



JITE (Journal of Informatics and Telecommunication Engineering)

Available online <http://ojs.uma.ac.id/index.php/jite> DOI : 10.31289/jite.v3i1.2622

Assessment IT Risk Management pada Laboratorium Teknik Komputer dan Jaringan Sekolah

Assessment IT Risk Management at The Computer and Network Laboratory School

Arlin Nurliyani*, Dedy Syamsuar, A. Haidar Mirza

Universitas Bina Darma Palembang, Indonesia

*Corresponding Email: arlin.ar1@gmail.com

Abstrak

Laboratorium Teknik Komputer dan Jaringan Sekolah merupakan sarana untuk belajar mengajar yang memiliki permasalahan pada teknologi informasi. Pada penelitian ini, akan dilaksanakan Assessment IT Risk Management pada Laboratorium Teknik Komputer dan Jaringan Sekolah. Penelitian ini dilakukan untuk mengetahui risiko apa saja yang terjadi. Dan penelitian ini, akan digunakan metode Framework NIST SP 800-30r1 untuk mendapatkan nilai risiko di Laboratorium Teknik Komputer dan Jaringan Sekolah. Sedangkan untuk teknik pengumpulan data akan menggunakan analisis kualitatif. Tahapan penilaian risiko yang dilakukan antara lain Prepare for Assessment, Conduct Assessment, Communicate Result, dan Maintain Assessment. Dari tahapan penilaian, tingkat risiko yang didapat berada pada posisi sedang. Penilaian ini diambil dari hasil wawancara terhadap lima responden yang terdapat pada manajemen organisasi Laboratorium Teknik Komputer dan Jaringan Sekolah. Risiko yang muncul berdampak serius pada aset, organisasi dan kegiatan di Laboratorium Teknik Komputer dan Jaringan Sekolah.

Kata Kunci: Risk Management, Laboratorium Sekolah, Framework NIST SP 800-30r1, Analisis Kualitatif, Risiko

Abstract

The Computer and Network Engineering Laboratory School is a means for teaching and learning that has problems with information technology. In this research, IT Risk Management Assessment will be carried out at the Computer and Network Engineering Laboratory of School. This research was conducted to determine what risks of what happened. In this study, the NIST SP 800-30r1 Framework method will be used to obtain risk scores. While for data collection techniques will use qualitative analysis. The stages of risk assessment carried out include Prepare for Assessment, Conduct Assessment, Communicate Result, and Maintain Assessment. From the assessment stage, the level of risk obtained is in a moderate position. This assessment was taken from the results of interviews with five respondents in the organization management of The Computer and Network Engineering Laboratory School. Emerging risks have a serious impact on assets, organization and activities in The Computer and Network Engineering Laboratory School.

Keywords: Risk Management, Laboratorium School, NIST SP 800-30r1 Framework, Qualitative Analysis, Risk

How to Cite: Nurliyani, A., Syamsuar, D., dan Mirza, A. H. (2019). Assessment IT Risk Management at The Computer and Network Laboratory School. JITE (Journal of Informatics and Telecommunication Engineering). 3 (1): 115-124

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada saat ini menjadi penting dalam kehidupan sehari-hari. Hampir disetiap kegiatan dan layanan public pemerintah telah dihubungkan dengan teknologi informasi dan komunikasi. Dalam hal ini pula, pemerintah diharuskan memfasilitasi pemanfaatan 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.

Jaringan komputer merupakan sekumpulan komputer, printer, maupun peralatan teknologi lainnya yang saling terhubung satu sama lain dan sehingga menjadi informasi data bergerak melalui kabel-kabel dan memungkinkan pengguna dalam bertukar data dan informasi melalui media teknologi (Haryanto, 2012).

Bidang keahlian Teknik Komputer dan Jaringan (TKJ) di SMK Negeri 3 OKU berdiri pada Agustus 2003 oleh Bapak Drs. Sidarta, SE yang merupakan kepala sekolah dan selaku koordinator jaringan

informasi sekolah kabupaten OKU. Pada awal berdiri siswa (Angkatan I TKJ) diambil dari jurusan lain yang telah lulus tes penerimaan siswa baru di SMK Negeri 3 OKU. Fasilitas yang ada pada saat itu hanya memiliki 20 unit komputer, switch, hub, access point dan 2 ruang laboratorium TKJ. Laboratorium yang terhubung dengan jaringan hanya laboratorium TKJ 2 dan 3, laboratorium 1 tidak di hubungkan dengan perangkat jaringan karena difokuskan untuk perakitan komputer. Dan penghubung jaringan komputer bagi laboratorium 2 dan 3 SMK Negeri 3 OKU menggunakan kabel UTP yang disertai konektor RJ45. Sedangkan jaringan internet yang terhubung di SMK Negeri 3 OKU menggunakan layanan dari telkom *speedy*.

Ancaman awal yang dapat terjadi pada komputer adalah *local attack*, bahaya berinternet, dan *hacker attack*. Local attack yaitu usaha orang lain yang ingin masuk ke system computer secara langsung, baik itu mengakses data ataupun hanya sekedar membaca data. (Setiawan, 2006)

Risiko-risiko bermunculan pada laboratorium TKJ SMK Negeri 3 OKU, di karenakan belum pernahnya dilakukan Assessment IT Risk Management pada Laboratorium TKJ SMK Negeri 3 OKU. Assessment IT Risk Management

merupakan sebuah cara untuk pengelolaan risiko dan memberi penilaian pada risiko yang terjadi di Laboratorium TKJ SMK Negeri 3 OKU. Risiko-risiko yang terdapat di Laboratorium TKJ SMK Negeri 3 OKU harus dikelola dengan baik agar tidak berdampak buruk bagi kegiatan yang akan dilaksanakan di Laboratorium TKJ SMK Negeri 3 OKU.

Risiko yaitu sebagai peluang terjadinya *bad outcome* (hasil yang buruk), dan besarnya peluang diestimasikan (Hardanto,2006).

Dari penjabaran latar belakang ini penulis bermaksud melakukan Assessment IT Risk Management pada Laboratorium TKJ SMK Negeri 3 OKU. Untuk meminimalisir risiko yang terjadi di laboratorium TKJ SMK Negeri 3 OKU. Untuk melaksanakan penelitian penulis menggunakan kerangka kerja (Framework) NIST SP 800-30r1 sebagai pedoman penilaian risiko.

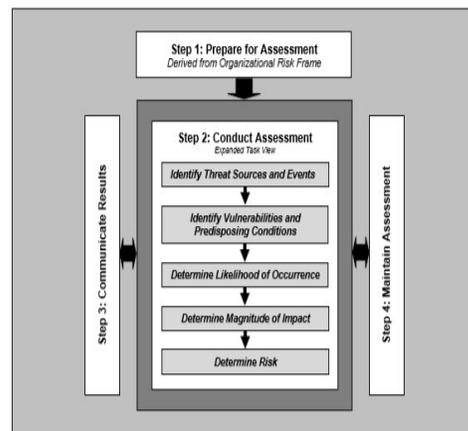
METODE PENELITIAN

Jaringan komputer (*Computer Network*) yaitu kumpulan komputer serta alat-alat lain didalam teknologi yang saling terhubung bersama menggunakan media komunikasi tertentu. Komputer yang bisa terhubung pada suatu jaringan dengan menggunakan beberapa media seperti

kabel, jaringan telepon, gelombang radio, satelit dan sinar *infrared* (Wagito, 2007).

Metode NIST SP 800-30r1

Metode penelitian yang digunakan dalam penelitian ini merupakan metode NIST SP 800-30r1. Manajemen Risiko merupakan proses yang memungkinkan manajer TI untuk menyeimbangkan operasional serta biaya ekonomi dari tindakan pengamanan dan pencapaian keuntungan dalam kemampuan misi dengan melindungi sistem TI serta data yang mendukung misi organisasi (NIST, 2012).



Gambar 1 Framework NIST SP 800-30r1

Skala Likert

Skala likert merupakan skala yang digunakan untuk mengukur sikap, pendapat, dan persepsi seseorang atau sekelompok orang tentang fenomena sosial (Situmorang, 2010).

Setiap kriteria serta sub criteria akan ditransformasikan dalam bentuk suatu pernyataan. Pada penelitian ini digunakan alat ukur dalam penilaian variable dengan menggunakan skala likert. Skala likert yang digunakan memiliki 5 tingkatan yaitu skala 1 sampai 5. Responden diminta untuk memilih satu alternative jawaban yang telah disediakan seperti pada table 1.

Tabel 1 Pengukuran Skala Likert

Penilaian	Nilai
Sangat Rendah	1
Rendah	2
Cukup	3
Tinggi	4
Sangat Tinggi	5

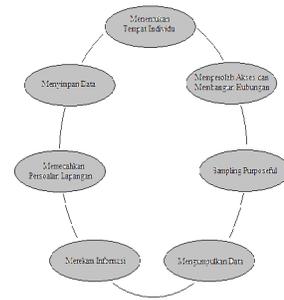
Metode Analisis Data

Analisis Data Kualitatif merupakan upaya yang berkelanjutan, berulang, dan terus-menerus. Masalah reduksi data, penyajian data dan penarikan kesimpulan/verifikasi menjadi gambaran keberhasilan secara berurutan sebagai rangkaian kegiatan analisis yang saling susul-menyusul. (Miles & A. Michael, 1992)

Metode Pengumpulan data

Pengumpulan data kualitatif merupakan dengan berfokus pada jenis data aktual dan prosedur pengumpulannya. Akan tetapi, pengumpulan data melibatkan lebih banyak dari itu. Pengumpulan data mencakup pencarian izin, pelaksanaan

strategis sampling kualitatif yang baik, mengembangkan cara-cara untuk merekam informasi, baik secara digital maupun kertas, menyimpan data, dan mengantisipasi persoalan etika yang mungkin muncul. (Creswell, 2014)



Gambar 2 Lingkaran Aktivitas Pengumpulan Data Kualitatif

HASIL DAN PEMBAHASAN

Analisis Responden

Pada penelitian *Assessment IT Risk Management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU ini, peneliti menggunakan analisis kualitatif. Dalam kegiatan ini, responden akan diwawancarai dengan beberapa pertanyaan tentang risk management pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Responden yang diwawancarai merupakan para guru dan staf yang bekerja sehari-hari di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Karakteristik Responden

Dari pengambilan data primer, responden yang memenuhi syarat sebagai narasumber yang akan diwawancara oleh

penulis berjumlah 5 orang. Kelima narasumber inilah yang mengetahui seluruh kegiatan yang terjadi di laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Adapun narasumber yang sesuai dengan kualifikasi antara lain dapat dilihat dari tabel 2.

Tabel 2 Data Responden

No	Nama	Jabatan	Masa Kerja	Ket
R1	Riadi, S.ST, M.Kom.	Kepala Program Studi TKJ	15 Tahun	PNS
R2	Russadayana, S.Kom.	Kepala Bengkel TKJ	13 Tahun	PNS
R3	Desy Saraswaty, S.Kom.	Guru TKJ/Teknisi	12 Tahun	PNS
R4	Reni Aprilina, S.Pd.	Guru TKJ/Teknisi	10 Tahun	Honor
R5	Sri Wahyuni, S.Pd.	Guru TKJ/Teknisi	2 Tahun	Honor

Hasil Penelitian

Pada penelitian *Assessment Risk Management* pada Laboratorim Teknik Komputer dan Jaringan SMK Negeri 3 OKU 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 Negeri 3 OKU. Dari para staf yang ada pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, bahwa belum terdapat dokumentasi secara jelas tentang managemen risiko didalam kegiatan yang terdapat di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pendokumentasian secara keseluruhan masih manual dan tidak adanya data tentang pengelolaan risiko yang terjadi.

Prepare for Assessment

Pada proses *Prepare for Assessment* yang merupakan tahapan persiapan/perencanaan dalam penilaian kegiatan *Assessment Risk Manajement*. Sesuai dengan metode penelitian kualitatif yang dilakukan oleh penulis maka langkah-langkah yang dijalankan penulis akan disesuaikan dengan metode penelitian pengumpulan data dari John W. Creswell. Adapun aktivitas pengumpulan data yaitu menentukan tempat/individu; memperoleh akses dan membangun hubungan; *sampling purposeful*; mengumpulkan data; merekam informasi; persoalan lapangan; dan menyimpan data.

Conduct Assessment

Tahap *conduct assesment* ini penilaian risiko akan dilaksanakan pada ketiga ruang laboratorium. Untuk mendapatkan hasil penilaian risiko pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU ini, maka akan dilakukan analisis dan wawancara terhadap 5 responden yang terdapat di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU sebagai bagian dari tim ahli pada manajemen laboratorium.

a). Identity Threat Sources 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 Penilaian - Identity Threat Source and Event

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	Outsider/orang luar	2+3+2+3+1	44	Sedang
2	Insider/orang dalam	3+2+4+3+1	52	Sedang
3	TrustedInsider/orang Kepercayaan	1+1+1+1+2	24	Sedang
Accidental				
4	User	2+1+3+3+2	44	Sedang
5	Administrator	1+1+1+1+2	24	Sedang
Structural				
6	Alat Penyimpanan	3+3+2+3+2	52	Sedang
7	Alat Pemrosesan	3+3+2+3+2	52	Sedang
8	Alat Komunikasi	2+3+1+2+1	36	Sedang
9	Kontrol Suhu Ruangan	3+3+1+1+2	40	Sedang
10	Sistem Operasi	2+1+1+1+1	24	Sedang
11	Alat Jaringan	3+3+1+3+2	48	Sedang
12	Virus	3+1+2+2+2	40	Sedang
Environmental				
13	Api	1+1+4+3+1	40	Sedang
14	Angin/Hujan Badai	2+2+2+3+1	40	Sedang
15	Telekomunikasi	2+1+1+2+1	28	Sedang
16	Tenaga Listrik	2+2+3+2+1	40	Sedang

b). Identity Vulnerability and Predisposing Conditions

Dalam mengidentifikasi kerentanan dan kondisi predisposisi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, dilakukan *assessment* pada kerentanan dan kondisi predisposisi sumber ancaman yang telah dilakukan.

Tabel 4 Skala Penilaian - Identity Vulnerability and Predisposing Conditions

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	Outsider/orang luar	2+2+2+3+1	40	Sedang
2	Insider/orang	3+1+1+3+1	36	Sedang

3	TrustedInsider/orang Kepercayaan	1+1+1+1+2	24	Sedang
Accidental				
4	User	3+1+3+3+2	48	Sedang
5	Administrator	2+1+1+1+1	24	Sedang
Structural				
6	Alat Penyimpanan	3+3+1+3+2	48	Sedang
7	Alat Pemrosesan	3+3+1+2+1	40	Sedang
8	Alat Komunikasi	2+3+1+2+1	36	Sedang
9	Kontrol Suhu Ruangan	3+3+2+2+1	44	Sedang
10	Sistem Operasi	2+1+1+1+1	24	Sedang
11	Alat Jaringan	3+3+1+3+1	44	Sedang
12	Virus	3+1+2+2+1	36	Sedang
Environmental				
13	Api	2+1+3+3+1	40	Sedang
14	Angin/Hujan Badai	3+2+2+3+2	48	Sedang
15	Telekomunikasi	3+1+1+2+2	36	Sedang
16	Tenaga Listrik	3+2+3+2+2	48	Sedang

c). Determine Likelihood of Occurrence

Menentukan Kemungkinan Ancaman yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, sehingga dilakukan *assessment* pada kemungkinan terjadi yang disebabkan oleh sumber ancaman.

Tabel 5 Skala Penilaian –Determine Likelihood of Occurrence

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	Outsider/orang luar	2+3+3+3+4	60	Sedang
2	Insider/orang dalam	3+2+2+3+4	56	Sedang
3	TrustedInsider/orang Kepercayaan	2+1+1+1+4	36	Sedang
Accidental				
4	User	3+1+3+3+3	52	Sedang
5	Administrator	2+1+1+1+3	32	Sedang
Structural				
6	Alat Penyimpanan	3+3+1+2+3	48	Sedang
7	Alat Pemrosesan	3+3+1+3+3	52	Sedang
8	Alat Komunikasi	3+3+1+2+4	52	Sedang
9	Kontrol Suhu Ruangan	2+3+1+1+2	36	Sedang
10	Sistem Operasi	2+1+1+1+4	36	Sedang
11	Alat Jaringan	3+3+1+3+2	48	Sedang
12	Virus	3+1+2+3+3	48	Sedang
Environmental				
13	Api	2+1+3+3+3	48	Sedang
14	Angin/Hujan Badai	2+2+2+3+3	48	Sedang

15	Telekomunikasi	3+1+1+1+3	36	Sedang
16	Tenaga Listrik	3+2+3+2+3	52	Sedang

d). Determine magnitude of Impact

Selanjutnya menentukan dampak ancaman yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, ketika dilakukan *assessment* pada dampak ancaman yang disebabkan oleh sumber ancaman.

Tabel 6 Skala Penilaian –Determine Magnitude of Impact

No	Threat Source	Penilaian Responden R1+R2+R3+R4+R5	Penilaian Semi Kualitatif ((PR:25)*100)	Nilai Kualitatif
Adversarial				
1	Outsider/orang luar	2+3+3+3+3	56	Sedang
2	Insider/orang dalam	1+4+3+3+4	60	Sedang
3	Trusted Insider/orang Kepercayaan	1+2+1+1+3	32	Sedang
Accidental				
4	User	1+3+3+3+3	52	Sedang
5	Administrator	1+2+1+2+3	36	Sedang
Structural				
6	Alat Penyimpanan	3+3+3+3+3	60	Sedang
7	Alat Pemrosesan	3+4+1+2+3	52	Sedang
8	Alat Komunikasi	3+3+2+2+2	48	Sedang
9	Kontrol Suhu Ruangan	3+3+1+1+3	44	Sedang
10	Sistem Operasi	1+2+1+1+3	32	Sedang
11	Alat Jaringan	3+2+1+3+2	44	Sedang
12	Virus	1+3+1+2+3	40	Sedang
Environmental				
13	Api	1+4+4+3+3	60	Sedang
14	Angin/Hujan Badai	3+4+3+3+3	64	Sedang
15	Telekomunikasi	1+3+2+1+3	40	Sedang
16	Tenaga Listrik	2+4+3+2+3	56	Sedang

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 mencocokkan antara nilai *likelihood* dan *impact* dapat

digunakan dengan penyesuaian pada table 7.

Tabel 7 Skala Penilaian - Tingkat Risiko (Kombinasi Dari Likelihood Dan Dampaknya)

Kemungkinan (Kejadian Ancaman Terjadi dan Hasil di Dampak negatif)	Tingkat Dampak				
	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Sangat Tinggi	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Tinggi	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Sedang	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Rendah	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Sangat Rendah	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi

Communicate Results

Dalam sesi *communicate result*, penulis akan membicarakan apa yang didapat dari kegiatan *assessment IT risk management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Dari hasil wawancara dan pemberian kuesioner kepada para responden, maka hasil yang di dapat dari penelitian *assessment IT risk management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU cukup baik. Responden yang menjadi narasumber pada penelitian ini hanya sedikit yaitu terdapat 5 responden, kelima responden tersebut merupakan guru mata pelajaran produktif dan staf pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Tabel 8 Hasil Assessment Scale

No	Threat Source	Nilai Kualitatif				
		Source Event	Vulnerability Predisposing	Likelihood	Impact	Risk
<i>Adversarial</i>						
1	Outsider/ orang luar	Sedang	Sedang	Sedang	Sedang	Sedang
2	Insider/ orang dalam	Sedang	Sedang	Sedang	Sedang	Sedang
3	Trusted Insider / orang Kepercayaan	Sedang	Sedang	Sedang	Sedang	Sedang
<i>Accidental</i>						
4	User	Sedang	Sedang	Sedang	Sedang	Sedang
5	Administrator	Sedang	Sedang	Sedang	Sedang	Sedang
<i>Structural</i>						
6	Alat Penyimpanan	Sedang	Sedang	Sedang	Sedang	Sedang
7	Alat Pemrosesan	Sedang	Sedang	Sedang	Sedang	Sedang
8	Alat Komunikasi	Sedang	Sedang	Sedang	Sedang	Sedang
9	Kontrol Suhu Ruang	Sedang	Sedang	Sedang	Sedang	Sedang
10	Sistem Operasi	Sedang	Sedang	Sedang	Sedang	Sedang
11	Alat Jaringan	Sedang	Sedang	Sedang	Sedang	Sedang
12	Virus	Sedang	Sedang	Sedang	Sedang	Sedang
<i>Environmental</i>						
13	Api	Sedang	Sedang	Sedang	Sedang	Sedang
14	Angin/Hujan Badai	Sedang	Sedang	Sedang	Sedang	Sedang
15	Telekomunikasi	Sedang	Sedang	Sedang	Sedang	Sedang
16	Tenaga Listrik	Sedang	Sedang	Sedang	Sedang	Sedang

Maintain Assessment

Hasil penilaian yang dilaksanakan pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU cukup baik, dari semua tahapan assessmen IT risk management yang dilakukan mengeluarkan skala penilaian pada kategori sedang. Hasil ini didapat dari analisis kuesioner dan wawancara terhadap kelima responden/narasumber yang dianggap pantas untuk memberikan penilaian tentang risiko. Masih banyaknya kekurangan yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU sehingga membuat penilaian risiko berada pada kategori sedang. Kekurangan yang sangat

tampak pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU adalah belum adanya dokumen risk management sebagai acuan dalam menghadapi risiko dan dengan penelitian inidiharapkan akan adanya dokumen risk management untuk Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Dokumen manajemen laboratorium belum memadai sehingga untuk mengetahui peralatan dan perlengkapan yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU masih mengalami kesulitan. Dan pada saat pengambilan data peralatan dan perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU penulis melakukan penyusunan manajemen peralatan dan perlengkapan. Buku inventaris tata kelola Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU disusun kembali secara rapi untuk mempermudah mengelola peralatan dan perlengkapan. Kemudian kekurangan sumber daya manusia akan dipenuhi secepatnya dengan mencari toolman yang sesuai, agar peralatan dan perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dapat dikelola dengan baik.

Hasil dan cara penanggulangan yang telah dijabarkan pada poin maintain assessment, diharapkan agar nilai

kemunculan risiko tidak akan naik sehingga bertahan pada level yang telah didapatkan. Bahkan diharapkan pada tingkat risiko dapat diminimalisir dengan baik sehingga skala penilaian yang ada dapat turun pada tingkatan bawah. Perbaikan manajemen harus dilakukan dengan segera untuk meminimalisir segala dampak dan risiko yang muncul sehingga efek yang berpengaruh pada organisasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU tidak mengalami kerugian yang berarti. Dan kegiatan belajar mengajar pada peserta didik dan guru tidak berpengaruh jika risiko muncul pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

SIMPULAN

Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU belum ada dokumen *risk management* dan juga penilaian risiko belum pernah dilakukan, dalam pelaksanaan *assessment IT risk management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU akan menggunakan metode *NIST SP 800-30r1* dan teknik pengumpulan data kualitatif. Keempat kategori sumber ancaman yang mempengaruhi munculnya risiko pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

yaitu *adversarial, accidental, structural*, dan *environmental*. Hasil *assessment IT risk management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU menunjukkan tingkat risiko yang ada berada pada posisi sedang yang berarti munculnya efek buruk yang serius terhadap individu, aset dan organisasi. Aset yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU masih terlindungi dan tidak berpengaruh pada peserta didik dan guru pada proses belajar mengajar di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

DAFTAR PUSTAKA

- Creswell, J. W. (2014). Penelitian Kualitatif & Desain Riset Memilih Diantara Lima Pendekatan (edisi 3). Yogyakarta, Indonesia: Pustaka Pelajar.
- Miles, M. B., & A. Michael, H. (1992). Analisis Data Kualitatif. Jakarta: Universitas Indonesia.
- Setiawan, D. (2006). Sistem Keamanan Komputer. Jakarta: Elex Media Komputindo.
- Situmorang, S. H. (2010). Analisis Data : Untu Riset Manajemen dan Bisnis. Medan. Indonesia: USU Press.
- Haryanto, E.V. (2012). Jaringan Komputer. Jakarta, Indonesia : Penerbit Andy.
- National Institute Standard and Technology (NIST). (2012). Guide for Conducting – NIST Special Publication 800-30 (Revision 1). USA.
- Wagito. (2007). Jaringan Komputer : Teori dan Implementasi Berbasis Linux. Jakarta, Indonesia : Penerbit Gava Media.
- Riadi. (2012). Tesis Analisis Dan Desain Jaringan Intranet SMK Negeri 3 Ogan Komering Ulu Menggunakan Metode Network Development Life Cycle. Palembang, Indonesia : Universitas Bina Darma Palembang..

- Hardanto, S.S. (2006). Manajemen Risiko Bagi Bank Umum. Jakarta, Indonesia : Penerbit Elex Media Komputindo.
- Kurniawan, N.B. (2013). Manajemen Risiko Teknologi Informasi Pada Badan Pusat Statistik. Bandung, Indonesia.
- Stoneburner, G., A. Goguen and Feringa A. (2002). Risk Management Guide for Information Technology System, Recommendation of National Institute of Standards and Technology Special Publication 800-30. USA.