) dilanjutkan dengan Risk Analyst (Analisis Risiko)

Risiko) dan berlanjut ke tahapan Risk Evaluation (Evaluasi Risiko).

4.2. Identifikasi Aset

Mengidentifikasi risiko pada INLISLite dimulai dengan mengenali aset - aset pada sisi Teknologi dan Infrastruktur yang ada untuk menunjang penggunaan INLISLite itu sendiri, melalui proses wawancara dengan Petugas layanan otomasi dan koordinator pemeliharaan infrastruktur IT Dinas Kearsipan dan Perpustakaan Provinsi NTT.

Tabel 1. Aset terkait aplikasi INLISLITE

Elemen Sistem Informasi	Aset Organisasi
Hardware	8 AIO PC client 1 Server Komputer
Software	Integrated Library System Lite (INLISLite) Terinstall pada masing - masing AIO PC Client
Data	- Data Buku - Data User - Data Riwayat Pelanggaran Peminjam

4.3. Daftar Kemungkinan Risiko

Setelah mengetahui daftar aset yang berhubungan dengan INLISLite, selanjutnya melakukan proses identifikasi risiko yang mengancam keberadaan setiap aset.

Tabel 2. Identifikasi Kemungkinan Risiko

Asal Risiko	Bentuk Risiko
Alam/Lingkungan	Badai
	Banjir
	Debu
	Gempa bumi
	Kebakaran
	Kelembapan
Manusia	Petir
	Akses tanpa otorisasi
	Cybercrime
	Hilangnya data
	Pencurian Perangkat
Malfungsi Hardware dan System	Perusakan Perangkat
	Data corrupt
	Gagal Backup
	Koneksi Jaringan Terputus
	Kerusakan hardware karena masalah tegangan listrik
	Lemot karena spesifikasi sudah tua
	Overheat
	Server Down
	System Crash

Dari proses identifikasi risiko, telah ditemukan sebanyak 3 sumber risiko, antara lain risiko yang bersumber dari Alam atau lingkungan, dari manusia dan dari malfungsi system. dari ketiga sumber diatas, telah ditemukan total 19 risiko spesifik yang mengancam penggunaan dan keamanan aplikasi INLISLite.

4.4. Dampak Kemungkinan Risiko

Merespon temuan risiko, selanjutnya dilakukan proses identifikasi dampak yang ditimbulkan dari masing - masing risiko.

Tabel 3. Identifikasi Dampak Risiko

Asal Risiko	ID	Bentuk Risiko	Dampak
Alam/ Lingkungan	R 01	Badai	hardware komputer yang terdampak akan rusak dan mengganggu penggunaan Aplikasi INLISLite
	R 02	Banjir	hardware komputer yang terdampak akan rusak dan mengganggu penggunaan Aplikasi INLISLite
	R 03	Debu	Hardware mudah panas, memperlambat kinerja hardware dan respon system sehingga penggunaan aplikasi INLISLite menjadi terhambat
	R 04	Gempa bumi	hardware komputer yang terdampak akan rusak dan mengganggu penggunaan Aplikasi INLISLite
	R 05	Kebakaran	hardware komputer yang terdampak akan rusak dan menghentikan penggunaan system informasi
	R 06	Petir	korsleting listrik membuat hardware rusak dan menghambat aktivitas penggunaan system informasi
Manusia	R 07	Akses tanpa otorisasi	Data penting instansi teredit, terhapus atau hilang akibat diakses user gelap, penggunaan system informasi akan terhambat.
	R 08	Cybercrime	Aplikasi tak dapat diakses, data penting instansi diambil atau hilang dan aplikasi INLISLite tidak dapat dioperasikan
	R 09	Hilangnya data	Mengganggu manajemen data oleh user sehingga penggunaan aplikasi INLISLite terhenti
	R 10	Pencurian Perangkat	Instansi mengalami kerugian materil dan waktu akibat hilangnya aset instansi, serta penggunaan aplikasi INLISLite dapat terhenti.
	R 11	Perusakan Perangkat	Aktivitas penggunaan aplikasi INLISLite terhenti dan instansi mengalami kerugian waktu dan finansial
Malfungsi Hardware dan System	R 12	Data corrupt	Data tidak dapat diakses sehingga menghambat alur kerja pemanfaatan aplikasi INLISLite. instansi mengalami kerugian waktu
	R 13	Gagal Backup	Hilangnya data pada periode tertentu mengakibatkan terhentinya aktivitas penggunaan aplikasi INLISLite. instansi mengalami kerugian waktu
	R 14	Koneksi Jaringan Terputus	Menghambat fungsi real time system sehingga terpaksa beralih offline membuat instansi mengalami kerugian waktu
	R 15	Kerusakan hardware karena masalah tegangan listrik	Hardware yang rusak membuat aktivitas pengoperasian aplikasi terhenti dan instansi mengalami kerugian waktu dan finansial
	R 16	Lemot karena spesifikasi sudah tua	Butuh waktu ekstra untuk melakukan aktivitas dengan aplikasi INLISLite membuat kinerja user menjadi tidak efisien dan menghambat alur kerja user. instansi mengalami kerugian waktu.
	R 17	Overheat	Mengurangi umur hardware akibat throttling. Pada waktu yang lama membuat dalam komponen hardware korslet sehingga menghambat aktivitas user
	R 18	Server Down	Aktivitas system informasi berhenti total sebagai akibat terputusnya akses ke database utama. instansi mengalami kerugian waktu
	R 19	System Crash	Aplikasi INLISLite tidak dapat diakses sehingga aktivitas user berhenti, instansi mengalami kerugian waktu

4.5. Analisis Risiko

Setelah dipetakan risiko beserta dampaknya, tahapan selanjutnya adalah menganalisis risiko. Dalam tahap ini akan dilakukan penilaian terhadap risiko dengan acuan tabel kriteria likelihood yakni besaran frekuensi atau seberapa sering risiko tersebut terjadi dan tabel kriteria impact yakni besaran efek atau seberapa besar dampak dari risiko tersebut.

Tabel 4. Likelihood

Likelihood		Deskripsi	Frekuensi per Tahun
Rating	Kriteria		
1	Rare	Risiko yang ada hampir tidak pernah terjadi	> 2 tahun
2	Unlikely	Risiko yang ada punya kemungkinan terjadi tetapi kecil (jarang)	1 – 2 tahun
3	Possible	Risiko yang ada mungkin saja terjadi (kadang-kadang)	7 – 12 bulan
4	Likely	Risiko yang ada kemungkinan besar terjadi (sering)	4 – 6 bulan
5	Almost Certain	Risiko yang ada Hampir selalu terjadi	1 – 3 bulan

Tabel 5. Impact

Impact		Deskripsi
Rating	Kriteria	
1	Insignificant	Risiko yang terjadi tidak mengganggu aktivitas instansi dan pengoperasian aplikasi.
2	Minor	Risiko yang terjadi sedikit mengambat pengoperasian aplikasi. namun aktivitas sentral instansi tidak terganggu
3	Moderate	Risiko yang terjadi mengakibatkan gangguan terhadap jalannya sebagian aktivitas instansi dan pengoperasian aplikasi..
4	Major	Risiko yang terjadi menahan nyaris semua aktivitas instansi dan pengoperasian aplikasi.
5	Catastrophic	Risiko yang terjadi menghentikan aktivitas instansi pengoperasian aplikasi karena mengalami gangguan total.

Dan berikut rincian dari penilaian risiko dengan Impact dan Likelihood, dapat dilihat di tabel 6 dibawah.

Tabel 6. Tabel penilaian risiko

ID	Bentuk Risiko	Likelihood	Impact
R01	Badai	3	4
R02	Banjir	3	3
R03	Debu	3	2
R04	Gempa bumi	3	4
R05	Kebakaran	1	5
R06	Petir	3	4
R07	Akses tanpa otorisasi	3	1
R08	Cybercrime	3	3
R09	Hilangnya data	3	3
R10	Pencurian Perangkat	2	3
R11	Perusakan Perangkat	3	3
R12	Data corrupt	3	3
R13	Gagal Backup	2	2
R14	Koneksi Jaringan Terputus	3	4
R15	Kerusakan hardware karena masalah tegangan listrik	4	4
R16	Lemot karena spesifikasi sudah tua	3	2
R17	Overheat	3	3
R18	Server Down	3	4
R19	System Crash	3	4

4.6. Evaluasi Risiko (Risk Evaluation)

Selesai mengidentifikasi risiko dan segala dampaknya, tahapan akhir dari Risk Asesment adalah Risk Evaluation atau Evaluasi Risiko. Proses mengevaluasi risiko akan menggunakan Matrix evaluasi risiko yakni penggabungan Indikator Likelihood dan Impact sebagai acuan.

Tabel 7. Matrix Evaluasi Risiko Berdasarkan Likelihood dan impact

Almost Certain	Medium	Medium	High	High	High
Likely	Medium	Medium	Medium	High	High
Possible	Low	Medium	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	Medium
Rare	Low	Low	Low	Medium	Medium
	Insignifi- cant	Minor	Moderat e	Major	Catastro phic

Tabel 8. Matrix Pengelompokkan Hasil Evaluasi Risiko

Almost Certain					
Likely				R15	
Possible	R07	R03, R16	R02, R09, R08, R11, R12, R17	R01, R04, R06, R14, R18, R19	
Unlikely		R13	R10		
Rare					R05
	Insignifi- cant	Minor	Moderat e	Major	Catastro phic

Setelah mengelompokkan seluruh resiko ke dalam matrix resiko, selanjutnya diurutkan berdasarkan tingkat resiko, selengkapnya bisa dilihat pada tabel dibawah.

Tabel 9. Tingkat Resiko

ID	Daftar Risiko	Likelihood	Impact	Risk Level
R15	Kerusakan hardware karena masalah tegangan listrik	4	4	High
R01	Badai	3	4	Medium
R02	Banjir	3	3	Medium
R03	Debu	3	2	Medium
R04	Gempa Bumi	3	4	Medium
R05	Kebakaran	1	5	Medium
R06	Petir	3	4	Medium
R08	Cybercrime	3	3	Medium
R09	Hilangnya data	3	3	Medium
R10	Pencurian Perangkat	2	3	Medium
R11	Perusakan perangkat	3	3	Medium
R12	Data Corrupt	3	3	Medium
R14	Koneksi Jaringan Terputus	3	4	Medium
R16	Lemot karena spesifikasi sudah tua	3	2	Medium
R17	Overheat	3	3	Medium
R18	Server Down	3	4	Medium
R19	System Crash	3	4	Medium
R07	Akses tanpa otorisasi	3	1	Low
R13	Gagal backup	2	2	Low

4.7. Perlakuan Risiko (Risk Treatment)

Pada bagian ini, penulis memberi usulan respon yang diambil untuk menyikapi setiap risiko pada aplikasi INLISLite.

Tabel 10. Penanganan Risiko

ID	Daftar Risiko	Level Resiko	Tindak Lanjut
R15	Kerusakan hardware karena masalah tegangan listrik	HIGH	Mengganti segera hardware yang rusak dan mencegah dengan melakukan maintenance terhadap UPS.
R01	Badai	MEDIUM	Mengatur tempat aman bagi hardware agar tidak terdampak serius.
R02	Banjir	MEDIUM	Menyediakan peralatan penunjang pembersihan dan manajemen ruang kantor agar barang elektronik terhindar dari air.
R03	Debu	MEDIUM	Rutin mengontrol kebersihan ruangan dan hardware.
R04	Gempa Bumi	MEDIUM	Memindahkan server cadangan pada tempat berbeda. Memasang proteksi khusus pada tempat atau ruangan baik server utama maupun server cadangan. Menjalankan prosedur mirroring database
R05	Kebakaran	MEDIUM	Memindahkan server cadangan pada tempat berbeda. Menjalankan prosedur mirroring database. Menyediakan pemadam api ringan dalam gedung instansi untuk Mencegah terjadinya kebakaran.

R06	Petir	MEDIUM	Memindahkan server cadangan pada tempat berbeda. Menjalankan prosedur mirroring database. Menyematkan penangkal petir.
R08	Cybercrime	MEDIUM	Memastikan PC terhubung dengan jaringan terpercaya seperti private network. Mengganti software bajakan dengan yang berlisensi. Update berkala software. Penjadwalan penggantian password. Menggunakan data encryption seperti Wi-Fi Protected Access 2 (WPA2) Khususnya pada jaringan LAN di dalam kantor.
R09	Hilangnya data	MEDIUM	Membuat restore point pada PC. Penjadwalan backup data.
R10	Pencurian perangkat	MEDIUM	Menjadwalkan perubahan password. Menyediakan dan monitoring CCTV.
R11	Perusakan perangkat	MEDIUM	Menyediakan dan monitoring alat keamanan seperti CCTV, sensor deteksi kerusakan dan alarm.
R12	Data Corrupt	MEDIUM	Mencadangkan data secara rutin pada periode tertentu. Membersihkan PC secara rutin dalam jangka waktu tertentu untuk mencegah munculnya virus/ malware. Mengatasi file corrupt di windows dengan mencoba Kombinasi System File Checker (SFC) dan kode perintah DISM pada CMD
R14	Koneksi Jaringan Terputus	MEDIUM	Perlunya manajemen bandwidth.
R16	Lemot karena spesifikasi sudah tua	MEDIUM	Melakukan review PC untuk mengetahui mengetahui bagian mana saja dari hardware atau software yang sudah waktunya dilakukan peremajaan.
R17	Overheat	MEDIUM	Memberikan pendingin yang mumpuni. Manajemen sirkulasi udara dalam ruangan.
R18	Server Down	MEDIUM	Setiap hari melakukan pencadangan data secara rutin pada database utama Instansi. Mengurangi load server untuk mencegah server down.
R19	System Crash	MEDIUM	Manajemen task manager. Menonaktifkan aplikasi kurang penting di background process.
R07	Akses tanpa otorisasi	LOW	Mengadakan penggantian password secara berkala. Manajemen role. Melapor ke admin untuk direview penggunaan role.
R13	Gagal backup	LOW	Menjadwalkan backup rutin pada database utama dan aplikasi INLISLITE

5. KESIMPULAN DAN SARAN

Penelitian analisis risiko teknologi informasi terhadap aplikasi INLISLite di Dinas Kearsipan Dan Perpustakaan Provinsi NTT telah dilaksanakan. Proses ini menggunakan tahapan - tahapan mulai dari penilaian resiko yang mencakup proses identifikasi

risiko dilanjutkan dengan proses analisis risiko kemudian proses evaluasi risiko dan diakhiri proses perlakuan risiko. Hasilnya analisis risiko terdapat total 19 Risiko yang mengancam aplikasi. Terdapat 1 risiko yang masuk dalam *level of risk* tingkat *High* yang butuh penanganan segera yakni risiko kerusakan hardware karena masalah tegangan listrik. Kemudian terdapat 16 risiko yang masuk dalam *level of risk* tingkat *Medium*, seperti badai, banjir, debu, gempa bumi, kebakaran, petir, *cybercrime*, hilangnya data, pencurian perangkat, merusakkan perangkat, *data corrupt*, koneksi jaringan terputus, Lemot karena spesifikasi sudah tua, *overheat*, *server down*, *system crash*. Serta terdapat 2 risiko yang masuk dalam *level of risk* tingkat *Low*, yakni Akses tanpa otorisasi dan gagal backup.

Usulan penanggulangan risiko ini dapat ditindak lanjuti dan dikembangkan lebih jauh lagi sesuai kebutuhan instansi kedepannya.

DAFTAR PUSTAKA

- [1] Miftakhatun, M., 2020. Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000. *Journal of Computer Science and Engineering (JCSE)*, 1(2), pp.129-146.
- [2] Ramadhan, D.L., Febriansyah, R. and Dewi, R.S., 2020. Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ. *JURIKOM (Jurnal Riset Komputer)*, 7(1), pp.91-96.
- [3] Atmojo, S.A. and Manuputty, A.D., 2020. Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, 7(3), pp.546-558.
- [4] Rahmawati, A. and Wijaya, A.F., 2019. Analisis risiko teknologi informasi menggunakan ISO 31000 pada Aplikasi ITOP. *Jurnal SITECH: Sistem Informasi dan Teknologi*, 2(1), pp.13-20.
- [5] Hutabarat, F.M. and Manuputty, A.D., 2020. Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000. *Jurnal Bina Komputer*, 2(1), pp.52-65.
- [6] Utamajaya, J.N., Afrina, A. and Fitriah, A.N., 2021. ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PERUSAHAAN TOKO UJUNG PANDANG GROSIR PENAJAM PASER UTARA MENGGUNAKAN FRAMEWORK ISO 31000: 2018. *Sebatik*, 25(2), pp.326-334.
- [7] Pramadhani, I.B., 2020. Analisis Risiko Dengan ISO 31000 Di Perpustakaan UIN Sunan Ampel Surabaya. *JBMI (Jurnal Bisnis, Manajemen, dan Informatika)*, 16(3), pp.267-275.
- [8] Sirojun, A., Rabbani, M.N., Yusril, E., Rozas, I.S., Rahayu, Y. and Muniroh, L., ANALISIS LEVEL RISIKO PADA GARUDA JAYA GARMENT MENGGUNAKAN ISO 31000. *Manajerial: Jurnal Manajemen dan Sistem Informasi*, 19(1), pp.13-23.
- [9] Bodnar, G.H. and Hopwood, W.S., 2006. *Sistem informasi akuntansi*. Jakarta: Salemba Empat.
- [10] Haag, S. and Keen, P., 1996. *Information Technology: Tomorrow's Advantage Today*. McGraw-Hill Companies, Inc., PO Box 545, Blacklick, OH 43004, Attn: Order Service.
- [11] Ross, J.W., Weill, P. and Robertson, D., 2006. *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard business press.
- [12] Hanafi, M., 2006. *Manajemen risiko*. Yogyakarta: Unit Penerbit Dan Percetakan Sekolah Tinggi Manajemen YKPN
- [13] Djohanputro, B., 2008. *Manajemen risiko korporat*. Jakarta: Ppm.