Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, Vol. 8, No. 2, Agustus 2022, Hal. 189-195
e-ISSN 2502-8995 p-ISSN 2460-8181

PENILAIAN RISIKO JARINGAN KOMPUTER MENGGUNAKAN *FRAMEWORK* NIST SP 800-30 REVISI 1 PADA SMK MUHMMADIYAH 2 PEKANBARU

[1]Megawati, [2]Siti Rosnawati
[1]Sains dan Teknologi, Sistem Informasi, UIN Suska Riau, Pekanbaru, Indonesia
Email: [1]megawati.uin-suska.ac.id, [2]sitirosnawati98@gmail.com

ABSTRAK

Laboratorium Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru merupakan sarana untuk belajar mengajar yang beridiri pada tahun 2005. Pada saat ini laboratorium TKJ SMK Muhammadiyah 2 Pekanbaru belum pernah melakukan penilaian risiko pada perangkat dan peralatan jaringan serta kegiatan yang ada di lingkungan laboratorium sehingga suatu risiko tidak dapat diprediksi, maka kemungkinan risiko tersebut akan muncul akan semakin tinggi. Risiko yang muncul dapat merugikan suatu instansi, baik dari segi finansial maupun *non* finansial. Penelitian ini dilakukan untuk mengetahui risiko apa saja yang terjadi. Penelitian ini menggunakan metode *Framework* NIST SP 800-30r1 untuk mendapatkan nilai risiko di Laboratorium Jaringan TKJ SMK Muhammadiyah 2 Pekanbaru, metode ini adalah metode yang memberikan panduan manajemen dan penilaian risiko untuk sistem teknologi informasi yang merupakan standar dari pemerintahan *United States*. Sedangkan untuk teknik pengumpulan data menggunakan analisis kualitatif. Tahapan penilaian risiko yang dilakukan antara lain *Prepare for Assessment, Conduct Assessment, Communicate Result,* dan *Maintain Assessment*. Penilaian ini diambil dari hasil wawancara terhadap enam responden yang terdapat pada manajemen organisasi jurusan Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru. Dari tahapan penilaian, didapatkan satu (1) risiko level rendah, sembilan (9) risiko level sedang, enam (6) risiko level tinggi.

Kata kunci: Analisis Kualitatif, *Assessment Risk,* Laboratorium TKJ, NIST SP 800-30r1.

Abstract

The Computer and Network Engineering Laboratory of SMK Muhammadiyah 2 Pekanbaru is a means for teaching and learning that was established in 2005. At this time the TKJ laboratory of SMK Muhammadiyah 2 Pekanbaru had never conducted a risk assessment on network devices and equipment as well as activities in the laboratory environment so that there was no risk. predictable, then the likelihood that these risks will arise will be even higher. Risks that arise can harm an institution, both from a financial andperspective non- financial. This research was conducted to determine the risks that occur. This study uses themethod Framework NIST SP 800-30r1to obtain the risk value in the Computer Engineering Network and Network Laboratory of SMK Muhammadiyah 2 Pekanbaru, this method is a method that provides management guidance and risk assessment for information technology systems which are the standards of thegovernment United States. Meanwhile, the data collection technique used qualitative analysis. The stages of risk assessment carried out include Prepare for Assessment, Conduct Assessment, Communicate Result, and Maintain Assessment. This assessment was taken from the results of interviews with six respondents in organizational management, majoring in Computer and Network Engineering, SMK Muhammadiyah 2 Pekanbaru. From the assessment stage, one (1) low level risk, nine (9) medium level risk, six (6) high level risk were obtained.

Keywords*: Assessment Risk, Computer and Network Laboratory TKJ, Framework NIST SP 800- 30r1, Qualitative Analysis.*

A. PENDAHULUAN

Penggunaan teknologi informasi membawa perubahan perubahan besar dalam berbagai sektor, salah satunya pada bidang pendidikan. Dalam hal ini pula, pemerintah diharuskan memfasilitasi pemafaatan teknologi sesuai dengan Undang-Undang Nomor 11 tahun 2008 pasal 40 ayat 1 yang berbunyi Pemerintah memfasilitasi pemanfaatan teknologi informasi dan transaksi elektronik sesuai dengan ketentuan Peraturan Perundang undangan. Sehingga di setiap tempat yang berhubungan dengan pemerintahan harus disertakan teknologi informasi dan komunikasi dalam setiap pelayanan, mulai dari perkantoran sampai dengan sekolah [1].

Tingkat ketergantungan SMK Muhammadiyah 2 pada jaringan komputer

menimbulkan risiko terhadap sarana prasarana dan informasi sekolah terutama pada jurusan Teknik Komputer dan Jaringan (TKJ). Risiko sarana dan prasana SMK Muhammdiyah 2 yaitu sering terjadinya gangguan listrik, pemakaian siswa yang tidak megikuti prosedur, dan perangkat komputer dan jaringan yang sangat mudah rusak dan tidak stabil yang didukung oleh usia perangkat yang sudah cukup tua. Adapun resiko informasi yang menyebabkan salah satu risiko adalah risiko keamanan informasi, dimana informasi menjadi suatu yang penting yang harus tetap tersedia dan dapat digunakan, serta terjaga keberadaannya dari pihak yang tidak berwenang yang akan menggunakannya untuk kepentingan tertentu atau akan merusak informasi tersebut. Informasi merupakan sebuah aset penting bagi organisasi yang perlu dilindungi dan diamankan. Untuk risiko yang terjadi pada jaringan komputer sulit di perkirakan oleh pihak laboraturium dikarenakan tidak adanya dokumentasi dan tidak pernah melakukan penilaian risiko jaringan komputer di laboraturum Teknik Komputer dan jaringan.

Risiko yang bermunculan dikarenakan belum pernah dilakukan penilaian risiko. Penilaian risiko adalah segala proses pengelolaan risiko yang mencakup identifikasi, evaluasi, mitigasi dan pengendalian risiko terutama yang berhubungan dengan menyangkut keamanan informasi yang dapat mengancam kelangsungan usaha, strategi visi misi dan aktivitas organisasi untuk masa sekarang beserta masa yang akan datang [2]. Risiko-risiko yang terdapat pada jaringan komputer TKJ SMK Muhammadiyah 2 Pekanbaru harus dikelola dengan baik agar tidak berdampak buruk bagi kegiatan yang akan dilaksanakn di Laboratorium dan ruang Data center TKJ SMK Muhammadiyah 2 Pekanbaru.

Berdasarkan permasalahan diatas, maka penulis bermaksud untuk menganalisis penilaian risiko jaringan komputer pada Jurusan Teknik Komputer dan jaringan SMK Muhammadiyah 2 Pekanbaru. Pada penilaian ini nantinya penulis menggunakan *Framework* NIST SP 800-30r1 merupakan kerangka kerja yang dikeluarkan oleh *National Institute Standard and Technology* (NIST) pada tahun 2012.

B. LANDASAN TEORI

B.1. Penilian Risiko

Risiko atau ancaman merupakan sesuatu yang tidak pasti pada masa yang akan datang yang berkaitan dengan kerugian yang harus dipikul oleh organisasi. Berikut adalah 3 aspek yang memungkinkan terjadinya suatu ancaman atau risiko, yaitu:

1) Kemungkinan dari suatu kejadian ataupun peristiwa.
2) Dampaknya atau kosekuensi dari risiko ketika risiko tersebut terjadi (belum terjadi).
3) Probabilitas risiko yang merupakan kemungkinan akan terjadinya suatu kejadian yang berisiko.

Pada sebuah instansi pendidikan, ancaman atau risiko bisa datang dari bagian *eksternel* ataupun bagian *internal.* Ancaman yang timbul akibat dari bagian *eksternal* adalah adanya peraturan perundang-undangan baru, perkembangan teknologi, bencana alam dan lainnya. Sedangkan risiko yang muncul akibat dari bagian *internal* berupa dana operasional yang terbatas, sumber daya manusia yang tidak berkompeten, peralatan yang kurang atau memadai (Stoneburner, Goguen, dan Feringa, 2002).

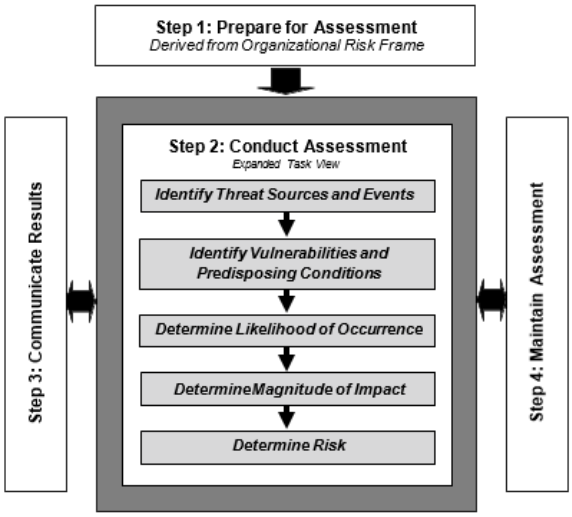
B.2. Jaringan Komputer

Menurut Kristanto (2003) akan menggunakan istilah jaringan komputer untuk mengartikan suatu himpunan interkoneksi sejumlah komputer yang dapat saling bertukar informasi. bentuk koneksinya tidak harus melalui kawat saja melainkan dapat menggunakan serat optik, gelombang mikro, atau bahkan satelit komunikasi.

B.3. NIST SP 800-30 Revisi 1

NIST (2012) NIST *Special Publication* 800-30r1 atau NIST SP 800- 30r1 merupakan untuk memberikan panduan untuk melakukan penilaian risiko dari sistem dan organisasi informasi federal, memperkuat panduan dalam NIST *Special Publication* 800-39. NIST *Special Publication* 800-30r1 juga memberikan panduan kepada organisasi tentang mengidentifikasi faktor risiko spesifik untuk dipantau secara berkelanjutan, sehingga organisasi dapat menentukan apakah risiko telah meningkat ke tingkat yang tidak dapat diterima (yaitu, melebihi toleransi risiko organisasi) dan tindakan yang berbeda harus diambil.

Pada gambar 1 dapat dilihat tahapan – tahapan *Risk Assessment Activities* dalam melakukan manajemen risiko dengan menggunakan NIST SP 800-30r1 *Framework.*



Gambar 1. *Framework* NISP SP 800-30r1

C. METODE PENELITIAN

C.1. Tahap Perencanaan

Pada tahap perencanaan ini merupakan taha awal dari penelitian. Dalam tahap perencanaan ini terdapat beberapa kegiatan yang harus dilakukaukan diantaranya menentukan masalah, menentukan tujuan, dan menentukan data yang dibutuhkan.Metode Penelitian memberikan penjelasan tentang langkah-langkah, data, lokasi penelitian, metode evaluasi yang digunakan serta penjelasan terstruktur tentang algoritma atau metode dari penelitian yang dibahas.

C.2. Sumber Data

Sumber data penelitian yaitu dari responden, yakni orang yang menjawab pertanyaan penelitian, yaitu tertulis dan lisan. Sumber data terbagi menjadi dua yaitu data primer serta data sekunder. Data primer merupakan observasi dan hasil wawancara, sementara data sekunder merupakan *website* sekolah dan penelitian terdahulu.

C.3. Metode NIST SP 800-30r1

Metode penelitian yang digunakan dalam penelitian ini merupakan metode NIST SP 800-30r1.

C.4. Metode Analisis Data

Data yang dikumpulkan oleh penulis dengan menggunakan metode pengumpulan data. Metode pengumpulan data yang akan digunakan penulis merupakan metode analisis kualitatif. Analisis Kualitatif yaitu analisis yang dilakukan dengan cara mendeskripsikan jawaban narasumber.

C.5. Metode Pengumpulan Data

Pengumpulan data mencangkup pencarian izin, pelaksanaan strategis *sampling* kualitatif yang baik, mengembangkan caracara untuk merekam informasi, baik secara digital maupun kertas, menyimpan data, dan mengantisipasi persoalan etika yang mungkin muncul.

D. HASIL DAN PEMBAHASAN

D.1. Analisa Perangkat Jaringan

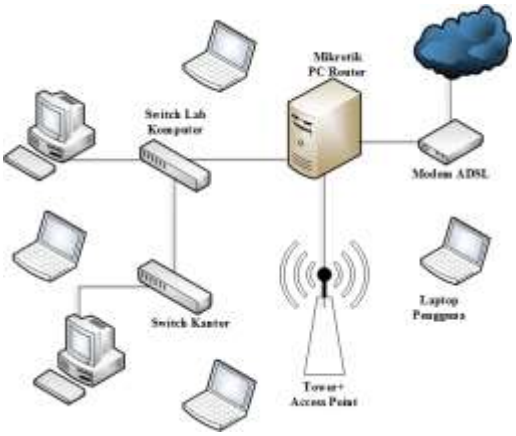
Berbagai macam perangkat teknologi informasi ada di Di Jurusan TKJ, perangkat jaringan, perangkat lunak, dsb. Diantara perangkat server jaringan komputer yang terdapat pada SMK Muhammadiyah 2 adalah sebagai berikut:

Tabel 1 Data Perangkat Jaringan

Perangkat	Jumlah	Kapasitas
Router	2	Microtik Ogma Corret OC 200, Celocia 8101
Gateway	2	Coude Router
Core Switch	1	Juniper ex4200
Switch Server	1	Juniper ex2200
Acces Point Indoor	5	TP Link 4 unit, Cisco 1 unit
Acces Point Outdoor	11	Microtik

D.2. Analisa Tata Kelola Jaringan

Jaringan internet pada SMK Muhammadiyah 2 Pekanbaru menggunakan jaringan 1 *Speedy* dari Telkom dan 1 *Speedy Local.* Jaringan internet tersebut terhubung dengan menggunakan jaringan fiber optik dengan kecepatan 20 Mbps. *Router* yang dipakai menggunakan *router Microtik Ogma corret OC* 2000 dan *Celocia* 8101. Dengan lokasi SMK Muhammadiyah 2 Pekanbaru yang luas dan struktur bangunan yang bertingkat, sehingga dibuatlah wireless LAN yang menggunakan teknologi *WiFi* di lingkungan SMK Muhammadiyah 2 Pekanbaru. Jaringan *wireless* LAN yang ada pada saat ini, belum dapat menjangkau keseluruhan lokasi yang ada di SMK Muhammadiyah 2 Pekanabaru. Jaringan *wireless* LAN hanya dipergunakan oleh *user* untuk mengakses layanan hotspot yang tersedia di SMK Muhammadiyah 2 Pekanbaru. Untuk jaringan *wireless* LAN SMK Muhammadiyah 2 Peknabru dapat digambar sebagai berikut.



Gambar 2 Skema Jaringan Komputer

D.3. Pemetaan RACI

RACI *Chart* terdiri 4 parameter yaitu [4]:

1) *Responsible* (R): orang yang melakukan suatu kegiatan atau melakukan pekerjaan.
2) *Acountable* (A): orang yang bertanggung jawab dan memiliki otoritas untuk memutuskan suatu perkara dari suatu pekerjaan.
3) *Consulted* (C): orang yang diperlukan umpan balik atau sarannya dan konstribusi akan kegiatan tersebut.
4) *Informad* (I): orang-orang yang perlu tau isi dari suatu keputusan atau tindakan.

Berdasarkan keterangan dari RACI *Chart* maka dapat ditetapkan jumlah kuesioner yang akan disebarkan untuk mendukung penelitian ini adalah sebanyak 6 responden. Adapun rincian kuesioner tersebut adalah Kepala Jurusan (1), Sekretaris Jurusan (2), Bendahara (3), Kepala Lab. TKJ (4), Bagian Humas (5), dan Manager BC TKJ (6).

Tabel 2 RACI *Chart*

Tugas atau Peran	Ketua Jurusan	Sekretaris	Bendahara	Ka.Lab TKJ	Humas	Manager BC
Mengembangkan, mengelola, mengoperasikan serta memelihara Lab. Jaringan TKJ perangkat jaringan dan perangkat server	R,A,C,I	R,C,I	R,C,I	R,A,C,I	R,C,I	R,A,C,I
Mengelola, mengoperasikan dan mengevaluasi kegiatan dan data perangkat di Lab. TKJ	R,A,C,I	R,C,I	R,C,I	R,A,C,I	R,A,C,I	R,C,I
Menentukan dan menyetujui serta bertanggung atas kerja guru dan kepengurusan Lab. TKJ	R,A,C,I	R,C,I	R,C,I	R,A,C,I	R,C,I	I
Memberikan solusi proses pengelolaan Lab. TKJ	R,C,I	I	I	R,A,C,I	R,I	R,A,C

D.4. Hasil Penelitian

Pada penelitian *Assessment Risk* Jaringan komputer pada Laboratorim Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru ini, menggunakan metode NIST SP 800-30r1 dan analisis Kualitatif. Dalam hal ini, penulis hanya memenejemen penilai risiko yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru.

1. Prepare for Assessment

Pada proses *Prepare for Assessment* yang merupakan tahapan persiapan/perencanaan dalam penilaian kegiatan *Assessment Risk Management*. Sesuai dengan metode penelitian kualitatif yang dilakukan oleh penulis maka langkahlangkah yang dijalankan penulis akan disesuaikan dengan metode penelitian pengumpulan data dari [5]. Adapun aktivitas pengumpulan data yaitu menentukan tempat/individu; memperoleh akses dan membangun hubungan; mengumpulkan data; merekam informasi; persoalan lapangan; dan menyimpan data.

2. Conduct Assessment

Pada tahapan ini akan di ketahui nilai risiko yang terdapat pada Laboratorium Jaringan Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru. Penilaian yang dilakukan meliputi sumber dan peristiwa ancaman, kerentanan dan kodisi predisposisi, kemungkinan yang terjadi, dampak dari ancaman, dan risiko yang terjadi. Dalam penerapannya untuk melakukan penilaian risiko, NIST SP 800- 30r1 dibagi menjadi 4 kategori penilaian. Dimana setiap kategori memiliki bobot nilai. Empat kategori tersebut adalah sebagai berikut:

1) *Adversarial* (25)
2) *Accidential* (25)
3) *Structural* (25)
4) *Enviromental* (25)

Dimana jika keempat kategori diatas digabungkan, maka bobot nilainya akan menjadi 100. Untuk mendapatkan nilai semi kualitatif pada skala penilaian, jumlah pada penilaian responden wajib berada pada perbandingan skala 100 dan nilai kualitatif didapat dari nilai semi kualitatif yang telah ditentukan oleh metode NIST SP 800-30r1.

Untuk mendapatkan nilai semi kualitatif, berikut rumus yang digunakan dalam NIST SP 800-30r1:

$$Penilaian\ Semi\ Kualitatif = \frac{\sum Penilaiain\ Responden}{\text{Bobot Kategori}} \times 100 \qquad (1)$$

a) Identity Threat Source and Events

Sebelum melakukan *assessment*, maka tentukan terlebih dahulu sumber ancaman yang akan dilakukan penilaian. Untuk skala penilaian dari *Identity Threat Source and Event.*

Tabel 3 Skala Hasil Penilaian - *Identity Threat Source and Event*

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5+R6	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	*Outsider*/orang luar	3+3+3+3+2+3	68	Moderate
2	*Insider*/orang dalam	4+4+3+2+2+4	72	Moderate
3	*Trusted*/*Insider*/orang Kepercayaan	4+2+3+2+2+2	60	Moderate
Accidential				
4	*User*	4+4+4+4+3+4	92	High
5	*Administrator*	3+4+2+1+3+1	56	Moderate
Structural				
6	Alat Penyimpanan	3+4+3+2+4+3	76	Moderate
7	Alat Pemrosesan	4+4+4+4+4+3	88	High
8	Alat Komunikasi	4+3+3+3+4+4	84	High
9	Kontrol Suhu Ruangan	4+4+4+3+4+3	88	High
10	Sistem Operasi	3+2+3+4+3+4	76	Moderate
11	Alat Jaringan	4+4+3+4+4+4	92	High
12	Virus	4+4+4+3+4+3	88	High
Environmental				
13	Api	3+2+3+4+3+4	76	Moderate
14	Angin/Hujan Badai	4+3+4+4+3+4	88	High
15	Telekomunikasi	4+3+3+4+3+4	84	High
16	Tenaga Listrik	4+4+4+4+4+4	96	Very High

b) Identity Vulnerability and Predisposing Conditions

Dalam mengidentifikasi kerentanan dan kondisi predisposisi pada Laboratorium Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru, dilakukan *assessment* pada kerentanan dan kondisi predisposisi sumber ancaman yang telah dilakukan.

Tabel 4 Skala Hasil Penilaian - *Identity Vulnerability and Predisposing Conditions*

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5+R6	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	*Outsider*/orang luar	3+3+3+3+3+3	72	Moderate
2	*Insider*/orang dalam	4+4+4+4+4+4	96	Very High
3	*Trusted*/*Insider*/orang Kepercayaan	4+2+2+1+2+1	48	Moderate
Accidential				
4	*User*	4+4+4+3+4+3	88	High
5	*Administrator*	3+3+2+1+4+1	56	Moderate
Structural				
6	Alat Penyimpanan	4+3+3+4+4+4	88	High
7	Alat Pemrosesan	4+3+3+4+4+4	88	High
8	Alat Komunikasi	4+3+3+4+4+4	88	High
9	Kontrol Suhu Ruangan	4+4+4+4+4+4	96	Very High
10	Sistem Operasi	3+3+3+4+4+4	84	High
11	Alat Jaringan	3+4+3+4+4+4	88	High
12	Virus	3+3+4+3+4+4	92	High
Environmental				
13	Api	3+3+3+4+4+4	84	High
14	Angin/Hujan Badai	4+3+3+4+4+4	88	High
15	Telekomunikasi	4+3+3+3+4+5	96	Very High
16	Tenaga Listrik	4+3+3+4+4+4	88	High

c) Determine Likelihood of Occurance

Menentukan Kemungkinan Ancaman yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru, sehingga dilakukan *assessment* pada kemungkinan terjadi yang disebabkan oleh sumber ancaman.

Tabel 5 Skala Hasil Penilaian – *Determine Likelihood of Occurrence*

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5+R6	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	*Outsider*/orang luar	3+3+3+2+4+4	76	Moderate
2	*Insider*/orang dalam	4+4+3+4+2+4	84	High
3	*Trusted*/*Insider*/orang Kepercayaan	3+3+1+1+4+1	52	Moderate
Accidential				
4	*User*	4+4+3+4+4+4	92	High
5	*Administrator*	0+1+1+1+2+1	20	Low
Structural				
6	Alat Penyimpanan	3+3+3+4+4+4	84	High
7	Alat Pemrosesan	3+3+3+3+4+3	76	Moderate
8	Alat Komunikasi	4+3+3+2+4+2	72	Moderate
9	Kontrol Suhu Ruangan	4+4+3+2+4+2	76	Moderate
10	Sistem Operasi	3+3+3+2+4+3	72	Moderate
11	Alat Jaringan	4+3+4+2+4+3	80	High
12	Virus	4+4+4+2+4+2	80	High
Environmental				
13	Api	2+3+3+2+4+2	64	Moderate
14	Angin/Hujan Badai	4+4+3+3+4+3	84	High
15	Telekomunikasi	4+3+3+3+4+3	80	High
16	Tenaga Listrik	4+4+3+2+3+2	76	Moderate

d) Determine Magnitude of Impact

Selanjutnya menentukan dampak ancaman yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru, ketika dilakukan *assessment* pada dampak ancaman yang disebabkan oleh sumber ancaman.

Tabel 6 Skala Hasil Penilaian – *Determine Magnitude of Impact*

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5+R6	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	*Outsider*/orang luar	3+5+3+4+4+4	92	High
2	*Insider*/orang dalam	4+4+4+4+2+4	88	High
3	*Trusted*/*Insider*/orang Kepercayaan	3+2+2+1+4+1	52	Moderate
Accidential				
4	*User*	4+5+4+3+4+3	92	High
5	*Administrator*	4+2+2+1+4+1	56	Moderate
Structural				
6	Alat Penyimpanan	4+3+3+4+4+4	88	High
7	Alat Pemrosesan	4+3+3+4+4+4	88	High
8	Alat Komunikasi	4+3+3+4+4+4	88	High
9	Kontrol Suhu Ruangan	4+5+4+4+4+4	100	Very High
10	Sistem Operasi	3+3+3+4+4+4	84	High
11	Alat Jaringan	4+3+4+4+4+4	92	High
12	Virus	4+4+5+4+4+3	96	Very High
Environmental				
13	Api	2+4+3+4+4+4	84	High
14	Angin/Hujan Badai	4+4+3+4+4+4	92	High
15	Telekomunikasi	3+4+3+4+2+4	80	High
16	Tenaga Listrik	4+4+4+4+4+3	92	High

e) Determine Risk

Dalam menentukan tingkat risiko dapat dilakukan dengan mencocokkan antara penilaian

likelihood dan *impact* dengan melihat tabel pada *NIST SP 800- 30r1* untuk mendapatkan nilai untuk tingkat risikonya. Untuk mencocokan antara nilai *likelihood* dan *impact* dapat digunakan dengan penyesuaian pada table 7.

Tabel 7 Skala Hasil Penilaian – *Determine Magnitude of Impact* (Kombinasi dari *Likelihood* dan *Impact*)

Likelihood (Threat Event Occurs and Resul in Advers Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

3. Communicate Results

Dalam sesi *communicate result*, penulis akan membicarakan apa yang didapat dari kegiatan *assessment IT risk management* pada Laboratorium Jaringan SMK Muhammadiyah 2 Pekanbaru.

Tabel 8 Hasil *Assessment Scale*

No	Threat Source	Source Event	Vulnerability Predisposing	Likelihood	Impact	Risk
			Adversarial			
1	Outsider/orang luar	Moderate	Moderate	Moderate	High	Moderate
2	Insider/orang dalam	Moderate	Very High	High	High	High
3	Trusted Insider/orang Kepercayaan	Moderate	Moderate	Moderate	Moderate	Moderate
			Accidential			
4	User	High	High	Moderate	High	High
5	Administrator	Moderate	Moderate	Low	Moderate	Low
			Structural			
6	Alat Penyimpanan	Moderate	High	High	High	High
7	Alat Pemrosesan	High	Moderate	Moderate	High	Moderate
8	Alat Komunikasi	High	High	Moderate	High	Moderate
9	Kontrol Suhu Ruangan	High	Very High	Very High	Moderate	High
10	Sistem Operasi	Moderate	High	Moderate	High	Moderate
11	Alat Jaringan	High	High	High	High	High
12	Virus	High	High	High	Very High	Very High
			Environmental			
13	Api	Moderate	High	Moderate	High	Moderate
14	Angin/Hujan Badai	High	High	High	High	High
15	Telekomunikasi	High	Very High	High	High	High
16	Tenaga Listrik	Very High	High	Very High	High	Moderate

4. Maintain Assessment

Hasil penilaian yang dilaksanakan pada Laboratorium Jaringan SMK Muhammadiyah 2 Pekanbaru cukup baik, dari semua tahapan *assessmen IT risk management* yang dilakukan mengeluarkan skala penilaian pada kategori sangat tinggi, tinggi, sedang, dan rendah. Hasil ini didapat dari analisis kuesioner dan wawancara terhadap keenam responden/narasumber yang dianggap pantas untuk memberikan penilaian tentang risiko. Dari hasil penilaian maka direkomendasikan beberapa kontrol berdasarkan NIST SP 800-30 r1 dan pihak manajemen yang dapat dilakukan terhadap risiko yang terlihat pada tabel berikut.

Tabel 9 Rekomendasi pengendalian

No	Threat Source	Rekomendasi Pengendalian
	Adversarial	
1	Outsider/orang luar	Melakukan pengawasan dan pengecekan peralatan maupun perlengkapan yang digunakan pada setiap kegiatan yang ada di Lab. Jaringan TKJ
2	Insider/orang dalam	
3	Trusted Insider/orang Kepercayaan	
	Accidential	
4	User	Melakukan pengawasan terhadap peralatan dan perlengkapan praktik. Hal ini dilakukan agar tidak terjadi kerusakan pada peralatan dan perlengkapan.
5	Administrator	
	Structural	
6	Alat Penyimpanan	Melakukan perawatan, pengecekan dan service berkala terhadap alat penyimpanan, alat pemrosesan, alat komunikasi, peralatan kontrol suhu ruangan dan jaringan. Kegiatan perawatan, pengecekan dan service wajib dilakukan secara berkala minimal 1 minggu sekali. Terutama perangkat yang sudah tua dan harus diperhatikan dengan baik agar tidak menimbulkan risiko yang besar pada Lab. Jaringan TKJ
7	Alat Pemrosesan	
8	Alat Komunikasi	
9	Kontrol Suhu Ruangan	
10	Sistem Operasi	
11	Alat Jaringan	
12	Virus	
	Environmental	
13	Api	Melakukan pengecekan kabel yang dipasang agar tidak terjadi konsleting ketika aliran listrik sehingga tidak akan memicu api.
14	Angin/Hujan Badai	Melakukan perbaikan pada atap yang mengalami kebocoran dan kerusakan gedung lainnya.
15	Telekomunikasi	Menghubungkan/koordinasi dengan provider penyedia/anggara.
16	Tenaga Listrik	Memakai UPS agar aruh listrik terkendali dengan baik.

E. KESIMPULAN

1. Laboratorium Jaringan Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru belum ada dokumen risk management dan juga penilaian risiko belum pernah dilakukan, dalam pelaksanaan *assessment IT risk* jaringan komputer di SMK Muhammadiyah 2 Pekanbaru akan menggunakan metode NIST SP 800-30r1 dan teknik pengumpulan data kualitatif.
2. Keempat kategori sumber ancaman yang mempengaruhi munculnya risiko pada Laboratorium Jaringan Teknik Komputer dan Jaringan SMK Muhammadiyah 2 Pekanbaru yaitu *adversarial, accidential structural, dan environmental.*
3. Hasil *assessment IT risk* jaringan komputer pada SMK Muhammadiyah 2 Pekanbaru menunjukkan tingkat risiko yang ada berada pada posisi sangat tinggi, tinggi, sedang, dan rendah yang berarti munculnya efek buruk yang parah dan serius terhadap individu, aset dan organisasi.

REFERENSI

[1] Arlin Nurliyani, A. H. M., Dedy Syamsuar. (2019). Assessment it risk management pada laboratorium teknik komputer dan jaringan sekolah. *JITE (Journal of Informatics and Telecommunication Engineering)*.

[2] NIST, S. (2012). 800-30, revision 1. *Guide for Conducting Risk Assessments*. Projects, Science, R. D. D., dan of Defence Canberra ACT 2600 Australia,

[3] Stoneburner, G., Goguen, A., dan Feringa, A. (2002). Risk management guide for information

technology systems. *Nist special publication*, *800*(30), 800–30.

[4] Dirk Steupetaet, R. M. B. P. S. R., Steven De Haes. (2009). *Enterprise risk: Identify, govern and manage it risk, the risk it framework exposure draft*. IT Governance Institute.

[5] Creswell, J. (2014). Penelitian kualitatif & desain riset: Memilih di antara lima pendekatan.(a. lazuardi, trans.). *Yogyakarta: Pustaka Pelajar.(Original work published 1998)*.

[6] Kristanto, A. (2003). *Jaringan komputer*. Yogyakarta: Graha Ilmu.

[7] Sugiyono, S. (2010). *Metode penelitian kuantitatif dan kualitatif dan r&d*. Alfabeta Bandung.