JIKB
Jurnal Ilmu Komputer dan Bisnis

Jurnal Ilmu Komputer dan Bisnis (JIKB)
Desember-2022, Vol. XIII, No.2a, hal.155-165
ISSN(P): 2087-3921; ISSN(E): 2598-9715

Analisis Manajemen Risiko Teknologi Informasi dan Keamanan Aset Dengan Menggunakan Nist Sp 800-30 Revisi 1

[1]Alma Iftina Azzahra Ain, [2]Awalludiyah Ambarwati, [3]Lukman Junaedi
[1,2,3]Universitas Narotama Surabaya

Alamat Surat
Email: heart.hole.12@gmail.com, ambawati1578@yahoo.com, lukman.junaedi@narotama.ac.id

Article History:
Diajukan: 10 Oktober 2022; Direvisi: 21 November 2022; Diterima: 29 November 2022

ABSTRAK

Teknologi informasi memiliki peran yang sangat penting dalam melakukan kegiatan operasional di SMK Teknik PAL Surabaya. Namun tidak selamanya menggunakan teknologi informasi sesuai dengan harapan. Dalam penggunaanya akan muncul berbagai risiko yang dapat menggangu kegiatan operasional sekolah. Risiko-risiko yang muncul ini harus ditangani agar masalah yang ditimbulkan tidak menyebabkaan penggunaan teknologi informasi mejadi suatu hambatan. Dalam mengatasi permasalahan yang muncul dilakukan dengan cara melakukan manajemen risiko terhadap penggunaan teknologi informasi. Dalam penelitian ini analisis manajemen risiko dilakukan dengan menggunakan NIST SP 800-30 Revisi 1. Tahapan dalam NIST SP 800-30 Revisi 1 yaitu, melakukan identifikasi sumber ancaman, identifikasi peristiwa ancaman, identifikasi kerentanan, penentuan kemungkinan, identifikasi dampak, penentuan risiko, rekomendasi pengendalian dan dokumen hasil. Maka berdasarkan hasil dari penelitian yang telah dilakukan, SMK Teknik PAL Surabaya memiliki 2 tingkat risiko tinggi, 1 tingkat risiko sedang, dan 5 tingkat risiko rendah. Dari hasil tersebut dibuat rekomendasi pengendalian untuk mengatasi permasalahan pada teknologi informasi.

Kata kunci: NIST SP 800-30 Revisi 1; Manajemen Risiko; Teknologi Informasi

ABSTRACT

Information technology plays a very important role in operational activities at SMK Teknik PAL Surabaya. However, the use of information technology is not always in line with expectations. In its use, there are various risks that interfere with school operational activities. These risks should be handled so that they do not create barriers to the use of information technology. The way to solve the problem is to conduct risk management on the use of information technology. This research used risk management analysis using NIST SP 800-30 Revision 1. The stages of NIST SP 800-30 Revision 1 were identification of threat sources, identification of threat events, identification of vulnerabilities, determination of possibilities, identification of impacts, determination of risks, recommendations for control and outcome documents. Thus, the research results revealed that SMK Teknik PAL Surabaya had 2 high risk levels, 1 moderate risk level, and 5 low risk levels. From these results, control recommendations were created to overcome problems in information technology.

Keywords: NIST SP 800-30 Revision 1; Risk Management; Information Technology

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini sangat cepat sehingga menjadi kebutuhan yang sangat penting untuk kehidpan sehari-hari. Karena setiap kegiatan yang manusia lakukan di bumi

https://doi.org/10.47927/jikb.v13i2a.403

telah menggunakan teknologi informasi. Salah satunya adalah kegiatan yang dilakukan dalam dunia pendidikan sekarang sudah menggunakan teknologi informasi, dimulai dari administrasi sampai dengan kegiatan pembelajaran. Teknologi informasi memudahkan para pelajar dan guru dalam melakukan pembelajaran dan operasional sekolah. Hanya saja dalam melakukan kegiatan belajar yang terkait dengan teknologi informasi sering kali timbul berbagai risiko yang dapat mengganggu kegiatan sekolah. Seperti terjadi masalah pada salah satu server di laboraturium komputer SMK Teknik PAL Surabaya yang menyebabkan dua dari lima laboraturium komputer tidak bisa digunakan. Hal ini mengakibatkan kegiatan Ujian Akhir Semester dan TryOut yang dilakukan didua laboraturium mengalami penundaaan. Kejadian ini membuat keributan karena pelaksanaan TryOut dilakukan Secara serempak diseluruh Indonesia. Dan juga terjadi masalah dalam kegagalan pengambilan data yang dilakukan. Dari masalah yang terjadi di SMK Teknik PAL Surabaya, dikarenakan tidak pernah melakukan analisis manajemen risiko IT. Manajemen risiko merupakan mengidentifikasi dan memerikan nilai pada risiko diikuti oleh aplikasi dari sumber daya untuk meminimalkan, memantau, dan mengendalikan dampak peristiwa yang tidak diinginkan(Santoso & Ernawati, 2017).

Untuk meminimalisir risiko yang terjadi di Sekolah Menengah Kejuruan Teknik PAL Surabaya. Penelitian ini akan menggunakan kerangka kerja (framework) NIST SP 800-30 Revisi 1 yang digunakan untuk: melakukan proses analisis manajemen risiko teknologi informasi dan keamanan asset, risiko apa saja yang terjadi, daan bagaimana mengatasi risiko yang terjadi di SMK Teknik PAL Surabaya. NIST SP 800-30 telah terbukti memberikan kontribusi yang lebih seperti: memberikan pengetahuan mengenai keamanan informasiyang sifatnya konsisten dan komprehensif bagi pengambil kebijakan, pengambil keputusan tidak ragu-ragu untuk mengambil resiko karena setiap resiko telah diselidiki dengan baik (Syafitri, 2016). Penelitian ini dilakukan dengan tujuan menganalisis risiko yang terjadi di SMK Teknik PAL Surabaya dan membuat rekomendasi berdasarkan nilai tingkat risiko yang dihasilkan.

Penelitian yang membahas tentang penilaian risiko keamanan informasi menggunakan kerangka kerja pada sistem informasi akademik perguruan tinggi. Permasalahan yang ada yaitu terdapat celah kerawanan pada keamanan informasi dan terjadinya bencana alam yang mengakibatkan kerusakan pada aset. Setelah dilakukan penilaian risiko, hasil yang diperoleh pada penelitian ini yaitu 1 tingkat risiko tinggi, 5 tingkat risiko sedang, dan 52 tingkat risiko rendah (Syafitri, 2016).

Dalam penelitian ini membahas tentang manajemen risiko keamanan informasi menggunakan *framework* NIST SP 800-30. Dengan tujuan dapat mengurangi dampak peristiwa sistem dan teknologi informasi di institusi perguruan tinggi, melindungi proses bisnis organisasi yang penting dari ancaman keamanan, mengurangi risiko yang menyebabkan kerugian di organisasi STMIK Sumedang. Hasil dari penelitian ini dengan membuat rekomendasi standar kebijakan keamanan informasi, baik itu informasi yang ada di lembaga atau informasi yang dikelola Sistem dan Teknologi Informasi yang digunakan (Mahardika, 2017).

Pada penelitian yang membahas mengenai manajemen risiko yang dilakukan pada sistem informasi di lembaga pendidikan. Dengan melakukan proses manajemen risiko yaitu penilaian risiko, peringatan risiko dan evaluasi risiko (Harsanto & Hidayat, 2018). Berikut pada table 1 adalah beberapa penelitian terdahulu.

Tabel 1. Penelitian Terdahulu

Judul	Penulis dan Tahun	Tujuan	Hasil
Analisis Manajemen Risiko Sistem Informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur	Dian Ayu Permatasari, Widhy Hayuhardhika Nugraha Putra, Andi Reza Perdanakusuma, 2019	untuk engidentifikasi potensi risiko pada sistem E-LKPJ dengan menggunakan kerangka kerja NIST SP 800-30	Hasil dari penelitian ini adalah penilaian tingkat risiko meliputi sumber daya manusia memiliki tingkat risiko tinggi, kata sandi memiliki tingkat risiko sedang, serta listik dan jaringan

Judul	Penulis dan Tahun	Tujuan	Hasil
(Permatasari et al., 2019)			internet memiliki tingkat risiko rendah.
Analisis Manajemen Risiko TI Pada Keamanan Data E-Learning Dan Aset TI Menggunakan NIST SP 800-30 Revisi 1 (Putra, 2019)	Riszullah Ramadhan Putra, Eman Setiawan, Awalludiyah Ambarwati, 2019	menganalisis berbagai risiko hal tersebut menjadi suatu acuan bagi manajemen dalam melakukan pencegahan, penanganan, serta perbaikan terhadap berbagai kemungkinan risiko tersebut.	Hasil akhir dari penilaian ini berupa rekomendasi pendekatan mitigasi untuk perlindungan sistem pembelajaran online Universitas Narotama.
Information Technology Risk Assessment Sistem Informasi Elektronik Kinerja Pegawai Universitas Islam Negeri (metode NIST SP 800-30 Rev 1) (Dalafranka et al., 2018)	Muhammad Leandry Dalafranka, Dedy Syamsuar, Yesi Novaria Kunang, 2018	untuk mengetahui dan menganalisis risiko yang ada pada penerapan Sistem Elektronik Laporan Kinerja Pegawai di Universitas Islam Negeri Raden Fatah Palembang	menghasilkan laporan risiko teknologi informasi pada penerepan sistem tersebut.
Risk Assessment dan Business Impact Analysis BPK RI dalam pengembangan DRP BPK RI dengan Standar NIST 800-30 Rev 1. (Kurniawan et al., 2017)	Fuad Kurniawan, Lukito Edi Nugroho, Sri Suning Kusumawari, 2017	Penelitian ini bertujuan menjawab permasalahan tersebut dengan melakukan penilaian risiko (risk assessment) dan analisis dampak bisnis.	Hasil penelitian menemukan 27 aset SI dari 17 proses yang ada di BPK RI, 14 aset memiliki dampak tinggi dan 7 aset dengan tingkat kritikalitas yang tinggi.
Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency (Al Fikri et al., 2019)	Muhamad Al Fikria, Fandi Aditya Putrab, Yohan Suryantoa, Kalamullah Ramlia, 2019	memfasilitasi stakeholders di bidang informasi manajemen risiko keamanan pada penerapan alat standar alternatif dengan membuktikan apakah teknik baru ini benar relevan dengan organisasi umum (profit dan nonprofit) atau tidak	4 tinggi (prioritas), 20 sedang (prioritas kedua), 15 rendah (prioritas terakhir), dan 3 sangat rendah (tidak prioritas) skenario risiko.
University Information System Security Risk Assessment using NIST 800-30 (Johan et al., 2019)	Monika Evelin Johan, Moh Fahrur Rizqon, Ir. Jarot S. Suroso M. Eng, 2019	penilaian risiko di UIS untuk mengidentifikasi berbagai kemungkinan risiko dan mencegahnya dengan menetapkan manajemen risiko.	Hasil penelitian ini telah mengidentifikasi 32 skenario risiko, risiko yang diprioritaskan, memberikan arahan dalam mengelola risiko dan menerima proses apakah risiko dapat diterima atau harus dimitigasi.
Maintaining The Continuity of The Company's Operation using the NIST Framework for SME (Wahyudi et al., 2019)	Eko Haryadi, Dewi Yuliandari, Abdussomad, Diah Wijayanti, Mike Amelia, Syafrianto, 2019	Tujuan dari penelitian ini adalah membuat perusahaan memiliki kemampuan untuk memahami posisi keamanan teknologi informasi dan informasi sistem.	Pada Bagian Penentuan Resiko masih menemukan beberapa daerah di posisi Tinggi, itu artinya perbaikan masih diperlukan dengan prioritas dan menjadi perhatian penuh dari manajemen

1.1.Manajemen Risiko

Manajemen Resiko adalah penerapkan fungsi-fungsi manajemen dalam penanggulangan resiko, terutama resiko yag dihadapi oleh organisai/lembaga, perusahaan, keluarga dan masyarakat (Subekti & Nur'aini, 2019). Tujuan dari manajemen risiko adalah untuk mengenali risiko dalam sebuah proyek dan mengembangkan strategi untuk mengurangi atau bahkan menghindarinya, dilain sisi juga harus dicari cara untuk memaksimalkan peluang yang ada (Meilani et al., 2019). Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Seta & Rahayu, 2017).

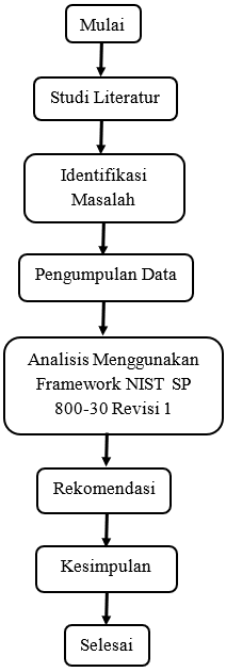
1.2.Teknologi Informasi

Teknologi informasi adalah suatu kombinasi antara teknologi komputer dan teknologi komunikasi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dengan mendalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan dan merupakan informasi yang strategis untuk pengambilan keputusan (Naibaho, 2017).

1.3. NIST SP 800-30 Revisi 1

National Institute of Standards and Technology (NIST) merupakan organisasi pemeritah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standard teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. Kegiatan utama adalah meneliti berbagai ilmu untuk mempromosikan dan meningkatkan infrastruktur teknologi (Firmansyah, 2014)

2. METODE



Gambar 1. Alur Penelitian

Sesuai alur penelitian diatas langkah pertama yaitu melakukan persiapan dan studi literatur untuk mencari referensi tentang analisis manajemen risiko teknologi informasi. Yang berbentuk buku yang terkait dengan penelitian, dan jurnal sebagai pendukung bagi penulis dalam penulisan Laporan Penelitian. Langkah Kedua, melakukan identifikasi masalah terhadap objek objek penelitian. Langkah ketiga, melakukan pengumpulan data dengan cara melakukan observasi langsung guna untuk melihat dan mengamati aset teknologi yang digunakan dan wawancara pada 1 narasumber yang bertanggung jawab terhadap IT di sekolah. Langkah keempat, pengolahan data

dilakukan dengan menggunakan Framework NIST SP 800-30 Revisi 1. Langkah kelima, membuat rekomendasi kontrol. Langkah terakhir yaitu penulisan laporan penelitian.

Penelitian dilakukan di SMK Teknik PAL Surabaya dan bagian IT yang bertujuan menganalisis risiko pada teknologi informasi yang ada. Dalam penelitian ini menggunakan dua sumber data yaitu data Primer dan data Skunder, data Primer diproleh langsung dari observasi pada tempat penelitian dengan melakukan wawancara dan mengambil kuisioner dari pihak yang bertanggung jawab terhadap teknologi informasi yang ada. Sedangkan data Sekunder diperoleh dari sumber – sumber yang dijadikan acuan pada literature untuk analisis risiko pada penelitian ini.

Metode pengumpulan data dalam penelitian ini adalah wawancara, kuisioner, observasi dan studi Pustaka. Wawancara dilakukan terhadap beberapa narasumber yang dalam hal ini bertanggung jawab dalam penggunaan teknologi informasi, diantaranya wawancara kepada wakil kepala sekolah bidang SarPras. Kuisioner dilkukan terhadap penilaian risiko, sebagaimana diatur dalam NIST 800-30 Revisi 1 terdapat 6 tahap penilaian risiko, yaitu:

2.1 Identifikasi Sumber Ancaman
Mengidentifikasi dan mengkarakterisasi sumber ancaman yang terjadi pada teknologi informasi SMK Teknik PAL Surabaya, sebagai karakteristik penargetan untuk ancaman musuh dan rentang efek untuk ancaman non-permusuhan.

2.2 Identifikasi Peristiwa Ancaman
SMK Teknik PAL Surabaya mengidentifikasi peristiwa ancaman yang harus dipertimbangkan selama penilaian risiko yang berguna untuk menggambarkan peristiwa tersebut.

2.3 Identifikasi Kerentanan
Identifikasi kerentanan dan kondisi predisposisi dari teknologi informasi SMK Teknik PAL Surabaya yang mempengaruhi kemungkinan bahwa peristiwa ancaman yang menimbulkan dampak merugikan.

2.4 Menentukan Kemungkinan
Untuk menentukan kemungkinan kejadian ancaman secara keseluruhan dengan menerapkan proses tiga langkah. Pertama, menilai kemungkinan bahwa peristiwa ancaman akan dimulai (untuk peristiwa ancaman permusuhan) atau akan terjadi (untuk peristiwa ancaman non-permusuhan). Kedua, menilai kemungkinan bahwa peristiwa ancaman setelah dimulai atau terjadi, akan mengakibatkan dampak buruk terhadap operasi dan aset Sekolah. Kemudian menilai kemungkinan keseluruhan sebagai gabungan dari kemungkinan inisiasi / kejadian dan kemungkinan menghasilkan dampak yang merugikan.

Tabel 2. Skala Penilaian

Kemungkinan Inisiasi atau Kejadian Ancaman	**Kejadian Ancaman Kemungkinan Mengakibatkan Dampak Merugikan**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

2.5 Identifikaasi Dampak

Pada tahap ini akan menjelaskan bagaimana risiko akan berpengaruh pada sistem dan aset teknologi informasi yang ada di SMK Teknik PAL Surabaya akan menghasilkan berupa definisi dampak dari risiko-risiko tersebut.

2.6 Menentukan Risiko

Menentukan level tingkatan pada risiko, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan pada metode NIST SP 800-30 Revisi 1.

3. HASIL DAN PEMBAHASAN

3.1 Data Aset

Dalam menentukan asset yang penting dengan mengumpulkan informasi tentang asset kebutuhan keamanan, dan ancaman. Aset IT merupakan aset yang digunakan dalam kegiatan operasional sekolah. Berikut beberapa aset yang digunakan oleh SMK Teknik PAL dapat dilihat pada table 3.

Tabel 3. Aset IT SMK Teknik PAL

No.	Aset	Kategori Aset
1	Komputer	Hardware
2	Server	
3	Laptop	
4	Wirelees router	Network
5	Mikrotik	
6	Switch/hub	
7	Kabel LAN	
8	Website sekolah	Sistem Informasi
9	PPDB online	
10	Sistem pembayaran sekolah	

3.2 Identifikasi Sumber Ancaman

Pada tahap ini akan dilakukan identifikaasi ancaman yang terjadi pada teknologi informasi SMK Teknik PAL. Tingkat kerentanan, dampak, kemungkinan, dan penentuan risiko dalam penelitian ini diperoleh dari hasil wawancara dan kuisioner dengan pihak SMK Teknik PAL terhadap teknologi informasi. Pada tabel 4 berikut ini menjelaskan mengenai identifikasi pada teknologi informasi.

Tabel 4. Sumber Ancaman

No.	Sumber Ancaman	Rentang Efek
1	Listrik padam	Tinggi
2	Koneksi internet lambat	Sedang
3	Server mati	Sedang
4	Serangan hacker	Rendah
5	Proses pengajuan yang lama untuk perbaikan peralatan TI	Sedang
6	Kabel jaringan dimakan hewan pengerat	Sedang
7	Perangkat keras rusak	Rendah
8	Memori penuh	Tinggi

3.3 Identifikasi Kerentanan

Pada tahapan identifikasi kerentanan ini dilakukan berdasarkan sumber ancaman yang ada. Dengan cara menganalisis kerentanan atau kelemahan yang dimiliki oleh SMK Teknik PAL dan berpotensi terjadi dimasa depan.

Tabel 5. Kerentanan

No.	Ancaman	Kerentanan	Rentang Efek
1	Listrik padam	Tidak ada cadangan listrik, listrik masih ikut PT. PAL	Sedang
2	Koneksi internet lambat	Dipakai terlalu banyak orang, Kurangnya jumlah bandwidth internet	Rendah
3	Server mati	Beban kerja yang dilakukan terlalu tinggi, listrik mati	Sedang
4	Serangan hacker	Belum ada pencegahan supaya tidak terjadi *hacking*	Sedang
5	Proses pengajuan yang lama untuk perbaikan peralatan TI	Birokrasi yang panjang dan rumit	Rendah
6	Kabel jaringan dimakan hewan pengerat	Kabel dipasang diatas plafon, tidak ada pelindung kabel	Sedang
7	Perangkat keras rusak	Terlalu sering diinstal ulang	Rendah
8	Memori penuh	kapasitas server kurang	Sedang

3.4 Penentuan Kemunngkinan

Tujuan dari Langkah ini adalah untuk menentukan tingkat kemungkinan terjadinya suatu peristiwa ancaman dari teknologi informasi. Hasil dari kemungkinan risiko yang menentukan dapat dilihat pada tabel 6.

Tabel 6. Kemungkinan Keseluruhan

No.	Risiko	Kemungkinan Peristiwa Ancaman Yang Terjadi	Kemungkinan Ancaman yang Menghasilkan Dampak Buruk	Kemungkinan Keseluruhan
1	Listrik padam	Tinggi	Tinggi	Tinggi
2	Koneksi internet lambat	Tinggi	Sedang	Sedang
3	Server mati	Sedang	Tinggi	Sedang
4	Serangan hacker	Rendah	Sedang	Rendah
5	Proses pengajuan yang lama untuk perbaikan peralatan TI	Sedang	Rendah	Rendah
6	Kabel jaringan dimakan hewan pengerat	Rendah	Rendah	Rendah
7	Perangkat keras rusak	Rendah	Sedang	Rendah
8	Memori penuh	Rendah	Rendah	Rendah

3.5 Identifikasi Dampak

Identifikasi dampak dilakukan untuk menentukan potensi dampak buruk dalam kegiatan di SMK Teknik PAL. Informasi dari analisis dampak untuk penilaian risiko dapat dilihat pada table 7.

Tabel 7. Identifikasi Dampak

No.	Risiko	Dampak Yang Terjadi	Rentang Efek
1	Listrik padam	Semua perangkat IT mati, kegiatan operasional terganggu	Tinggi
2	Koneksi internet lambat	Sinkron data server lama	Sedang
3	Server mati	Tidak bisa akses E-learning, gaji, dan spp	Tinggi
4	Serangan hacker	Kemungkinan sistem terkena hack dampaknya rendah karena hanya terdapat data umum	Rendah
5	Proses pengajuan yang lama untuk perbaikan peralatan TI	Operasional Terhambat	Rendah
6	Kabel jaringan dimakan hewan pengerat	Koneksi terputus	Sedang
7	Perangkat keras rusak	Operasional Terhambat	Rendah
8	Memori penuh	Akses data menjadi lambat	Sedang

3.6 Menentukan Risiko

Penentuan risiko ini bertujuan untuk menilai tingkat risiko terhadap sistem, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan. Tingkat risikoyang teridentifikasi tersebut menjadi salah satu penentu sejauh mana aset teknologi informasi terancam oleh kejaadian tersebut. Penentuan risiko dapat dilihat pada tabel 8.

Tabel 8. Tingkat Risiko

Risiko	Kemungkinan Keseluruhan	Rentang Efek	Rentang Efek
Listrik padam	Tinggi	Tinggi	Tinggi
Koneksi internet lambat	Sedang	Sedang	Sedang
Server mati	Tinggi	Tinggi	Tinggi
Serangan hacker	Rendah	Rendah	Rendah
Proses pengajuan yang lama untuk perbaikan peralatan TI	Rendah	Rendah	Rendah

Risiko	Kemungkinan Keseluruhan	Rentang Efek	Rentang Efek
Kabel jaringan dimakan hewan pengerat	Rendah	Sedang	Rendah
Perangkat keras rusak	Rendah	Rendah	Rendah
Memori penuh	Rendah	Sedang	Rendah

3.7 Mengkomunikasikan Hasil Penilaian

Setelah melakukan penilaian risiko pada aset IT harus segera mambagikan informasi hasil penilaian kepada pihaak yang bertanggung jawab mengenai penilaian risiko aset IT yang berpengaaruh pada kegiatan operasional SMK Teknik PAL. Daalam menentukaan penilaian aset IT yang bertujuan untuk menggambarkan semua tingkat risiko yang harus segeraa dilakukan Tindakan mitigasi terhadaap permasalahaan yang ada di SMK Teknik PAL Surabaya.

3.8 Mempertahankan Penilaian Risiko

Hasil penilaian risiko menginformasikan keputusan manajemen risiko dan memandu respon risiko. Untuk mendukung tinjauan berkelanjutan atas keputusaan manajemen risiko, organisasi memelihara penilaaaian risiko untuk memasukkan setiap perubahan yang terdeteksi melalui pemantauan risiko. Dalam menjaga penilaian perlu dilakukan pemantauan terhadap risiko secara berkala untuk memastikan informaasi yang diperlukan sekolah.

3.9 Rekomendasi

Tahap ini merupakan hasil dari proses penilaian untuk meminimalisir atau bahkan mencegah maasalah padaa aset IT diperlukan membuat rekomendasi Tindakan pengendaaliaan risiko. Rekomendasi risiko ini dilakukan agar proses operasionaal sekolah dimasa depan terhindar dari berbagai risiko atau ancaman. Yang dapat dilihat pada tabel 9 berdasarkan tingkat risiko.

Tabel 9. Rekomendasi

Risiko	Tingkat risiko	Rekomendasi
Listrik padam	Tinggi	menyediakan genset
Koneksi internet lambat	Sedang	menambah bandwidth internet dan melakukan routing bandwidth sesuai kebutuhan
Server mati	Tinggi	menyediakan UPS atau menggunakan VPS
Serangan hacker	Rendah	melakukan backup data dan pentesting
Perangkat keras rusak	Rendah	melakukan pengajuan sebelum hardware tersebut rusak atau out of date
Proses pengajuan yang lama untuk perbaikan peralatan TI	Rendah	
Kabel jaringan dimakan hewan pengerat	Rendah	memasang pelindung pada kabel dan mengatasi hewan pengerat dengan racun atau perangkap
Memori penuh	Rendah	Menambah SSD

4. SIMPULAN DAN SARAN

Berdasarkan dari hasil analisis risiko teknologi informasi yang dilakukan melalui wawancara dan kuisioner pada SMK Teknik PAL Surabaya. Kesimpulan yang didapat sebagai berikut: (1) ancaman yang muncul di SMK Teknik PAL terdapat 8 ancaman antara lain listrik mati, koneksi internet lambat, server mati, proses pengajuan yang lama untuk perbaikan peralatan IT, kabel jaringan dimakan hewan pengerat, perangkat keras rusak, serangan hacker, dan memori penuh., (2) hasil dari penilaian risiko yang dilakukan pada teknologi informasi mendapat 2 tingkat tinggi, 1 tingkat sedang, dan 5 tingkat rendah.

Saran untuk melakukan penelitian selanjutnya yaitu dengan melanjutkan penelitian ini ke tahap mitigasi risiko dan evaluasi dan penilaian. Selain itu, dapat menggunakan metode lain seperti OCTAVE ALLEGRO, FMEA (Failure Mode and Effect Analysis), dan metode lainnya. Dengan demikian diharapkan dapat memperkaya kajian keilmuan tentang analisis risiko teknologi informasi.

5. DAFTAR PUSTAKA

Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. Procedia Computer Science, 161, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Dalafranka, M. L., Syamsuar, D., & Novaria, Y. (2018). Information Technology Risk Assessment Sistem Informasi Elektronik Kinerja Pegawai Universitas Islam Negeri. Seminar Nasional Teknologi Informasi Dan Komunikasi (SEMNASTIK) X, 153–158.

Firmansyah, H. (2014). Implementasi framework manajemen risiko terhadap penggunaan teknologi informasi perbankan. Seminar Dan Call Paper Munas Aptikom, 10, 172–178.

Harsanto, K., & Hidayat, D. (2018). Sistem Informasi Manajemen Risiko dengan Menggunakan Framework National Institute of Standards and Technology pada Lembaga Pendidikan. Jurnal Ipsikom, 6(1).

Johan, M. E., Rizqon, M. F., & Suroso, I. J. S. (2019). University information system security risk assessment using NIST 800-30. International Journal of Recent Technology and Engineering, 8(3), 8380–8385. https://doi.org/10.35940/ijrte.C6511.098319

Kurniawan, F., Nugroho, L. E., & Kusumawardani, S. S. (2017). Risk Assessment dan Business Impact Analysis BPK RI dalam Pengembangan DRP BPK RI dengan Standar NIST 800-30 Rev 1 . November, 125–136.

Mahardika, F. (2017). Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang). 02(02), 1–8.

Meilani, Y. I., Syamsuar, D., & Kunang, Y. N. (2019). Assessment Resiko Teknologi Pada Implementasi Sistem Informasi Akademik E-University. Jurnal Bina Komputer, 1(1), 54–60. https://doi.org/10.33557/binakomputer.v1i1.154

Naibaho, R. S. (2017). Peranan Dan Perencanaan Teknologi Informasi Dalam Perusahaan. Jurnal Warta, 12(52).

Permatasari, D. A., Putra, W. H. N., & Perdanakusuma, A. R. (2019). Analisis Manajemen Risiko Sistem Informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 3(6), 6001–6008. http://j-ptiik.ub.ac.id

Putra, R. R. (2019). Analisis Manajemen Risiko Ti Pada Keamanan Data E - Learning Dan Aset It Menggunakan NIST SP 800 – 30 Revisi 1. JATISI (Jurnal Teknik Informatika Dan Sistem Informasi), 6(1), 96–105. https://doi.org/10.35957/jatisi.v6i1.154

Santoso, H. B., & Ernawati, L. (2017). Manajemen Risiko Pada Pusat Data Perguruan Tinggi Dengan Kerangka Kerja NIST 800-30 (Studi Kasus : Universitas Kristen Duta Wacana). Jurnal Informatika Dan Sistem Informasi (JUISI) Universitas Ciputra, 03(02), 8–17.

Seta, H. B., & Rahayu, T. (2017). Manajemen Risiko Aplikasi Pembelajaran Berbasis Online. Seminar Nasional Teknologi Informasi Dan Multimedia, 7–12.

Subekti, H., & Nur'aini, S. (2019). Manajemen resiko di smk muhammadiyah 3 yogyakarta. Al Fatih-Jurnal Pendidikan Dan Keislaman, II(2), 214–231.

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi, 2(2), 8–13. https://doi.org/10.24014/coreit.v2i2.2356

Wahyudi, I., Bahri, S., & Handayani, P. (2019). Aplikasi Pembelajaran Pengenalan Budaya Indonesia. V(1), 135–138. https://doi.org/10.31294/jtk.v4i2