JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i3.6672

PENILAIAN RISIKO BERBASIS ISO 31000:2018 PADA UNIT TIK PERGURUAN TINGGI (STUDI KASUS: POLITEKNIK NEGERI LAMPUNG)

Pradana Marlando[1], Mardiana[2], Misfa Susanto[3]

[1,2,3] Universitas Lampung; Jalan Prof. Soemantri Brojonegoro No. 1 Bandar Lampung 35145; (0721) 704947

Keywords:
Risk;
Information Technology Risk Management;
ISO 31000:2018.

Corespondent Email:
mardiana@eng.unila.ac.id

Abstrak. Teknologi informasi sangat umum digunakan untuk sebuah organisasi kecil hingga besar yang sudah menjadi kebutuhan sehari-hari sehingga muncul risiko risiko baru terkait penggunaan teknologi informasi. Risiko-risiko tersebut memiliki dampak dan membutuhkan penanggulangan risiko yang berbeda. Dalam rangka menjaga proses bisnis tetap berjalan dengan baik karenanya diperlukan sebuah manajemen risiko yang baik tidak terkecuali perguruan tinggi dalam pelaksanaan proses bisnisnya. Peneliti melakukan penilaian risiko dengan menggunakan ISO 31000:2018 pada Unit TIK selaku penanggung-jawab kegiatan teknologi informasi di Politeknik Negeri Lampung. Penelitian ini menghasilkan penilaian risiko pada Unit TIK selaku pengelola TI di Politeknik Negeri Lampung guna menanggulangi risiko-risiko yang ada. Berdasarkan Penelitian ini menghasilkan sebuah identifikasi 30 risiko, dengan rincian 3 risiko level tinggi, 19 risiko level menengah, dan 8 risiko level rendah yang diberikan respon guna mengurangi atau mencegah risiko tersebut.

Abstract. *Information Technology are commonly used in industries for daily work so that arise the risk related to information technology use. The Risks have their own impact and require risk management. In order to keep business process going well, risk management is needed and there is no exception for univesities in implementing business process. Researchers conducted a risk risk assessment using ISO 31000:2018 on the ICT as a unit in charge of information technology activities at the Lampung State Polytechnic. With this research, it is hoped that the Lampung State Polytechnic, especially the ICT, will have risk management to address existing risks. Based on this research, an identification of 30 risks was produced, with details of 3 high-level risks, 19 medium-level risks, and 8 low-level risks that were responded to in order to reduce or prevent these risks.*

1. PENDAHULUAN

Pada era modern saat ini, penggunaan teknologi informasi merupakan hal yang sangat umum digunakan untuk sebuah organisasi kecil hingga besar. Penggunaan teknologi informasi ini digunakan untuk mempermudah pekerjaan manusia. Teknologi informasi yang baik akan dapat memberikan informasi yang relevan yang dapat digunakan manajerial untuk mengambil keputusan yang terbaik. Dengan teknologi informasi pula fungsi-fungsi manajemen seperti *Planning – Organizing – Actuating – Controlling* dapat berjalan dengan efektif dan efisien [1]. Proses yang *real time* dan *reliable* dapat dimanfaatkan untuk menunjang kebutuhan mendesak dan cepat. Pada perguruan

tinggi hal ini tentu berperan penting dalam menjalankan fungsi dan tugas perguruan tinggi serta memaksimalkan potensi yang tersedia pada perguruan tinggi [2].

Perguruan tinggi secara umum dipimpin oleh seorang dosen yang diberikan tugas tambahan. Hal ini membuat seorang pimpinan perguruan tinggi membutuhkan sebuah teknologi informasi yang dapat digunakan secara efektif dan efisien sebagai penyedia informasi [3]. Namun apakah teknologi informasi yang digunakan sudah dapat menyediakan informasi yang tepat dan sesuai dengan kebutuhan. Jika tidak maka teknologi informasi yang digunakan dapat dikatakan tidak baik karena investasi teknologi informasi yang tepat pada saat ini adalah sesuatu yang sangat berharga. Karenanya tata kelola teknologi informasi dibutuhkan untuk menjamin bahwa teknologi informasi tersebut mendukung perguruan tinggi untuk mencapai tujuan atau *goal* dari pimpinan yang telah ditentukan [4]. Hal ini akan menjadi fokus utama dari teknologi informasi di perguruan tinggi di bidang pendidikan pada penelitian ini mengambil studi kasus di Politeknik Negeri Lampung dan UPA TIK sebagai unit pengelolanya [5].

Teknologi informasi merupakan alat bantu yang vital, karena jika salah satu teknologi informasi bermasalah atau tidak dapat digunakan akan berdampak untuk keseluruhan proses yang ada [6]. Perguruan Tinggi memiliki server tersendiri untuk mengelola data dan juga menggunakan server pihak luar untuk beberapa teknologi informasinya. Tentunya hal tersebut akan memberikan keuntungan tersendiri untuk Perguruan Tinggi, namun hal tersebut juga memiliki kelemahan [7]. Karenanya sebuah manajemen risiko perlu dilakukan

Manajemen risiko merupakan hal yang wajib dimiliki atau dilakukan oleh sebuah organisasi dalam menghadapi proses bisnis. Manajemen risiko dapat mengurangi dampak yang diakibatkan sebuah risko dari suatu sistem [8]. Dengan manajemen risiko seluruh Sumber Daya Manusia yang ada di organisasi dapat melakukan pencegahan sesuai dengan prosedur yang tepat [9]. Prosedur itu umumnya didokumentasikan agar seluruh Sumber Daya Manusia dapat memahami dan mengaplikasikannya. Risiko-risiko tersebut juga dapat terjadi pada kasus di Politeknik Negeri Lampung khususnya di bagian teknologi informasi. Basis data di Politeknik Negeri Lampung merupakan hal yang sangat vital, karena basis data perlu dilindungi pada server yang aman dan *reliable*. Tidak hanya sekedar data, basis data pada perguruan tinggi dapat mencakup hal yang bersifat pribadi. Namun apakah server yang telah dilindungi dapat dikatakan aman dan *reliable*? Tentu tidak, kesalahan atau kegagalan tidak hanya terjadi pada internal organisasi namun juga eksternal yang diluar kendali kita [10]. Sebuah manajemen risiko yang tepat dari UPA TIK selaku penanggung jawab terkait TI akan dapat melindungi server dari kegagalan atau kesalahan dengan dampak seminimal mungkin karena kemungkinan untuk mencegah akan sulit. Sebuah manajemen risiko perlu dilakukan secara terstruktur dan terkendali agar dapat dilakukannya pengendalian risiko yang tepat untuk proses bisnis di Polinela, karenanya sebuah framework manajemen risiko diperlukan dalam pembuatan dokumentasi [11].

framework International Organization for Standardization (ISO) adalah sebuah standar pelaksanaan dari sebuah manajemen risiko tersebut. ISO 31000:2018 dikembangkan untuk organisasi menciptakan dan menjaga nilai dari tujuan yang diharapkan dengan cara melakukan manajemen risiko, membuat keputusan atau kebijakan dari risiko tersebut dan menentukan objektif dan peningkatan yang dibutuhkan [12].

Berdasarkan permasalahan di atas, maka diperlukan sebuah penilaian risiko untuk teknologi informasi yang saat ini digunakan di Politeknik Negeri Lampung khususnya pada UPA TIK selaku pengelola TI . Dalam hal ini, akan dilakukan penilaian risiko berbasis standar ISO 31000:2018.

2. TINJAUAN PUSTAKA

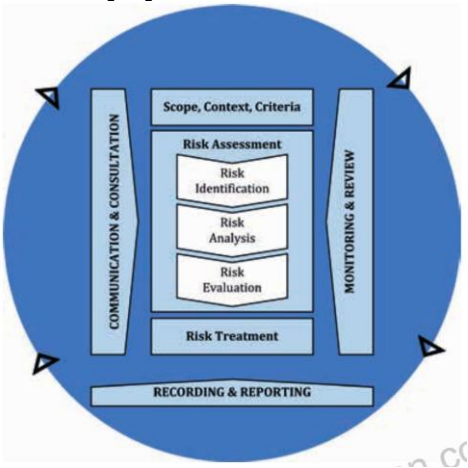
2.1. Manajemen Risiko TI

Risiko merupakan peluang terjadinya sesuatu yang memiliki dampak pada suatu proses bisnis [8]. Manajemen risiko adalah segala proses kegiatan yang dilakukan untuk meminimalkan bahkan mencegah terjadinya risiko perusahaan [13] atau definisi lainnya adalah aktivitas manajemen yang dilakukan berdasarkan tingkatan pada tingkat pimpinan pelaksana. Kegiatan penemuan serta analisis sistematis terhadap kerugian yang mungkin

dihadapi oleh perusahaan atau organisasi [14]. Dengan demikian manajemen Risiko Teknologi informasi adalah segala sesuatu kegiatan yang dilakukan untuk memanajemen risiko terkait dengan teknologi informasi.

2.2. ISO 31000:2018

Proses manajamen risiko sebaiknya merupakan bagian yang terpadu dari manajemen, menyatu dalam budaya dan praktik, dan disesuaikan penggunaannya dengan proses bisnis organiasi. Proses manajemen risiko dijelaskan pada gambar dibawah ini [12].



Gambar 1. Proses manajemen risiko

Proses manajemen risiko pada ISO 31000:2018 memiliki beberapa proses kegiatan yang yaitu 1. Komunikasi dan Konsultasi, 2. Penetapan Suatu Ruang Lingkup, Konteks, dan Kriteria, 3. Penilaian Risiko, 4. Perlakuan Risiko, 5. Pemantauan dan Tinjauan, 6. Pencatatan dan Pelaporan.

3. METODE PENELITIAN

Dalam penelitian ini menggunakan data-data kualitatif yang dikumpulkan dengan metode studi literatur, wawancara, observasi ke pihak-pihak yang bertanggung jawab dalam kasus ini adalah Kepala UPA TIK terkait pengambilan data yang diperlukan [15]. Data-data tersebut dikumpulkan untuk dijadikan *evidence* pada penelitian ini. Penelitian ini akan dilaksanakan di Politeknik Negeri Lampung (Polinela) sebagai objek yang akan diteliti. Penelitian ini akan berfokus di UPA TIK Polinela sebagai unit yang bertanggung jawab untuk teknologi informasi yang ada di Polinela [16]. Penilaian risiko dilakukan berdasarkan ISO 31000:2018 yaitu dengan dilakukannya identifikasi risiko guna mendapatkan seluruh data terkait dengan risiko, analisis risiko guna menilai level risiko, dan evaluasi risiko tersebut. Setelah dilakukan evaluasi risiko, risiko tersebut akan diberikan perlakukan risiko guna mengurangi atau mencegah terjadinya risiko tersebut yang selanjutnya perlakukan risiko tersebut dilaporkan ke UPA TIK untuk ditindaklanjuti. Alur Penelitian yang dilakukan ditampilkan pada gambar 2.

Gambar 2. Alur Penelitian

3.1. Identifikasi dan Analisis Risiko

Identifikasi ini dilakukan dalam tahap penilaian risiko pada alur proses. Tujuan dari identifikasi risiko adalah untuk menemukan, memahami, dan mendeskripsikan risiko yang dapat membantu atau mencegah objektif dari pencapaian suatu tujuan organisasi. Risiko-risiko tersebut akan dikategorikan pada kategori asset yaitu, 1. Aset perangkat keras, 2. Aset perangkat lunak, 3. Aset sumberdaya manusia, 4. Aset data dan informasi. Pada tahapan ini akan menghasilkan daftar risiko TI yang ada serta mendapatkan data kemungkinan terjadinya dan dampak yang dihasilkan dari risiko.

Adapun klasifikasi dari terjadinya kemungkinan adalah 1. Sangat besar, 2. Besar, 3. Sedang, 4. Kecil, 5. Sangat Kecil.

Tabel 1. Klasifikasi kemungkinan terjadi risiko

Kemungkinan Terjadi	Persentase Terjadi
Sangat Besar (SB)	81-99%
Besar (B)	61-80%
Sedang (S)	41-60%
Kecil (K)	21-40%
Sangat Kecil (SK)	1-20%

Sedangkan untuk klasifikasi dampak yang terjadi adalah 1. Ekstrem, 2. Besar, 3. Sedang, 4. Rendah, 5. Sangat Rendah.

Tabel 2. Klasifikasi kemungkinan terjadi risiko

Dampak	Rincian Dampak
Ekstrem (E)	Penurunan drastis kinerja atau tenaga pendukung dalam hal teknis maupun sistem dan berakibatnya tidak tercapainya target organisasi.
Besar (B)	Penurunan besar dalam kinerja atau tenaga pendukung dengan dampak yang cukup mengganggu dalam pencapaian target. Kinerja teknis dan sistem akan cukup mengalami penurunan nilai
Sedang (S)	Terjadi penurunan kinerja atau tenaga pendukung dengan dampak yang kecil pada pencapaian target.
Rendah (R)	Sedikit penurunan terjadi pada kinerja, masih dapat ditoleransi oleh organisasi dalam pencapaian target.
Sangat Rendah (SR)	Gangguan minim terhadap kinerja namun tidak ada dampak menyeluruh terhadap pencapaian target secara teknis atau operasional.

3.2. Evaluasi Risiko

Tujuan dari evaluasi risiko adalah membantu pengambilan keputusan, berdasarkaan manfaat keluaran dari analisis risiko, tentang risiko mana yang membutuhkan perlakuan serta implementasi perlakuan. Evaluasi risiko melibatkan perbandingan tingkat risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan. Pada tahapan ini akan menghasilkan matriks risiko berdasarkan kemungkinan terjadi dan dampak yang dihasil. Terdapat tiga level risiko yaitu Tinggi (T), Menengah(M), dan Rendah(R). Risiko yang dinilai tinggi adalah risiko yang mampu mengancam ketercapaian tujuan organisasi, sedangkan risiko dengan nilai menengah dan rendah akan dijadikan bahan pertimbangan untuk kebijakan lainnya. Selanjutnya matriks ini akan digunakan untuk bagaimana perlakuan risiko dilakukan.

Dampak

Kemungkinan — Matriks Risiko	SR	R	S	B	E
SK	R	R	R	R	M
K	R	R	M	M	T
SK	R	M	M	T	T
B	R	M	M	T	T
SB	M	M	T	T	T

Gambar 3. Matrik Risiko

3.3. Perlakuan Risiko

Perlakuan risiko dilakukan dengan pemilihan satu opsi atau lebih untuk pemodifikasian risiko dan pengimplementasian opsi tersebut. Diharapkan dengan perlakuan risiko tersebut dapat mengurangi dampak atau kemungkinan terjadinya dari risiko tersebut.

3.4. Pelaporan Risiko

Pelaporan risiko dilakukan dengan memberikan hasil penilaian risiko dan perlakuan risiko kepada UPA TIK. Pelaporan tersebut dapat digunakan sebagai manajemen risiko TI yang dilakukan oleh UPA TIK terhadap.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Identifikasi dan Analisis Risiko

Dari hasil indentifikasi yang dilakukan dengan cara wawancara dan telaah dokumen dengan Kepala UPA TIK, didapatkan daftar risiko yang dipetakan dalam kategori Sumberdaya Manusia, Perangkat Keras, Perangkat Lunak, serta Data dan Informasi.

Tabel 3. Identifikasi Risiko

Kode Risiko	Resiko	Kategori Aset
R1	Keterampilan staf TI tidak sesuai dengan teknologi,	Sumberdaya Manusia
R2	Staf Kurang memahami bisnis	
R3	Kurangnya kemampuan investigasi proses *recruitment*, kurangnya pelatihan	
R4	Ketergantungan terhadap orang atau pegawai (bukan sistem)	
R5	Penyalahgunaan hak akses oleh staf	
R6	Sistem error oleh staf	
R7	Informasi yang dimasukkan salah oleh pengguna	
R8	Pencurian data sensitif oleh staf	
R9	*Enterprise* arsitektur kompleks dan tidak fleksibel, sehingga menimbulkan kehilangan peluang bisnis	Perangkat Keras
R10	*Enterprise* arsitektur tidak sesuai dengan tujuan dan tidak mendukung prioritas bisnis	
R11	Infrastruktur baru yang dipasang menyebabkan sistem tidak stabil	
R12	Sistem tidak dapat menanggulangi volume transaksi yang terus bertambah	
R13	Sistem tidak dapat menanggulangi load ketika ada aplikasi baru	
R14	Server kritis rusak pada NOC (insiden)	
R15	Perangkat keras dirusak dengan sengaja	
R16	Perangkat keras gagal beroperasi karena panas yang berlebihan	
R17	Komponen perangkat keras dikonfigurasi tidak benar	
R18	Modifikasi perangkat lunak tidak sengaja menimbulkan hasil yang tidak diharapkan	Perangkat Lunak
R19	Malfungsi dapat terjadi pada perangkat lunak yang kritis	
R20	Perangkat lunak aplikasi telah usang	
R21	Ketidakmampuan mengembalikan perangkat lunak ke versi awal ketika telah diganti dengan versi terbaru yang bermasalah	
R22	Gangguan *malware* terhadap server operasional yang kritikal	
R23	Berhentinya layanan karena adanya DOS *attack*	
R24	Perusakan *website* (*deface*)	
R25	Serangan virus	
R26	Terjadi kegagalan ketika mengadopsi perangkat lunak baru.	
R27	Komponen perangkat keras rusak yang menyebabkan kerusakan data.	Data & Informasi
R28	Basis data rusak sehingga data tidak dapat diakses.	
R29	*Backup* media hilang atau *backup* tidak diperiksa dengan efektif.	
R30	Data terubah secara tidak sengaja.	

Terdapat 30 risiko yang dipetakan dalam empat kategori aset. Adapun delapan risiko pada aset sumberdaya manusia, delapan risiko pada aset perangkat keras, 9 risiko pada aset perangkat lunak dan 4 risiko pada data dan informasi. Berdasarkan daftar risiko tersebut

selanjutnya risiko tersebut akan dinilai kemungkinan dan dampak dari risiko tersebut.

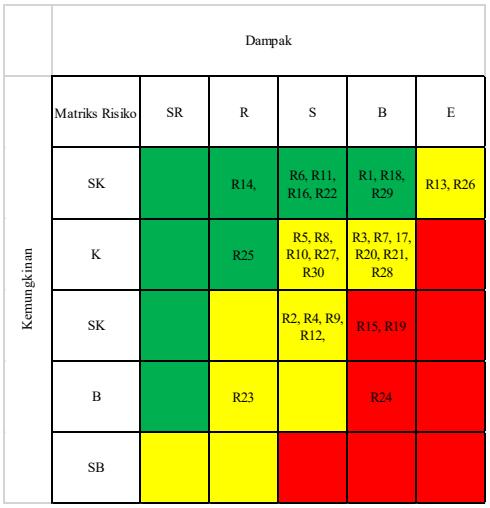
Tabel 4. Hasil Penilaian Risiko

Kode Risiko	Kemungkinan	Dampak
R1	1	4
R2	3	3
R3	2	4
R4	3	3
R5	2	3
R6	1	3
R7	2	4
R8	2	3
R9	3	3
R10	2	3
R11	1	3
R12	3	3
R13	1	5
R14	1	2
R15	3	4
R16	1	3
R17	2	4
R18	1	4
R19	3	4
R20	2	4
R21	2	4
R22	1	3
R23	4	2
R24	4	4
R25	2	2
R26	1	5
R27	2	3
R28	2	4
R29	1	4
R30	2	3

Selanjutnya hasil ini akan di evaluasi yang dipetakan dalam suatu matriks risiko.

4.2. Hasil Evaluasi Risiko

Berdasarkan hasil identifikasi dan analisis risiko terkait dengan kemungkinan dan dampak yang dihasilkan dari risiko, risiko tersebut dapat digambarkan ke dalam matrik risiko untuk dilakukan penilaian dari level risiko tersebut. Dari hasil tersebut didapatkan tiga risiko yang memiliki level tinggi yaitu R15, R19, dan R24. Level risiko menengah terdapat 18 risiko dan 9 risiko rendah. Selanjutnya risiko yang telah dievaluasi akan diberikan perlakuan guna memberikan rekomendasi atau perbaikan terkait risiko yang ada.



Gambar 4. Hasil Matrik Risiko

4.3. Hasil Perlakuan Risiko

Selanjutnya hasil dari evaluasi risiko tersebut dipetakan berdasarkan level risiko untuk direspon dalam tabel perlakuan risiko. Dalam tabel ini dituliskan saran terkait mengurangi atau mencegah dari risiko tersebut sehingga dampak dari risiko dapat diminimalisir atau dihilangkan.

Tabel 5. Hasil Perlakuan Risiko

Resiko	Kode Risiko	Level	Respon Risiko
Perangkat keras dirusak dengan sengaja	R15	T	Perangkat keras yang dirusak dengan sengaja perlu mitigasi lebih lanjut mengapa hal tersebut dilakukan. Perlakuan dapat disesuaikan dengan berdasarkan hasil mitigasi. Namun untuk tindak pencegahan dapat dilakukan dengan pengamanan perangkat keras yang penting. pengecekan dan pengendalian
Malfungsi dapat terjadi pada	R19	T	

Resiko	Kode Risiko	Level	Respon Risiko
perangkat lunak yang kritis			dari perangkat lunak yang ada wajib dilakukan secara periodik dan dilaporkan. guna melakukan pencegahan dan *error* dari perangkat lunak Kendali atas *website* dan proteksi keamanan untuk *website* publik wajib dilakukan UPA TIK. *Deface* memiliki potensi perusakan proses bisnis yang tinggi karena intensitas dan jika sering terjadi UPA TIK wajib memperketat keamanan terkait *websitenya* guna memastikan transaksi berjalan dengan lancar
Perusakan *website* (deface)	R24	T	
Kurang memahami bisnis	R2	M	staf yang kurang memahami proses bisnis dapat dilakukan pelatihan/ magang terlebih dahulu terhadap seniornya sebelum diberikan praktik langsung atau tanggung jawab.
Kurangnya kemampuan investigasi proses *recruitment*, kurangnya pelatihan	R3	M	staf yang direkrut namun tidak memiliki kemampuan TI dapat dimutasi hingga dapat dilakukan proses *recruitment* ulang guna memenuhi kebutuhan dan diharapkan proses investigasi dilakukan lebih baik
Ketergantu-ngan terhadap orang atau pegawai (bukan sistem)	R4	M	Standar Operasional Prosedur atau panduan dapat menjadi solusi terkait ketergantungan akan staf. Dengan adanya SOP atau panduan diharapkan seluruh kegiatan juga dapat dilakukan dengan staf memberikan pemahaman dan peraturan dapat mencegah
penyalahgu-naan hak akses oleh staf	R5	M	penyalahgu-naan hak akses yang dilakukan oleh staf. Selain itu juga, diharapkan pimpinan dapat terus mengontrol stafnya
Informasi yang dimasukkan salah oleh pengguna	R7	M	lakukan *backup* secara berakala
Pencurian data sensitive oleh staf	R8	M	Data sensitif diharapkan dijaga di

Resiko	Kode Risiko	Level	Respon Risiko
			tempat yang dapat diakses bagi yang memiliki wewenang.
Enterprise arsitektur kompleks dan tidak fleksibel, sehingga menimbulkan kehilangan peluang bisnis	*R9*	M	*Enterprise* arsitektur dapat dikaji ulang guna memaksimal-kan peluang bisnis guna mencapai tujuan strategisnya
Enterprise arsitektur tidak sesuai dengan tujuan dan tidak mendukung prioritas bisnis	*R10*	M	*Enterprise* arsitektur dapat dikaji ulang guna memaksimal-kan peluang bisnis guna mencapai tujuan strategisnya
Sistem tidak dapat menanggula-ngi volume transaksi yang terus bertambah	R12	M	*Upgrade* sistem dan infrastruktur
Sistem tidak dapat menanggula-ngi load ketika ada aplikasi baru	R13	M	*Upgrade* sistem dan infrastruktur
Komponen perangkat keras dikonfigurasi tidak benar	R17	M	pemahaman terkait perangkat keras dan konfigurasi perlu diberikan
perangkat lunak aplikasi telah usang	R20	M	*update* perangkat lunak
Ketidakmam-puan mengembali-kan perangkat lunak ke versi awal ketika telah diganti dengan versi terbaru yang bermasalah	R21	M	selalu sediakan *backup* sebelum melakukan modifikasi
Berhentinya layanan karena adanya DOS *attack*	R23	M	proteksi keamanan jaringan
Terjadi kegagalan ketika mengadopsi perangkat lunak baru	R26	M	sebelum mengadopsi perangkat lunak baru, dapat memastikan kebutuhan spesifikasi dan infrastruktur yang diperlukan guna mencegah kegagalan.
Komponen perangkat keras rusak yang menyebabkan kerusakan data	R27	M	Selalu sediakan *backup* data dan *monitoring* kesehatan dari perangkat keras
Basis data rusak sehingga data tidak dapat diakses,	R28	M	Selalu sediakan *backup* server
Data terubah secara tidak sengaja	R30	M	Lakukan *backup* secara berakala
Keterampilan staf TI tidak sesuai dengan teknologi	R1	R	Pelatihan Staf, rekrutmen staf, hingga mutasi staf yang memiliki keterampilan yang dibutuhkan merupakan opsi yang dapat dilakukan guna mencegah terjadinya risiko tersebut. pencegahan dapat dilakukan dengan pelatihan dan pembiasaan.
Sistem error oleh staf	R6	R	Sedangkan perbaikan dapat dilakukan dengan *maintenance* atau *backup*

Resiko	Kode Risiko	Level	Respon Risiko
infrastruktur baru yang dipasang menyebabkan sistem tidak stabil	R11	R	Infrastruktur di-*install* dan diuji coba secara bertahap dapat menjadi solusi sebelum infrastruktur tersebut dipasang. Jika sudah terjadi dapat dilakukan penyesuaian perangkat terkait infrastruktur guna menstabilkan sistem
Server kritis rusak pada NOC (insiden)	R14	R	pemantauan NOC secara berkala dan penyelesaian seperti *restart*, perbaikan atau penggantian dapat dilakukan
Perangkat keras gagal beroperasi karena panas yang berlebihan	R16	R	Proteksi terhadap perangkat keras yang vital sangat penting dilakukan, selain itu pelatihan dan pemahaman akan pentingnya perangkat keras wajib dilakukan guna mencegah ketidak sengajaan.
Modifikasi perangkat lunak tidak sengaja menimbulkan hasil yang tidak diharapkan	R18	R	selalu sediakan *backup* sebelum melakukan modifikasi
gangguan *malware* terhadap server	R22	R	*backup* merupakan solusi, namun kehilangan data mungkin
operasional yang kritikal			menjadi akibatnya. Proteksi terhadap server merupakan langkah pencegahan dini dari *malware*.
Serangan virus	R25	R	selalu proteksi dengan *antivirus* yang mamadai
Backup media hilang atau *backup* tidak diperiksa dengan efektif	*R29*	R	lakukan *backup* secara berakala dan disimpan ditempat yang aman

4.4. Pelaporan Risiko

Risiko yang telah dilakukan penilaian dan perlakukan risiko tersebut selanjutnya dilaporkan ke UPA TIK untuk diterima dan dilaksanakan. UPA TIK memantau risiko yang ada dalam rangka pelaksanaan manajemen risiko.

5. KESIMPULAN

Berdasarkan dari penelitian ini, teridentifikasi sebanyak 30 Risiko dari empat kategori aset yang ada di UPA TIK. Setelah dilakukan analisis risiko pada 30 risiko tersebut, terdapat tiga risiko atau 10% yang memiliki level tinggi yang mana membutuhkan perhatian tambahan guna mengurangi dampak yang signifikan pada proses bisnis. Level menengah terdapat 19 atau 63% dan Level rendah terdapat delapan atau 26% yang dapat diterima dan digunakan sebagai pengambilan kebijakan lainnya. Hasil dari penelitian ini berupa penilaian dan perlakuan risiko dapat dijadikan bahan acuan untuk dilakukan manajemen risiko pada UPA TIK yang terdokumentasi, sehingga seluruh pihak yang terlibat dapat melakukan manajemen risiko karena manajemen risiko yang baik adalah ketika UPA TIK mengelola risikonya dengan terstruktur terlepas dari jumlah risiko yang teridentifikasi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Marius Robert Seran, "Teknologi Informasi Pembentuk Multiplier Effect Dalam Bisnis Corporasi," J. Manag. Small Mediu. Enterp., vol. 3, no. 2, pp. 263–274, 2016.

[2] A. Nikmat, "Analisis Manajemen Risiko Teknologi Informasi Pada Sistem Informasi Akademik (Siak) Universitas Muhammadiyah Sukabumi (UMM) Menggunakan Iso 31000," J. Manaj. dan Teknol. Inf., vol. 14, no. 1, pp. 49–58, 2024, doi: 10.59819/jmti.v14i1.3321.

[3] D. Andika and A. Wijaya, "Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2018 Pada Pt. Trust Lerinvital Timur," J. Mnemon., vol. 5, no. 2, pp. 111–118, 2022, doi: 10.36040/mnemonic.v5i2.4778.

[4] M. R. A. Ahadis, G. F. Nama, R. Annisa, and M. A. Muda, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Pada PT Bank Rakyat Indonesia Unit 1 Pringsewu," J. Inform. dan Tek. Elektro Terap., vol. 13, no. 2, pp. 1454–1462, 2025.

[5] P. Kanantyo and F. S. Papilaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," J. Tek. Inform. dan Sist. Inf., vol. 8, no. 4, pp. 1896–1908, 2021.

[6] P. Hayati et al., "Teknologi Informasi dan Kinerja Perguruan Tinggi," J. Student Res., vol. 2, no. 6, pp. 20–27, 2024.

[7] N. Cholis and F. Fadli, "Pemanfaatan Teknologi Informasi, Sistem Pengendalian Intern, Akuntabilitas Publik Dan Kinerja Instansi Pemerintah," J. Fairness, vol. 7, no. 2, pp. 127–136, 2021, doi: 10.33369/fairness.v7i2.15152.

[8] L. Ernawati and H. B. Santoso, "Identifikasi dan Analisa Risiko Penerapan Teknologi Informasi di Lingkungan Perguruan Tinggi," Seri Pros. Semin. Nas. Din. Inform., vol. 1, no. 1, pp. 21–28, 2017.

[9] V. P. P. Wijaya, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 9, no. 2, pp. 1295–1307, 2022, doi: 10.35957/jatisi.v9i2.2087.

[10] R. Andrew and G. Cudivia, "Risiko Penggunaan Berlebih Dari Teknologi Informasi Dan Komunikasi Di Area Yang Mengalami Pembatasan Temporer (Studi Pada Sektor Perguruan Tinggi)," in Prosiding Serina, 2020, no. 2019, pp. 39–46.

[11] S. D. Kuncoro, R. A. Ghaisan, Z. M. Usamah, and A. Wulansari, "Manajemen Risiko Teknologi Informasi: Studi Kasus pada Perusahaan Jasa," J. Ilm. Sain dan Teknol., vol. 3, no. 1, pp. 313–323, 2023, doi: 10.21512/comtech.v4i1.2682.

[12] ISO 31000, BSI Standards Publication Risk management — Guidelines. Switzerland: British Standards Institution, 2018.

[13] Badan Standardisasi Nasional, Manajemen risiko - Prinsip dan Pedoman (ISO 31000:2009,DT). Jakarta: Badan Standardisasi Nasional, 2011.

[14] A. R. Viyanto, O. S. Latuihamallo, F. M. Tua, and A. Gui, "Manajemen Risiko Teknologi Informasi: Studi Kasus Pada Perusahaan Jasa," Comtech, vol. 4, no. 1, pp. 43–54, 2013.

[15] D. P. Natalie and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000:2018 pada PT Bayu Buana Tbk," JURIKOM (Jurnal Ris. Komputer), vol. 9, no. 5, p. 1290, 2022, doi: 10.30865/jurikom.v9i5.4797.

[16] Rencana Strategis Jangka Panjang Politeknik Negeri Lampung, Rencana Strategis. Bandar Lampung: Tim Penyusun, 2019.