ASSESSMENT IT RISK MANAGEMENT PADA LABORATORIUM TEKNIK KOMPUTER DAN JARINGAN SMK NEGERI 3 OKU

TESIS

Oleh

ARLIN NURLIYANI

Enterprise IT Infrastructure

162420001

PROGRAM STUDI TEKNIK INFORMATIKA – S2

PROGRAM PASCASARJANA

UNIVERSITAS BINA DARMA

PALEMBANG

2019

ASSESSMENT IT RISK MANAGEMENT PADA LABORATORIUM TEKNIK KOMPUTER DAN JARINGAN SMK NEGERI 3 OKU

Tesis ini diajukan sebagai salah satu syarat
untuk memperoleh gelar

MAGISTER KOMPUTER

Oleh

ARLIN NURLIYANI

Enterprise IT Infrastructure

162420001

PROGRAM STUDI TEKNIK INFORMATIKA – S2

PROGRAM PASCASARJANA

UNIVERSITAS BINA DARMA

PALEMBANG

2019

Halaman Pengesahan Penguji Tesis

Judul Tesis : ***ASSESSMENT IT RISK MANAGEMENT*** **PADA LABORATORIUM TEKNIK KOMPUTER DAN JARINGAN SMK NEGERI 3 OKU**

Oleh **ARLIN NURLIYANI** NIM 162420001, Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika – S2 konsentrasi ENTERPRISE IT INFRASTRUCTURE, Program Pascasarjana Universitas Bina Darma pada tanggal 27 Februari 2019 dan telah dinyatakan **LULUS**.

Palembang, 27 Februari 2019
Mengetahui,
Program Studi Teknik Informatika – S2
Universitas Bina Darma
Direktur

.....
Dr. Ir. Hj. Hasmawaty AR, M.M., M.T

Tim Penguji :

Penguji I,

.....
Dedy Syamsuar, P.hD.

Penguji II,

.....
A.Haidar Mirza, S.T., M.Kom.

Penguji III,

.....
Dr.Widya Cholil, S.Kom., M.IT.

Penguji IV,

.....
Dr. Edi Surya Negara, M.Kom

Halaman Pengesahan Pembimbing Tesis

Judul : ***ASSESSMENT IT RISK MANAGEMENT*** **PADA LABORATORIUM TEKNIK KOMPUTER DAN JARINGAN SMK NEGERI 3 OKU**

Oleh **ARLIN NURLIYANI** NIM 162420001, Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika – S2 konsentrasi Enterprise IT Infrastructure, Program Pascasarjana Universitas Bina Darma pada tanggal 27 Februari 2019 dan telah dinyatakan **LULUS**.

Mengetahui,
Program Studi Teknik Informatika-S2
Universitas Bina Darma
Ketua,

.....
Darius Antoni, S.Kom., M.M., Ph.D.

Tim Pembimbing
Pembimbing I,

.....
DedySyamsuar., Ph.D.

Pembimbing II,

.....
A.HaidarMirza, S.T., M.Kom.

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : ARLIN NURLIYANI
NIM : 162420001

Dengan ini menyatakan bahwa:

1. Karya tulis Saya Tesis ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik Magister di Universitas Bina Darma;
2. Karya tulis ini murni gagasan, rumusan dan penelitian Saya sendiri dengan arahan tim pembimbing;
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar pustaka;
4. Karena yakin dengan keasliaan karya tulis ini, Saya menyatakan bersedia Tesis yang Saya hasilkan di unggah ke internet;
5. Surat Pernyataan ini Saya tulis dengan sungguh-sungguh dan apabila terdapat penyimpangan atau ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima sanksi dengan aturan yang berlaku di perguruan tinggi ini.

Demikian Surat Pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, Februari 2019
Yang Membuat Pernyataan,

ARLIN NURLIYANI
NIM: 162420001

ABSTRAK

Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU 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 SMK Negeri 3 OKU. Penelitian ini dilakukan untuk mengetahui risiko apa saja yang terjadi.Dan penelitian ini, akandigunakan metode *FrameworkNIST SP 800-30r1*untukmendapatkannilai risiko diLaboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. 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 tahapanpenilaian, 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 SMK Negeri 3 OKU . Risiko yang muncul berdampak serius pada aset, organisasi dan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Kata Kunci :*Assessment IT Risk Management,* Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, *Framework NIST SP 800-30r1,* Analisis Kualitatif, Risiko

ABSTRACT

The Laboratotium Teknik Komputer dan Jaringan SMK Negeri 3 OKU *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 SMK Negeri 3 OKU. 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 in The* Laboratotium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. *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* Laboratotium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. *Emerging risks have a serious impact on assets, organization and activities in The* Laboratotium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Keywords : *Assessment IT Risk Management, Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, NIST SP 800-30r1 Framework, Qualitative Analysis, Risk*

DIPERSEMBAHKAN KEPADA

- *Almarhumah Mbah Uti (Mbah Ngadimah) yang selalu percaya bahwa bekal terbaik untuk menjalani hidup adalah ilmu.*
- *Papa (Bapak Amirudin Wardi) dan Mama (Ibu Amil Makiyah) yang telah memberikan dukungan dalam mencari ilmu yang merupakan madrasah pertama dalam mendapatkan ilmu.*
- *Anak (Uwo Nuur Phathiyyah Aisyah Rahmi dan Adik Nayra Phathimah Almeerah Rahmi) yang menjadi pendorong agar dapat terus belajar dan dapat menjadi teladan bagi mereka dalam menjalankan kehidupan dan masa depan.*
- *Suami (A' Hendri Rustandi), Adik (Ardo Okilanda, M.Pd., Wuri Syaputri, M.Pd, Ario Aklando(Alm), dan Aryu Mulya Sari) dan Keluarga besar yang selalu mendukung setiap keputusan yang akan dilaksanakan.*
- *Dan para guru mulai dari TK sampai Pascasarjana yang telah memberikan ilmu sebagai bekal untuk menjalani kehidupan dan masa depan.*

KATA PENGANTAR

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

Puji syukur kehadirat Allah SWT karena berkat rahmat dan karunia-Nya jualah, hasil tesis ini dapat diselesaikan guna memenuhi salah satu syarat untuk diteruskan menjadi tesis sebagai proses akhir dalam menyelesaikan pendidikan dibangku kuliah.

Proposal ini disusun sebagai salah satu syarat untuk untuk memperolehgelar Magister Komputer pada Universitas Bina Darma Palembang.Dalam penulisan hasil tesis ini, tentunya masih jauh dari sempurna. Hal ini dikarenakan keterbatasnya pengetahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan hasil tesis ini diharapkan adanya saran dan kritik yang diberikan bersifat membangun.

Pada kesempatan yang baik ini, tak lupa penulis menghaturkan terima kasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasehat dan pemikiran dalam penulisan hasil tesis ini, terutama kepada :

1. Prof. Ir. H. BochariRahman, M.Sc. selakuRektorUniversitasBinaDarma.
2. Dr. Ir. Hj. Hasmawaty AR., M.M., M.T.selakuDirektur Pascasarjana Universitas Bina Darma.
3. Darius Antoni, S.Kom., M.M., PhD., selakuKetua Program StudiTeknik Informatika
4. DedySyamsuar, Ph.D., selakuPembimbing I yang telah memberikan bimbingan danarahandalampenulisan hasil tesisini.
5. Muhammad. HaidarMirza, S.T., M.Kom, selakuPembimbingII yang telahmemberikanbimbingan dan arahan dalampenulisanhasil tesisini.
6. PihakSekretariatPascasarjanaUniversitasBinaDarma Palembang yang telahmemberikanbimbinganpelayanandenganbaik.
7. Staf dan dewan guru SMK Negeri 3 OKU yang telah membantu memberikan dukungan, bimbingan dan partisipasi dalam penentuan hasil tesis ini.

Palembang,Februari 2019
Penulis

ArlinNurliyani
162420001

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL


Universitas
Bina
Darma

BAB I

PENDAHULUAN

1.1 Latar Belakang

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 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.

SMK Negeri 3 OKU merupakan sekolah kejuruan yang berbasis bidang keahlian teknologi. Didalam lingkungan SMK Negeri 3 OKU memiliki beberapa bidang keahlian antara lain Teknik Kontruksi BatuBeton (TKBB), Teknik Gambar Bangunan (TGB), Teknik Pengelasan (TPL), Teknik Instalasi Tenaga Listrik (TITL), Teknik Kendaraan Ringan (TKR), Teknik Pemesian (TPM), Teknik Survey Pemetaan (TSP), danTeknik Komputer dan Jaringan (TKJ). Sebagai sekolah yang memiliki basis teknologi, SMK Negeri 3 OKU di wajibkan memiliki fasilitas pendukung kegiatan belajar mengajar bagi semua bidang keahlian dan terkhusus TKJ.

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. Fasilitas ini sudah cukup untuk membuka jurusan TKJ dikarenakan kurikulumnya hanya seputar perakitan komputer. Seiring perkembangannya sebagai penunjang belajar mengajar untuk siswa TKJ, SMK Negeri 3 OKU memberikan fasilitas tiga bangunan laboratorium TKJ. Ketiga laboratorium jurusan TKJ memiliki fungsi masing-masing yaitu laboratorium TKJ 1 sebagai Laboratorium khusus kegiatan perakitan komputer, laboratorium TKJ 2 merupakan laboratorium kegiatan multimedia, dan laboratorium TKJ 3 dikhususkan untuk pengembangan jaringan.

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*.

Selain itu juga, yang membuat kepala program studi dan ketua bengkel TKJ bertugas sangat berat. Sering terjadi kehilangan di Laboratorium TKJ. Ini di sebabkan kurangnya pengetahuan manajemen laboratorium yang dimiliki kepala

bengkel dikarenakan tidak pernah diadakannya pelatihan manajemen laboratorium. Sehingga untuk memanajemen seluruh perlengkapan komputer di laboratorium masih belum bisa dikatakan layak. Banyak sekali barang bekas komputer yang tidak di ketahui kelayakannya, apa masih bisa dipakai atau tidak. Karena yang paling banyak bermasalah pada laboratorium TKJ SMKNegeri 3 OKU adalah perangkat komputer dan jaringan yang sangat mudah rusak dan tidak stabil yang didukung oleh usia perangkat yang sudah cukup tua. Untuk risiko yang terjadi di laboratorium TKJ juga sulit di perkirakan oleh kepala bengkel di karenakan tidak pernah melakukan penilaian risiko pada laboratorium TKJ.

Begitu banyak risiko-risiko yang bermunculan di 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 dikelolah dengan baik agar tidak berdampak buruk bagi kegiatan yang akan dilaksanakan di Laboratorium TKJ SMK Negeri 3 OKU.

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. Karena menurut penulis *FrameworkNIST SP 800-30r1* merupakan kerangka kerja yang

simpel yang dapat digunakan untuk melakukan penilaian risiko. *FrameworkNIST SP 800-30r1* merupakan kerangka kerja yang di keluarkan oleh *National Institute Standard and Technology (NIST)* pada tahun 2012.

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang dari penelitian ini maka dapat di identifikasikan permasalahan sebagai berikut :

1. Usia perangkat komputer yang sudah cukup tua dan sudah banyak yang rusak
2. Sering terjadinya kehilangan pada perangkat komputer dan jaringan di Laboratorium TKJ SMK Negeri 3 OKU.
3. Belum adanya sumber daya manusia yang mengerti tentang manajemen laboratorium TKJ.
4. Belum pernah di lakukan penilaian risiko pada Laboratorium TKJ SMK Negeri 3 OKU.

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini agar terarah dan tidak terlalu meluas, maka batasan masalah pada penelitian ini adalah membahas mengenai cara melakukan *Assessment* risiko pada laboratorium TKJ SMK Negeri 3 OKU dengan menganalisis risiko-risiko pada perangkat dan peralatan jaringan komputer serta kegiatan yang ada di lingkungan laboratorium TKJ SMK Negeri 3 OKU.

1.4 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka dapat dirumuskan permasalahannya adalah “Risiko-risiko apakah yang terdapat pada Laboratorium

Teknik Komputer dan Jaringan SMK Negeri 3 OKUsaat dilakukan *assessment IT risk management* ?.”

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalahsebagaiberikut:

1. Mengetahui penyebab kerusakan dan risiko yang terjadi pada peralatan dan perangkat jaringan di laboratorium TKJ SMK Negeri 3 OKU.
2. Menanggulangi dan meminimalisir risiko yang terjadi pada perangkat dan peralatan jaringan komputer di laboratorium TKJ SMK Negeri 3 OKU jika terjadi kerusakan.
3. Mengetahui tingkat risiko yang mempengaruhi jaringan komputer di laboratorium TKJ SMK Negeri 3 OKU.
4. Melindungi aset yang terdapat di laboratorium TKJ SMK Negeri 3 OKU.
5. Mengetahui pengaruh yang terjadi pada peserta didik dan guru yang beraktifitas di laboratorium TKJ SMK Negeri 3 OKU.

1.6 Manfaat Penelitian

Adapun manfaat daripenelitian ini antara lain :

1. Agar dapat dengan mudah mengetahui penyebab masalah yang terjadi pada perangkat komputer dan jaringan di laboratorium TKJ SMK Negeri 3 OKU.
2. Agar menjadi masukkan bagi para guru dan siswa yang menggunakan laboratorium TKJ SMK Negeri 3 OKU untuk dapat mengantisipasi dan meminimalisir masalah kerusakan perangkat komputer dan

jaringan serta dapat menanggulangi dengan mudah perangkat dan peralatan jaringan komputer bila terjadi rusak/bermasalah.

3. Dapat memberi perlindungan kepada aset yang terdapat di laboratorium TKJ SMK Negeri 3 OKU.
4. Agar dapat menjadi referensi apabila ingin membuat dokumen manajemen risiko untuk laboratorium TKJ SMK Negeri 3 OKU.
5. Memberi pelajaran dan pengajaran tentang manajemen risiko di laboratorium TKJ SMK Negeri 3 OKU.

1.7 Ruang Lingkup Penelitian

Dalam penulisan tesis ini, penulis akan membatasi ruang lingkup penelitian dengan menitik beratkan permasalahan pada “Kegiatan yang terjadi di lingkungan laboratorium TKJ SMK Negeri 3 OKU” .

1.8 Susunan Dan Struktur Penelitian

Susunan dan struktur proposal tesis ini maksudnya agar dapat memberikan garis besarnya secara jelas sehingga terlihat hubungan antara bab yang satu dengan bab yang lainnya. Susunan dan struktur proposal tesis dijabarkan di bawah ini sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini akan dibahas mengenai latar belakang, identifikasi masalah, batasan masalah, rumusan masalah, tujuan, manfaat penelitian, ruang lingkup penelitian, serta susunan dan struktur penelitian yang merupakan landasan dasar dilakukan penelitian.

BAB II KAJIAN PUSTAKA

Bab ini memberikan pembahasan tentang kajian pustaka, penelitian terdahulu, dan kerangka berfikir yang akan memberikan gambaran dan referensi awal dari penelitian yang dilaksanakan.

BAB III METODOLOGI PENELITIAN

Pada bab ini akan membahas tentang desain dan jadwal penelitian, data penelitian, metode penelitian, sumber data, dan metode pengumpulan data yang merupakan tahapan yang akan dilakukan dalam penelitian.

BAB IV GAMBARAN UMUM OBJEK PENELITIAN

Dimana bab ini membahas tentang objek pada penelitian seperti sejarah SMK Negeri 3 OKU, profil SMK Negeri 3 OKU, struktur organisasi, sejarah dan profil jurusan Teknik Komputer dan Jaringan, peralatan dan perlengkapan yang berkaitan tentang apa yang akan ditelitih.

BAB V PEMBAHASAN

Dalam bab ini akan dibahas tentang hasil dari penelitian yang dilaksanakan, dari bab ini akan didapat hasil dari setiap tahapan yang telah dilakukan peneliti melalui pendekatan kepada responden yang ada.

BAB VI KESIMPULAN DAN SARAN

Bab ini memberikan kesimpulan dari semua kegiatan penelitian yang telah dilakukan dan selain itu untuk memperbaiki permasalahan yang terjadi pada penelitian, maka di buat juga saran pada bab ini.


Universitas
Bina
Darma

BAB II

KAJIAN PUSTAKA

2.1 Sistem Keamanan Jaringan Komputer

2.1.1 Jaringan komputer

Menurut Edy Victor Haryanto(2012 : 12) 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.

Menurut Wagito (2007 :11) 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*. Jaringan komputer memiliki 3 tipe berdasarkan luas cakupan area yaitu :

1. LAN (*Local Area Network*) merupakan suatu jaringan yang terbatas pada daerah yang relatif kecil seperti ruangan ataupun gedung.
2. MAN (*Metropolitan Area Network*) yaitu meliputi area geografi yang lebih luas seperti antar suatu kota.

3. WAN (*Wide Area Network*) yaitu meliputi area geografi yang lebih luas lagi seperti antar Negara.

2.1.2 Keamanan Jaringan Komputer

Keamanan jaringan komputer merupakan sistem untuk melindungi jaringan komputer terhadap serangan serta ancaman yang tidak dikehendaki. Tujuannya untuk mengantisipasi resiko jaringan komputer yang dapat berbentuk ancaman fisik maupun logik. Ancaman fisik merupakan kegiatan yang merusak bagian fisik komputer yaitu hardware komputer sehingga ancaman logik seperti pencurian data.

2.2 Manajemen Risiko

2.2.1 Definisi Risiko

Menurut Sulad Sri Hardanto (2006 :1)definisi risiko yaitu sebagai peluang terjadinya *bad outcome* (hasil yang buruk), dan besarnya peluang diestimasikan. Risiko sebagai peluang terjadinya hasil yang tidak diinginkan dan risiko hanya terkait dengan situasi yang memungkinkan munculnya hasil negatif serta berkaitan dengan kemampuan memperkirakan terjadinya hasil negatif tadi.Dapat disimpulkan bahwa risiko selalu dihubungkan dengan kemungkinan terjadimya sesuatu yang merugikan yang tidak diduga/ tidak diinginkan.

Untuk memudahkan pengenalan risiko, perlu dilakukan klasifikasi sehingga mengenal karakter dari risiko. Risiko dapat dikategorikan pada risiko murni dan risiko spekulatif. Cara lain mengklasifikasi risiko yaitu mengategorikan ke dalam risiko sistematik dan risiko spesifik.

a. Risiko Murni yaitu risiko yang bisa mengakibatkan kerugian pada perusahaan, tetapi tidak ada kemungkinan menguntungkan. Perusahaan menghadapi berbagai hal dalam risiko ini. Misalnya, kekayaan mesin yang menanggung risiko murni. Ada kemungkinan mesin mengalami kerusakan, mulai dari kerusakan kecil sampai besar. Tetapi, tidak mungkin keadaan sebaliknya dapat terjadi. Kekayaan berupa gedung juga ada kemungkinan mengalami kerugian berupa kerusakan atau kehancuran.
b. Risiko Spekulatif merupakan risiko yang dapat mengakibatkan dua kemungkinan, merugikan atau menguntungkan perusahaan.
c. Risiko Sistematik disebut resiko yang tidak dapat didiversifikasi . Ciri dari risiko sistematik merupakan tidak dapat dihilangkan atau dikurangi dengan cara penggabungan berbagai resiko.
d. Risiko Spesifik atau risiko yang dapat didiversifikasi dapat dihilangkan melalui proses penggabungan (pooling). Konsep risiko sistematik dan spesifik sangat berguna dalam menangani risiko keuangan. Banyak risiko yang berkaitan dengan keuangan perusahaan dapat ditekan dengan menerapkan diversifikasi.

2.2.2 Definisi Manajemen Risiko

Menurut *National Institute Standard and Technology (NIST; 2012)* 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. Manajemen risiko juga dapat dijabarkan pengorganisasian struktural metodologi dalam pengelolaan ketidakpastian ancaman dalam suatu rangkaian aktifitas sehingga dapat mengendalikan risiko. Manajemen risiko suatu sistem pengawasan risiko dan perlindungan harta benda, hak milik serta keuntungan badan usaha atau perorangan atas kemungkinan timbulnya kerugian karena adanya suatu risiko. Adapun tahapan proses pengelolaan risiko antara lain :

a. Identifikasi risiko

   Pada tahap ini pihak manajemen perusahaan melakukan tindakan berupa mengidentifikasi setiap bentuk risiko yang dialami perusahaan, termasuk bentuk-bentuk risiko yang mungkin akan dialami oleh perusahaan. Identifikasi ini dilakukan dengan cara melihat potensi-potensi risiko yang sudah terlihat serta yang akan terlihat.

b. Mengidentifikasi bentuk-bentuk risiko

   Pada tahap ini diharapkan pihak manajemen perusahaan telah mampu menemukan bentuk dan format risiko yang dimaksud. Bentuk-bentuk risiko yang diidentifikasi di sini telah mampu dijelaskan secara detail timbulnya risiko tersebut. Pada tahap ini pihak manajemen perusahaan juga sudah mulai mengumpulkan

serta menerima berbagai data-data baik bersifat kualitatif serta kuantitatif.

c. Menempatkan ukuran-ukuran risiko

Pada tahap ini pihak manajemen perusahaan sudah menempatkan ukuran atau skala yang dipakai, termasuk rancangan model metodologi penelitian yang akan digunakan. Data-data yang masuk juga sudah dapat diterima, baik yang berbentuk kualitatif dan kuantitatif serta pemilahan data dilakukan berdasarkan pendekatan metodologi yang digunakan. Dengan kepemilikan rancangan metodologi penelitian yang ada diharapkan pihak manajemen perusahaan telah memiliki fondasi kuat guna melakukan pengolahan data.

d. Menempatkan alternatif-alternatif

Pada tahap ini pihak manajemen perusahaan telah melakukan pengolahan data. Hasil pengolahan kemudian dijabarkan dalam bentuk kualitatif dan kuantitatif beserta akibat-akibat atau pengaruh-pengaruh yang akan timbul jika keputusan- keputusan tersebut diambil. Berbagai bentuk penjabaran yang dikemukakan tersebut dipilah serta ditempatkan sebagai alternatif-alternatif keputusan.

e. Menganalisis setiap alternatif

Pada tahap ini dimana setiap alternatif yang ada selanjutnya dianalisis dan dikemukakan berbagai sudut pandang serta efek-

efek yang mungkin timbul. Dampak yang mungkin timbul baik secara jangka pendek serta jangka panjang dipaparkan secara komprehensif serta sistematis, dengan tujuan mampu diperoleh suatu gambaran secara jelas dan tegas. Kejelasan serta ketegasan dangat penting guna membantu pengambilan keputusan secara tepat.

f. Memutuskan suatu alternatif

Pada tahap ini setelah berbagai alternatif dipaparkan serta dijelaskan baik dalam bentuk lisan dan tulisan oleh para manajemen perusahaan maka diharapkan pihak manajer perusahaan sudah memiliki pemahaman secara khusus serta mendalam. Pemilihan satu alternatif dari berbagai alternatif yang ditawarkan artinya mengambil alternatif yang terbaik dari berbagai alternatif yang ditawarkan termasuk dengan menolak berbagai alternatif lainnya. Dengan pemilihan satu alternatif sebagai solusi dalam menyelesaikan berbagai permasalahan diharapkan pihak manajer perusahaan sudah memiliki fondasi kuat dalam menugaskan pihak manajemen perusahaan untuk bekerja berdasarkan konsep dan koridor yang ada.

g. Melaksanakan alternatif yang dipilih

Pada tahap ini setelah alternatif dipilih serta ditegaskan serta dibentuk tim untuk melaksanakan ini, maka artinya manajer perusahaan sudah mengeluarkan Surat Keputusan (SK) yang

dilengkapi dengan rincian biaya. Rincian biaya yang dialokasikan tersebut telah disetuju oleh bagian keuangan serta otoritas pengambil penting lainnya.

h. Mengontrol alternatif yang dipilih tersebut

Pada tahap ini alternatif yang dipilih telah dilaksanakan oleh pihak tim manajemen beserta para manajer perusahaan. Tugas utama manajer perusahaan merupakan melakukan kontrol yang maksimal guna menghindari timbulnya berbagai risiko yang tidak diinginkan.

i. Mengevaluasi jalannya alternatif yang dipilih

Pada tahap ini setelah alternatif dilaksanakan dan kontrol dilakukan maka selanjutnya pihak tim manajemen secara sistematis melaporkan kepada pihak manajer perusahaan. Pelaporan tersebut berbentuk data-data yang bersifat fundamental serta teknikal serta dengan tidak mengesampingkan informasi yang bersifat lisan. Tujuan melakukan evaluasi dari alternatif yang dipilih tersebut merupakan bertujuan agar pekerjaan tersebut dapat terus dilaksanakan sesuai dengan yang direncanakan.

2.3 *NIST SP 800*

NIST (*National Institute of Standard and Technology*) merupakan organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standar serta teknologi untuk meningkatkan fasilitas

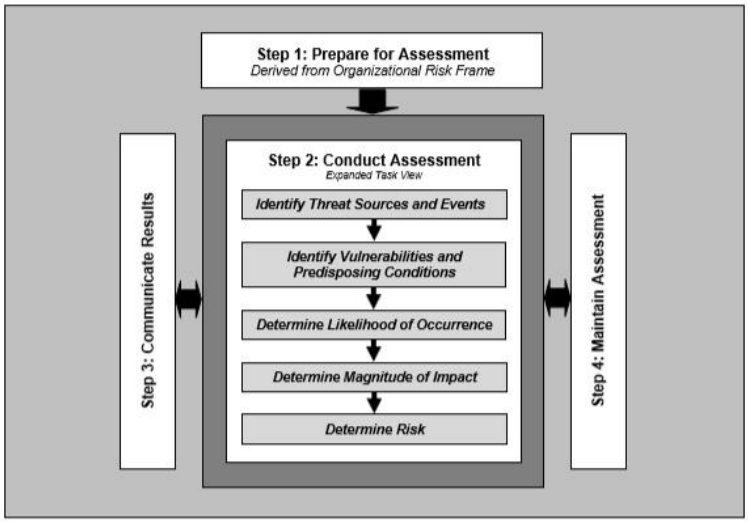
dan kualitas kehidupan. Kegiatan utama merupakan meneliti berbagai ilmu untuk mempromosikan dan meningkatkan infrastruktur teknologi. *NIST* mengeluarkan rekomendasi melalui publikasi khusus 800 tentang Risk Management Guide for Information Technology System.Terdapat tiga proses dalam manajemen risiko yang dikeluarkan oleh *NIST* yaitu *risk identification, risk mitigation dan risk evaluation. NIST SP 800 Framework* merupakan kerangka kerja pendukung dalam pembuatan dokumen manajemen risiko.*NIST SP 800* memiliki beberapa versi pengembangan antara lain *NIST SP 800-30, NIST SP 800-30r1* serta *NIST SP 800-39.*

2.3.1 *NIST SP 800-30r1*

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*. Penilaian risiko, yang dilakukan di ketiga tingkatan dalam hirarki manajemen risiko, merupakan bagian dari keseluruhan proses manajemen risiko - yang memberikan para pemimpin senior / eksekutif dengan informasi yang diperlukan untuk menentukan tindakan yang tepat dalam menanggapi risiko yang teridentifikasi. Secara khusus, dokumen ini memberikan panduan untuk melaksanakan masing-masing langkah dalam proses penilaian risiko (yaitu, mempersiapkan penilaian, melakukan penilaian, mengkomunikasikan hasil penilaian, dan mempertahankan penilaian) dan bagaimana penilaian risiko dan organisasi lainnya proses manajemen risiko saling melengkapi dan saling

menginformasikan. *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 2.1 dapat dilihat tahapan – tahapan *Risk Assessment Activities* dalam melakukan mnajemen risiko dengan menggunakan *NIST SP 800-30r1 Framework.* Adapun sedikit penjelasan dari tahapan-tahapan *Risk Assessment Activities* dari kerangka kerja *NIST SP800-30r1* antara lain merupakan sebagai berikut :



Gambar 2.1 *NIST SP 800-30r1 Framework*

Step 1 Prepare for Assessment

Langkah pertama dalam proses penilaian risiko merupakan mempersiapkan untuk penilaian. Tujuan dari ini langkah ini merupakan untuk menetapkan konteks untuk penilaian risiko. Konteks ini didirikan

dan diinformasikan oleh hasil dari langkah framing risiko dari proses manajemen risiko. framing risiko mengidentifikasi, untuk Misalnya, informasi organisasi mengenai kebijakan dan persyaratan untuk melakukan resiko penilaian, metodologi penilaian khusus untuk dipekerjakan, prosedur untuk memilih risiko faktor yang harus dipertimbangkan, ruang lingkup penilaian, kekakuan dari analisis, tingkat formalitas, dan persyaratan yang memfasilitasi penentuan risiko yang konsisten dan berulang di seluruh organisasi. Organisasi menggunakan strategi manajemen risiko sejauh praktis untuk memperoleh informasi untuk mempersiapkan diri untuk penilaian risiko. Mempersiapkan penilaian risiko meliputi tugas-tugas sebagai berikut :

- Mengidentifikasi tujuan dari penilaian;
- Mengidentifikasi lingkup penilaian;
- Mengidentifikasi asumsi dan kendala terkait dengan penilaian;
- Mengidentifikasi sumber-sumber informasi yang akan digunakan sebagai masukan untuk penilaian; dan
- Mengidentifikasi model risiko dan pendekatan analitik (yaitu, penilaian dan analisis pendekatan) ke pekerjaan selama pengkajian

Step 2 Conduct Assessment

Langkah kedua dalam proses penilaian risiko merupakan untuk melakukan penilaian. Tujuan dari ini Langkah merupakan untuk menghasilkan daftar risiko keamanan informasi yang dapat diprioritaskan oleh tingkat risiko dan digunakan untuk menginformasikan keputusan

respon risiko. Untuk mencapai tujuan ini, organisasi menganalisis ancaman dan kerentanan, dampak dan kemungkinan, dan ketidakpastian yang terkait dengan penilaian risiko proses. Langkah ini juga mencakup pengumpulan informasi penting sebagai bagian dari tugas masing-masing dan dilakukan sesuai dengan konteks penilaian didirikan di Siapkan langkah risiko proses penilaian. Harapan untuk penilaian risiko merupakan untuk cukup menutupi seluruh ancaman ruang sesuai dengan definisi khusus, bimbingan, dan arahan yang didirikan selama mempersiapkan langkah. Namun, dalam praktiknya, cakupan yang memadai dalam sumber daya yang tersedia dapat mendikte generalisasi sumber ancaman, peristiwa ancaman, dan kerentanan untuk memastikan cakupan penuh dan menilai spesifik, sumber rinci, peristiwa, dan kerentanan hanya sebagai diperlukan untuk mencapai risiko tujuan penilaian. Melakukan penilaian risiko termasuk berikut tugas-tugas khusus :

- Mengidentifikasi sumber-sumber ancaman yang relevan dengan organisasi;
- Mengidentifikasi peristiwa ancaman yang dapat dihasilkan oleh sumber-sumber;
- Identifikasi kerentanan dalam organisasi yang dapat dimanfaatkan oleh ancaman sumber melalui peristiwa ancaman spesifik dan kondisi predisposisi yang dapat mempengaruhi sukses eksploitasi;

- Menentukan kemungkinan bahwa sumber ancaman diidentifikasi akan memulai acara ancaman khusus dan kemungkinan bahwa peristiwa ancaman akan berhasil;
- Menentukan dampak negatif terhadap operasi organisasi serta aset, individu, lainnya organisasi, serta bangsa yang dihasilkan dari eksploitasi kerentanan dengan ancaman sumber (melalui peristiwa ancaman khusus); dan
- Menentukan risiko keamanan informasi sebagai kombinasi dari kemungkinan eksploitasi ancaman kerentanan serta dampak dari eksploitasi tersebut, termasuk ketidakpastian terkait dengan penentuan risiko

Tugas-tugas khusus disajikan secara berurutan untuk kejelasan. Namun, dalam praktiknya, beberapa iterasi antara tugas-tugas merupakan penting dan diharapkan. Tergantung pada tujuan risikon penilaian, organisasi mungkin menemukan penataan kembali tugas-tugas yang menguntungkan. Apapun penyesuaianorganisasi membuat untuk tugas-tugas yang dijelaskan di bawah, penilaian risiko harus memenuhi tujuan menyatakan, lingkup, asumsi, serta kendala yang ditetapkan oleh organisasi memulai penilaian. Untuk membantu organisasi dalam melaksanakan tugas individu dalam proses penilaian risiko, satu set template disediakan dalam Lampiran D melalui I. lampiran ini memberikan informasi yang berguna untuk organisasi dalam menilai risiko dan juga dapat digunakan untuk merekam hasil penilaian yang

dihasilkan selama perhitungan penting dan analisis. Template merupakan teladan serta dapat disesuaikan dengan organisasi sesuai dengan persyaratan misi / bisnis yang spesifik organisasi. Menggunakan template tidak diperlukan untuk melakukan npenilaian risiko.

Step 3 Communicate Results

Langkah ketiga dalam proses penilaian risiko merupakan untuk mengkomunikasikan hasil penilaian dan berbagirisiko yang berhubungan dengan informasi. Tujuan dari langkah ini merupakan untuk memastikan bahwa para pengambil keputusan di seluruh organisasi memiliki informasi terkait risiko yang tepat dibutuhkan untuk menginformasikan serta risiko panduan keputusan. Berkomunikasi dan berbagi informasi terdiri dari tugas-tugas tertentu sebagai berikut :

- Mengkomunikasikan hasil penilaian risiko; dan
- Berbagi informasi yang dikembangkan dalam pelaksanaan penilaian risiko, untuk mendukung risiko lain kegiatan manajemen.

Step 4 Maintain Assessment

Langkah keempat dalam proses penilaian risiko merupakan untuk mempertahankan penilaian. Tujuan dari ini Langkah ini untuk menjaga saat ini, pengetahuan spesifik dari organisasi risiko dikenakan. Hasil risiko penilaian menginformasikan keputusan manajemen risiko dan respon risiko panduan. Untuk mendukung berkelanjutan review keputusan manajemen risiko (misalnya, keputusan akuisisi, keputusan otorisasi untuk sistem informasi dan kontrol umum,

keputusan koneksi), organisasi mempertahankan risiko penilaian untuk menggabungkan perubahan dideteksi melalui pemantauan risiko. Pemantauan Risikomenyediakan organisasi dengan sarana untuk, secara berkelanjutan: (i) menentukan efektivitas daritanggapan risiko; (ii) mengidentifikasi risiko-berdampak perubahan ke sistem informasi organisasi serta lingkungan di mana sistem tersebut beroperasi; dan (iii) memverifikasi kepatuhan. Risiko mempertahankan penilaian meliputi tugas-tugas khusus berikut:

- faktor risiko Memantau diidentifikasi dalam penilaian risiko secara berkelanjutan serta pemahaman perubahan terhadap faktor-faktor tersebut; dan
- Update komponen penilaian risiko yang mencerminkan kegiatan monitoring dilakukan oleh organisasi.

2.4 Sumber Ancaman

Menurut Deris Setiawan (2006 : 5) 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.

Taxonomy Sumber Ancaman Yang Mampu Memulai Peristiwa Ancaman dengan memberikan: (i) deskripsi dari input yang berpotensi bermanfaat ke *sumber ancaman* tugas identifikasi; (ii) taksonomi contoh sumber ancaman berdasarkan jenis, deskripsi, dan faktor risiko (yaitu, karakteristik) yang digunakan untuk menilai kemungkinan dan / atau dampak dari ancaman

tersebutsumber-sumber yang memulai peristiwa ancaman; (iii) seperangkat skala penilaian yang disesuaikan untuk penilaian faktor-faktor risiko tersebut; dan (iv) template untuk meringkas serta mendokumentasikan hasil dari ancaman identifikasi sumber Task 2-1. Taksonomi dan skala penilaian dalam penjelasan ini dapat digunakan oleh organisasi sebagai titik awal dengan penyesuaian yang sesuai untuk menyesuaikan dengan spesifik organisasi kondisi. Tabel 2.7 dan 2.8, output dari Task 2-1, memberikan masukan yang relevan ke tabel risiko di bawah.

Task 2-1 :Identifikasi dan gambarkan sumber-sumber ancaman yang menjadi perhatian, termasuk kemampuan, niat, dan penargetankarakteristik untuk ancaman per*adversary*an dan berbagai efek untuk ancaman non-per*adversary*an. Wacana kali ini menyediakan seperangkat tabel contoh untuk digunakan dalam mengidentifikasi sumber ancaman:

- Tabel 2.1 menyediakan seperangkat input yang patut dicontoh untuk tugas identifikasi sumber ancaman;
- Tabel 2.2 memberikan taksonomi teladan yang dapat digunakan untuk mengidentifikasi dan mengkarakterisasi sumber ancaman;
- Tabel 2.3, 2.4, dan 2.5 memberikan skala penilaian teladan untuk menilai faktor-faktor risiko (yaitu, karakteristik) darisumber ancaman per*adversary*an berkaitan dengan kemampuan, niat, dan penargetan;
- Tabel 2.6 memberikan skala penilaian teladan untuk menilai rentang efek dari peristiwa ancaman yang diprakarsai olehsumber ancaman non-per*adversary*an; dan

- Tabel 2.7 dan 2.8 menyediakan template untuk meringkas dan mendokumentasikan hasil identifikasi sumber ancamandan karakterisasi.

Jika suatu jenis sumber ancaman tertentu berada di luar lingkup penilaian risiko atau tidak relevan dengan organisasi, makainformasi dalam Tables 2.7 dan 2.8 dapat dipotong sesuai. Informasi yang dihasilkan dalam Task 2-1 memberikan ancaman input sumber ke tabel risiko.

Tabel 2.1 Inputs - Anti Identifikasi Suatu Ancaman

Deskripsi	**Disediakan untuk**		
	Tingkat 1	**Tingkat 2**	**Tingkat 3**
Dari Tingkat 1: (Tingkat Organisasi) • Sumber informasi ancaman yang dianggap kredibel (misalnya, open source dan / atau ancaman rahasia laporan, penilaian risiko / ancaman sebelumnya). (**Bagian 3.1** , **Task 1-4**) • Informasi dan panduan sumber ancaman khusus untuk Tingkat 1 (misalnya, ancaman yang terkait dengan organisasi tata kelola, misi inti / fungsi bisnis, manajemen / kebijakan operasional, prosedur, dan struktur, misi eksternal / hubungan bisnis). • Taksonomi sumber ancaman, dianotasikan oleh organisasi, jika perlu. (**Tabel 2.2**) • Karakterisasi sumber ancaman per*adversary*an dan non-per*adversary*an. - Skala penilaian untuk menilai kemampuan, maksud, dan penargetan *adversary*, yang diberi catatan oleh organisasi, jika perlu. (**Tabel 2.3, Tabel 2.4, Tabel 2.5**) - Skala penilaian untuk menilai berbagai efek, yang dijelaskan oleh organisasi, jika diperlukan (**Tabel 2.6**)	Tidak	Ya	Ya *jika tidak disediakan oleh Tingkat 2*

• Sumber ancaman diidentifikasi dalam penilaian risiko sebelumnya, jika sesuai.			
Dari Tingkat 2: (Misi / tingkat proses bisnis) • Informasi dan panduan sumber ancaman khusus untuk Tingkat 2 (misalnya, ancaman yang terkait dengan misi / bisnis proses, segmen EA, infrastruktur umum, layanan dukungan, kontrol umum, dan eksternal ketergantungan). • Misi / karakterisasi spesifik proses bisnis dari ancaman per*adversary*an dan non-per*adversary*an sumber.	Ya Melalui RAR	Ya Melalui Teman berbagi	Ya
Dari Tingkat 3: (Tingkat sistem informasi) • Informasi dan panduan sumber ancaman khusus untuk Tingkat 3 (misalnya, ancaman yang terkait dengan informasi sistem, teknologi informasi, komponen sistem informasi, aplikasi, jaringan, lingkungan operasi). • Karakteristik khusus sistem informasi dari sumber ancaman per*adversary*an dan non-per*adversary*an	Ya Melalui RAR	Ya Melalui RAR	Ya Melalui Teman berbagi

TABEL 2.2 Taxonomi Sumber Ancaman

Jenis Sumber Ancaman	Deskripsi	Karakteristik
ADVERSARIAL • Individu - Outsider - Orang dalam - Orang Asing Tepercaya - Orang Istimewa Istimewa • Grup - AD hoc - Mapan • Organisasi - Pesaing - Pemasok - Mitra	Individu, kelompok, organisasi, atau negara yang berusaha mengeksploitasi ketergantungan organisasi pada dunia maya sumber daya (yaitu informasi dalam bentuk elektronik, informasi dan teknologi komunikasi, dan kemampuan komunikasi dan penanganan informasi disediakan oleh	Kemampuan, Niat, Penargetan

- Pelanggan • Negara bangsa	teknologi tersebut).	
KEBETULAN • Pengguna • Pengguna / Administrator Istimewa	Tindakan keliru yang dilakukan oleh individu dalam perjalanan melaksanakan tanggung jawab sehari-hari mereka.	Berbagai efek
STRUKTURAL • Peralatan Teknologi Informasi (TI) - Penyimpanan - Memproses - Komunikasi - Tampilan - Sensor - Kontroler • Pengendalian Lingkungan - Kontrol Suhu / Kelembaban - Sumber Daya listrik • Perangkat Lunak - Sistem operasi - Jaringan - Aplikasi General-Purpose - Aplikasi Khusus Misi	Kegagalan peralatan, kontrol lingkungan, atau perangkat lunak karena penuaan, penipisan sumber daya, atau lainnya keadaan yang melebihi perkiraan operasi parameter.	Berbagai efek
LINGKUNGAN • Bencana alam atau buatan manusia - Api - Banjir / Tsunami - Angin badai / Tornado - Hurricane - Gempa bumi - Pemboman - Diserbu • Peristiwa Alam yang Tidak Biasa (misalnya, bintik matahari)	Bencana alam dan kegagalan infrastruktur penting yang mana organisasi bergantung, tetapi yang berada di luar kendali organisasi. Catatan: Bencana alam dan buatan manusia juga bisa ditandai dalam hal keparahan dan / atau durasi mereka. Namun, karena sumber ancaman dan peristiwa ancaman sangat	Berbagai efek

• Kegagalan Infrastruktur / Outage - Telekomunikasi - Tenaga listrik	diidentifikasi, tingkat keparahan dan durasi bisa termasuk dalam deskripsi peristiwa ancaman (misalnya, Badai kategori 5 menyebabkan kerusakan luas pada fasilitas perumahan sistem misi-kritis, membuat mereka sistem tidak tersedia selama tiga minggu)	

Tabel 2.3 Skala Penilaian - Karakteristik Kemampuan *Adversary*

Nilai Kualitatif	Nilai Semi-Kuantitatif		Deskripsi
Sangat Tinggi	96-100	10	*Adversary* memiliki tingkat keahlian yang sangat canggih, sumber daya yang baik, dan dapat menghasilkanpeluang untuk mendukung berbagai serangan yangsukses, berkelanjutan, dan terkoordinasi.
Tinggi	80-95	8	*Adversary* memiliki tingkat keahlian yang canggih, dengan sumber daya dan peluang yang signifikanuntuk mendukung beberapa serangan terkoordinasi yang sukses.
Sedang	21-79	5	*Adversary* memiliki sumber daya, keahlian, dan peluang yang moderat untukmendukung banyak keberhasilanserangan.
Rendah	5-20	2	*Adversary* memiliki sumber daya, keahlian, dan peluang terbatas untuk mendukung serangan yang sukses.
Sangat Rendah	0-4	0	*Adversary* memiliki sumber daya, keahlian, dan peluang yang sangat terbatas untuk mendukung keberhasilanmenyerang.

Tabel 2.4: Skala Penilaian - Karakteristik Maksud *Adversary*

Nilai Kualitatif	Nilai Semi-Kuantitatif		Deskripsi
Sangat Tinggi	96-100	10	*Adversary* berusaha melemahkan, merintangi, atau menghancurkan misi inti atau bisnisfungsi, program, atau perusahaan dengan mengeksploitasi kehadiran dalam sistem

			informasi organisasiatau infrastruktur. *Adversary* prihatin tentang mengungkapan tradecraft hanya sejauh ituakan menghalangi kemampuannya untuk menyelesaikan tujuan yang dinyatakan.
Tinggi	80-95	8	*Adversary* berusaha merusak / menghambat aspek kritis dari misi inti atau fungsi bisnis,program, atau perusahaan, atau menempatkan diri dalam posisi untuk melakukannya di masa depan, dengan mempertahankan kehadirandalam sistem informasi atau infrastruktur organisasi. *Adversary* sangat prihatinmeminimalkan deteksi serangan / penyingkapan dari perdagangan, khususnya saatmempersiapkan serangan di masa depan.
Sedang	21-79	5	*Adversary* mencari untuk memperoleh atau memodifikasi informasi kritis atau sensitif tertentu atau mengganggu / mengacaukansumber daya cyber organisasi dengan membangun pijakan dalam informasi organisasisistem atau infrastruktur. *Adversary* khawatir tentang meminimalkan deteksi serangan / pengungkapandari tradecraft, terutama ketika melakukan serangan dalam jangka waktu lama. *Adversary* bersediauntuk menghambat aspek misi organisasi / fungsi bisnis untuk mencapai tujuan ini.
Rendah	5-20	2	*Adversary* secara aktif mencari untuk mendapatkan informasi penting atau sensitif atau untuk merebut / mengganggusumber daya cyber organisasi, danmelakukannya tanpa khawatir tentang deteksi serangan / pengungkapantradship.
Sangat Rendah	0-4	0	*Adversary* berusaha merampas, mengganggu, atau merusak sumber daya maya organisasi, dan melakukannyatanpa mempedulikan tentang deteksi serangan / pengungkapan dari tradecraft.

Tabel 2.5: Skala Penilaian - Karakteristik Target *Adversary*

Nilai Kualitatif	Nilai Semi-Kuantitatif		Deskripsi
Sangat Tinggi	96-100	10	*Adversary* menganalisis informasi yang diperoleh melalui pengintaian dan serangan

			untuk menargetkan secara terus-menerusorganisasi,perusahaan, program, misi atau fungsi bisnis tertentu, yang berfokus pada spesifikinformasi atau sumber daya bernilai tinggi atau misi-kritis, aliran pasokan, atau fungsi; karyawan tertentuatau posisi; mendukung penyedia / pemasok infrastruktur; atau organisasi mitra.
Tinggi	80-95	8	*Adversary* menganalisis informasi yang diperoleh melalui pengintaian untuk menargetkan secara tetap spesifikorganisasi, perusahaan, program, misi atau fungsi bisnis, dengan fokus pada nilai tinggi tertentu atauinformasi penting misi, sumber daya, aliran pasokan, atau fungsi, dukungankaryawan tertentufungsi-fungsi itu, atau posisi kunci.
Sedang	21-79	5	*Adversary* menganalisis informasi yang tersedia secara publik untuk menargetkan nilai tinggi yang terus-menerus spesifikorganisasi (dan posisi kunci, seperti Chief Information Officer), program, atau informasi.
Rendah	5-20	2	*Adversary* menggunakan informasi publik yang tersedia untuk menargetkan kelas organisasi bernilai tinggi atauinformasi, dan mencari target peluang dalam kelas itu.
Sangat Rendah	0-4	0	*Adversary* mungkin atau mungkin tidak menargetkan organisasi atau kelas organisasi tertentu.

Tabel 2.6 Skala Penilaian –Berbagai Pengaruh untuk sumber ancaman non-per*adversary*an

Nilai Kualitatif	Nilai Semi-Kuantitatif		Deskripsi
Sangat Tinggi	96-100	10	Efek dari kesalahan, kecelakaan, atau tindakan alam **menyapu** , melibatkan hampir semua cybersumber daya dari [Tier 3: system informasi; Tingkat 2: proses misi / bisnis atau

			segmen EA,infrastruktur umum, atau layanan dukungan;Tingkat 1: struktur organisasi / tata kelola].
Tinggi	80-95	8	Efek dari kesalahan, kecelakaan, atau tindakan alam sangat **luas** , melibatkan sebagian besar dunia mayasumber daya dari [Tingkat 3: sistem informasi; Tingkat 2: proses misi / bisnis atau segmen EA,infrastruktur umum, atau layanan dukungan; Tingkat 1: struktur organisasi / tata kelola], termasukbanyak sumber daya penting
Sedang	21-79	5	Efek dari kesalahan, kecelakaan, atau tindakan alam sangat **luas** , melibatkan porsi yang signifikansumber daya maya dari [Tingkat 3: sistem informasi; Tingkat 2: misi / proses bisnis atauSegmen EA, infrastruktur umum, atau layanan dukungan; Tingkat 1: organisasi / pemerintahanstruktur], termasuk beberapa sumber daya penting.
Rendah	5-20	2	Efek dari kesalahan, kecelakaan, atau tindakan alam **terbatas** , yang melibatkan beberapa cybersumber daya dari [Tier 3: sistem informasi; Tingkat 2: proses misi / bisnis atau segmen EA,infrastruktur umum, atau layanan dukungan; Tingkat 1: struktur organisasi / tata kelola], tetapitidak melibatkan sumber daya penting.
Sangat Rendah	0-4	0	Efek dari kesalahan, kecelakaan, atau tindakan alam sangat **minim,** melibatkan beberapa jika ada cybersumber daya dari [Tier 3: sistem informasi; Tingkat 2: proses misi / bisnis atau segmen EA,infrastruktur umum, atau layanan dukungan; Tingkat 1: struktur organisasi / tata kelola], dantidak melibatkan sumber daya penting.

Tabel 2.7 Template - Identifikasi Suatu Ancaman *Adversary*

Identifikasi	**Sumber Ancaman Sumber informasi**	**Di Cakupan**	**Kemampuan**	**Maksud**	**Target**
Organisasi yang ditentukan	Tabel 2.2 dan Tugas 1-4 atau Organisasi yang ditentukan	Ya/Tidak	Tabel 2.3 Atau Organisasi yang ditentukan	Tabel 2.4 Atau Organisasi yang ditentukan	Tabel 2.5 Atau Organisasi yang ditentukan

Tabel 2.8 Template - Identifikasi Suatu Ancaman Non-*Adversary*

Identifikasi	**Sumber Ancaman** **Sumber informasi**	**Di Cakupan**	**Rentang Pengaruh**
Organisasi yang ditentukan	Tabel 2.2 dan Tugas 1-4 atau Organisasi yang ditentukan	Ya/Tidak	Tabel 26 Atau Organisasi yang ditentukan

2.5 Penelitian Terdahulu

Dalam melaksanakan penelitian ini, penulis mengambil beberapa referensi dari penelitian yang telah dilakukan sebelumnya. Dari penelitian-penelitian tersebut penulis dapat mengembangkan penelitian yang sedang dilaksanakan. Berikut ini merupakan daftar penelitian terdahulu yang penulis jadikan bahan referensi pada penelitian ini.

Tabel 2.9 Penelitian Terdahulu

NO	Judul	Penulis	Sumber	Pembahasan	Model	Hasil	Kesimpulan
1	Pengembangan Manajemen Resiko Teknologi Informasi Pada Sistem Penerimaan Peserta Didik Baru (Ppdb *Online*) Kemdikbud menggunakan *Framework NISTSp800-30*	***Imam Masyhuri* Dan *Febriliyan Samopa (2013)***	• Afifa, L. N. (2011). Usulan Panduan Pelaksanaan Manajemen Risiko Tata Kelola TIK Nasional. *Konferensi Teknologi Informasi dan Komunikasi untuk Indonesia* (pp. 368–372). Bandung. • Kemenkominfo. (2011). Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. • Massingham, P.	Pembahasan pada jurnal ini meliputi sistem Penerimaan Peserta Didik Baru (PPDB Online) KEMENDIKBUD. Kemudian pembahasan Analisis Manajemen risiko pada sistem PPDB Online, Identifikasi karakteristik sistem, factor ancaman dan kerentanan, menentukan dampak,	Jurnal ini menggunakan metodologi *FrameworkNIST* SP800-30, melakukan pengumpulan data melalui kajian pustaka, dokumen review,dan teknik wawancara.	Hasil dari penelitian tersebut risiko yang terdapat pada PPDB Online sudah dapat dikelompokkan. Ketika melakukan tahapan penilaian risiko, maka diketahui besarnya risiko yang didapat dari setiap daerah yang menggunakan PPDB Online. Sesudah mendapatkan data risiko pada PPDB Online, maka dapat dibuat strategi mitigasi resiko pada PPDB Online. Data dari hasil penelitian PPDB Online menunjukkan bahwa Kota Semarang memiliki penilaian	• Sistem PPDB Online Kemendikbud merupakan sistem yang sangat kompleks yang melibatkan banyak kabupaten/kota dan dalam hal ini berpotensi besar menimbulkan risiko. • Hasil penelitian mengidentifikasi berdasarkan 2 kelompok yaitu : Risiko berdasarkan tahapan kegiatan & Risiko berrdasarkan factor ancaman • Data yang didapat dari hasil penelitian PPDB Online menunjukkan bahwa Kota Semarang memiliki penilaian resiko tertinggi yaitu Tahap Persiapan : 10.00 Resiko Tinggi (*High Risk*) dan Tahap Pengumuman : 15.00 Resiko Sangat Ekstrim

			(2010). *Knowledge risk management*: a *Framework*. *Journal of Knowledge Management*, *14*(3), 464–485. doi:10.1108/13673271011050166.	kecenderungan, dan tingkatan risiko pada PPDB Online. Selanjutnya Melakukan Mitigasi Risiko pada PPDB		resiko tertinggi yaitu Tahap Persiapan : 10.00 Resiko Tinggi (*High Risk*) dan Tahap Pengumuman : 15.00 Resiko Sangat Ekstrim (*Extreme Risk*). Sedangkan Kota Batam memiliki penilaian resiko terendah, yaitu Tahap Persiapan : 1.67 Hampir tanpa resiko/sepele (*Negligible*) dan Tahap Pengumuman : 3.00 Resiko Rendah (*Low Risk*).	(*Extreme Risk*). Sedangkan Kota Batam memiliki penilaian resiko terendah, yaitu Tahap Persiapan : 1.67 Hampir tanpa resiko/sepele (*Negligible*) dan Tahap Pengumuman : 3.00 Resiko Rendah (*Low Risk*).
2	Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus Di Perpustakaan	**Arif Nurochman (2014)**	• Gibson, Darril. *Managing Risk in Information System*. Sudbury :Jones& Bartlett Learning. 2011. • Muntashir. Analisi	Pembahasan pada jurnal ini meliputi Sistem Informasi yang terdapat di perpustakaan Universitas	Jurnal ini menggunakan metodologi *FrameworkNIST* SP800-30, melakukan pengumpulan	Hasil dari penelitian tersebut pada Sistem Informasi yang terdapat di perpustakaan Universitas Gajah Mada Yogyakarta Risiko teknis terdiri dari	• Proses penilaian risiko mendeskripsikan profil risiko yang mengancam sistem informasi perpustakaan berdasarkan level risiko meliputi jeni s risiko teknis dan risiko manusia.

	Universitas Gajah Mada Yogyakarta)		Webometrics pada perpustakaan Perguruan Tinggi Negeri di Indonesia. Visi Pustaka. Vol 14. No.2. Agustus 2012 • Pinontoan Jimmy H. Manajemen Risiko TI – Konsep-konsep. Majalah PC Media. Oktober 2010	Gajah Mada Yogyakarta, Analisis management risiko, Karakteristik, Identifikasi risiko dan Mitigasi risiko yang terdapat pada Sistem Informasi yang terdapat di perpustakaan Universitas Gajah Mada Yogyakarta.	data melalui kajian pustaka, dokumen review,dan teknik wawancara.	backup server hang dan level risiko tinggi, listrik level risiko tinggi, keamanan sistem dengan level risiko tinggi, password dengan level risiko tinggi, dan otoritas hak akses dengan lvel risiko sedang. Jenis risiko manusia teridentifikasi profil risiko dengan ranking sedang.	• Penilaian risiko hanya berdasarkan kejadian yang bersifat “incidental” yang diantisipasi dengan memaksimalkan peran IT support dan kesadaran dari pustakawan dalam mengantisipasi berbagai ancaman risiko sistem informasi. • Mitigasi risiko pada perpustakaan UGM dilaksanakan dengan cara memindahkan risiko yakni dengan memindahkan server sistem informasi perpustakaan ke PSDI
3	Manajemen Resiko Pada Pengelolaan Data Di Bagian Pengolahan Data PT.	**Aulia Febriyanti Dan Bekti Cahyo Hidayanto (2012)**	• *Hisham, M. Haddad, Brunil, D. Romero. (2009). Asset Identification for SecurTIy Risk Assesment in Web Application.Interna*	Pembahasan pada jurnal ini meliputi sistem informasi. PT. Petrokimia Gresik, Analisis management	Jurnal ini menggunakan metodologi *FrameworkNIST* SP800-30, melakukan pengumpulan	Hasil dari penelitian tersebut pada Pengelolaan Data Di Bagian Pengolahan Data PT. Petrokimia Gresik maka risiko dapat di indentifikasi	• Proses pengolahan data dihasilkan resiko – resiko yang sudah teridentifikasi. • Mengidentifikasi resiko dan penilaian resiko pada pengolalaan data yang dilakukan oleh Tekinfo.

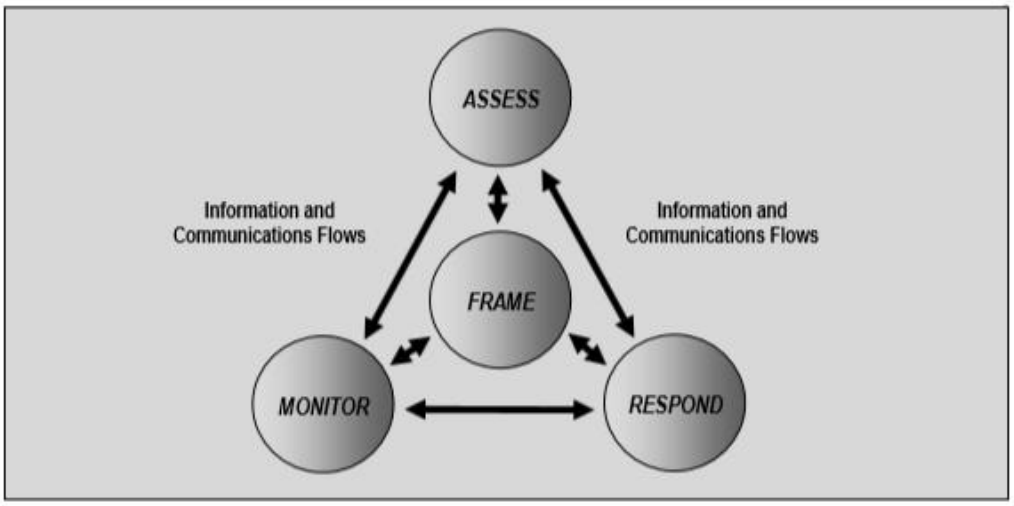
	Petrokimia Gresik		*tional Journal Of Software Engineering, IJSE, II*. • Carnaghan, C. (2005, October 28). *Business process modeling approaches in the context of process level audit risk assessment* • *NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems. July 2002*	risiko, Identifikasi risiko, Penilaian risiko dan Mitigasi risiko yang terdapat pada Sistem Informasi yang terdapat di PT. Petrokimi Gresik	data melalui kajian pustaka, dokumen review,dan teknik wawancara.	beberapa ancaman antara lain kebakaran, human eror, virus, hacking, sebagian data yang tidak berhasil di *back up* dan *restore, serta debugging* dan reverse engineering. Resiko tersebut ada karena pada umumnya terdapat kelemahan dalam hal dokumentasi, kurangnya dokumentasi tertulis pada setiap aktifitas, sehingga menimbulkan data atau informasi, kurang tersalurkan dengan baik.	Risiko yang ada dalam proses pengelolaan keamanan sistem informasi sebagai berikut: kebakaran, *virus*, human eror, *hacking*, Kehilangan sebagian data yang tidak berhasil di *back up* dan *restore*,*debugging*dan *reverse engineering*. • Diperoleh informasi berupa identifikasi ancaman yang berpotensial untuk menciptakan resiko bagi TI beserta dampak yang akan dihasilkan, dan mitigasi dengan menangani resiko.
4	Analisis Manajemen Resiko Teknologi Informasi	**Gilang M. Husein Dan Radiant**	• P. Hopkin, *Fundamentals of Risk Management: Understanding, Evaluating, and*	Pembahasan pada jurnal ini meliputi *Document Management*	Jurnal ini menggunakan metodologi *FrameworkCobit*	Hasil dari penelitian pada DMS JATEL tersebut diketahui bahwa terdapat 13 risiko	• Proses analisis manajemen risiko teknologi informasi mengidentifikasi risiko, memberikan penilaian terhadap risiko serta

	Penerapan Pada *Document Management System* di PT. Jabar Telematika (JATEL)	**Victor Imbar (2015)**	*Implementing Effective Risk Management*, London: Kogan Page, 2010. • *ISACA, COBIT 5The Risk IT Framework*: *Principles, Process Details, Management Guidelines, Maturity Models, Rolling Meadows, IL: ISACA, 2009.* • A. Y. Dewi, Analisis Nilai Teknologi Informasi & Implementasi *ISO 31000* Sebagai Manajemen Risiko Teknologi Informasi (Studi	*System(DMS)* produk arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL), Analisis management risiko, Identifikasi risiko dan Assessment risiko pada *DMS* produk arsip elektronik di JATEL	*5*melakukan pengumpulan data melalui kajian pustaka, dokumen review,dan teknik wawancara.	(*external attacks, malicious code, network congestion, system crash, database failure, data/document fraud, physical damage, hardware failure, power outage, force majure, inappropriate access, abuse of position of trust, dan disgruntled employees*) yang teridentifikasi dapat dikelompokan berdasarkan sumber daya TI (*application, information infrastructure, dan people*) dan dapat diklasifikasika *impact/consequences*nya berdasarkan *risk classification* (*security, availability,*	memberikan perlakuan yang lebih baik terhadap risiko yang mungkin terjadi pada *DMS* arsip elektronik ADEL dan NADINE di JATEL. • diketahui bahwa terdapat 13 risiko Dari risiko yang telah teridentifikasi, 6 diantaranya pada grafik sebaran risiko dan evaluasi risiko berdasarkan *likelihood* dan *impact* diketahui memiliki tingakatan medium *level of risk.* • Penanganan organisasi terhadap risiko yang terjadi pada *DMS* arsip elektronik ADEL dan NADINE secara umum sudah dilakukan dan dapat dikatakan sudah baik hanya saja JATEL tidak memiliki dokumen *Standard Operational Procedure* atau (SOP) yang berhubungan

			Kasus Layanan Pada Direktorat Jendral Pajak Republik Indonesia), Bandung, 2013.			*performance dan compliance*). Dari risiko yang telah teridentifikasi, 6 diantaranya pada grafik sebaran risiko dan evaluasi risiko berdasarkan *likelihood* dan *impact* diketahui memiliki tingakatan medium *level of risk.*	dengan manajemen risiko TI di organisasi. Strategi penanganan terhadap risiko yang memiliki fungsi kontrol dan mencegah terjadinya risiko (*risk prevention*) secara substantif dianggap sebagai strategi penanganan risiko yang paling baik. Penerapan *Data Center Tier* dan *Disaster Recovery Procedure* atau DRP juga memegang peranan penting pada implementasi manajemen risiko.

2.6. Kerangka Berpikir

Berdasarkan pengamatan sementara, kajian teori dan jurnal-jurnal dari penelitian sebelumnya, maka di buat kerangka berfikir tentang Assessmen manajemen risiko pada laboratorium TKJ SMK Negeri 3 OKU disesuaikan dengan proses manajemen risiko yang ada pada gambar 2.2.



Gambar 2.2 Kerangka Berpikir

Komponen pertama

Proses manajemen risiko ini akan membahas bagaimana organisasi *Frame Risk* atau membangunkonteks risiko, menggambarkan lingkungan di mana keputusan berbasis risiko yang dibuat. Tujuan dari komponen framing risiko merupakan untuk menghasilkan *strategi manajemen risiko* yang membahasbagaimana organisasi bermaksud untuk menilai risiko, menanggapi risiko, dan memonitor risiko-membuat eksplisit dantransparan persepsi risiko bahwa organisasi secara rutin menggunakan dalam membuat investasi dan keputusan operasional. Strategi manajemen risiko menetapkan dasar untuk mengelola risiko dan menjelaskan batas-batas untuk keputusan berbasis risiko

dalam organisasi. Dalam penelitian ini, *Frame Risk* berada pada lingkungan SMK Negeri 3 OKU yang berpusat di Laboratorium TKJ. Sehingga yang akan di bahas pada proses ini merupakan risiko yang terjadi di Laboratorium TKJ SMK Negeri 3 OKU.

Komponen Kedua

Proses manajemen risiko ini membahas bagaimana organisasi *Assess Risk* dalam konteks organisasi *Frame Risk* . Tujuan dari komponen *Assess Risk* merupakan untukmengidentifikasi: (i) ancaman terhadap organisasi (yaitu, operasi, aset, atau individu) atau ancaman diarahkanmelalui organisasi terhadap organisasi lain atau Bangsa; (ii) kerentanan internal daneksternal untuk organisasi;(iii) bahaya (yaitu, dampak negatif) yang mungkin terjadi mengingat potensi untuk ancaman mengeksploitasi kerentanan; dan (iv) kemungkinan yang merugikan akan terjadi. Hasil akhirnya merupakanpenentuan risiko (yaitu, biasanya fungsi dari tingkat risiko dan kemungkin risiko yang terjadi pada laboratorium TKJ SMK Negeri 3 OKU).

Komponen Ketiga

Proses manajemen risiko membahas bagaimana organisasi *Respond Risk* pada risiko ditentukan berdasarkan hasil *Assess Risk*. Tujuan dari *Respond Risk* komponen merupakan untuk memberikan respon yang konsisten, merespon secara luas risiko yang sesuai dengan*Frame Risk* organisasi dengan: (i) mengembangkan program alternatif tindakan untuk menanggapi risiko; (ii) mengevaluasi program alternatif tindakan; (iii) menentukan program yang tepat tindakankonsisten dengan toleransi risiko organisasi; dan (iv) respon risiko menerapkan

berdasarkanprogram yang dipilih tindakan. Hal ini diperlukan untuk merespon risiko yang terdapat pada laboratorium TKJ SMK Negeri 3 OKU setelah dilakukannya penilaian risiko.

Komponen Keempat

Proses manajemen risiko membahas organisasi *Monitor Risk*yaitu bagaimana dapat memonitor risiko dari waktu ke waktu.Tujuan dari komponen pemantauan risiko merupakan untuk menentukan efektivitas berkelanjutantanggapan risiko (konsisten dengan kerangka risiko organisasi), mengidentifikasi perubahan risiko yang berdampakuntuk sistem informasi organisasi dan lingkungan di mana sistem beroperasi;danmemverifikasi bahwa risiko direncanakan tanggapan dilaksanakan dan persyaratan keamanan informasiberasal dari dan dapat dilacak pada misi organisasi / fungsi bisnis, undang-undang federal,arahan, peraturan, kebijakan, standar, dan pedoman puas. Dan dari proses ini dapat dipantau risiko-risiko yang muncul pada laboratorium TKJ SMK Negeri 3 OKU.


Universitas
Bina
Darma

BAB III

METODOLOGI PENELITIAN

3.1 Tempat Penelitian

Lokasi penelitian akan dilaksanakan di SMK Negeri 3 OKU, yang beralamatkan di jalan Ms. Oeding No. 695 Baturaja Kabupaten Ogan Komering Ulu Provinsi Sumatera Selatan., Telp. (0735) 320906. Penelitian ini, menggambil area khusus di Laboratorium Komputer pada jurusan Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

3.2 Waktu Penelitian

Waktu pelaksanaan penelitian yang dilakukan penulis dapat dilihat pada tabel 3.1 dibawah ini.

Tabel 3.1 Jadwal Penelitian

Uraian Pelaksanaan Penelitian	Tahun 2017 – 2018																			
	November				Desember				Januari				Februari				Maret			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Pengajuan Judul Penelitian																				
Pengesahan Judul Penelitian																				
Bimbingan Proposal																				
Sidang Proposal																				
Perbaikan Proposal																				
Penelitian																				
Sidang Hasil																				
Perbaikan Hasil Penelitian																				
Penyusunan Tesis																				
Sidang Tesis																				
Administrasi																				
Seminar																				

3.3 Sumber Data

Sumber data penelitian yaitu sumber subjek dari tempat mana data bisa didapatkan. Jika peneliti memakai kuisioner atau wawancara didalam pengumpulan datanya, maka sumber data itu dari responden, yakni orang yang menjawab pertanyaan peneliti, yaitu tertulis ataupun lisan. Sumber data berbentuk responden ini digunakan didalam penelitian. Sumber data terbagi menjadi dua yaitu data primer serta data sekunder. Data primer merupakan data yang diperoleh peneliti secara langsung (dari tangan pertama), sementara data sekunder merupakan data yang diperoleh peneliti dari sumber yang sudah ada.

3.4 Variabel Penelitian

Sugiyono (2010:38) menyatakan, variabel penelitian merupakan suatu atribut atau nilai atau sifat orang, objek atau kegiatan yang memiliki variasi tertentu yang ditetapkan oleh peneliti guna dipelajari dan selanjutnya ditarik kesimpulannya. Dari penjelasan diatas penelitian ini memiliki tiga variable penting untuk di amati antara lain :

3.4.1 Komponen manusia (*Human)*

Komponen manusia sebagai pengguna utama dalam setiap teknologi, faktor risiko terbesar dalam bidang apapun merupakan *human*. Komponen manusia menilai system informasi dari sisi penggunaan system pada frekwensi serta luasnya fungsi dan penyelidikan sistem informasi. Pengguna juga berhubungan dengan siapa yang menggunakan,tingkat penggunanya,pelatihan, pengetahuan, harapan dan sikap menerima atau menolak sistem.

3.4.2 Komponen Organisasi

Komponen Organisasi sebagai kegiatan untuk berkumpulnya *human* untuk mengembangkan ataupun menggunakan teknologi. Dari komponen ini penulis dapat meneliti kinerja risiko yang akan terjadi pada laboratorium TKJ SMK Negeri 3 OKU. Sehingga dapat mengukur riiko terbesar serta terendah dari beberapa kegiatan yang di lakukan untuk menanggulangi risiko.

3.4.3 Komponen Teknologi

Komponen teknologi sebagai acuan dalam penelitian ini, teknologi yang di fokuskan kali ini merupakan jaringan yang terdapat pada laboratorium SMK Negeri 3 OKU. Pada kegiatan penelitian kali ini, penulis akan mengamati risiko yang terjadi pada peralatan jaringan. Teknologi jaringan yang di amati risikonya akan di ukur tingkat risiko yang dimiliki. Komponen teknologi inilah tujuan utama penelitian yang penulis amati.

3.5 *Sampling Purposeful*

Sampling Purposeful yaitu penentuan strategi *sampling* individu ataupun tempat. Sampling ini bukan sebuah sampel probabilitas yang kemungkinan menentukan seorang peneliti pada kesimpulan statik pada populasi. *Sampling Purposeful* yang akan mencontohkan kelompok masyarakat yang dapat memberikan informasi terbaik pada peneliti tentang permasalahan riset yang sedang dilaksanakan.

3.6 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini merupakan metode *NIST SP 800-30r1*. Metode *NIST SP 800-30r1* merupakan metode manajemen risiko yang dirancang oleh *National Institute of Standards and Technology United States of America Department of Commerce* sebagai dokumen informasi dalam mengelolah keamanan teknologi informasi pada sebuah organisasi. *NIST SP 800-30r1* merupakan metode perbaikan dari metode *NIST SP 800-30* serta *NIST SP 800-39. NIST SP 800-30r1* di keluarkan pada tahun 2012 sebagai perbaikan metode *NIST* terdahulunya.

3.6.1 Kerentanan Dan Kondisi Predisposisi

Identifikasi kerentanan dan kondisi predisposisi yang memengaruhi kemungkinan terjadinya peristiwa ancaman kekhawatiran menghasilkan dampak buruk. Tujuan utama dari penilaian kerentanan merupakan untuk memahami sifat serta tingkatan organisasi, misi / proses bisnis, dan sistem informasi mana yang rentan terhadap sumber ancaman yang diidentifikasi Tugas 2-1 dan peristiwa ancaman yang diidentifikasi dalam Tugas 2-2 yang dapat diprakarsai oleh sumber ancaman tersebut. Kerentanan di Tingkat 1 dapat menyebar di seluruh organisasi dan dapat memiliki dampak buruk yang luas jika dieksploitasi oleh peristiwa ancaman. Untuk Misalnya, kegagalan organisasi untuk mempertimbangkan kegiatan rantai suplai dapat mengakibatkan organisasi memperoleh subversi komponen yang dapat dieksploitasi oleh *adversary* untuk mengganggu misi organisasi / fungsi bisnis atau untuk mendapatkan informasi sensitif informasi organisasi.

Kerentanan pada Tingkat 2 dapat dijelaskan dalam hal misi / bisnis organisasi proses, arsitektur perusahaan, penggunaan beberapa sistem informasi, atau infrastruktur umum / layanan bersama. Di Tingkat 2, kerentanan biasanya melintasi atau menjangkau batas sistem informasi. Kerentanan di Tingkat 3 bisa dijelaskan dalam hal teknologi informasi yang digunakan dalam sistem informasi organisasi, yang lingkungan di mana sistem tersebut beroperasi, dan / atau kurangnya atau kelemahan dalam kontrol keamanan khusus sistem. Ada potensi hubungan banyak-ke-banyak antara kejadian ancaman dan kerentanan. Berbagai peristiwa ancaman bias mengeksploitasi kerentanan tunggal, dan sebaliknya, beberapa kerentanan dapat dimanfaatkan oleh peristiwa ancaman tunggal. Itu keparahan dari kerentanan merupakan penilaian dari kepentingan relatif dari mitigasi kerentanan tersebut. Awalnya, itu Sejauh mana mitigasi tidak direncanakan dapat berfungsi sebagai pengganti untuk keparahan kerentanan. Begitu risiko terkait dengan kerentanan tertentu telah dinilai, tingkat keparahan dampak dan paparan dari kerentanan yang diberikan kontrol keamanan diimplementasikan dan kerentanan lainnya dapat dipertimbangkan dalam menilai kerentanan kerasnya. Penilaian keparahan kerentanan mendukung respons risiko.

Kerentanan dapat diidentifikasi dengan beragam derajat perincian dan spesifisitas. Tingkat rincian yang disediakan dalam penilaian kerentanan tertentu konsisten dengan tujuan penilaian risiko dan jenis input yang diperlukan untuk mendukung kemungkinan dan penentuan dampak. Karena

ukuran dan kompleksitas organisasi, misi / proses bisnis yang terus meningkat, dan informasi sistem yang mendukung proses tersebut, jumlah kerentanan cenderung besar dan dapat meningkatkan keseluruhan kompleksitas analisis. Oleh karena itu, organisasi memiliki pilihan untuk menggunakan tugas identifikasi kerentanan memahami sifat umum dari kerentanan (termasuk ruang lingkup, jumlah, dan jenis) yang relevan dengan penilaian (lihat Tugas 1-3) dan melakukan katalogisasi kerentanan khusus yang diperlukan untuk melakukannya. Organisasi menentukan yang mana kerentanan relevan dengan peristiwa ancaman untuk mengurangi ruang potensi risiko yang akan dinilai. Di Selain mengidentifikasi kerentanan, organisasi juga mengidentifikasi kondisi predisposisi yang mungkin mempengaruhi kerentanan terhadap kerentanan tertentu. Kondisi predisposisi yang ada dalam organisasi (termasuk misi / proses bisnis, sistem informasi, dan lingkungan operasi) dapat berkontribusi (yaitu, meningkatkan atau mengurangi) kemungkinan bahwa satu atau lebih peristiwa ancaman, setelah dimulai oleh sumber ancaman, menghasilkan dampak yang merugikan operasi organisasi, aset organisasi, individu, organisasi lain, atau Bangsa. Organisasi menentukan kondisi predisposisi mana yang relevan dengan peristiwa ancaman untuk mengurangi ruang potensial risiko untuk dinilai. Organisasi menilai luasnya kondisi predisposisi untuk mendukung penentuan tier (s) di mana respons risiko bisa paling efektif.

Menyediakan seperangkat tabel contoh untuk digunakan dalam mengidentifikasi kerentanan dan kondisi predisposisi:

- Tabel 3.2 menyediakan seperangkat input yang patut dicontoh untuk tugas identifikasi kondisi kerentanan dan predisposisi;
- Tabel 3.3 memberikan skala penilaian teladan untuk menilai tingkat keparahan kerentanan yang teridentifikasi;
- Tabel 3.4 menyediakan template untuk meringkas /mendokumentasikan hasil identifikasi kerentanan;
- Tabel 3.5 memberikan taksonomi teladan yang dapat digunakan untuk mengidentifikasi dan mengkarakterisasi kondisi predisposisi;
- Tabel 3.6 memberikan skala penilaian teladan untuk menilai luasnya kondisi predisposisi; dan
- Tabel 3.7 menyediakan template untuk meringkas / mendokumentasikan hasil mengidentifikasi kondisi predisposisi.

Informasi yang dihasilkan dalam Tugas 2-3 memberikan kerentanan dan mempengaruhi masukan kondisi ke tabel risiko.

TABEL 3.2 : INPUTS - KERENTANAN DAN KONDISI PREDISPOSISI

Deskripsi	Disediakan untuk		
	Tingkat1	Tingkat2	Tingkat3
Dari Tingkat 1 (Tingkat Organisasi) - Sumber informasi kerentanan yang dianggap kredibel (misalnya, sumber terbuka dan / atau rahasia kerentanan, penilaian risiko / kerentanan sebelumnya, Misi dan / atau Analisis Dampak Bisnis). (Bagian 3.1, Tugas 1-4.) - Informasi kerentanan dan panduan khusus untuk Tier 1 (misalnya, kerentanan yang terkait dengan organisasi tata kelola, misi inti / fungsi bisnis, manajemen / kebijakan operasional, prosedur, dan struktur, misi eksternal / hubungan bisnis). - Taksonomi kondisi predisposisi, dijelaskan oleh organisasi, jika perlu. (Tabel F-4)	Tidak	Ya	Ya Jika tidak disediakan oleh Tingkat 2

- Karakterisasi kerentanan dan kondisi predisposisi. - Skala penilaian untuk menilai tingkat keparahan kerentanan, yang dijelaskan oleh organisasi, jika perlu. (Tabel F-2) - Skala penilaian untuk menilai pervasiveness dari kondisi predisposisi, yang dianotasikan oleh organisasi, jika perlu. (Tabel F-5) - Business Continuity Plan, Continuity of Operation Plan untuk organisasi, jika ada rencana seperti itu didefinisikan untuk seluruh organisasi.			
Dari Tingkat 2: (Misi / tingkat proses bisnis) - Informasi dan panduan Kerentanan khusus untuk Tingkat 2 (misalnya, kerentanan yang terkait dengan organisasi misi / proses bisnis, segmen EA, infrastruktur umum, layanan dukungan, umum kontrol, dan dependensi eksternal). - Rencana Kelangsungan Bisnis, Kesinambungan Rencana Operasi untuk misi / proses bisnis, jika seperti itu rencana ditentukan untuk proses individu atau unit bisnis.	Ya Melalui RAR	Ya Melalui Berbagi Peer	Ya
Dari Tingkat 3: (Tingkat sistem informasi) - Informasi kerentanan dan panduan khusus untuk Tier 3 (misalnya, kerentanan yang terkait dengan informasi sistem, teknologi informasi, komponen sistem informasi, aplikasi, jaringan, lingkungan operasi). - Laporan penilaian keamanan (yaitu, kekurangan dalam kontrol yang dinilai diidentifikasi sebagai kerentanan). - Hasil kegiatan pemantauan (misalnya, umpan data otomatis dan tidak disengaja). - Penilaian Kerentanan, laporan Tim Merah, atau laporan lain dari analisis sistem informasi, subsistem, produk teknologi informasi, perangkat, jaringan, atau aplikasi. - Contingency Plans, Disaster Recovery Plans, Insiden Reports. - Laporan kerentanan vendor / pabrikan	Ya Melalui RAR	Ya Melalui RAR	Ya Melalui Berbagi Peer

TABEL 3.3: SKALA PENILAIAN - TINGKAT KERENTANAN

Nilai Qualitatif	Nilai Semi Qualitatif		Deskripsi
Sangat Tinggi	96-100	10	Kerentanan diekspos dan dieksploitasi, dan eksploitasinya dapat mengakibatkan dampak yang parah. Pengendalian keamanan yang relevan atau remediasi lainnya tidak dilaksanakan dan tidak direncanakan; atau tanpa keamanan ukuran dapat diidentifikasi untuk memulihkan kerentanan
Tinggi	80-95	8	Kerentanan merupakan kekhawatiran yang tinggi, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan / atau keparahan dampak yang dapat dihasilkan dari eksploitasinya. Pengendalian keamanan yang relevan atau remediasi lainnya direncanakan tetapi tidak dilaksanakan; kompensasi kontrol di

			tempat dan setidaknya minimal efektif
Sedang	21-79	5	Kerentanan merupakan kekhawatiran sedang, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan / atau keparahan dampak yang dapat dihasilkan dari eksploitasinya. Pengendalian keamanan yang relevan atau remediasi lainnya diterapkan sebagian dan agak efektif.
Rendah	5-20	2	Kerentanan merupakan masalah kecil, tetapi efektivitas remediasi dapat ditingkatkan. Pengendalian keamanan yang relevan atau remediasi lainnya sepenuhnya dilaksanakan dan agak efektif.
Sangat Renda	0-4	0	Kerentanan tidak menjadi perhatian. Pengendalian keamanan yang relevan atau remediasi lainnya sepenuhnya dilaksanakan, dinilai, dan efektif.

TABEL 3.4: TEMPLATE - IDENTIFIKASI KEMAMPUAN

Identifier	**Kerentanan** **Sumber informasi**	**Kerentanan** **Kerasnya**
Organisasi-didefinisikan	Tugas 2-3, Tugas 1-4 atau Organisasi yang ditentukan	Tabel F-2 atau Organisasi yang ditentukan

TABLE 3.5 : TAXONOMY OF PREDISPOSING CONDITIONS

Jenis Kondisi Predisposisi	**Deskripsi**
INFORMASI-TERKAIT - Informasi Keamanan Nasional yang Diklasifikasikan - Kompartemen - Informasi Unclassified Terkendali - Informasi Identitas Pribadi - Program Akses Khusus - Ditentukan Perjanjian - TIDAK ADA - Kepemilikan	Perlu menangani informasi (seperti yang dibuat, dikirim, disimpan, diproses, dan / atau ditampilkan) dengan cara tertentu, karena sensitivitasnya (atau kurangnya kepekaan), persyaratan hukum atau peraturan, dan / atau kontrak atau perjanjian organisasi lainnya.
TEKNIS - Arsitektur - Kepatuhan dengan standar teknis - Penggunaan produk atau lini produk tertentu - Solusi untuk dan / atau pendekatan untuk kolaborasi berbasis pengguna dan berbagi informasi - Alokasi fungsi keamanan spesifik untuk kontrol umum - Fungsional - Multiuser jaringan - Single-user - Berdiri sendiri / tidak di-jaringan - Fungsionalitas terbatas (mis. Komunikasi, sensor, pengontrol yang disematkan)	Perlu menggunakan teknologi dengan cara tertentu
OPERASIONAL / LINGKUNGAN - Mobilitas - Situs-tetap (tentukan lokasi)	Kemampuan untuk mengandalkan kontrol fisik, prosedural, dan personil disediakan oleh lingkungan

- Semi-seluler - Berbasis darat, Lintas Udara, Berbasis Laut, Ruang Angkasa - Ponsel (mis., Perangkat genggam) - Populasi dengan akses fisik dan / atau logis ke komponen dari sistem informasi, misi / proses bisnis, segmen EA - Ukuran populasi - Pembersihan / pemeriksaan populasi	operasional

TABLE 3.6 SKALA PENILAIAN - PERVASIVENSI KONDISI PREDISPOSISI

Nilai Qualitatif	Nilai Semi Qualitatif		Deskripsi
Sangat Tinggi	96-100	10	Berlaku untuk **semua** misi organisasi / fungsi bisnis (Tingkat 1), misi / proses bisnis (Tingkat 2), atau sistem informasi (Tingkat 3).
Tinggi	80-95	8	Berlaku untuk **sebagian besar** misi organisasi / fungsi bisnis (Tingkat 1), misi / proses bisnis (Tingkat 2), atau sistem informasi (Tingkat 3).
Sedang	21-79	5	Berlaku untuk **banyak** misi organisasi / fungsi bisnis (Tingkat 1), misi / proses bisnis (Tingkat 2), atau sistem informasi (Tingkat 3).
Rendah	5-20	2	Berlaku untuk **beberapa** misi organisasi / fungsi bisnis (Tingkat 1), misi / proses bisnis (Tingkat 2), atau sistem informasi (Tingkat 3).
Sangat Renda	0-4	0	Berlaku untuk **beberapa** misi organisasi / fungsi bisnis (Tingkat 1), misi / proses bisnis (Tingkat 2), atau sistem informasi (Tingkat 3).

TABEL 3.7 TEMPLATE - IDENTIFIKASI KONDISI PREDISPOSING

Identifier	**Kondisi predisposisi Sumber informasi**	**Pervasif kondisi**
Organisasi-didefinisikan	Tabel F-4, Tugas 1-4 atau Organisasi yang ditentukan	Tabel F-5 atau Organisasi yang ditentukan

3.6.2 Menentukan Kemungkinan Terjadi Ancaman

Menentukan kemungkinan bahwa peristiwa ancaman yang menjadi perhatian menghasilkan dampak buruk, dengan mempertimbangkan: (i) karakteristik sumber ancaman yang dapat memulai peristiwa; (ii) kerentanan / predisposisi kondisi diidentifikasi; dan (iii) kerentanan

organisasi yang mencerminkan upaya perlindungan / penanggulangan direncanakan atau diimplementasikan untuk menghalangi kejadian semacam itu.

Organisasi menggunakan proses tiga langkah untuk menentukan kemungkinan kejadian ancaman secara keseluruhan. Pertama, organisasi menilai kemungkinan bahwa peristiwa ancaman akan dimulai (untuk peristiwa ancaman per*adversary*an) atau akan terjadi (untuk peristiwa ancaman non-per*adversary*an). Kedua, organisasi menilai kemungkinan bahwa peristiwa ancaman sekali dimulai atau terjadi, akan mengakibatkan dampak negatif terhadap operasi dan aset organisasi, individu, organisasi lain, atau Bangsa. Akhirnya, organisasi menilai kemungkinan keseluruhan sebagai kombinasi kemungkinan inisiasi / kejadian dan kemungkinan menghasilkan dampak yang merugikan.

Organisasi menilai kemungkinan inisiasi peristiwa ancaman dengan mempertimbangkan karakteristik ancaman sumber kekhawatiran termasuk kemampuan, niat, dan penargetan (lihat Tugas 2-1 dan Lampiran D). Jika peristiwa ancaman membutuhkan lebih banyak kemampuan daripada yang dimiliki *adversary* (dan *adversary* sadar akan fakta ini), maka *adversary* tidak diharapkan untuk memulai acara. Jika *adversary* tidak berharap untuk mencapai tujuan yang dimaksudkan dengan mengeksekusi peristiwa ancaman, maka *adversary* tidak diharapkan untuk memulai peristiwa. Dan akhirnya, jika lawan tidak aktif menargetkan khusus organisasi atau fungsi misi / bisnis mereka, lawan

tidak diharapkan untuk memulai peristiwa ancaman. Organisasi menggunakan skala penilaian pada Tabel 3.9 dan memberikan alasan untuk penilaian yang memungkinkan pertimbangan eksplisit pencegahan dan ancaman bergeser. Organisasi dapat menilai kemungkinan terjadinya peristiwa ancaman (non-per*adversary*an) menggunakan Tabel 3.10 dan memberikan alasan yang sama untuk penilaian.

Organisasi menilai kemungkinan bahwa peristiwa ancaman menghasilkan dampak buruk dengan mempertimbangkan perangkat mengidentifikasi kerentanan dan kondisi predisposisi (lihat Tugas 2-3 dan Lampiran F). Untuk kejadian ancaman yang diprakarsai oleh *adversary*, organisasi mempertimbangkan karakteristik sumber ancaman yang terkait. Untuk peristiwa ancaman non-per*adversary*an, organisasi mempertimbangkan tingkat keparahan dan durasi yang diantisipasi dari peristiwa tersebut (sebagaimana yang termasuk dalam uraian tentang peristiwa). Organisasi menggunakan skala penilaian dalam Tabel G-4 dan memberikan alasan untuk penilaian yang memungkinkan eksplisit pertimbangan sebagaimana dinyatakan di atas. Peristiwa ancaman yang tidak ada kerentanan atau kondisi predisposisi diidentifikasi, miliki kemungkinan sangat rendah menghasilkan dampak buruk. Peristiwa ancaman semacam itu dapat disorot dan dipindahkan ke akhir tabel (atau ke tabel terpisah), sehingga mereka dapat dilacak untuk dipertimbangkan dalam penileian risiko lanjutan. Namun, tidak pertimbangan lebih lanjut selama penilaian saat ini dibenarkan.

Kemungkinan keseluruhan dari acara ancaman merupakan kombinasi dari: (i) kemungkinan bahwa acara ini akan terjadi (misalnya, karena kesalahan manusia atau bencana alam) atau diprakarsai oleh *adversary*; dan (ii) kemungkinan bahwa inisiasi / kejadian akan terjadi menghasilkan dampak buruk. Organisasi menilai kemungkinan kejadian ancaman secara keseluruhan dengan menggunakan input dari Tabel G-2, G-3, dan G-4. Algoritma atau aturan khusus apa pun untuk menggabungkan nilai kemungkinan yang ditentukan bergantung pada: (i) umum sikap organisasi terhadap risiko, termasuk toleransi risiko secara keseluruhan dan toleransi terhadap ketidakpastian; (ii) spesifik toleransi terhadap ketidakpastian dalam berbagai faktor risiko; dan (iii) pembobotan organisasi faktor risiko. Sebagai contoh, organisasi dapat menggunakan salah satu aturan berikut (atau dapat menentukan aturan yang berbeda): (i) menggunakan maksimum dari keduanya nilai kemungkinan; (ii) menggunakan minimum dari dua nilai kemungkinan; (iii) mempertimbangkan kemungkinan inisiasi / kejadian hanya, dengan asumsi bahwa jika peristiwa ancaman dimulai atau terjadi, kejadian tersebut akan menghasilkan dampak yang merugikan; (iv) pertimbangkan kemungkinan dampak saja, dengan asumsi bahwa jika peristiwa ancaman dapat mengakibatkan dampak yang merugikan, *adversary* akan memulai acara; atau (v) mengambil rata-rata tertimbang dari dua nilai kemungkinan. Organisasi membuat aturan yang digunakan secara eksplisit.

Menyediakan seperangkat tabel contoh untuk digunakan dalam menentukan kemungkinan peristiwa ancaman:

- Tabel 3.8 menyediakan seperangkat input yang patut dicontoh untuk tugas penentuan kemungkinan;
- Tabel 3.9 memberikan skala penilaian teladan untuk menilai kemungkinan inisiasi untuk ancaman per*adversary*an acara;
- Tabel 3.10 memberikan skala penilaian teladan untuk menilai kemungkinan peristiwa ancaman non-per*adversary*an terjadi;
- Tabel 3.11 memberikan skala penilaian teladan untuk menilai kemungkinan kejadian ancaman yang merugikan dampak jika peristiwa dimulai (per*adversary*an) atau terjadi (non-per*adversary*an); dan
- Tabel 3.12 memberikan skala penilaian teladan untuk menilai kemungkinan keseluruhan peristiwa ancaman (yaitu, a kombinasi kemungkinan inisiasi / kejadian dan kemungkinan dampak).

Informasi yang dihasilkan dalam menyediakan input kemungkinan kejadian ancaman ke tabel risiko.

TABLE 3.8 INPUTS - PENETAPAN DARI LIKELIHOOD

Deskripsi	Disediakan untuk		
	Tingkat1	Tingkat2	Tingkat3
Dari Tingkat 1 (Tingkat Organisasi) - Informasi dan panduan kemungkinan khusus untuk Tier 1 (misalnya, informasi kemungkinan terkait dengan tata kelola organisasi, misi inti / fungsi bisnis, manajemen / kebijakan operasional, prosedur, dan struktur, misi eksternal / hubungan bisnis). - Panduan tentang tingkat organisasi yang kemungkinan besar tidak perlu dipertimbangkan lebih	Tidak	Ya	Ya Jika tidak disediakan oleh Tingkat 2

lanjut. - Skala penilaian untuk menilai kemungkinan inisiasi peristiwa ancaman (peristiwa ancaman adversarial), dianotasikan oleh organisasi, jika perlu. (**Tabel G-2**) - Skala penilaian untuk menilai kemungkinan kejadian kejadian ancaman (ancaman non-per*adversary*an acara), dianotasikan oleh organisasi, jika perlu. (**Tabel G-3**) - Skala penilaian untuk menilai kemungkinan kejadian ancaman yang mengakibatkan dampak buruk, dianotasikan oleh organisasi, jika perlu. (**Tabel G-4**) - Skala penilaian untuk menilai kemungkinan keseluruhan peristiwa ancaman yang dimulai atau terjadi dan mengakibatkan dampak merugikan, yang dijelaskan oleh organisasi, jika perlu. (**Tabel G-5**)			
Dari Tingkat 2: (Misi / tingkat proses bisnis) - Informasi dan panduan kemungkinan khusus untuk Tier 2 (misalnya, informasi kemungkinan terkait dengan misi / proses bisnis, segmen EA, infrastruktur umum, layanan dukungan, umum kontrol, dan dependensi eksternal).	Ya Melalui RAR	Ya Melalui Berbagi Peer	Ya
Dari Tingkat 3: (Tingkat sistem informasi) - Informasi dan panduan kemungkinan khusus untuk Tier 3 (misalnya, informasi kemungkinan terkait dengan sistem informasi, teknologi informasi, komponen sistem informasi, aplikasi, jaringan, lingkungan operasi). - Data historis tentang serangan dunia maya yang sukses dan tidak berhasil; tingkat deteksi serangan. - Laporan penilaian keamanan (yaitu, kekurangan dalam kontrol yang dinilai diidentifikasi sebagai kerentanan). - Hasil kegiatan pemantauan (misalnya, umpan data otomatis dan tidak disengaja). - Penilaian Kerentanan, laporan Tim Merah, atau laporan lain dari analisis sistem informasi, subsistem, produk teknologi informasi, perangkat, jaringan, atau aplikasi. - Contingency Plans, Disaster Recovery Plans, Insiden Reports. - Laporan kerentanan vendor / pabrikan.	Ya Melalui RAR	Ya Melalui RAR	Ya Melalui Berbagi Peer

TABEL3.9 SKALA PENILAIAN - PENCAPAIAN ANCAMAN (ADVERSARY)

Nilai Qualitatif	Nilai Semi Qualitatif		Deskripsi
Sangat Tinggi	96-100	10	*Adversary***hampir pasti** untuk memulai peristiwa ancaman.
Tinggi	80-95	8	*Adversary***sangat mungkin** untuk memulai peristiwa ancaman
Sedang	21-79	5	*Adversary***agak cenderung** memulai acara memperlakukan.
Rendah	5-20	2	*Adversary***tidak mungkin** memulai peristiwa ancaman.
Sangat Renda	0-4	0	*Adversary***sangat tidak mungkin** untuk memulai peristiwa ancaman

TABEL 3.10 SKALA PENILAIAN - PENCAPAIAN ANCAMAN (NON-ADVERSARY)

Nilai Qualitatif	Nilai Semi Qualitatif		Deskripsi
Sangat Tinggi	96-100	10	Kesalahan, kecelakaan, atau tindakan alam **hampir pasti** terjadi; atau terjadi **lebih dari 100 kali setahun**
Tinggi	80-95	8	Kesalahan, kecelakaan, atau tindakan alam **sangat mungkin** terjadi; atau terjadi **antara 10-100 kali setahun** .
Sedang	21-79	5	Kesalahan, kecelakaan, atau tindakan alam **agaknya mungkin** terjadi; atau terjadi **antara 1-10 kali a tahun**
Rendah	5-20	2	Kesalahan, kecelakaan, atau tindakan alam **tidak mungkin** terjadi; atau terjadi **kurang dari sekali setahun** , tetapi **lebihdari sekali setiap 10 tahun**
Sangat Renda	0-4	0	Kesalahan, kecelakaan, atau tindakan alam **sangat tidak mungkin** terjadi; atau terjadi **kurang dari sekali setiap 10tahun**

TABEL 3.11 SKALA PENILAIAN - PENCAPAIAN ANCAMAN YANG MENGHASILKAN DAMPAK LUAR BIASA

Nilai Qualitatif	Nilai Semi Qualitatif		Deskripsi
Sangat Tinggi	96-100	10	Jika peristiwa ancaman dimulai atau terjadi, **hampir pasti** akan berdampak buruk
Tinggi	80-95	8	Jika peristiwa ancaman dimulai atau terjadi, **kemungkinan besar** akan berdampak buruk
Sedang	21-79	5	Jika peristiwa ancaman dimulai atau terjadi, itu **agak cenderung** memiliki dampak buruk.
Rendah	5-20	2	Jika peristiwa ancaman dimulai atau terjadi, **kemungkinan tidak** akan berdampak buruk
Sangat Renda	0-4	0	Jika peristiwa ancaman dimulai atau terjadi, **sangat tidak mungkin** terjadi dampak negatif

TABLE 3.12 SKALA PENILAIAN - KESELURUHAN

Kemungkinan Kejadian Ancaman Inisiasi atau Kejadian	Kejadian Peristiwa Ancaman Kemungkinan Menghasilkan Dampak yang Merugikan				
	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Sangat Tinggi	Rendah	Sedang	Tinggi	Sangat Tinggi	Sangat Tinggi
Tinggi	Rendah	Sedang	Sedang	Tinggi	Sangat Tinggi
Sedang	Rendah	Rendah	Sedang	Sedang	Tinggi
Rendah	Sangat Rendah	Rendah	Rendah	Sedang	Sedang
Sangat Rendah	Sangat Rendah	Sangat Rendah	Rendah	Rendah	Rendah

3.6.3 Menentukan Dampak

Menentukan dampak merugikan dari peristiwa ancaman yang memprihatinkan mengingat: (i) karakteristik sumber ancaman yang dapat memulai peristiwa; (ii) kondisi kerentanan / predisposisi yang diidentifikasi; dan (iii) kerentanan yang mencerminkan upaya perlindungan / penanggulangan yang direncanakan atau dilaksanakan untuk menghambat acara semacam itu. Organisasi menggambarkan dampak buruk dalam hal potensi bahaya yang disebabkan organisasi operasi dan aset, individu, organisasi lain, atau Bangsa. Di mana peristiwa ancaman terjadi dan apakah efek dari peristiwa yang terkandung atau menyebar, mempengaruhi tingkat keparahan dampak. Menilai dampak dapat melibatkan mengidentifikasi aset atau target potensial dari sumber ancaman, termasuk sumber informasi (misalnya, informasi, data repositori, sistem informasi, aplikasi, teknologi informasi, tautan komunikasi), orang, dan fisik sumber daya (misalnya, bangunan, pasokan listrik), yang dapat dipengaruhi oleh peristiwa ancaman. Dampak organisasi didefinisikan dan diprioritaskan pada Tingkat 1 dan 2, dan dikomunikasikan ke Tingkat 3 sebagai bagian dari pembingkaian

risiko. Di Tingkat 3, dampaknya terkait dengan kemampuan sistem informasi (misalnya, pemrosesan, tampilan, komunikasi, penyimpanan, dan pengambilan) dan sumber daya (misalnya, basis data, layanan, komponen) yang dapat dikompromikan.

Menyediakan seperangkat tabel contoh untuk digunakan dalam menentukan dampak merugikan.

- Tabel 3.13 menyediakan seperangkat input yang patut dicontoh untuk tugas penentuan dampak;
- Tabel 3.14 memberikan contoh yang representatif tentang dampak buruk bagi organisasi yang berfokus pada bahaya terhadap organisasi operasi dan aset, individu, organisasi lain, dan Bangsa;
- Tabel 3.15 memberikan skala penilaian teladan untuk menilai dampak peristiwa ancaman; dan
- Tabel 3.16 menyediakan template untuk meringkas / mendokumentasikan dampak buruk.

Informasi yang dihasilkan dalam Tugas 2-5 memberikan masukan dampak merugikan ke tabel risiko

TABEL 3.13 INPUTS - DETERMINASI DAMPAK

Deskripsi	Disediakan untuk		
	Tingkat1	Tingkat2	Tingkat3
Dari Tingkat 1 (Tingkat Organisasi) - Informasi dampak dan panduan khusus untuk Tingkat 1 (misalnya, informasi dampak yang terkait dengan organisasi tata kelola, misi inti / fungsi bisnis, manajemen dan kebijakan operasional, prosedur, dan struktur, misi eksternal / hubungan bisnis). - Panduan tentang tingkat dampak organisasi yang luas yang tidak memerlukan pertimbangan lebih lanjut. - Identifikasi misi kritis / fungsi bisnis.	Tidak	Ya	Ya Jika tidak disediakan oleh Tingkat 2

- Kumpulan contoh dampak, yang dijelaskan oleh organisasi, jika perlu. (**Tabel H-2**) - Skala penilaian untuk menilai dampak dari peristiwa ancaman, yang dijelaskan oleh organisasi, jika perlu. (**Tabel H-3**)			
Dari Tingkat 2: (Misi / tingkat proses bisnis) - Informasi dampak dan panduan khusus untuk Tingkat 2 (misalnya, informasi dampak yang terkait dengan misi / proses bisnis, segmen EA, infrastruktur umum, layanan dukungan, umum kontrol, dan dependensi eksternal). - Identifikasi aset bernilai tinggi.	Ya Melalui RAR	Ya Melalui Berbagi Peer	Ya
Dari Tingkat 3: (Tingkat sistem informasi) - Informasi dampak dan panduan khusus untuk Tier 3 (misalnya, informasi kemungkinan mempengaruhi informasi sistem, teknologi informasi, komponen sistem informasi, aplikasi, jaringan, lingkungan operasi). - Data historis tentang serangan dunia maya yang sukses dan tidak berhasil; tingkat deteksi serangan. - Laporan penilaian keamanan (yaitu, kekurangan dalam kontrol yang dinilai diidentifikasi sebagai kerentanan). - Hasil kegiatan pemantauan berkelanjutan (misalnya, umpan data otomatis dan tidak disengaja). - Penilaian Kerentanan, laporan Tim Merah, atau laporan lain dari analisis sistem informasi, subsistem, produk teknologi informasi, perangkat, jaringan, atau aplikasi. - Contingency Plans, Disaster Recovery Plans, Insiden Reports	Ya Melalui RAR	Ya Melalui RAR	Ya Melalui Berbagi Peer

TABEL 3.14 CONTOH DAMPAK LUAR BIASA

Jenis Dampak	Dampak
HARM TO OPERASI	- Ketidakmampuan melakukan fungsi misi / bisnis saat ini. - Dengan cara yang cukup tepat waktu. - Dengan keyakinan yang cukup dan / atau benar. - Dalam batasan sumber daya yang direncanakan. - Ketidakmampuan, atau kemampuan terbatas, untuk melakukan misi / fungsi bisnis di masa depan. - Ketidakmampuan untuk mengembalikan misi / fungsi bisnis. - Dengan cara yang cukup tepat waktu. - Dengan keyakinan yang cukup dan / atau benar. - Dalam batasan sumber daya yang direncanakan. - Bahaya (misalnya, biaya keuangan, sanksi) karena ketidakpatuhan. - Dengan hukum atau peraturan yang berlaku. - Dengan persyaratan kontrak atau persyaratan lain dalam perjanjian mengikat lainnya (misalnya kewajiban). - Biaya keuangan langsung. - Kerusakan relasional. - Kerusakan kepercayaan hubungan.

	- Kerusakan pada citra atau reputasi (dan karenanya hubungan kepercayaan di masa depan atau potensial).
HARM DENGAN ASET	- Kerusakan atau kehilangan fasilitas fisik. - Kerusakan atau kehilangan sistem informasi atau jaringan. - Kerusakan atau kehilangan teknologi atau peralatan informasi. - Kerusakan atau kehilangan komponen komponen atau persediaan. - Kerusakan atau kehilangan aset informasi. - Hilangnya kekayaan intelektual
HARM KE INDIVIDU	- Cedera atau korban jiwa. - Penganiayaan fisik atau psikologis. - Pencurian identitas. - Hilangnya Informasi Identitas Pribadi. - Kerusakan pada citra atau reputasi.
HARM KE LAIN ORGANISASI	- Bahaya (misalnya, biaya keuangan, sanksi) karena ketidakpatuhan. - Dengan hukum atau peraturan yang berlaku. - Dengan persyaratan kontrak atau persyaratan lain dalam perjanjian mengikat lainnya. - Biaya keuangan langsung. - Kerusakan relasional. - Kerusakan kepercayaan hubungan. - Kerusakan reputasi (dan karenanya hubungan kepercayaan di masa depan atau potensial).
HARM KE BANGSA	- Kerusakan atau ketidakmampuan sektor infrastruktur penting. - Kehilangan kesinambungan operasi pemerintah. - Kerusakan relasional. - Kerusakan kepercayaan hubungan dengan pemerintah lain atau dengan entitas nonpemerintah. - Kerusakan reputasi nasional (dan karenanya hubungan kepercayaan di masa depan atau potensial). - Kerusakan kemampuan saat ini atau masa depan untuk mencapai tujuan nasional. - Bahaya pada keamanan nasional

TABEL 3.15 SKALA PENILAIAN - DAMPAK EVENT ANCAMAN

Nilai Qualitatif	Nilai Semi Qualitatif		Deskripsi
Sangat Tinggi	96-100	10	Peristiwa ancaman dapat diperkirakan memiliki **beberapa** efek samping yang **parah atau bencana** operasi organisasi, aset organisasi, individu, organisasi lain, atau Bangsa
Tinggi	80-95	8	Peristiwa ancaman bisa diharapkan memiliki efek buruk yang **parah atau bencana** operasi organisasi, aset organisasi, individu, organisasi lain, atau Bangsa. SEBUAH efek samping yang parah atau katastropik berarti bahwa, misalnya, peristiwa ancaman mungkin: (i) menyebabkan a degradasi yang parah dalam atau hilangnya kemampuan misi ke tingkat dan durasi organisasi itu tidak dapat melakukan satu atau lebih fungsi utamanya; (ii) mengakibatkan kerusakan besar aset organisasi; (iii) mengakibatkan kerugian finansial besar; atau (iv) menghasilkan kerusakan parah atau bencana kepada individu yang melibatkan korban jiwa atau cedera serius yang mengancam jiwa

Sedang	21-79	5	Peristiwa ancaman dapat diperkirakan memiliki efek buruk yang **serius** pada operasi organisasi, aset organisasi, individu organisasi lain, atau Bangsa. Efek merugikan yang serius berarti, misalnya, peristiwa ancaman mungkin: (i) menyebabkan degradasi misi yang signifikan kemampuan ke tingkat dan durasi yang organisasi mampu melakukan fungsi utamanya, tetapi efektivitas fungsi berkurang secara signifikan; (ii) menghasilkan kerusakan yang signifikan terhadap aset organisasi; (iii) menghasilkan kerugian finansial yang signifikan; atau (iv) menghasilkan kerusakan yang signifikan terhadap individu yang tidak melibatkan korban jiwa atau cedera serius yang mengancam jiwa.
Rendah	5-20	2	Peristiwa ancaman dapat diperkirakan memiliki efek merugikan **terbatas** pada operasi organisasi, aset organisasi, individu organisasi lain, atau Bangsa. Efek merugikan terbatas berarti, misalnya, peristiwa ancaman mungkin: (i) menyebabkan penurunan kemampuan misi menjadi luas dan durasi bahwa organisasi mampu melakukan fungsi utamanya, tetapi keefektifan fungsi terlihat berkurang; (ii) menghasilkan kerusakan kecil pada organisasi aktiva; (iii) menghasilkan kerugian finansial kecil; atau (iv) mengakibatkan kerusakan kecil bagi individu.
Sangat Renda	0-4	0	Peristiwa ancaman dapat diharapkan memiliki efek merugikan yang **dapat diabaikan** pada organisasi operasi, aset organisasi, individu organisasi lain, atau Nation

TABEL 3.16 TEMPLATE - IDENTIFIKASI DAMPAK ADVERSE

Jenis Dampak	**Dampak** **Aset yang Terkena Dampak**	**Dampak Maksimum**
Tabel H-2 atau Organisasi-didefinisikan	Tabel H-2 atau Organisasi yang ditentukan	Tabel H-3 atau Organisasi yang ditentukan

3.6.4 Menentukan Risiko

Menilai Risiko Pada Organisasi, Individu, Dan Bangsa dengan memberikan: (i) deskripsi tentang input yang berpotensi bermanfaat terhadap risiko penetapan tugas termasuk pertimbangan untuk ketidakpastian penentuan; (ii) skala penilaian teladan untuk menilai tingkat risiko; (iii) tabel untuk mendeskripsikan konten (yaitu, input data) untuk penentuan risiko per*adversary*an dan non-per*adversary*an; dan (iv) template untuk meringkas dan mendokumentasikan hasil penentuan risiko

Tugas 2-6 Itu skala penilaian dalam apendiks ini dapat digunakan sebagai titik awal dengan penyesuaian yang sesuai untuk menyesuaikan untuk setiap kondisi spesifik organisasi. Tugas 2-6**:** Tentukan risiko bagi organisasi dari peristiwa ancaman yang menjadi perhatian mengingat: (i) dampaknya yang akan dihasilkan dari peristiwa; dan (ii) kemungkinan terjadinya peristiwa. Wacana ini menyediakan seperangkat tabel contoh untuk digunakan dalam menentukan risiko:

- Tabel 3.17 menyediakan seperangkat input teladan untuk tugas penentuan risiko dan ketidakpastian;
- Tabel 3.18 dan 3.19 memberikan skala penilaian teladan untuk menilai tingkat risiko;

Informasi yang dihasilkan dalam Tugas 2-6 memberikan masukan risiko ketabel risiko dibawah.

Tabel 3.17 Inputs – Risiko

Deskripsi	**Disediakan untuk**		
	Tingkat 1	**Tingkat 2**	**Tingkat 3**
Dari Tingkat 1 (Tingkat Organisasi) - Sumber informasi risiko dan ketidakpastian yang diidentifikasi untuk penggunaan di seluruh organisasi (misalnya, spesifik informasi yang mungkin berguna dalam menentukan kemungkinan seperti kemampuan, maksud, dan sasaran penargetan). - Panduan untuk berbagai tingkat risiko organisasi (termasuk ketidakpastian) yang tidak memerlukan	Tidak	Ya	Ya *Jika tidak disediakan oleh Tingkat 2*

pertimbangan lebih lanjut. - Kriteria penentuan ketidakpastian. - Daftar peristiwa berisiko tinggi dari penilaian risiko sebelumnya. - Skala penilaian untuk menilai tingkat risiko sebagai kombinasi dari kemungkinan dan dampak, dianotasi oleh organisasi, jika perlu. (**Tabel 3.3**) - Skala penilaian untuk menilai tingkat risiko, yang dicatat oleh organisasi, jika diperlukan. (**Tabel 3.4**)			
Dari Tingkat 2: (Misi / tingkat proses bisnis) - Informasi dan panduan terkait risiko khusus untuk Tingkat 2 (misalnya, risiko dan ketidakpastian informasi terkait untuk misi / proses bisnis, segmen EA, infrastruktur umum, layanan dukungan, umum kontrol, dan dependensi eksternal).	*Ya Melalui RAR*	Ya *Melalui Teman Berbagi*	Ya
Dari Tingkat 3: (Tingkat sistem informasi) - Informasi dan panduan terkait risiko khusus untuk Tingkat 3 (misalnya, informasi kemungkinan mempengaruhi sistem informasi, teknologi informasi, komponen sistem informasi, aplikasi, jaringan, lingkungan operasi).	*Ya Melalui RAR*	*Ya Melalui RAR*	Ya *Melalui Teman Berbagi*

Tabel 3.18 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

Tnggi	Sangat Rendah	Rendah	Sedang	Tnggi	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

Tabel 3.19 SKALA PENILAIAN - TINGKAT RISIKO

Nilai Kualitatif	Nilai Semi-Kuantitatif		Deskripsi
Sangat Tinggi	96-100	10	**Risiko yang sangat tinggi** berarti bahwa suatu peristiwa ancaman dapat diperkirakan memiliki **beberapa parah atau** efek merugikan **bencana** pada operasi organisasi, aset organisasi,individu, organisasi lain, atau Bangsa.
Tinggi	80-95	8	**Berisiko tinggi** berarti bahwa peristiwa ancaman bisa diharapkan untuk memiliki **berat atau bencana** yang merugikan berpengaruh pada operasi organisasi, aset organisasi, individu, organisasi lain, atau Bangsa
Sedang	21-79	5	**Risiko sedang** berarti bahwa peristiwa ancaman dapat diharapkan memiliki efek buruk yang **serius** operasi organisasi, aset organisasi, individu, organisasi lain, atau Bangsa.
Rendah	5-20	2	**Risiko rendah** berarti bahwa peristiwa ancaman dapat diharapkan memiliki efek merugikan **terbatas** pada operasi organisasi, aset organisasi, individu, organisasi lain, atau Bangsa.
Sangat Rendah	0-4	0	**Risiko yang sangat rendah** berarti bahwa peristiwa ancaman dapat diharapkan memiliki efek buruk yang **dapat diabaikan** operasi organisasi, aset organisasi, individu, organisasi lain atau bangsa

3.7 Skala Likert

Skala likert merupakan skala yang di gunakan 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. Jawaban dari setiap pernyataan memiliki gradasi dari sangat negative hingga sangat positif. Sistem penilaian digunakan untuk mengetahui persepsi dari responden yang diminta untuk memberi penilaian sesuai fakta yang terdapat pada laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Responden diminta untuk memilih satu alternative jawaban yang telah disediakan seperti pada table 3.20.

Tabel 3.20 Pengukuran Skala Likert

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

3.8 Metode Analisis Data

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

Metthew B. Miles dan A. Michael (1992:20) Analisis Data Kualitatif merupakan upaya yang berkelanjutan, berulang, dan terus-menerus. Masalah reduksi data, penyajian data dan penarikkan kesimpulan/verifikasi menjadi

gambaran keberhasilan secara berurutan sebagai rangkaian kegiatan analisis yang saling susul-menyusul.

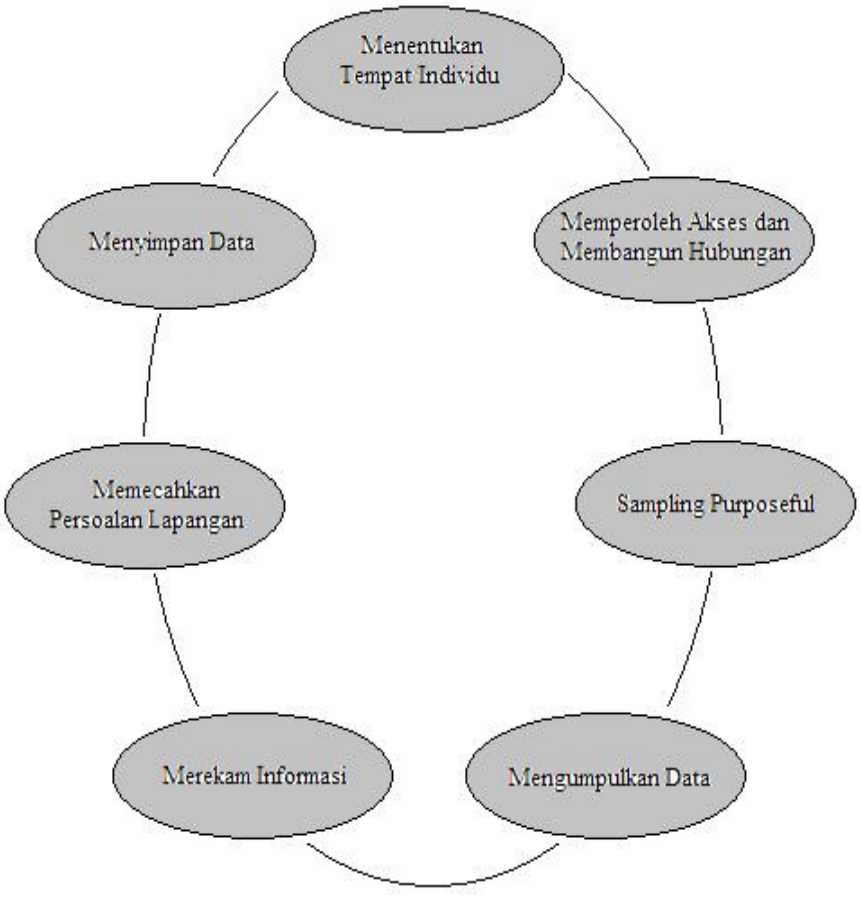
John W. Creswell (2014:59) Analisis Data Kualitatif merupakan penelitian yang dimulai dengan asumsi dan penggunaan kerangka penafsiran/teoritis yang membentuk atau mempengaruhi studi tentang permasalahan riset yang terkait dengan makna yang dikenakan oleh individu atau kelompok pada suatu permasalahan sosial atau pun manusia. Untuk mempelajari permasalahan ini para peneliti kualitatif menggunakan pendekatan mutahir dalam penelitian, pengumpulan data dalam lingkungan alamiah yang peka terhadap masyarakat dan tempat penelitian dan analisis data yang bersifat induktif maupun deduktif dan pembentukan sebuah pola atau tema. Laporan atau presentasi tertulis akhir mencangkup berbagai suara dari para partisipan, refleksivitas dari peneliti, deskripsi dan intepretasi tentang masalah penelitian dan kontribusinya pada literatur atau seruan bagi perubahan.

3.9. Metode Pengumpulan Data

John W. Creswell (2014:205) Pengumpulan data kualitatif merupakan dengan berfokus pada jenis data aktual dan prosedur pengumpulannya. Akan tetapi, pengumpulan data melibatkan lebih banyak dari itu. Pengumpulan data mencangkup 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. Dalam proses pengumpulan data dilapangan, para peneliti sering kali memilih untuk hanya melakukan wawancara dan pengamatan. Proses

pengumpulan data kualitatif harus peka terhadap hasil yang diharapkan. Sehingga, ada baiknya memvisualisasikan fase-fase pengumpulan data dengan mengunakan lingkaran aktifitas untuk mencangkup semua hingga data yang diinginkan dapat terkumpul dengan maksimal melalui teknik pengumpulan data kualitatif.

Dari keterangan di atas, John W. Creswell memberikan solusi untuk melaksanakan kegiatan pengumpulan data dengan menggunakan lingkaran aktivitas. Lingkaran aktivitas ini berguna untuk penyempurnaan dalam penggambil sampel data yang akan diperlukan penulis untuk melengkapi hasil penelitian secara kualitatif. Adapun lingkaran aktivitas pengumpulan data dapat di lihat pada gambar 3.1 dibawah ini.



Gambar 3.1 Lingkaran Aktivitas Pengumpulan Data Kualitatif

Adapun beberapa pendekatan-pendekatan dalam pengumpulan data pada riset kualitatif, yang di kualtifikasikan dalam empat bentuk data antara lain:

3.9.1 Pengamatan

Beberapa kegiatan yang harus dilakukan dalam melaksanakan pengamatanpada analisis data kualitatif merupakan sebagai berikut :

- Mengumpulkan catatan lapangan dengan melakukan pengamatan sebagai seorang partisipan
- Mengumpulkan catatan lapangan dengan melakukan pengamatan sebagai seorang pengamat
- Mengumpulkan catatan lapangan dengan menghabiskan lebih banyak waktu sebagai partisipan dari pada pengamat
- Mengumpulkan catatan lapangan dengan menghabiskan lebih banyak waktu sebagai pengamat dari pada partisipan.
- Mengumpulkan catatan lapangan pertama dengan mengamati sebagai “outsider” dan kemudian dengan masuk kedalam lingkungan dan mengamati sebagai seorang “insider”.

3.9.2 Wawancara

Beberapa kegiatan yang harus dilakukan dalam melaksanakan wawancara pada analisis data kualitatif merupakan sebagai berikut :

- Melaksanakan wawancara tak terstruktur, wawancara terbuka dan membuat catatan-catatan wawancara.
- Melaksanakan wawancara tak terstruktur, wawancara terbuka, merekam wawancara tersebut dan menulis wawancara tersebut.

- Melaksanakan wawancara semi terstruktur, merekam wawancara tersebut dan menulis wawancara tersebut.
- Melaksanakan wawancara kelompok fokus, merekam wawancara tersebut dan menulis wawancara tersebut.
- Melaksanakan beragam jenis wawancara : e-mail, tatap muka, kelompok fokus, kelompok fokus online, telepon.

3.9.3 Dokumen

Beberapa kegiatan yang harus dilakukan dalam membuat dokumen pada analisis data kualitatif merupakan sebagai berikut :

- Menulis catatan lapangan selama studi riset.
- Meminta seorang partisipan untuk memelihara jurnal atau diary selama studi riset tersebut.
- Mengumpulkan surat pribadi dari para partisipan.
- Menganalisis dokumen publik (misal : memo, notulen, rekaman, dan arsip resmi).
- Mempelajari autobiografi dan biografi.
- Meminta para patisipan untuk membuat foto atau video.
- Melaksanakan audit tabel.
- Meninjau rekam medis.

3.9.4 Bahan Audiovisual

Beberapa kegiatan yang harus dilakukan dalam membuat audiovisual pada analisis data kualitatif merupakan sebagai berikut :

- Mempelajari bukti jejak fisik (misal : telapak kaki di tanah)

- Merekam dalam video atau memfilmkan situasi sosial, individual, atau kelompok.
- Mempelajari halaman utama website
- Mengumpulkan suara (misal: musik, tawa, alarm)
- Mengumpulkan e-mail atau pesan diskusi dan pesan teks telepon (misal : facebook, twitter, Whatsapp).
- Mempelajari benda atau objek ritual favorit.


Universitas
Bina
Darma

BAB IV

GAMBARAN UMUM OBJEK PENELITIAN

4.1 Sejarah SMK Negeri 3 OKU

Pada awalnya, lebih kurang tahun 1974 SMK Negeri 3 Ogan Komering Ulu merupakan sekolah teknik swasta yang bernama Sekolah Teknik Menengah (STM) Korpri, yang didirikan oleh Korpri. (Korpri berdiri berdasarkan **Keppres Nomor 82 Tahun 1971. Tanggal 29 November 1971**), beralamat di Jalan Kapten M. Nur No. 295 Desa Sukaraya Kecamatan Baturaja Timur. Tahun 1981 – 1985 STM Korpri ini dipimpin oleh kepala sekolah yang bernama Drs. Syafiudin. Sebagai sekolah swasta tentu saja dengan segenap kesederhanaannya, dimana hanya memiliki ruang belajar sebanyak 3 (tiga) lokal dan ditambah 1 (satu) ruang praktik. Tenaga pendidik sebanyak 3 (tiga) orang guru tetap, 7 (tujuh) orang guru tidak tetap, dan 2 (dua) orang pegawai tetap dan 5 (lima) orang pegawai tidak tetap.

Kemudian pada tanggal 22 November 1985 STM Korpri Baturaja statusnya dinegerikan dengan Surat Keputusan Mendikbud Nomor : 0597/0/1985 dengan nama Sekolah Teknologi Menengah (STM) Negeri Baturaja, dengan kepala sekolah yang pertama bernama Drs. Nila Utama. Penerimaan pertama siswa baru tahun ajaran 1986/1987 berjumlah 144 orang siswa yang terdiri dari 2 (dua) jurusan, yaitu Jurusan Mesin dan Jurusan Bangunan.

Pada tahun 1989 Sekolah Teknologi Menengah (STM) Negeri Baturaja pindah alamat dengan menempati gedung baru yang berlokasi di Jalan Imam

Bonjol No. 695 Desa Tanjung Kemala Kecamatan Baturaja Timur (setelah terjadi pemekaran desa sekarang menjadi Desa Air Paoh Kecamatan Baturaja Timur).

Adapun gedung baru ini dibangun di atas tanah dengan luas 42.630 M2, dengan luas bangunan 5.829,25 M2, luas halaman dan taman 36.300,75 M2, luas lapangan tempat bermain dan olahraga 500 M2. Tanah lokasi SMK Negeri 3 OKU merupakan Sertipikat Hak Pakai No. 03 Badan Pertanahan Nasional Kantor Pertanahan Kabupaten Ogan Komering Ulu Nomor : 04.08.14.07.2.00003.

4.1.1 Visi

Menjadi pusat pendidikan yang unggul dan mampu menghasilkan lulusan tingkat menengah yang berstandar nasional, berwawasan lingkungan, berkarakter bangsa dan mampu bersaing di era global."

4.1.2 Misi

- Menumbuhkan secara intensif daya juang untuk mencapai keunggulan kompetitif bagi seluruh warga sekolah.
- Menerapkan berbagai metode pembelajaran yang inovatif, kreatif, edukatif, dan produktif sesuai jenis kompetensi yang akan dicapai dengan memanfaatkan teknologi informasi dan komunikasi (TIK).
- Mengoptimalkan sumber daya sekolah dalam memberikan pelayanan prima.
- Mengintegrasikan program yang dimiliki dengan jiwa wirausahaan, berbudaya lingkungan.

4.1.3 Tujuan

Adapun tujuan dari SMK Negeri 3 OKU adalah :

- Mempersiapkan peserta didik menjadi manusia produktif, mampu bekerja mandiri, dan dapat diserap oleh DU/DI sebagai tenaga kerja tingkat menengah sesuai dengan kompetensi yang dimilikinya.
- Memberikan pembekalan agar mampu berkarir, ulet dan giat dalam berkompetisi, mampu beradaptasi di lingkungan kerja dan dapat mengembangkan sikap profesional sesuai kompetensi yang dimilikinya
- Membekali peserta didik dalam ilmu pengetahuan, teknologi, seni dan wawasan entrepreneur agar mampu mengembangkan diri dikemudian hari baik secara mandiri maupun melanjutkan pada jenjang pendidikan lebih tinggi.

4.2 Profil SMK Negeri 3 OKU

SMK Negeri 3 OKU merupakan sekolah menengah kejuruan teknik pertama di Kabupaten Ogan Komering Ulu. Pada awal pendirian bernama Sekolah Teknik Menengah Korpri, dari awal berdiri tahun 1974 sampai sekarangtelah mengalami beberapa kali perubahan nama dan status. Saat ini, SMK Negeri 3 OKU merupakan sekolah negeri yang di miliki pemerintah Kabupaten Ogan Komering Ulu yang beralamatkan di Jalan M.S. Oeding No. 695 Desa Air Paoh Kecamatan Baturaja Timur Kabupaten Ogan Komering Ulu Provinsi Sumatera Selatan Telepon (0735) 320906 dengan NPSN 10604741 dan luas tanah 42630 m^2 serta luas bangunan 5511 m^2.

Pada awal didirikan SMK Negeri 3 OKU menyelenggarakan tiga Program Studi yaitu : Teknik Konstruksi Bangunan, Teknik Mesin Perkakas, dan Teknik Instalasi Listrik. Dalam perkembangannya dan sesuai dengan kebutuhan lokal, saat ini SMK Negeri 3 OKU membuka enam Program Keahlian yaitu : Teknik Bangunan, Teknik Survei dan Pemetaan, Teknik Ketenagalistrikan, Teknik Mesin, Teknik Otomotif, dan Teknik Komputer dan Informatika.

Dari enam program keahlian tersebut, terdapat delapan Kompetensi Keahlian, yaitu : Teknik Bangunan, (TKBB) Teknik Gambar Bangunan (TGB), Teknik Survei dan Pemetaan (TSP), Teknik Instalasi Tenaga Listrik (TITL), Teknik Pemesinan (TPM), Teknik Pengelasan (TPL), Teknik Kendaran Ringan (TKR), dan Teknik Komputer dan Jaringan (TKJ).

4.2.1 Data Siswa Dalam 3 Tahun Terakhir

Adapun data siswa dalam 3 tahun terakhir di SMK Negeri 3 OKU dapat dilihat pada tabel 4.1.

Tabel 4.1 Data Siswa SMK Negeri 3 OKU

Tahun Pelajaran	Jumlah Pendaftar (Calon Siswa Baru)	Kelas X		Kelas XI		Kelas XII		Total	
		Jml Siswa	Jml Rombel	Jml Siswa	Jml Rombel	Jml Siswa	Jml Rombel	Jml Siswa	Jml Rombel
2016/2017	763	515	14	428	12	379	12	1322	38
2017/2018	800	432	12	486	14	408	12	1326	38
2018/2019	616	432	12	387	12	459	14	1277	38

4.2.2 Data Guru

Adapun data guru pada tahun ajaran 2017/2018 di SMK Negeri 3 OKU dapat dilihat pada tabel 4.2.

Tabel 4.2 Data Guru SMK Negeri 3 OKU

Jumlah Guru/Staf	Bagi Sekolah Negeri
Guru tetap (PNS)/GTY Sekolah Swasta	72
Guru tidak tetap (GTT)	24
Staf TU Tetap (PNS)	3
Staf TU Tidak Tetap (PTT)	17

4.2.3 Data Ruang Kelas

Adapun data ruang untuk kegiatan belajar mengajar di SMK Negeri 3 OKU dapat dilihat pada tabel 4.3.

Tabel 4.3 Data Ruangan SMK Negeri 3 OKU

Uraian	Jumlah Ruang
Ruang Kelas Asli	24
Ruang lainnya yang digunakan sebagai ruang belajar	1
Bengkel Mesin	2
Bengkel Bangunan	4
Bengkel Listrik	3
Bengkel TKR	2
Bengkel TKJ	3
Jumlah Ruang Kelas Seluruh	**39**

4.2.4 Struktur Organisasi SMK Negeri 3 OKU

Sebagai lembaga pendidikan negeri, dalam susunan kepegawaian dan struktur organisasi SMK Negeri 3 OKU wajib mengikuti organisasi induk yaitu Dinas Pendidikan Kabupaten Ogan Komering Ulu. Terdapat dua sistem kepegawaian yang ada di SMK Negeri 3 OKU yaitu pendidik (guru) dengan tugas pokok mengajar, melatih, dan mendidik siswa serta tenaga kependidikan (tata usaha) sebagai tenaga pendukung dalam penyelenggaraan pendidikan di sekolah.

Beberapa jabatan yang terdapat di SMK Negeri 3 OKU antara lain Kepala Sekolah, Wakil Kepala Sekolah, Kepala Program Keahlian, Kepala Bengkel/Lab, Kepala Perpustakaan, Koordinator BP/BK, Ketua Unit Produksi, dan Pembina Bidang Kegiatan. Kemudian dari sisi kepegawaian (tenaga kependidikan), terdapat Koordinator Kepegawaian, Bendahara Rutin, Bendahara BOS, dan Pengelola Bidang Kegiatan. Secara lengkap struktur organisasi SMK Negeri 3 OKU untuk tahun pelajaran 2017/2018 ditampilkan pada gambar 4.1 berikut ini:

Gambar 4.1 Struktur Organisasi SMK Negeri 3 OKU

4.3 Sejarah Teknik Komputer dan Jaringan SMK N 3 OKU

Program studi Teknik Komputer dan Jaringan didirikan pada tahun ajaran 2003/2004 tepatnya pada bulan agustus 2003. Sejarah terbentuknya Program studi Teknik Komputer dan Jaringan, pada awal tahun ajaran 2003/2004 kepala SMK Negeri 3 OKU bapak Drs. Sidarta, SE selaku koordinator jaringan sekolah kabupaten Ogan Komering Ulu diundang rapatkoordinasi Jaringan Informasi Sekolah (JIS) direktorat sekolah menengah kejuruan di Jakarta. Dalam rapat tersebut Direktur Dikmenjur meminta sekolah – sekolah kejuruan yang ada di Indonesia membuka jurusan Teknik Informatika dan Komputer. Sekembalinya Kepala SMK Negeri 3 OKU dari rapat koordinasi dari Jakarta, para guru SMK Negeri 3 OKU mengadakan rapat dengan putusan menyepakati bersama untuk membuka jurusan Teknik Komputer.

Berhubung penerimaan siswa baru telah dilaksanakan dan tidak memungkinkan untuk membuka pendaftaran siswa baru, maka disepakati siswa untuk angkatan pertama jurusan Teknik Komputer dan Jaringan diambil dari siswa baru pada jurusan lain.Pada awal pendirian Teknik Komputer dan Jaringan memiliki fasilitas 2 ruang laboratorium dan 22 unit komputer, sebelum dibukanya jurusan Teknik Komputer dan Jaringan para guru SMK Negeri 3 OKU sering mengadakan pelatihan jaringan yang berpusat di perpustakaan SMK Negeri 3 OKU. Dalam materi silabus tingkat 1 jurusan Teknik Komputer dan Jaringan murni tentang perakitan komputer maka dengan modal komputer SMK Negeri 3 OKU dapat laksanakan kegiatan pelajaran dengan baik meskipun perangkat jaringan belum memadai.

4.3.1 Data Peralatan dan Perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

Dari awal berdiri pada tahun 2003 sampai saat ini, bidang keahlian Teknik Komputer dan Jaringan hanya mendapatkan satu kali bantuan oleh pemerintah. Bantuan itu dikirim pada awal tahun 2008 berupa 32 perangkat komputer zyrex dengan komponen-komponen terpisah yang belum dirakit menjadi satu. Perakitan komputer-komputer tersebut dilakukan 2 kali pengerjaan selama 1 tahun. Fasilitas pendukung yang ada di laboratorim TKJ antara lain 4 hub, 4 switch, 4 lan tester, 6 krimping tool, kabel UTP dengan sambungan konektor RJ 45, 2 router sisco, 1 switch sisco, 4 router microtik, dan 10 access point. Peralatan ini sudah sangat membutuhkan perawatan dikarenakan usia perangkat-perangkat tersebut sudah lama. Dan dalam hal ini kepala bengkel TKJ diharuskan bekerja ekstra dalam merawat perangkat-perangka jaringan komputer yang ada pada laboratorium TKJ SMK Negeri 3 OKU.

Data peralatan pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dapat dilihat pada tabel 4.4. Untuk Data Perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dapat dilihat pada tabel 4.5.

Tabel 4.4 Daftar Peralatan Jaringan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

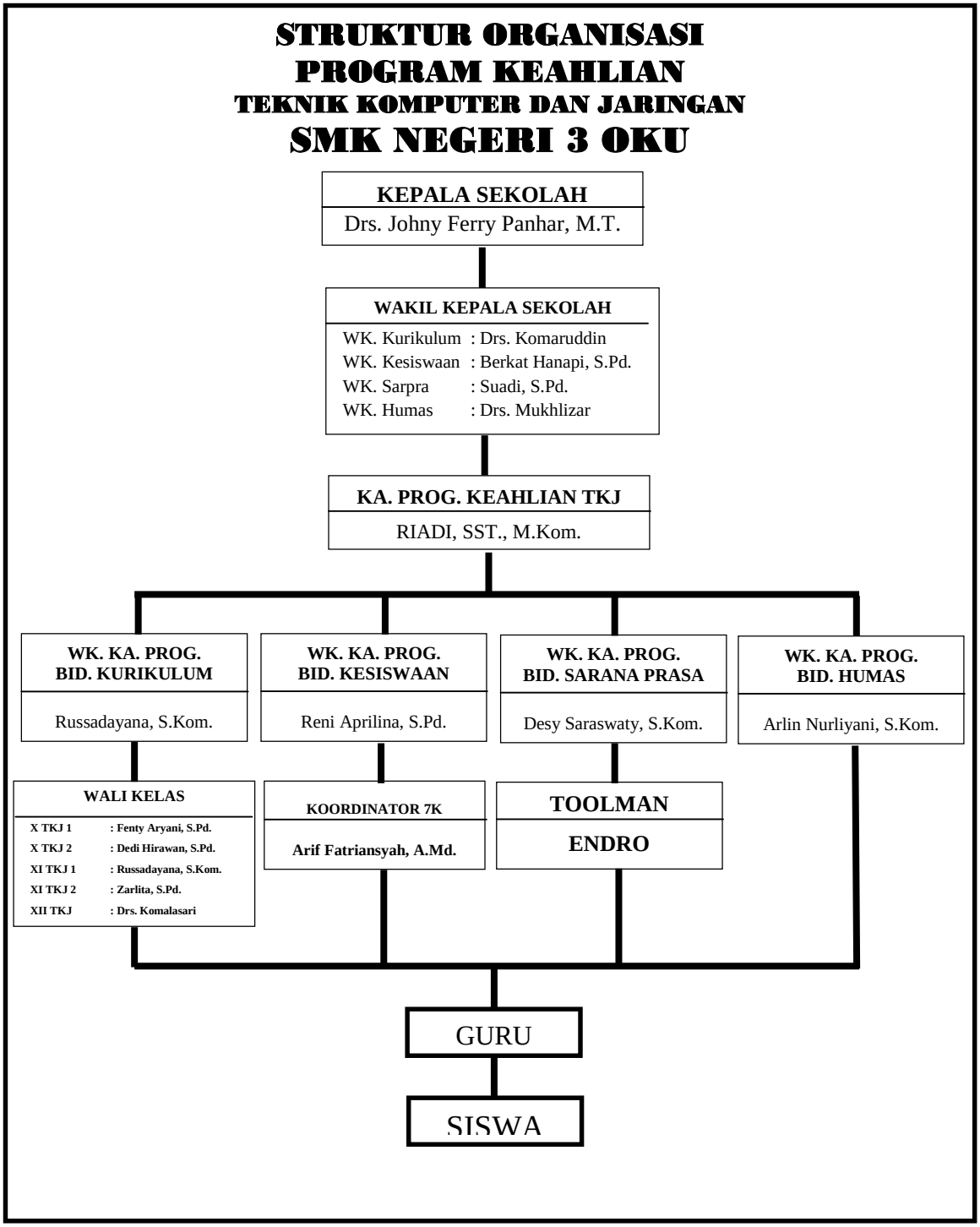
No	Peralatan	Jumlah	Keterangan
1	Monitor	46 unit	36 Baik , 10 Rusak
2	PC CPU	46 unit	32 Baik , 14 Rusak
3	PC Dekstop	102 unit	102 Baik
4	Laptop	10 unit	10 Baik
5	Headphone	146 unit	144 Baik , 2 Rusak
6	Keyboard	146 unit	134 Baik , 12 Rusak
7	Mouse	146 unit	144 Baik , 2 Rusak
8	Kabel UTP	1000 meter	910 Baik, 90 Rusak
9	Konektor RJ45	300 buah	300 Baik
10	Hub/Switch	15 unit	13 Baik , 2 Rusak
11	PC Server	6 unit	5 Baik , 1 Rusak
12	Lan Tester	8 buah	7 Baik, 1 Rusak
13	Krimping Tools	15 buah	10 Baik, 5 Rusak
14	Accesspoint	3 unit	3 Baik
15	Router Cisco	2 unit	2 Baik
16	Router Mikrotik	4 unit	4 Baik
17	Wireless Router	2 unit	2 Baik
18	Obeng +/-	20 buah	10 Obeng + , 10 Obeng -
19	Vacum	1 unit	1 Baik
20	Lan Card	51 buah	42 Baik , 9 Rusak
21	Terminal Adapter	50 unit	50 Baik
22	Stabilizer (stavol)	37 unit	50 Baik
23	UPS	7 unit	5 Baik , 2 Rusak
24	CD/DVD Rom External	7 unit	6 Baik , 1 Rusak
25	Speaker	3 unit	3 Baik
26	Printer	5 unit	3 Baik , 2 Rusak
27	Proyektor	5 unit	3 Baik , 2 Rusak
28	Kuas Pembersih	5 buah	5 Baik
29	Tang	5 buah	3 Baik
30	Antena Grid	2 unit	2 Baik

Tabel 4.5 Data Perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

No	Nama Barang	Merek	Bahan	Tahun Pembuatan/ Pembelian	Jumlah Barang/ Regester	Perolehan Harga Beli	Keadaan	Ket
1	Meja Guru ½ Biro	Lokal	Multi Plek	1990	3 Buah	Proyek ADB	Baik	
2	Meja Guru ½ Biro	Lokal	Multi Plek	2014	3 Buah	Dana APBN	Baik	
3	Kursi Jok Hitam	Lokal	Busa/Kayu	1990	1 Buah	Proyek ADB	Baik	
4	Kursi Putar	Lokal	Busa/Besi	2014	1 Buah	Dana PSG	Baik	
5	Kursi Plastik	Twin-Fan	Plastik	2014	108 Buah	Dana PSG	Baik	
6	Rak Kayu	Lokal	Kayu	2013	1 Buah	Dana PSG	Baik	
7	Lemari Kayu/Kaca	Lokal	Kayu	2014	2 Buah	Dana PSG	Baik	
8	Lemari Besi	Elite	Besi	1990	1 Buah	Proyek ADB	Baik	
9	Lemari Besi	Yunika	Besi	2013	2 Buah	Dana PSG	Baik	
10	AC	Gree ½ PK		2016	1 Unit	Dana BOS	Kurang Baik	
11	Meja Siswa	Lokal	Kayu	2014	36 Buah	Dana PSG	Baik	
12	Blower			2015	1 Buah	Dana PSG	Baik	
13	Kipas Angin	Miyoko	Plastik	2014	1 Buah	Dana PSG	Baik	
14	Meja Komputer	Lokal	Kayu	2008	32 Buah	Dana APBD	Baik	
15	Meja Praktek	Lokal	Kayu/Besi	2008	3 Buah	Dana APBD	Baik	

4.3.2 Struktur Organisasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

Struktur organisasi dalam laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU disesuaikan dengan struktur organisasi pada program keahlian Teknik Komputer dan Jaringan. Dan struktur organisasi laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dapat di lihat pada gambar 4.2.



Gambar 4.2 Struktur Organisasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

4.4 Jaringan Komputer di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

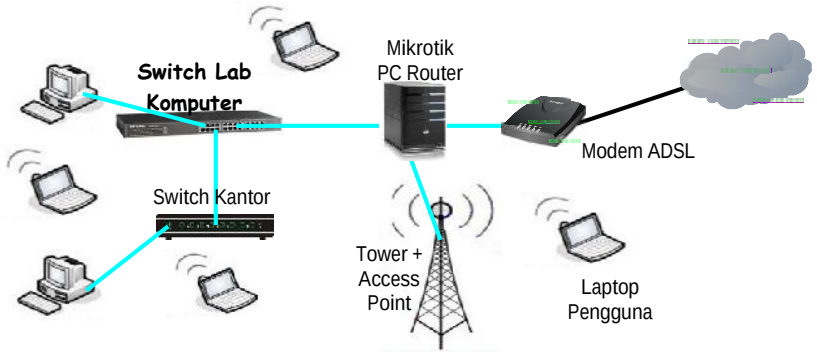
Laboratorium Teknik Komputer dan Jaringan memiliki tiga ruangan antara lain Laboratorium Perakitan, Laboratorium Multimedia dan Laboratorium Jaringan. Ketiga laboratorium yang ada memiliki fungsi yang berbeda sesuai dengan kebutuhan para siswa dan guru untuk melakukan kegiatan belajar mengajar. Laboratorium Perakitan di gunakan untuk melakukan kegiatan pembelajaran tentang sistem perakitan komputer seperti membongkar PC, melakukan perawatan PC, memperbaiki PC, dan sejenisnya. Laboratorium Multimedia digunakan untuk kegiatan yang bersangkutan dengan software komputer seperti membuat program aplikasi, membuat web, mengenal database, mempelajari microsoft office dan sebagainya. Sedangkan Laboratorium Jaringan diperuntukan untuk siswa mempelajari jaringan komputer seperti pengkoneksian jaringan, membuat kabel jaringan, mensetting router, setting keamanan jaringan dan lainnya.

Dari ketiga laboratorium tersebut, jaringan yang telah dipasang permanen hanya pada Laboratorium Multimedia. Hal ini disebabkan Laboratorium Multimedia digunakan sebagai tempat pengelolahan software, karena dari itu Laboratorium Multimedia telah dipasang jaringan secara permanen. Sedangkan dua laboraorium lain jaringan terpasang apabila akan digunakan. .

Jaringan internet pada SMK Negeri 3 OKU menggunakan jaringan Indi Home dari Telkom. Jaringan internet tersebut terhubung dengan menggunakan jaringan fiber optik dengan kecepatan 20 Mbps. Router yang dipakai

menggunakan router ISR dari telkom yang berfungsi sebagai router, internet gateway, DHCP server, wifi hotspot dan internet security.Dengan lokasi SMK Negeri 3 OKU yang luas dan struktur tanah yang bertingkat, sehinggadibuatlah wireless LAN yang menggunakan teknologi WiFi di lingkungan SMK Negeri 3 OKU. Jaringan wireless LAN yang ada pada saat ini, belum dapat menjangkau keseluruhan lokasi yang ada di SMK Negeri 3 OKU. Jaringan wireless LAN hanya dipergunakan oleh user untuk mengakses layanan hotspot yang tersedia di SMK Negeri 3 OKU. Untuk jaringan wireless LAN SMK Negeri 3 OKU, perangkat yang digunakan adalah :

1. Access Point (AP) outdoor sebanyak satu unit.
2. PC Router Mikrotik yang sekaligus difungsikan sebagai Web Proxy untuk otentikasi pengguna hotspot.
3. Tower Three Angle setinggi 48 meter, tempat dipasangnya AP Outdoor.
4. Antena Omni Directional sebanyak satu unit.
5. PC pengguna yang dilengkapi dengan Wireless Adapter Client sebanyak 5 unit masing-masing di Bengkel Teknik Mesin, Bengkel Teknik Bangunan, Bengkel Teknik Listrik, Ruang Perpustakaan, dan Ruang AutoCAD dan laptop pengguna, baik guru, pegawai, maupun siswa.



Gambar 4.3 Skema Jaringan Komputer SMK Negeri 3 OKU

4.5 Kuesioner

Dalam penelitian ini, kuesioner yang di buat merujuk pada metode *NIST SP 800-30r1*. Kuesioner ini telah disesuaikan dengan pernyataan yang terdapat dalam modul dokumen *NIST SP 800-30r1*. Untuk mendapatkan penilaian secara objektif, penulis menggunakan angka 1 sampai 5 untuk melambangkan tingkatan penilaian. Kuesioner ini akan diisi oleh narasumber/responden yang memahami tentang manajemen Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Adapun pertanyaan dan pernyataan yang terdapat pada kuesioner dapat dilihat di bawah ini.

1. **Pilih skala penilaian sumber dan peristiwa ancaman yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan yang pernah di hadapi oleh Bapak/Ibu beri tanda (X) pada pernyataan yang sesuai dengan risiko yang di alami.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Ancaman yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
2	Ancaman yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
3	Ancaman yang di bawa oleh *TrustedInsider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Accidential						
4	Ancaman dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
5	Ancaman dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Structural						
6	Ancaman dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya					
7	Ancaman dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya					
8	Ancaman dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya					
9	Ancaman dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya					
10	Ancaman dari kegagalan sistem operasi yang melebihi					

	perkiraan operasi					
11	Ancaman dari kegagalan jaringan karena penuaan dan penipisan sumber daya					
12	Ancaman dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat					
Environmental						
13	Ancaman dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
14	Ancaman dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
15	Ancaman dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
16	Ancaman dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					

2. Pilih skala penilaian daritingkat kerentanan keamanan dan kondisi predisposisi yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan apa yang dihadapi Bapak/Ibu dengan memberikan tanda (X) pada pernyataan yang sesuai.

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
2	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
3	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *TrustedInsider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Accidential						
4	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
5	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Structural						
6	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya					
7	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya					
8	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya					

9	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kontrol suhu ruangan karena penuaan sumber daya					
10	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan sistem operasi yang melebihi perkiraan operasi					
11	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan jaringan karena penuaan dan penipisan sumber daya					
12	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat					
Environmental						
13	Kerentanan dan kondisi predisposisi yang di sebabkan api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
14	Kerentanan dan kondisi predisposisi yang di sebabkan angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
15	Kerentanan dan kondisi predisposisi yang di sebabkan Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
16	Kerentanan dan kondisi predisposisi yang di sebabkan Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					

3. Bagaimana menurut Bapak/Ibu tentang kemungkinan ancaman yang terjadi pada laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pilih salah satu dari pernyataan dibawah ini, beri tanda (X) pada pernyataan yang sesuai dengan kejadian yang terjadi.

No	**Deskripsi**	**1**	**2**	**3**	**4**	**5**
Adversarial						
1	Besarnya kemungkinan ancaman yang di dapat dari *Outsider*/orang luar saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
2	Besarnya kemungkinan ancaman yang di dapat dari *Insider*/orang dalam saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
3	Besarnya kemungkinan ancaman yang di dapat dari *TrustedInsider*/orang Kepercayaan saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Accidential						
4	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
5	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					

Structural						
6	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya					
7	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya					
8	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya					
9	Besarnya kemungkinan ancaman yang di dapat dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya					
10	Besarnya kemungkinan ancaman yang di dapat dari kegagalan sistem operasi yang melebihi perkiraan operasi					
11	Besarnya kemungkinan ancaman yang di dapat dari kegagalan jaringan karena penuaan dan penipisan sumber daya					
12	Besarnya kemungkinan ancaman yang di dapat dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat					
Environmental						
13	Besarnya kemungkinan ancaman yang di dapat dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
14	Besarnya kemungkinan ancaman yang di dapat dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
15	Besarnya kemungkinan ancaman yang di dapat dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
16	Besarnya kemungkinan ancaman yang di dapat dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					

4. Pilih skala nilai dari dampak yang akan muncul di Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU dari risiko yang sering dihadapi, isi sesuai dengan beri tanda (X) isi pernyataan berikut.

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya dampak yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
2	Besarnya dampak yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
3	Besarnya dampak yang di bawa oleh *TrustedInsider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Accidential						
4	Besarnya dampak dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik					

	Komputer dan Jaringan SMK Negeri 3 OKU					
5	Besarnya dampak dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Structural						
6	Besarnya dampak dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya					
7	Besarnya dampak dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya					
8	Besarnya dampak dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya					
9	Besarnya dampak dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya					
10	Besarnya dampak dari kegagalan sistem operasi yang melebihi perkiraan operasi					
11	Besarnya dampak dari kegagalan jaringan karena penuaan dan penipisan sumber daya					
12	Besarnya dampak dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat					
Environmental						
13	Besarnya dampak dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
14	Besarnya dampak dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
15	Besarnya dampak dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
16	Besarnya dampak dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					

5. Pilih nilai dari tingkat Risiko yang berpengaruh pada Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan risiko yang dihadapi dan beri tanda (X) pada pernyataan berikut.

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya risiko yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
2	Besarnya risiko yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
3	Besarnya risiko yang di bawa oleh *TrustedInsider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
Accidential						
4	Besarnya risiko dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
5	Besarnya risiko dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					

Structural						
6	Besarnya risiko dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya					
7	Besarnya risiko dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya					
8	Besarnya risiko dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya					
9	Besarnya risiko dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya					
10	Besarnya risiko dari kegagalan sistem operasi yang melebihi perkiraan operasi					
11	Besarnya risiko dari kegagalan jaringan karena penuaan dan penipisan sumber daya					
12	Besarnya risiko dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat					
Environmental						
13	Besarnya risiko dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
14	Besarnya risiko dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
15	Besarnya risiko dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					
16	Besarnya risiko dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU					


Universitas
Bina
Darma

BAB V

PEMBAHASAN

5.1 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 penulis 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.

Dalam penelitian ini, responden yang masuk dalam analisis penulis dan cocok sebagai responden yang akan di wawancarai berjumlah 5 orang. Sebagai bukti tertulis, penulis juga memberikan kuesioner kepada responden sebagai berkas untuk melengkapi penelitian. Ketika wawancara kepada responden, penulis tidak lupa merekam percakapan dari para responden yang telah penulis pilih sebagai narasumber di penelitian ini.

5.2 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 5.1.

Tabel 5.1 Data Responden *Assessment IT Risk Management* Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

No	Nama	Jabatan	Masa Kerja	Keterangan
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

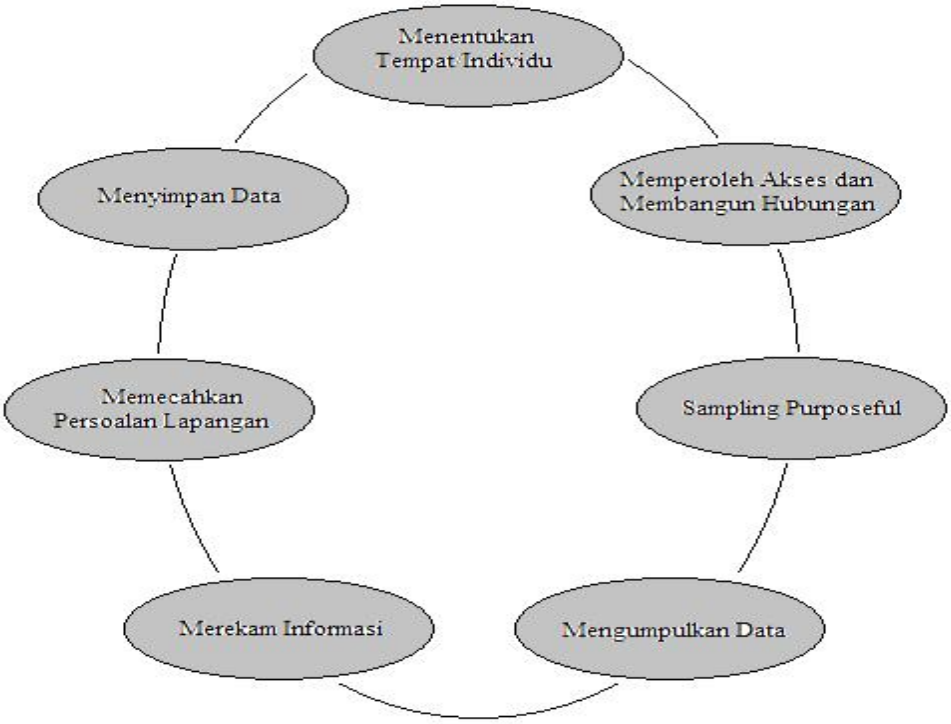
5.3 Hasil Penelitian

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.

Dan dalam hal ini, penulis melakukan kegiatan *assesment risk management* dengan mengikuti prosedur metode *NIST SP 800-30r1*. Lankah-langkah yang dilakukan penulis dalam penelitian ini antara lain *Prepare for Assessment, Conduct Assessment, Communicate Results,* dan *Maintain Assessment.*

5.4 *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 dapat dilihat pada gambar 5.1.



Gambar 5.1 Aktivitas-Aktivitas Pengumpulan Data

5.4.1 Menentukan Tempat/Individu

Dalam penelitian ini, penulis telah menentukan tempat terlaksananya kegiatan penelitian ini. Di halaman sebelumnya, penulis telah menjelaskan bahwa penulis akan melaksanakan kegiatan di Laboratorium Teknik

Komputer dan Jaringan SMK Negeri 3 OKU. Penulis akan melaksanakan kegiatan penelitian mengenai *Assessment IT Risk Management*.

5.4.2 Memperoleh Akses dan Membangun Hubungan

Sebelum melakukan penelitian secara lanjut, penulis telah berkoordinasi dengan jajaran staf dan kepala SMK Negeri 3 OKU. Untuk melaksanakan penelitian, penulis telah melakukan administrasi dengan baik dalam memasuki kawasan penelitian. Didalam kawasan penelitian, penulis dibantu pembimbing yang berasal dari SMK Negeri 3 OKU.

5.4.3 *Sampling Purposeful*

Pada penelitian ini, sampel yang diambil tidak banyak hanya narasumber yang mengajar penuh di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU atau lebih tepatnya guru pada matapelajaran produktif yang mengajar menggunakan ruang Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selain itu pula yang menjadi narasumber pada penelitian ini adalah staf yang mengelolah Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Responden yang dapat memberikan keterangan tentang keadaan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU berjumlah 5 orang responden.

5.4.4 Mengumpulkan Data

Pengumpulan data yang dilakukan dengan melakukan pengamatan selama beberapa bulan pada kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Kemudian melakukan pendekatan dengan melakukan wawancara kepada narasumber untuk mencari tahu

keadaan yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selain itu juga penulis meminta izin untuk melihat dokumen yang berkaitan dengan manajemen/pengelolaan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU kepada kepala bengkel Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

5.4.5 Merekam Informasi

Untuk merekam informasi penulis mendokumentasikan dengan melakukan wawancara kepada setiap responden dan merekam wawancara tersebut menggunakan video. Tidak hanya itu, penulis mengajukan kuesioner kepada responden yang telah disesuakan dengan dokumen *NIST SP 800-30r1*. Sebagai prosedur dari penelitian yang telah dilakukan penulis pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

5.4.6 Persoalan Lapangan

Terkadang dalam setiap penelitian tidak selalu berjalan mulus, saat melakukan penelitian terdapat kendala yang dihadap penulis. Dari pengamatan yang dilakukan penullis, persoalan yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU adalah kurangnya pendokumentasian/pendataan peralatan. Dalam hal ini, penulis pun melakukan pendataan dengan dibantu responden dalam membuat dokumentasi.

5.4.7 Menyimpan Data

Sebagai prinsip penyimpanan dan penanganan data yang telah dilakukan dalam pengumpulan data pada penelitian ini. Penulis membuat

softcopy dokumen video wawancara dan scan kuesioner yang telah penulis lakukan dengan responden. Agar semuanya aman, penulis memback-up ulang file tersebut ke email.

5.5 *Conduct Assessment*

Setelah melakukan perencanaan penilaian, proses selanjutnya adalah *conduct assessment* yang merupakan tahapan penilaian risiko. Untuk mendapatkan hasil dari tahapan *conduct assessment* penulis melakukan wawancara terhadap 5 responden yang merupakan bagian dari tim pelaksanan teknis yang terdapat pada manajemen Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Kelima responden ini juga merupakan guru yang mengajar pada mata pelajaran produktif untuk jurusan Teknik Komputer dan Jaringan di SMK Negeri 3 OKU.

Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU memiliki 3 ruang yaitu laboratorium perakitan, laboratorium multimedia dan laboratorium jaringan. Pada tahap *conduct asssessment* 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. Selanjutnya, proses *Conduct Assessment* memiliki lima poin penilaian yaitu *Identity Threat Sources and Events, Identity Vulnerability and Predisposing Conditions, Determine Likelihood of Occurrence, Determine magnitude of Impact,* dan *Determine Risk.* Pada

tahapan ini akan di ketahui nilai risiko yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Penilaian yang dilakukan meliputi sumber dan peristiwa ancaman, kerentanan dan kodisi predisposisi, kemungkinan yang terjadi, dampak dari ancaman, dan risiko yang terjadi.

5.5.1 *Identity Threat Sources and Events*

Untuk mengidentifikasi ancaman pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, maka dilakukan *assessment* pada sumber ancaman. Sebelum melakukan *assessment*, maka tentukan terlebih dahulu sumber ancaman yang akan dilakukan penilaian. Untuk skala penilaian dari *Identity Threat Source and Event* dapat dilihat pada tabel 5.2.Pada tabel 5.2 dapat dilihat ada 16 *Threat source* dan terbagi dalam 4 kategori yang akan dilakukan penilaian. 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*.

Tabel 5.2 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
Accidential				
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

Dari hasil kuesioner yang dibagikan kepada responden, maka di dapat skala penilaian sebagai berikut. Pada *threat source* kategori *advesarial*, ketiga poin yaitu sumber ancaman *Outsider, Insider,* dan *Trusted Insider* memiliki nilai kualitatif sedang. Kemudian pernyataan didapat dari karakteristik kemampuan *adversary* bahwa *adversary* memiliki sumber daya, keahlian dan peluang sedang dalam melakukan ancaman. Dari tujuan*adversary* didapat juga bahwa *adversary* dapat memperoleh/memodifikasi informasi kritis yang bisa mengacaukan sumber daya *cyber.* Dan pada target *adversary* didapat bahwa *adversary* menganalisis informasi yang ttersedia untuk menagetkan nilai tinggi dalam kemunculn risiko pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selanjutnya, *threat source* pada kategori *accidential* yaitu *user* dan *administrator;*kategori *structural* yaitu alat penyimpanan, alat pemrosesan, alat komunikasi, kontrol suhu ruangan, sistem operasi, alat jaringan, dan virus; serta kategori *evironmental* yaitu api, angin/hujan badai, telekomunikasi, dan tenaga listrik mendapatkan nilai kualitatif sedang. Sehingga mendapatkan pernyataan dari karakteristik ancaman yang mempengaruhi bahwa efek yang didapat dari ancaman tersebut

sangat luas serta melibatkan sumber daya yang sangat signifikan jika ancaman hadir.

5.5.2 *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. Untuk skala penilaian dari *Identity Vulnerability and Predisposing Conditions* dapat dilihat pada tabel 5.3.Dari tabel 5.3 dapat dilihat ada 16 *Threat source* dan terbagi dalam 4 kategori yang akan dilakukan penilaian. Dalam mendapatkan nilai semi kualitatif pada skala penilaian, jumlah nilai dari penilaian responden diwajibkan berada pada perbandingan skala 100 dan nilai kualitatif didapat dari nilai semi kualitatif yang telah ditentukan oleh metode *NIST SP 800-30r1*.

Tabel 5.3 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 dalam	3+1+1+3+1	36	Sedang
3	*TrustedInsider*/orang Kepercayaan	1+1+1+1+2	24	Sedang
Accidential				
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

Pada hasil kuesioner yang dibagikan kepada responden, di dapat skala penilaian sebagai berikut. Pada *threat source* kategori *advesarial*, ketiga poin yaitu sumber ancaman *Outsider, Insider,* dan *Trusted Insider;* kategori *accidential* yaitu *user* dan *administrator;* kategori *structural* yaitu alat penyimpanan, alat pemrosesan, alat komunikasi, kontrol suhu ruangan, sistem operasi, alat jaringan, dan virus; serta kategori *evironmental* yaitu api, angin/hujan badai, telekomunikasi, dan tenaga listrik mendapatkan nilai kualitatif sedang pada penilaian *identity vulneraility and predisposing conditions*. Sehingga mendapatkan pernyataan bahwa kekwatiran akan kerentanan masih pada posisi sedang sehingga kemudahan eksploitasi dan dampak yang mengancam pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU masih dapat dikendalikan keamanannya secara relevan. Dan pada kondisi predisposising berlaku pada banyak kegiatan yang sedang berproses di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

5.5.3 *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. Untuk skala penilaian dari *Determine*

Likelihood of Occurrence dapat dilihat pada tabel 5.4.Dari tabel 5.4 dapat dilihat ada 16 *Threat source* dan terbagi dalam 4 kategori yang akan dilakukan penilaian. Dan untuk mendapatkan nilai semi kualitatif pada skala penilaian, jumlah nilai dari penilaian responden diwajibkan berada pada perbandingan skala 100 dan nilai kualitatif didapat dari nilai semi kualitatif yang telah ditentukan oleh metode *NIST SP 800-30r1*.

Tabel 5.4 Skala Penilaian –*Determine Likelihood of Occurence*

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
Accidential				
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

Hasil kuesioner yang dibagikan kepada responden, di dapat skala penilaian sebagai berikut. Pada *threat source* kategori *advesarial,* ketiga poin yaitu sumber ancaman *Outsider, Insider,* dan *Trusted Insider;* mendapatkan nilai kualitatif sedang pada penilaian *Determine likelihood of occurrence* sehingga dapat dikatakan*adversary* agak cenderung memulai

paristiwa yang mengancam Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Sedangkan, kategori *accidential* yaitu *user* dan *administrator;* kategori *structural* yaitu alat penyimpanan, alat pemrosesan, alat komunikasi, kontrol suhu ruangan, sistem operasi, alat jaringan, dan virus; serta kategori *evironmental* yaitu api, angin/hujan badai, telekomunikasi, dan tenaga listrik mendapatkan nilai kualitatif sedang pada penilaian*Determine likelihood of occurrence* dan didapat bahwa kemungkinan kecelakaan, kesalahan dan bencana agaknya akan mungkin terjadi antara 1 sampai 10 kali dalam setahun. Untuk mengakibatkan dampak buruk pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU ketika terjadi peristiwa ancaman akan agak cenderung menimbulkan dampak buruk pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

5.5.4 *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. Untuk skala penilaian dari *Determine magnitude of impact* dapat dilihat pada tabel 5.5.Dalam tabel 5.5 dapat dilihat ada 16 *Threat source* dan terbagi dalam 4 kategori yang akan dilakukan penilaian. Sehingga untuk mendapatkan nilai semi kualitatif pada skala penilaian, jumlah nilai dari penilaian responden diwajibkan berada pada

perbandingan skala 100 dan nilai kualitatif didapat dari nilai semi kualitatif yang telah ditentukan oleh metode *NIST SP 800-30r1*.

Tabel 5.5 Skala Penilaian –*DetermineMagnitude 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	*TrustedInsider*/orang Kepercayaan	1+2+1+1+3	32	Sedang
Accidential				
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

Dalam hasil kuesioner yang dibagikan kepada responden, di dapat skala penilaian sebagai berikut. Dari *threat source* kategori *advesarial*, ketiga poin yaitu sumber ancaman *Outsider*, *Insider,* dan *Trusted Insider;* kategori *accidential* yaitu *user* dan *administrator;* kategori *structural* yaitu alat penyimpanan, alat pemrosesan, alat komunikasi, kontrol suhu ruangan, sistem operasi, alat jaringan, dan virus; serta kategori *evironmental* yaitu api, angin/hujan badai, telekomunikasi, dan tenaga listrik mendapatkan nilai kualitatif sedang pada penilaian *Determine Magnitude of impact.* Sehingga didapat bahwa dampak yang terjadi

ketika ada ancaman diperkirakan efek buruk yang serius dapat muncul pada kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Dapat memunculkan kerusakan yang disignifikan terhadap aset yang ada dan efektifitas fungsi dari peralatan menghasilkan kerugian yang signifikan.

5.5.5 *Determine Risk*

Kemudian menentukan risiko ancaman yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, saat dilakukan *assessment* pada risiko ancaman yang disebabkan oleh sumber ancaman. Untuk skala penilaian dari *Determine risk* dapat dilihat pada tabel 5.6.Dari tabel 5.6 dapat dilihat ada 16 *Threat source* dan terbagi dalam 4 kategori yang akan dilakukan penilaian. Untuk mendapatkan nilai semi kualitatif pada skala penilaian, jumlah dari 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*.

Tabel 5.6 Skala Penilaian –*Determine Risk* (Responden)

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+2+3	52	Sedang
2	*Insider*/orang dalam	1+3+3+2+3	48	Sedang
3	*TrustedInsider*/orang Kepercayaan	1+1+3+1+3	32	Sedang
Accidential				
4	*User*	1+3+4+2+3	52	Sedang
5	*Administrator*	1+2+1+1+3	32	Sedang
Structural				
6	Alat Penyimpanan	3+3+1+2+2	44	Sedang
7	Alat Pemrosesan	3+3+1+2+3	48	Sedang

8	Alat Komunikasi	3+3+3+2+3	56	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+2+2	40	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+2+3	60	Sedang
15	Telekomunikasi	1+2+4+1+3	44	Sedang
16	Tenaga Listrik	2+4+4+2+3	60	Sedang

Dalam menentukan tingkat risiko dapat dilakukan dengan dua cara, cara pertama dapat dilaksanakan dengan meminta pendapat responden dengan mengisi kuesioner yang telah dibagikan penulis yang hasilnya dapat dilihat pada tabel 5.6. Dan cara kedua dengan mencocokkan antara penilaian *likelihood* dan *impact* serta 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 tabel 5.7. Dan hasil kombinasi yang telah disesuaikan dari tabel 5.7, maka hasilnya dapat dilihat pada tabel 5.8 yang telah disesuaikan dengan mencocokkan antara *likelihood* dan *impact.*

5.7 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
Tnggi	Sangat Rendah	Rendah	Sedang	Tnggi	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

Tabel 5.8 Skala Penilaian –*Determine Risk* (Kombinasi *Likelihood* dan *Impact*)

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

Pada hasil kuesioner yang dibagikan kepada responden dan hasil dari kombinasi *likelihood* dan *impact* di dapat skala penilaian sebagai berikut. Dari *threat source* kategori *advesarial*, ketiga poin yaitu sumber ancaman *Outsider, Insider,* dan *Trusted Insider;* kategori *accidential* yaitu *user* dan *administrator;* kategori *structural* yaitu alat penyimpanan, alat pemrosesan, alat komunikasi, kontrol suhu ruangan, sistem operasi, alat jaringan, dan virus; serta kategori *evironmental* yaitu api, angin/hujan badai, telekomunikasi, dan tenaga listrik mendapatkan nilai kualitatif sedang pada penilaian *Determine Risk.* Dan maka risiko yang muncul dalam ktegori sedang, dari peristiwa yang akan terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU akan

mendapat efek buruk yang serius bagi organisasi, aset yang ada dan individu yang akan menjadi pengguna.

5.6 *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.

Setelah penilaian manajemen risiko pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU diatas, para pengambil keputusan yang tidak lain adalah para responden telah menilai dengan baik kegiatan *assessment IT risk management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pada bahasan sebelumnya, telah didapat penilaian risiko pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Skala penilaian risiko merujuk pada skala penilaian *NIST SP 800-30r1*, untuk mengetahui tingkatan pada skala penilaian disesuaikan dengan persamaan antara nilai semi kualitatif dan nilai kualitatif. Pada skala nilai 100 dapat di jabarkan sebagai berikut, jika nilai semi kualitatif berkisar antara 0-4 maka skala nilai kualitatifnya sangat rendah; jika nilai semi kualitatif berkisar antara 5-20 maka skala nilai kualitatifnya

rendah; jika nilai semi kualitatif berkisar antara 21-79 maka skala nilai kualitatifnya sedang; jika nilai semi kualitatif berkisar antara 80-95 maka skala nilai kualitatifnya tinggi; jika nilai semi kualitatif berkisar antara 96-100 maka skala nilai kualitatifnya sangat tinggi. Dan hasil penilaian dari kelima skala penilaian yang dilaksanakan pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dapat dilihat pada tabel 5.9.

Tabel 5.9 Hasil *Assessment Scale IT Risk Management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU

No	*Threat Source*	Nilai Kualitatif				
		Source Event	***Vulnerability Predisposing***	***Likelihood***	***Impact***	***Risk***
Adversarial						
1	*Outsider*/orang luar	Sedang	Sedang	Sedang	Sedang	Sedang
2	*Insider*/orang dalam	Sedang	Sedang	Sedang	Sedang	Sedang
3	*TrustedInsider*/orang Kepercayaan	Sedang	Sedang	Sedang	Sedang	Sedang
Accidential						
4	*User*	Sedang	Sedang	Sedang	Sedang	Sedang
5	*Administrator*	Sedang	Sedang	Sedang	Sedang	Sedang
Structural						
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 Ruangan	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
Environmental						
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

Hasil dari penelitian yang telah dilaksanan melalui wawancara terhadap responden/narasumber maka didapat 4 kategori pada *threat source* yang dapat mengundang munculnya risiko terhadap Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Hasil penilaian dari keempat kategori *threat source* ini akan dijabarkan dan telah sesuaikan dengan apa yang dinyatakan oleh

narasumber melalui wawancara. Dan ada pun dari keempat kategori *threat source* tersebut antara lain sebagai berikut.

5.6.1 *Adversarial*

Threat source pada kategori*adversarial* yang dilakukan penilaian padaLaboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU antara lain *Outsider, Insider,* dan *Trusted Insider.* Dari ketiga poin tersebut didapatlah skala nilai kualitatif sedang pada karakteristik ancaman dan ini menunjukkan bahwa kemampuan dari *outsider, insider,* dan *trusted insider* memiliki sumber daya, keahlian dan peluang yang cukup untuk melakukan serangan. Kemudian untuk tujuan melakukan ancaman pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU ketiganya dapat dengan mudah memperoleh/ memodifikasi informasi dengan mengganggu/ mengacaukan sumber daya infrastruktur yang ada. Dan dari target, ketiganya menganalisis informasi dengan menargekan nilai tinggi.

Untuk kondisi predisposisi dan kerentanan, kategori *adversarial* memiliki skala nilai kualitatif sedang. Kerentanan yang akan terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUdalam tingkat kekwatiran sedang sehingga dapat dengan mudah dieksploitasi dan dalam pengendalian keamanan masih relevan serta sebagian agak efektif. Dan kondisi predisposisi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dapat berlaku pada banyak bagian diorganisasi. Dari kemungkinan yang terjadi karena *adversarial* yang berada pada tingkat sedang, maka dalam hal ini *outsider, insider,* dan *trusted insider* agak

cenderung memulai ancaman terhadap kegiatan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Sehingga dampak yang diperoleh juga berada pada posisi sedang, sehingga dapat diperkirakan bahwa efek buruk yang serius terjadi pada individu, aset, dan organisasi. Efek yang serius dari ancaman dapat menyebabkan degradasi yang signifikan pada kerusakan aset di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Dan tingkat risiko yang muncul juga berada pada kategori sedang, maka risiko yang muncul memiliki efek buruk yang serius terhadap individu, aset maupun organisasi yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Ancaman *adversarial* yang didapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU yang dilakukan oleh *Outsider/*orang luar biasanya terjadi ketika adanya pelatihan yang diadakan oleh institusi lain. Ada beberapa aset yang hilang di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU pada saat meminjam ruang Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU sebagai tempat untuk belajar. Terbongkarnya perangkat komputer secara sengaja yang dilakukan orang luar pada aset yang terdapat diLaboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU sehingga peralatan yang terdapat dalam perangkat komputer seperti *memory, VGA card* dan semacamnya tidak ada lagi. Selain itu pula berbagai kendala yang dihadapi dari *Outsider* berupa tersenggolnya kabel jaringan yang dapat menghambat konektifitas jaringan, membongkar tombol keyboard, menjatuhkan mouse,

dan sebagainya. Sedangkan dari *Insider*/orang dalam yang menjadikannya sebagai ancaman, apa yang dilakukan *Insider* tidak jauh berbeda dengan *Outsider.*Pada dasarnya *Insider* memiliki peluang yang lebih besar menjadi ancaman di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selain kegiatan yang hampir sama dengan yang dilakukan oleh *Outsider, Insider* suka melakukan pembobolan pada *accesspoint* yang terdapat di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selanjutnya dari *Trusted Insider/*orang terpercaya dalam hal ini yang menjadi ancaman biasanya ketika peminjaman peralatan yang ada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU*Trusted Insider* lupa dalam meletakkan/mengembalikan peralatan yang dipinjam sehingga berdampak pada kehilangan aset.

Munculnya skala penilaian sedang pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU tidak luput dari tata kelola yang masih kurang. Kekurangannya sumber daya manusia juga menjadi pemicu utama dalam penilaian ini. Pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU toolman yang dipercaya untuk mengelola peralatan dan kelengkapan, sudah selama dua tahun mengalami kekosongan. Sehingga peralatan dan perlengkapan yang ada dalam tata kelolanya belum baik. Pada manajemen Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUbelum adanya orang yang dapat mengurus manajemen peralatan dan perlengkapan sebab itu yang membuatnya rentan terhadap ancaman yang terjadi sehingga membuat dampak dan risiko yang serius

terhadap aset yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

5.6.2 *Accidential*

Pada *Threat source* dengan kategori *accidential* yang dilakukan penilaian pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU yaitu *user* dan *administrator*. Kedua poin tersebut didapatlah skala nilai kualitatif sedang sehingga pengaruh yang didapat dari kesalahan atau kecelakaan sangat luas yang melibatkan porsi yang signifikan pada sumber daya dan infrastruktur yang penting. Dan untuk kondisi predisposisi dan kerentanan, kategori *accidential* memiliki skala nilai kualitatif sedang. Kerentanan yang akan terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dalam tingkat kekwatiran sedang, maka dapat dengan mudah dieksploitasi dan dalam pengendalian keamanan masih relevan serta sebagian agak efektif. Dari kondisi predisposisi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUsehingga berlaku pada banyak bagian diorganisasi.

Dalam kemungkinan yang terjadi karena *accidential* yang berada pada tingkat sedang, dalam hal ini *user*dan*administrator*akan mengalami kesalahan atau kecelakaan agak mungkin terjadi antara 1 sampai 10 kali setahun jika memulai ancaman terhadap kegiatan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Kemudian dampak yang diperoleh juga berada pada posisi sedang dan dapat diperkirakan bahwa efek buruk yang serius terjadi pada individu, aset, dan organisasi. Efek yang

serius dari ancaman dapat menyebabkan degradasi yang signifikan pada kerusakan aset di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selanjutnya tingkat risiko yang muncul juga berada pada kategori sedang, maka risiko yang muncul memiliki efek buruk yang serius terhadap individu, aset maupun organisasi yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Dari ancaman *accidential* yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUyang berasal dari *user*yaitu tidak bertanggungjawab atas apa yang diamanahkan dalam penggunaan fasilitas. Kejadian yang mengancam Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU yang berasal dari pengguna biasanya hilangnya tombol pada keyboard, mouse yang terjatuh, kehilangan peralatan dan perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, tidak sengaja menyenggol kabel dan menarik kabel sehingga konektor dan kabel terputus, mencuri peralatan dan perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selain itu pula, pengguna melakukan pembobolan pada *accesspoint* sehingga kinerja admin terganggu. Melakukan kerusakan peralatan dan perlengkapan yang terdapat di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU secara sengaja dan tidak sengaja pada saat melakukan kegiatan praktik. Kurangnya kesadaran *user* dalam menjaga dan merawat peralatan serta perlengkapan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Perangkat komputer terjangkit virus dikarenakan

*user*membuka situs, melakukan download file yang tidak dikenal ataupun memasukan flashdisk/memory yang memiliki virus.

Sedangkan ancaman dari *administrator* dikarenakan *administrator* lalai akan tugas yang sedang dikerjakan seperti lupa akan sandi pada *accesspoint*, teledor dalam menyimpan alat dan peralatan yang ada sehingga peralatan dan perlengkapan hilang karena tidak tau dimana meletakkannya. Kurang mengawasi *user* pada saat praktik sehingga terjadi kerusakkan pada perlatan yang ada dan terjadi kehilangan pada perangkat. Seperti yang telah disampaikan pada pembahasan *adversarial*, bahwa kekurangan sumber daya manusia masih menjadi pemicu utama yang menyebabkan kerentanan terhadap ancaman yang terjadi dalam membuat dampak dan risiko yang serius terhadap aset yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Karena tidak adanya toolman yang dapat mengelola peralatan dan perlengkapan yang ada.

5.6.3 *Structural*

Dari*Threat source* dengan kategori *strutural* dengan dilaksanakan penilaian pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU yaitu alat penyimpanan, alat pemrosesan, alat komunikasi, kontrol suhu ruangan, sistem operasi, jaringan dan virus. Pada ketujuh poin tersebut maka didapatskala nilai kualitatif sedang dalam hal inidapat berpengaruh pada kesalahan atau kecelakaan dan menjadi sangat luas yang melibatkan porsi dengan signifikan pada sumber daya dan infrastruktur yang penting. Dalam kondisi predisposisi dan kerentanan, kategori *strutural* memiliki

skala nilai kualitatif sedang. Dan kerentanan yang akan terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUberada pada tingkat kekwatiran sedang, lalu dapat dengan mudah dieksploitasi dan dalam pengendalian keamanan yang masih relevan serta sebagian agak efektif. Pada kondisi predisposisi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU sehingga berlaku pada banyak bagian diorganisasi.

Kemungkinan terjadi pada *structural* yang berada dalam tingkat sedang, dalam hal ini alat penyimpanan, alat pemrosesan, alat komunikasi, kontrol suhu ruangan, sistem operasi, jaringan dan virus akan mengalami kesalahan atau kecelakaan agak mungkin terjadi antara 1 sampai 10 kali setahun dalam ancaman terhadap kegiatan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Sehingga dampak yang diperoleh juga berada pada posisi sedang sehingga bisa diperkirakan bahwa efek buruk yang serius terjadi pada individu, aset, dan organisasi. Efek yang serius dari ancaman dapat menyebabkan degradasi yang signifikan pada kerusakan aset di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Lalu tingkat risiko yang muncul juga berada pada kategori sedang, maka risiko yang muncul memiliki efek buruk yang serius terhadap individu, aset maupun organisasi yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Permasalahan dari *structural*sering terjadi pada kegiatan yang terdapat kinerja teknologi dan ini pula yang tidak dapat melepaskan Laboratorium

Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Ancaman pada peralatan penyimpanan biasanya sangat rentan terjadi terutama pada *harddisk*, *harddisk* yang sudah cukup tua biasanya banyak mengalami masalah dalam penggunaanya. Hal yang sering menjadi masalah ketika *harddisk* mengalami *badsector, badsector* terjadi karena tegangan listrik yang naik turun. Sehingga platter pada *harddisk* memiliki banyak goresan yang menyebabkan *harddisk* mengalami *badsector.* Selain itu pula *badsector* disebabkan oleh karena terlalu sering melakukan installasi sistem operasi. Sedangkan ancaman yang berasal dari alat pemrosesan yang terjadi ketika tegangan listrik tidak stabil sehingga suhu pada prosesor meningkat dan membuat kerusakan pada prosesor. Selain itu juga kurangnya perawatan pada perangkat komputer yang menyebabkan fan rusak sehingga menimbulkan panas yang berlebih membuat prosesor bekerja tidak optimal sehingga dapat membuat prosesor rusak.

Selanjutnya untuk alat komunikasi yang menjadi ancaman pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU yaitu kabel UTP dan konektor RJ45 sebagai alat komunikasi antar komputer. Keduanya rentan terhadap ancaman, sering terinjak oleh orang, tersenggol, patah bahkan putus. Kemudian Hub/switch yang terjadi karena port tidak bekerja sebagai mana mestinya, hub/ switch mati secara tiba-tiba dikarenakan tegangan listri yang naik turun. Selanjutnya kerusakan pada *LAN card* yang tidak dapat terkoneksi pada jaringan biasanya dikarenakan onboard. Ancaman dari kotrol suhu ruangan ini berhubungan dengan

pendingin ruangan, ketidak stabilan suhu pada ruangan menyebabkan perangkat mudah rusak dikarenkan kepanasan. Dan perangkat yang ada pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU sangat cepat panas dikarenakan sudah tuanya perangkat dan tidak ada stabilizer untuk mengontrol tegangan listrik.

Ancaman dari sistem operasi dapat membuat hang perangkat komputer yang disebabkan sistem booting berjalan tidak baik, komputer tidak dapat menampilkan sistem operasi pada layar monitor sehingga komputer tidak dapat di gunakan. Selanjutnya ancaman dari jaringan yang berasal dari kerusakan alat komunikasi jaringan dan perangkat komputer. Bukan hanya itu, permasalahan terjadi dapat berasal dari provider jaringan yang memutuskan sinyal jaringan tanpa pemberitahuan.Pembobolan *accesspoint* yang sering terjadi membuat akses jaringan melambat. Kesalahan konfigurasi jaringan pada saat mensetting alamat jaringan sehingga ketika IP di panggil tidak dapat berkomunikasi. Dan selanjutnya yang berasal dari virus yang menyebabkan hilangan dokumen penting yang tersimpan pada server Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dan komputer *client.* Virus biasanya muncul disebabkan *flashdisk*/*memory* yang dicolokkan keperangkat jaringan. Selain itu pula disebabkan ketidaktahuan *user* dalam membuka situs pada website yang berbahaya. Dan ketidaksengajaan *user* dalam mendownload file yang mengandung virus, virus yang masuk secara ilegal tidak hanya merusak sistem operasi tetapi juga dapat merusak perangkat jaringan yang ada seperti

virus worm yang dapat menggandakan diri sehingga *harddisk* menjadi penuh.

Selanjutnya ancaman yang berasal dari *structural* dapat juga mengundang dampak dan risiko yang serius.Dan pada tata kelola Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU masih belum tersusun rapih dan juga belum adanya dokumen *risk management.*Selain itu pula, Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dokumen manajemen laboratorium tidak tersusun dengan baik. Sehingga menyebabkan kerentanan terhadap ancaman yang terjadi dapat membuat dampak dan risiko yang serius terhadap aset di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

5.6.4 *Environmental*

Pada *Threat source* dengan kategori *environmental* yang dilakukan penilaian pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU yaitu api, angin/hujan badai, telekounikasi, tegangan listrik. Pada keempat poin tersebut dan didapat skala nilai kualitatif sedang lalu pengaruh yang didapat dari kesalahan atau kecelakaan sangat luas yang melibatkan porsi yang signifikan pada sumber daya dan infrastruktur yang penting. Pada kondisi predisposisi dan kerentanan, kategori *environmental*memiliki skala nilai kualitatif sedang. Dalam kerentanan yang akan terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUdari tingkat kekwatiran sedang, kemudian dapat dengan mudah dieksploitasi serta dalam pengendalian keamanan masih relevan serta sebagian agak

efektif. Sehingga kondisi predisposisi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUdapat berlaku pada banyak bagian diorganisasi.

Dari kemungkinan yang terjadi karena *environmental* yang berada pada tingkat sedang, untuk hal ini api, angin/hujan badai, telekounikasi, tegangan listrik dapat mengalami tindakan alam yang agak mungkin terjadi antara 1 sampai 10 kali setahun apabila memulai ancaman terhadap kegiatan Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Selain itu, dampak yang diperoleh juga berada pada posisi sedang serta dapat diperkirakan bahwa efek buruk yang serius dapat terjadi pada individu, aset, dan organisasi. Dari efek yang serius pada ancaman dapat menyebabkan degradasi yang signifikan pada kerusakan aset di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Sehingga tingkat risiko yang muncul juga berada pada kategori sedang, maka risiko yang muncul memiliki efek buruk yang serius terhadap individu, aset maupun organisasi yang terdapat pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

Permasalahan dari *environmental* sulit untuk dihindari, hal ini juga dirasakan pada manajemen yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.Pada ancaman *environmental* yang dikarenakan api biasanya disebabkan kosleting dari perangkat, kesalahan penyambungan kabel pada perangkat dapat membuat konsleting yang memicu keluarnya asap dan api. Hal ini dialami pada saat peraktik perakitan

komputer yang dilakukan *user* saat merakit perangkat komputer yang disebabkan kesalahan pada pencocokan slot kabel di *motherboard.* Sehingga menyebabkan *motherboard* rusak dan kabel yang ada menjadi terbakar. Kemudian ancaman yang dikarenakan angin/hujan badai yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Tidak luput dari lingkungan yang berada di perbukitan, Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU sering terjadi angin kencang di wilayah sekitar SMK Negeri 3 OKU. Karena itu angin yang kencang yang disertai hujan membuat atap terbang dan kebocoran terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, waktu sebelum UNBK tahun 2018 terjadi kebocoran yang menyebabkan 2 komputer server rusak karena terkena air hujan. Selain itu pula petir yang menyambar peralatan kadang terjadi ketika hujan, membuat peralatan jaringan seperti hub/switch, modem maupun *accesspoint* rusak tersambar.

Selanjutnya ancaman telekomunikasi ini disebabkan provider yang memutuskan komunikasi jaringan tanpa pemberitahuan terlebih dahulu, sehingga kegiatan yang ada pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU terkendala. Kegiatan praktik yang dilakukan tidak berjalan mulus jika komunikasi jaringannya tiba-tiba terputus. Setelah itu ancaman yang disebabkan tenaga listrik, tenaga listrik merupakan sumber utama dalam perangkat jaringan komputer. Tanpa tenaga listrik jaringan komputer tidak dapat bekerja dengan semestinya, permasalahan listrik juga terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK

Negeri 3 OKU. Hal yang sering terjadi karena permasalahan listrik adalah ketika listrik mati secara mendadak tanpa pemberitahuan dari PLN dan kegiatan praktik terganggu. Tegangan listrik yang tidak stabil dapat merusak perangkat jaringan komputer, hub/switch dan *accesspoint* yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU mengalami kerusakan karena daya listrik yang naik turun. *Harddisk* mengalami *bad sector* karena listrik mati secara mendadak dan *powersupply* mengalami disfungsi karena tegangan listrik yang tidak stabil. Stabilizer yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU tidak mencukupi untuk menopang seluruh perangkat jaringan yang ada sebab stabilizer yang ada sudah banyak yang rusak sehingga tidak dapat membantu.

Ancaman yang berasal dari *environmental*dapat mengundang dampak dan risiko yang serius. Dikarenakan tata kelola Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU masih belum tersusun rapih dan juga belum adanya dokumen *risk management.*Kemudian untuk dokumen manajemen laboratorium belum tersusun dengan baik. Karena itulah penyebabkan kerentanan terhadap ancaman yang terjadi dapat membuat dampak dan risiko yang serius terhadap aset di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.

5.7 *Maintain Assessment*

Hasil penilaian yang dilaksanakan pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKUcukup 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 yang terdapat di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. 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.

Selain itu juga, 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.

Dalam meminimalisir muncul risiko yang terjadi pada bersumber dari *adversarial,* akan dilakukan pengawasan dan pengecekan peralatan maupun perlengkapan yang digunakan pada setiap kegiatan yang ada di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Begitu juga dalam meminimalisir risiko pada sumber *accidential,* maka yang akan dilakukan adalah pengawasan terhadap peralatan dan perlengkapan praktik. Tidak hanya itu, untuk peralatan penunjang seperti keyboard, mouse, dan headphone akan disimpan apabila tidak melakukan tidak sedang melakukan kegiatan praktik. Hal ini dilakukan agar tidak terjadi kerusakan pada peralatan tersebut dan selanjutnya mengecek box CPU setelah kegiatan praktik dilakukan agar kehilangan pada perlengkapan dan peralatan jaringan tidak terjadi kembali. Untuk menanggulangi kebobolan pada *accesspoint,* akan dilakukan pembaharuan sandi minimal 1 bulan sekali sehingga *user* ilegal memiliki sedikit kemungkinan dalam akses yang ada.

Untuk menanggulangi munculnya risiko pada sumber *structural* dapat dilakukan perawatan, pengecekkan dan service berkala terhadap alat penyimpana, alat pemrosesan, alat komunikasi, peralatan kontrol suhu ruangan dan jaringan. Kegiatan perawatan, pengercekan dan service wajib dilakukan secara berkala minimal 1 minggu sekali. Ini disebabkan oleh perangkat yang sudah tua dan harus diperhatikan dengan baik agar tidak menimbulkan risiko yang besar pada manajemen Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Kemudian untuk meminimalisir risiko pada sistem operasi, sistem operasi harus disesuaikan dengan spesifikasi pada perangkat jaringan agar tidak menimbulkan hang pada *hardware*. Laboratorium Teknik Komputer dan Jaringan SMK Negeri

3 OKU memiliki CD original dari sistem operasi yang dibutuhkan sehingga dapat menanggulangi kendala dalam sistem operasi. Dalam menanggulangi virus, Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU melakukan penanaman antivirus pada perangkat jaringan komputer dan pemasangan firewall untuk mencegah serangan dari luar jaringan. Apabila virus menyebar pada sistem operasi akan dilakukan instalasi pada komputer yang terjangkit virus tersebut.

Kemudian untuk menanggulangi risiko yang muncul dari sumber *environmental* dapat dilakukan pengecekan kabel yang dipasang agar tidak terjadi konsleting ketika dialiri listrik sehingga tidak akan memicu api. Pada ancaman angin/hujan badai untuk meminimalisir telah dilakukan perbaikkan pada atap yang mengalami kebocoran. Bukan hanya itu, tata letak peralatan dan perlengkapan juga telah dilakukan perobakan dan disesuaikan untuk menghindari air hujan yang masuk ke ruangLaboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Untuk menaggulangi dampak yang terjadi oleh sambaran petir, maka dipasang penangkal petir pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Dalam meminimalisir ancaman telekomunikasi adalah dengan cara mengkomunikasikan dengan provider penyelenggara. Dan meminta pemberitahuan sebelumnya apabila terdapat masalah yang terjadi pada jaringan telekomunikasi dari provider penyelenggara. Selanjutnya ancaman yang disebabkan oleh tenaga listrik, untuk meminimalisir setidaknya harus memakai UPS untuk menanggulangi risiko yang ada. Agar arus listrik yang ada terkendali dengan baik, dan apabila listrik mati secara mendadak UPS dapat menyimpan cadangan listrik sehingga perangkat jaringan tidak mati secara mendadak.

Dari penjabaran hasil dan cara penanggulangan yang telah dijabarkan pada poin *maintain assessmen*t, diharapkan agar nilai kemunculan risiko tidak akan naik sehingga bertahan pada level yang telah didapatkan. Bahkan diharapkanpada 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.


Universitas
Bina
Darma

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil pembahasan pada penelitian *assessment IT risk management* pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU maka dapat di tarik kesimpulan sebagai berikut :

1. Laboratorium Teknik Komputerdan 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.
2. Keempat kategori sumber ancaman yang mempengaruhi munculnya risiko pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU yaitu *adversarial, accidential, structural,* dan *environmental*.
3. 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.
4. 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

6.2 Saran

Dari hasil penelitian telah dilaksanakan, ada beberapa saran yang perlu disampaikan antara lain sebagai berikut :

1. Diharapkan akan adanya dokumen IT Risk Management pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dan penelitian ini dapat menjadi acuan untuk pembuatannya.
2. Perlunya penambahan sumber daya sesegera mungkin agar risiko yang akan hadir dapat di minimalisir dengan cepat dan lebih baik.
3. Perbaiki tata kelola pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU dengan cara membuat aplikasi untuk manajemen Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU.


Universitas
Bina
Darma

DAFTAR PUSTAKA

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

Wahid, Misbah 2017, Jurnal : Asesmen Maturitas Manajemen Risiko Perusahaan Pada Kontraktor Kecil dan Menengah, Universitas Katolik Parahyangan Bandung.

Nurochman, A 2014, Jurnal : Manajemen RisikoSistem Informasi Perpustakaan (Studi Kasus Di Perpustakaan Universitas Gajah Mada Yogyakarta), Yogyakarta.

Creswell, J.W 2014, Penelitian Kualitatif & Desain Riset Memilih di Antara Lima Pendekatan Edisi 3, Yogyakarta, Penerbit Pustaka Pelajar.

Miles, Matthew B & A Michael Huberman 1992, Analisis Data Kualitatif, Jakarta : Penerbit Universitas Indonesia.

Haryanto, E.V 2012, Jaringan Komputer, Penerbit Andy : Universitas Potensi Utama.

Riadi, 2012, Tesis Analisis Dan Desain Jaringan Intranet SMK Negeri 3 Ogan Komering Ulu Menggunakan Metode *Network Development Life Cycle*, Universitas Bina Darma Palembang

Situmorang, S. H 2010, Analisis Data : Untu Riset Manajemen dan Bisnis. Medan. Indonesia: USU Press.

Wagito 2007, Jaringan Komputer : Teori dan Implementasi Berbasis Linux, Penerbit Gava Media.

Hardanto, S.S 2006, Manajemen Risiko Bagi Bank Umum, Penerbit Elex Media Komputindo.

National Institute Standard and Technology (NIST) 2012*, Guide for Conducting – NIST Special Publication 800-30 Revision 1, USA.*

Kurniawan, N.B 2013, Manajemen Risiko Teknologi Informasi Pada Badan Pusat Statistik, Produk Layanan: Pelayanan Statistik Terpadu, Bandung .

Stoneburner G, A. Goguen and Feringa, A 2002, Risk Management Guide for Information Technology System, Recommedation of National Institute of Standards and Technology Special Publication 800-30, USA.

Setiawan, Deris 2006, Sistem Keamanan Komputer, Penerbit Elex Media Komputindo, Jakarta.

Brown, W. C. 2006, IT Governance, Architectural Competency, and the Vasa. Information Management & Computer Security, 14. Diakses 25 Febuariuari 2010 dari http://proquest.umi.com/pqdweb?did=1073465011&sid=5&Fmt=3&clientId=68814&RQT=309&VName=PQD

Broadleaf Capital International (BCI) 2014, Strategic, enterprise, and risk management". Diunduh dari http://www.broadleaf.co.nz/erm/index.htm.

[Online]. Available: http://id.wikipedia.org/wiki/Manajemen_risiko. [Accessed 28 Mei 2015].

DAFTAR RIWAYAT HIDUP

ARLIN NURLIYANI

Kontak Pribadi

0821 7770 0580

arlin.ar1@gmail.com

Jalan Moro Seneng Blok O No. 47 RT.009 RW.004 Kel. Baturaja Permai
Kec. Baturaja Timur Kab. Ogan Komering Ulu Provinsi Sumatera Selatan

Tentang Saya

Sebagai seorang yang dikenal ramah, sederhana dan mampu menyelesaikan kendala dalam bidang IT, saya berkomitmen untuk selalu menyelesaikan tanggungjawab saya terhadap kepercayaan yang telah diberikan. Bekerja dalam bidang IT merupakan kebanggaan bagi saya karena ilmu yang saya pelajari tidak menjadi sia-sia

*Arlin Nurliyani, M.Kom. *

Biodata

Nama	Arlin Nurliyani
Tempat	Baturaja
Tanggal Lahir	1 Mei 1990
Status	Menikah
Agama	Islam
Hobi	Renang dan Travelling
Tinggi / Berat	155 cm / 50 kg

Softskills

- Jiwa Kepemimpinan
- Komunikasi
- Kemampuan Analisa
- Kerjasama Tim

Keahlian Komputer

Microsoft Office	90%
Networking	80%
Web Programming	79%
JavaProgramming	79 %
Linux	75 %

Bahasa

Indonesia	Aktif
Inggris	Pasif

Pengalaman Kerja

Tenaga PSP3 Agustus 2013- Agustus 2015

Program pertukaran 1000 pemuda seluruh Indonesia melalui Kementerian Pemuda dan Olahraga dengan tujuan menyampaikan 4 pilar kebangsaan ke masyarakat (penempatan Kota Bitung Provinsi Sulawesi Utara).

Guru Januari 2016– Juni 2018

Tenaga pengajar honorer pada jurusan Teknik Komputer dan Jaringan selain itu juga di percaya sebagai pembina organisasi Siswa Pecinta Alam (GRAPALA T3) pada tahun ajaran 2017/2018 di SMK Negeri 3 OKU.

Pendidikan Formal

TK ABA 1 Baturaja
Tahun 1994 - 1996

SD Negeri 24 Baturaja
Tahun 1996 - 2002

SMP Negeri 1 OKU
Tahun 2002-2005

SMK Negeri 3 OKU
Tahun 2005- 2008
Jurusan Teknik Komputer dan Jaringan

STMIK GI Multi Data Palembang
Tahun 2005- 2008
Jurusan Teknik Informatika – S1

Universitas Bina Darma
Tahun 2016 - 2019
Jurusan Teknik Informatika – S2

Organisasi

Agustus 2006–Agustus 2007
Purna Paskibra SMK Negeri 3 OKU
Jabatan Sekretaris

Agustus 2010 – Agustus 2011
Mapala Multi Data Palembang
Jabatan Ketua Umum

April 2011 – April 2013
Forum SAR Pecinta Alam Sumsel
Jabatan Sekretaris

Desember2012 – Desember2014
Desk Disaster Walhi Sumsel
Jabatan Sekretaris

SURAT KEPUTUSAN
DIREKTUR PROGRAM PASCASARJANA
NOMOR: 341/SK/PPs-UBD/IX/2018

TENTANG
PEMBIMBING TESIS MAHASISWA
PROGRAM STUDI TEKNIK INFORMATIKA JENJANG STUDI STRATA DUA (S2)
PROGRAM PASCASARJANA UNIVERSITAS BINA DARMA

DIREKTUR PROGRAM PASCASARJANA
UNIVERSITAS BINA DARMA

Menimbang : a. Bahwa mahasiswa semester akhir diharuskan membuat Tesis sebagai salah satu syarat untuk menyelesaikan studi pada Program Pascasarjana Program Studi Teknik Informatika-S2;
b. Bahwa untuk kelancaran pelaksanaan kegiatan dimaksud, dipandang perlu untuk menunjuk Pembimbing Tesis bagi setiap mahasiswa;
c. Bahwa untuk memenuhi butir-butir di atas, perlu diterbitkan Surat Keputusan sebagai landasan hukumnya.

Mengingat :
1. Undang-undang Nomor 20 tahun 2003;
2. Undang-undang Nomor 12 tahun 2012;
3. Peraturan Mentri Pendidikan Nasional Nomor 15 tahun 2005;
4. Surat Keputusan Direktur Jenderal Pendidikan Tinggi Depdiknas;
5. Akte Pendirian Yayasan Nomor 95 tanggal 28 Desember 2003;
6. Statuta Universitas Bina Darma;
7. Surat Keputusan Rektor Universitas Bina Darma Nomor: 078/SK/Univ-BD/VI/2009 tanggal 1 Juni 2009.

MEMUTUSKAN

Menetapkan :

PERTAMA : Menunjuk dan menugaskan saudara:
Dedy Syamsuar, Ph.D
Ahmad Haidar Mirza, S.T., M.Kom

Berturut-turut sebagai Pembimbing I dan Pembimbing II dalam penyusunan Tesis bagi mahasiswa dibawah ini:

Nama	:	Arlin Nurliyani
NIM	:	162420001
Angkatan	:	14
Konsentrasi	:	*Enterprise IT Infrastructure*
Judul Internship	:	Assessment IT Risk Management pada Laboratorium Teknik Kmputer dan Jaringan SMK Negeri 3 OKU

KEDUA : Surat Keputusan ini berlaku 6 (enam) bulan sejak tanggal ditetapkan dan apabila dalam waktu tersebut mahasiswa belum menyelesaikan Tesis, maka akan diterbitkan Surat Keputusan Pembimbing yang baru, dengan ketentuan apabila dikemudian hari terdapat kekeliruan dalam penetapan ini, akan diperbaiki sebagaimana mestinya;

KETIGA : Surat Keputusan asli ini diberikan kepada mahasiswa yang bersangkutan untuk dilaksanakan dan diindahkan sebagaimana mestinya.

Ditetapkan di: Palembang
Pada Tanggal: 08 September 2018
Direktur,

Dr. Ir. Hj. Hasmawaty AR, M.M., M.T.

Tembusan:
1. Pembimbing I dan II
2. Arsip

PEMERINTAH PROVINSI SUMATERA SELATAN
DINAS PENDIDIKAN
SEKOLAH MENENGAH KEJURUAN NEGERI 3 BATURAJA
NSS : 401110301003 NIS : 400003 NPSN : 10604741
Jalan M.S Oeding No.695 Air Paoh Baturaja – 32112
E-mail : smk3oku@yahoo.com

Nomor : 422/644 /SMKN.3/Disdik.SS/2017 12 Desember 2017
Lampiran : -
Perihal : Pemberian Izin Penelitian

Kepada
Direktur Program Pascasarjana
Universitas Binadarma
di
Palembang.

Dengan Hormat,

Menanggapi Surat Saudara Nomor : 058/IP/PPS,MTT/UBD/XII/2017, tanggal 09 Desember 2017 untuk mengadakan Penelitian dalam Lingkungan Sekolah Menegah Kejuruan (SMK) N3 OKU pada prinsipnya kami tidak berkeberatan (setuju) dengan catatan tidak akan dipublikasikan untuk umum, hanya semata-mata kepentingan penyusunan Tesis/Internship

Nama	: Arlin Nurliyani
NIM	: 162420001
Konsentrasi	: Enterprise IT Infrastructure
Tema	: Assessment IT Risk Managemen Pada Laboratorium Teknik Komputer dan jaringan (TKJ) SMK Negeri 3 OKU

Demikian Surat persetujuan Permohonan Izin Penelitian ini dibuat, untuk dapat dipergunakan sebagaimana mestinya.

Kepala Sekolah,

PEMERINTAH PROVINSI SUMATERA SELATAN
DINAS PENDIDIKAN
SMK NEGERI 3
BATURAJA OKU

Drs. Johny Ferry Panhar,MT
Pembina Tingkat I
Nip. 19640315198980310009

PEMERINTAH PROVINSI SUMATERA SELATAN
DINAS PENDIDIKAN
SEKOLAH MENENGAH KEJURUAN NEGERI 3 BATURAJA
NSS : 401110301003 NIS : 400003 NPSN : 10604741
Jalan M.S Oeding No.695 Air Paoh Baturaja – 32112
E-mail : smk3oku@yahoo.com

SURAT PERINTAH TUGAS

Nomor : 420 / 644 /SMK.3/Disdik.SS/2017

Dasar : Surat Direktur Program Pascasarjana Universitas Bina Darma Nomor : 058/IP/PPS,MTT/UBD/XII/2017, tanggal 09 Desember 2017, Perihal Izin Penelitian.

Memerintahkan Kepada Nama tersebut di bawah ini :

N a m a	: Riadi, S.ST, M.Kom
Nip	: 196610091990031003
Pangkat/Gol	: Pembina, IV/a
Jabatan	: Guru SMKN 3 OKU
A l a m a t	: Jalan M.S. Oeding Baturaja

Untuk : Menjadi Pendamping guna kepentingan penyusunan Tesis/Internship An.

Nama	: Arlin Nurliyani
NIM	: 162420001
Konsentrasi	: Enterprise IT Infrastructure
Tema	: Assessment IT Risk Managemen Pada Laboratorium Teknik Komputer dan jaringan (TKJ) SMK Negeri 3 OKU

Demikian Surat Perintah Tugas ini dibuat dengan sebenarnya, untuk dapat dipergunakan sebagaimana mestinya.

Dikeluarkan di Baturaja
Pada tanggal, 12 Desember 2017

Kepala Sekolah,

PEMERINTAH PROVINSI SUMATERA SELATAN DINAS PENDIDIKAN SMK NEGERI 3 BATURAJA OKU

Drs. Johny Ferry Panhar., M.T
NIP. 19640315 198903 1 009

Responden 1

Nama : Riadi, S.ST, M.Kom.

Jabatan : Kepala Program Studi Teknik Komputer dan Jaringan

1. **Pilih skala penilaian sumber dan peristiwa ancaman yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan yang pernah di hadapi oleh Bapak/Ibu beri tanda (X) pada pernyataan yang sesuai dengan risiko yang di alami.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Ancaman yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
2	Ancaman yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Ancaman yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Ancaman dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
5	Ancaman dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Ancaman dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Ancaman dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Ancaman dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Ancaman dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Ancaman dari kegagalan sistem operasi yang melebihi perkiraan operasi		X			
11	Ancaman dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Ancaman dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Ancaman dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Ancaman dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Ancaman dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
16	Ancaman dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

2. **Pilih skala penilaian dari tingkat kerentanan keamanan dan kondisi predisposisi yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan apa yang dihadapi Bapak/Ibu dengan memberikan tanda (X) pada pernyataan yang sesuai.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
2	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Structural						
6	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kontrol suhu ruangan karena penuaan sumber daya			X		
10	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan sistem operasi yang melebihi perkiraan operasi		X			
11	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Kerentanan dan kondisi predisposisi yang di sebabkan api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
14	Kerentanan dan kondisi predisposisi yang di sebabkan angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Kerentanan dan kondisi predisposisi yang di sebabkan Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
16	Kerentanan dan kondisi predisposisi yang di sebabkan Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

3. **Bagaimana menurut Bapak/Ibu tentang kemungkinan ancaman yang terjadi pada laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pilih salah satu dari pernyataan dibawah ini, beri tanda (X) pada pernyataan yang sesuai dengan kejadian yang terjadi.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya kemungkinan ancaman yang di dapat dari *Outsider*/orang luar saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
2	Besarnya kemungkinan ancaman yang di dapat dari *Insider*/orang dalam saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Besarnya kemungkinan ancaman yang di dapat dari *Trusted Insider*/orang Kepercayaan saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Accidential						
4	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Structural						
6	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya kemungkinan ancaman yang di dapat dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya		X			
10	Besarnya kemungkinan ancaman yang di dapat dari kegagalan sistem operasi yang melebihi perkiraan operasi		X			
11	Besarnya kemungkinan ancaman yang di dapat dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Besarnya kemungkinan ancaman yang di dapat dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Besarnya kemungkinan ancaman yang di dapat dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
14	Besarnya kemungkinan ancaman yang di dapat dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Besarnya kemungkinan ancaman yang di dapat dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
16	Besarnya kemungkinan ancaman yang di dapat dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

4. **Pilih skala nilai dari dampak yang akan muncul di Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU dari risiko yang sering dihadapi, isi sesuai dengan beri tanda (X) isi pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya dampak yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Besarnya dampak yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
3	Besarnya dampak yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Accidential						
4	Besarnya dampak dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya dampak dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Structural						
6	Besarnya dampak dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya dampak dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya				X	
8	Besarnya dampak dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya dampak dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Besarnya dampak dari kegagalan sistem operasi yang melebihi perkiraan operasi		X			
11	Besarnya dampak dari kegagalan jaringan karena penuaan dan penipisan sumber daya		X			
12	Besarnya dampak dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Besarnya dampak dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
14	Besarnya dampak dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
15	Besarnya dampak dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
16	Besarnya dampak dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	

5. **Pilih nilai dari tingkat Risiko yang berpengaruh pada Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan risiko yang dihadapi dan beri tanda (X) pada pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya risiko yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

2	Besarnya risiko yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Besarnya risiko yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya risiko dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya risiko dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Structural						
6	Besarnya risiko dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya risiko dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya risiko dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya risiko dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Besarnya risiko dari kegagalan sistem operasi yang melebihi perkiraan operasi		X			
11	Besarnya risiko dari kegagalan jaringan karena penuaan dan penipisan sumber daya		X			
12	Besarnya risiko dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Besarnya risiko dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
14	Besarnya risiko dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
15	Besarnya risiko dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
16	Besarnya risiko dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	

Responden 2

Nama : Russadayana, S.Kom.

Jabatan : Kepala Bengkel Teknik Komputer dan Jaringan

1. **Pilih skala penilaian sumber dan peristiwa ancaman yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan yang pernah di hadapi oleh Bapak/Ibu beri tanda (X) pada pernyataan yang sesuai dengan risiko yang di alami.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Ancaman yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Ancaman yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
3	Ancaman yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Ancaman dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
5	Ancaman dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Ancaman dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Ancaman dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Ancaman dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Ancaman dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Ancaman dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Ancaman dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Ancaman dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Ancaman dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Ancaman dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Ancaman dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Ancaman dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

2. **Pilih skala penilaian dari tingkat kerentanan keamanan dan kondisi predisposisi yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan apa yang dihadapi Bapak/Ibu dengan memberikan tanda (X) pada pernyataan yang sesuai.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
2	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
3	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
5	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kontrol suhu ruangan karena penuaan sumber daya			X		
10	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Kerentanan dan kondisi predisposisi yang di sebabkan api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Kerentanan dan kondisi predisposisi yang di sebabkan angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Kerentanan dan kondisi predisposisi yang di sebabkan Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Kerentanan dan kondisi predisposisi yang di sebabkan Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

3. **Bagaimana menurut Bapak/Ibu tentang kemungkinan ancaman yang terjadi pada laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pilih salah satu dari pernyataan dibawah ini, beri tanda (X) pada pernyataan yang sesuai dengan kejadian yang terjadi.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya kemungkinan ancaman yang di dapat dari *Outsider*/orang luar saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Besarnya kemungkinan ancaman yang di dapat dari *Insider*/orang dalam saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
3	Besarnya kemungkinan ancaman yang di dapat dari *Trusted Insider*/orang Kepercayaan saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
5	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya kemungkinan ancaman yang di dapat dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Besarnya kemungkinan ancaman yang di dapat dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya kemungkinan ancaman yang di dapat dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Besarnya kemungkinan ancaman yang di dapat dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Besarnya kemungkinan ancaman yang di dapat dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Besarnya kemungkinan ancaman yang di dapat dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Besarnya kemungkinan ancaman yang di dapat dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Besarnya kemungkinan ancaman yang di dapat dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

4. **Pilih skala nilai dari dampak yang akan muncul di Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU dari risiko yang sering dihadapi, isi sesuai dengan beri tanda (X) isi pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya dampak yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
2	Besarnya dampak yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
3	Besarnya dampak yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya dampak dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
5	Besarnya dampak dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya dampak dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya dampak dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya dampak dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya dampak dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Besarnya dampak dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya dampak dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Besarnya dampak dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Besarnya dampak dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Besarnya dampak dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya dampak dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Besarnya dampak dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

5. **Pilih nilai dari tingkat Risiko yang berpengaruh pada Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan risiko yang dihadapi dan beri tanda (X) pada pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya risiko yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

2	Besarnya risiko yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
3	Besarnya risiko yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya risiko dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
5	Besarnya risiko dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya risiko dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya risiko dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya risiko dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya risiko dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Besarnya risiko dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya risiko dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Besarnya risiko dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Besarnya risiko dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Besarnya risiko dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya risiko dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Besarnya risiko dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

Responden 3

Nama : Desy Saraswaty, S.Kom.

Jabatan : Guru Jurusan Teknik Komputer dan Jaringan

1. **Pilih skala penilaian sumber dan peristiwa ancaman yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan yang pernah di hadapi oleh Bapak/Ibu beri tanda (X) pada pernyataan yang sesuai dengan risiko yang di alami.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Ancaman yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
2	Ancaman yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
3	Ancaman yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Ancaman dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Ancaman dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Ancaman dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya		X			
7	Ancaman dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya		X			
8	Ancaman dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya	X				
9	Ancaman dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Ancaman dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Ancaman dari kegagalan jaringan karena penuaan dan penipisan sumber daya	X				
12	Ancaman dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Ancaman dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
14	Ancaman dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Ancaman dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Ancaman dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

2. **Pilih skala penilaian dari tingkat kerentanan keamanan dan kondisi predisposisi yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan apa yang dihadapi Bapak/Ibu dengan memberikan tanda (X) pada pernyataan yang sesuai.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
2	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
3	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya	X				
7	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya	X				
8	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya	X				
9	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kontrol suhu ruangan karena penuaan sumber daya	X				
10	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan sistem operasi yang melebihi perkiraan operasi		X			
11	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan jaringan karena penuaan dan penipisan sumber daya	X				
12	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Kerentanan dan kondisi predisposisi yang di sebabkan api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Kerentanan dan kondisi predisposisi yang di sebabkan angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Kerentanan dan kondisi predisposisi yang di sebabkan Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Kerentanan dan kondisi predisposisi yang di sebabkan Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

3. **Bagaimana menurut Bapak/Ibu tentang kemungkinan ancaman yang terjadi pada laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pilih salah satu dari pernyataan dibawah ini, beri tanda (X) pada pernyataan yang sesuai dengan kejadian yang terjadi.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya kemungkinan ancaman yang di dapat dari *Outsider*/orang luar saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Besarnya kemungkinan ancaman yang di dapat dari *Insider*/orang dalam saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
3	Besarnya kemungkinan ancaman yang di dapat dari *Trusted Insider*/orang Kepercayaan saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya	X				
7	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya	X				
8	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya	X				
9	Besarnya kemungkinan ancaman yang di dapat dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Besarnya kemungkinan ancaman yang di dapat dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya kemungkinan ancaman yang di dapat dari kegagalan jaringan karena penuaan dan penipisan sumber daya	X				
12	Besarnya kemungkinan ancaman yang di dapat dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Besarnya kemungkinan ancaman yang di dapat dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Besarnya kemungkinan ancaman yang di dapat dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Besarnya kemungkinan ancaman yang di dapat dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Besarnya kemungkinan ancaman yang di dapat dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

4. **Pilih skala nilai dari dampak yang akan muncul di Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU dari risiko yang sering dihadapi, isi sesuai dengan beri tanda (X) isi pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya dampak yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Besarnya dampak yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Besarnya dampak yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya dampak dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya dampak dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya dampak dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya dampak dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya	X				
8	Besarnya dampak dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Besarnya dampak dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Besarnya dampak dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya dampak dari kegagalan jaringan karena penuaan dan penipisan sumber daya	X				
12	Besarnya dampak dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Besarnya dampak dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
14	Besarnya dampak dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya dampak dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
16	Besarnya dampak dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

5. **Pilih nilai dari tingkat Risiko yang berpengaruh pada Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan risiko yang dihadapi dan beri tanda (X) pada pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya risiko yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

2	Besarnya risiko yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Besarnya risiko yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
Accidential						
4	Besarnya risiko dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
5	Besarnya risiko dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya risiko dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya	X				
7	Besarnya risiko dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya	X				
8	Besarnya risiko dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya risiko dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Besarnya risiko dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya risiko dari kegagalan jaringan karena penuaan dan penipisan sumber daya	X				
12	Besarnya risiko dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Besarnya risiko dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
14	Besarnya risiko dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya risiko dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
16	Besarnya risiko dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	

Responden 4

Nama : Reni Aprilina, S.Pd.

Jabatan : Guru Jurusan Teknik Komputer dan Jaringan

1. **Pilih skala penilaian sumber dan peristiwa ancaman yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan yang pernah di hadapi oleh Bapak/Ibu beri tanda (X) pada pernyataan yang sesuai dengan risiko yang di alami.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Ancaman yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Ancaman yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Ancaman yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Ancaman dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Ancaman dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Ancaman dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Ancaman dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Ancaman dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Ancaman dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Ancaman dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Ancaman dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Ancaman dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Ancaman dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Ancaman dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Ancaman dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
16	Ancaman dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

2. **Pilih skala penilaian dari tingkat kerentanan keamanan dan kondisi predisposisi yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan apa yang dihadapi Bapak/Ibu dengan memberikan tanda (X) pada pernyataan yang sesuai.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya		X			
8	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kontrol suhu ruangan karena penuaan sumber daya	X				
10	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Kerentanan dan kondisi predisposisi yang di sebabkan api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Kerentanan dan kondisi predisposisi yang di sebabkan angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Kerentanan dan kondisi predisposisi yang di sebabkan Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
16	Kerentanan dan kondisi predisposisi yang di sebabkan Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

3. **Bagaimana menurut Bapak/Ibu tentang kemungkinan ancaman yang terjadi pada laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pilih salah satu dari pernyataan dibawah ini, beri tanda (X) pada pernyataan yang sesuai dengan kejadian yang terjadi.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya kemungkinan ancaman yang di dapat dari *Outsider*/orang luar saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Besarnya kemungkinan ancaman yang di dapat dari *Insider*/orang dalam saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Besarnya kemungkinan ancaman yang di dapat dari *Trusted Insider*/orang Kepercayaan saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya		X			
7	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya		X			
8	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Besarnya kemungkinan ancaman yang di dapat dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Besarnya kemungkinan ancaman yang di dapat dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya kemungkinan ancaman yang di dapat dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Besarnya kemungkinan ancaman yang di dapat dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Besarnya kemungkinan ancaman yang di dapat dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Besarnya kemungkinan ancaman yang di dapat dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya kemungkinan ancaman yang di dapat dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Besarnya kemungkinan ancaman yang di dapat dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

4. **Pilih skala nilai dari dampak yang akan muncul di Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU dari risiko yang sering dihadapi, isi sesuai dengan beri tanda (X) isi pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya dampak yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Besarnya dampak yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Besarnya dampak yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya dampak dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya dampak dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Structural						
6	Besarnya dampak dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya dampak dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya		X			
8	Besarnya dampak dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Besarnya dampak dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Besarnya dampak dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya dampak dari kegagalan jaringan karena penuaan dan penipisan sumber daya			X		
12	Besarnya dampak dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Besarnya dampak dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Besarnya dampak dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya dampak dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Besarnya dampak dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

5. **Pilih nilai dari tingkat Risiko yang berpengaruh pada Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan risiko yang dihadapi dan beri tanda (X) pada pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya risiko yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

2	Besarnya risiko yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
3	Besarnya risiko yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Accidential						
4	Besarnya risiko dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
5	Besarnya risiko dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Besarnya risiko dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya		X			
7	Besarnya risiko dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya		X			
8	Besarnya risiko dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Besarnya risiko dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya	X				
10	Besarnya risiko dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Besarnya risiko dari kegagalan jaringan karena penuaan dan penipisan sumber daya		X			
12	Besarnya risiko dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Besarnya risiko dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Besarnya risiko dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Besarnya risiko dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Besarnya risiko dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

Responden 5

Nama : Sri Wahyuni, S.Pd.

Jabatan : Guru Jurusan Teknik Komputer dan Jaringan

1. **Pilih skala penilaian sumber dan peristiwa ancaman yang terjadi di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan yang pernah di hadapi oleh Bapak/Ibu beri tanda (X) pada pernyataan yang sesuai dengan risiko yang di alami.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Ancaman yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
2	Ancaman yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
3	Ancaman yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Accidential						
4	Ancaman dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
5	Ancaman dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Structural						
6	Ancaman dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya		X			
7	Ancaman dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya		X			
8	Ancaman dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya	X				
9	Ancaman dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya		X			
10	Ancaman dari kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Ancaman dari kegagalan jaringan karena penuaan dan penipisan sumber daya		X			
12	Ancaman dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat		X			
Environmental						
13	Ancaman dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Ancaman dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
15	Ancaman dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
16	Ancaman dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				

2. **Pilih skala penilaian dari tingkat kerentanan keamanan dan kondisi predisposisi yang terjadi pada Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan apa yang dihadapi Bapak/Ibu dengan memberikan tanda (X) pada pernyataan yang sesuai.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
2	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
3	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
Accidential						
4	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
5	Kerentanan dan kondisi predisposisi yang di pengaruhi tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
Structural						
6	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya		X			
7	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya	X				
8	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya	X				
9	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kontrol suhu ruangan karena penuaan sumber daya		X			
10	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan sistem operasi yang melebihi perkiraan operasi	X				
11	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh kegagalan jaringan karena penuaan dan penipisan sumber daya	X				
12	Kerentanan dan kondisi predisposisi yang di pengaruhi oleh virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat	X				
Environmental						
13	Kerentanan dan kondisi predisposisi yang di sebabkan api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU	X				
14	Kerentanan dan kondisi predisposisi yang di sebabkan angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
15	Kerentanan dan kondisi predisposisi yang di sebabkan Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			
16	Kerentanan dan kondisi predisposisi yang di sebabkan Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU		X			

3. **Bagaimana menurut Bapak/Ibu tentang kemungkinan ancaman yang terjadi pada laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU. Pilih salah satu dari pernyataan dibawah ini, beri tanda (X) pada pernyataan yang sesuai dengan kejadian yang terjadi.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya kemungkinan ancaman yang di dapat dari *Outsider*/orang luar saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
2	Besarnya kemungkinan ancaman yang di dapat dari *Insider*/orang dalam saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
3	Besarnya kemungkinan ancaman yang di dapat dari *Trusted Insider*/orang Kepercayaan saat mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
Accidential						
4	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya kemungkinan ancaman yang di dapat dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
Structural						
6	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya kemungkinan ancaman yang di dapat dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya				X	
9	Besarnya kemungkinan ancaman yang di dapat dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya		X			
10	Besarnya kemungkinan ancaman yang di dapat dari kegagalan sistem operasi yang melebihi perkiraan operasi				X	
11	Besarnya kemungkinan ancaman yang di dapat dari kegagalan jaringan karena penuaan dan penipisan sumber daya		X			
12	Besarnya kemungkinan ancaman yang di dapat dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Besarnya kemungkinan ancaman yang di dapat dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Besarnya kemungkinan ancaman yang di dapat dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya kemungkinan ancaman yang di dapat dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
16	Besarnya kemungkinan ancaman yang di dapat dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

4. **Pilih skala nilai dari dampak yang akan muncul di Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU dari risiko yang sering dihadapi, isi sesuai dengan beri tanda (X) isi pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya dampak yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
2	Besarnya dampak yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU				X	
3	Besarnya dampak yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
Accidential						
4	Besarnya dampak dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya dampak dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
Structural						
6	Besarnya dampak dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya			X		
7	Besarnya dampak dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya dampak dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya		X			
9	Besarnya dampak dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Besarnya dampak dari kegagalan sistem operasi yang melebihi perkiraan operasi			X		
11	Besarnya dampak dari kegagalan jaringan karena penuaan dan penipisan sumber daya		X			
12	Besarnya dampak dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Besarnya dampak dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Besarnya dampak dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya dampak dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
16	Besarnya dampak dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

5. **Pilih nilai dari tingkat Risiko yang berpengaruh pada Laboratorium SMK Negeri 3 OKU Teknik Komputer dan Jaringan SMK Negeri 3 OKU, isi sesuai dengan risiko yang dihadapi dan beri tanda (X) pada pernyataan berikut.**

No	Deskripsi	1	2	3	4	5
Adversarial						
1	Besarnya risiko yang di bawa oleh *Outsider*/orang luar untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

2	Besarnya risiko yang di bawa oleh *Insider*/orang dalam untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
3	Besarnya risiko yang di bawa oleh *Trusted Insider*/orang Kepercayaan untuk mengekploitasi Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
Accidential						
4	Besarnya risiko dari tindakan keliru yang dilakukan *User* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
5	Besarnya risiko dari tindakan keliru yang dilakukan *Administrator* saat melaksanakan kegiatan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
Structural						
6	Besarnya risiko dari kegagalan peralatan penyimpanan karena penuaan dan penipisan sumber daya		X			
7	Besarnya risiko dari kegagalan peralatan pemrosesan karena penuaan dan penipisan sumber daya			X		
8	Besarnya risiko dari kegagalan peralatan komunikasi karena penuaan dan penipisan sumber daya			X		
9	Besarnya risiko dari kontrol suhu ruangan karena penuaan dan penipisan sumber daya			X		
10	Besarnya risiko dari kegagalan sistem operasi yang melebihi perkiraan operasi			X		
11	Besarnya risiko dari kegagalan jaringan karena penuaan dan penipisan sumber daya		X			
12	Besarnya risiko dari virus yang masuk ke peralatan yang melebihi perkiraan operasi pada perangkat			X		
Environmental						
13	Besarnya risiko dari api yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
14	Besarnya risiko dari angin/hujan badai yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
15	Besarnya risiko dari Telekomunikasi yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		
16	Besarnya risiko dari Tenaga Listrik yang menyebabkan kerusakan luas pada fasilitan di Laboratorium Teknik Komputer dan Jaringan SMK Negeri 3 OKU			X		

Journal of Informatics and Telecommunication Engineering
Sekretariat : Universitas Medan Area, Gedung Fakultas Teknik, Program Studi Informatika
Alamat : Jalan Kolam Nomor 1 Medan Estate/Jalan PBSI Nomor 1
E-mail : jite@uma.ac.id

Nomor : 032/UMA/JITE/VII/2019 Medan, 08 Juli 2019
Lamp : 1 lembar
Hal : Surat Penerimaan Naskah Publikasi Jurnal

KepadaYth :
Bapak/Ibu **Arlin Nurliyani**

Assalamu'alaikum Wr. Wb

Kami mengucapkan terima kasih banyak atas partisipasi Bapak yang telah *submit paper* di *Journal of Informatic and Telecommunication Engineering* (JITE) Volume 3 Nomor 1 tahun 2019. Dengan ini kami sampaikan bahwa, *paper* yang bertanda dibawah ini :

Judul : Assessment It Risk Management Pada Laboratorium Teknik Komputer Dan Jaringan Smk Negeri 3 OKU
Penulis : 1. Arlin Nurliyani
2. Dedy Syamsuar, P.hD
3. A.Haidar Mirza, S.T., M.Kom.

Berdasarkan hasil *review, paper* yang Bapak/Ibu kirimkan **dinyatakan DITERIMA** untuk diterbitkan pada Jurnal JITE Volume 3 No 1, Juli 2019 ISSN:2549-6247 (Print) ISSN: 2549-6255 (Online). Selanjutnya, kami menginformasikan hal-hal sebagai berikut : Hasil perbaiki *paper* (jika ada) diharapkan untuk dikirim kembali paling lama tanggal 12 juli 2019 agar dapat segera diterbitkan.

Demikian surat ini kami sampaikan, atas perhatian dan kerjasamanya yang baik dari Bapak/Ibu, kami ucapkan terima kasih

Wassalamu'alaikum, Wr.Wb.

Hormat kami,

Muhathir, ST., M.Kom
Pimpinan Redaksi

Universitas Bina Darma

PROGRAM PASCASARJANA

SERTIFIKAT

KUNJUNGAN INDUSTRI

SINGAPURA - MALAYSIA

18 - 22 AGUSTUS 2017

Arlin Nurliyani

SERTIFIKAT DIBERIKAN KEPADA :

ATAS PARTISIPASINYA SEBAGAI PESERTA
YANG DILAKSANAKAN OLEH PROGRAM PASCASARJANA UNIVERSITAS BINA DARMA

Dr. Ir. Hj. Hasmawaty AR, M.M., M.T
Direktur Pascasarjana

Universitas Bina Darma *ISO 9001 :2001*	**FORMULIR PERBAIKAN TESIS**	Nomor Dok :	IK/TA-MM/01
		Nomor Revisi :	0[redacted]
		Tgl. Berlaku :	01 Juli 2017
		Klausa ISO :	7.5.1 dan 8.2.3

Nama : ARLIN NURLIYANI

NIM : 162420001

KONSENTRASI : ENTERPRISE IT INFRASTRUCTURE

JUDUL TESIS : ***ASSESSMENT IT RISK MANAGEMENT*** **PADA LABORATORIUM TEKNIK KOMPUTER DAN JARINGAN SMK NEGERI 3 OKU**

Dosen Pembimbing I : Dedy Syamsuar, Ph.D.

Dosen Pembimbing II : A. Haidar Mirza, S.T., M.Kom.

Tanggal Ujian : 27 Februari 2019

Telah diperbaiki dan di konsultasikan dengan pembimbing/penguji Tesis

No	Nama Dosen Penguji	Tanggal	Tanda Persetujuan
1.	Dedy Syamsuar, Ph.D.		1.....
2.	A. Haidar Mirza, S.T., M.Kom.		2.....
3.	Dr. Widya Cholil, S.Kom., M.TI.		3.....
4.	Dr. Edi Surya Negara, M.Kom		4.....

***Nb**
Pembimbing 2 harap memeriksa kembali format dari tesis yang telah di perbaiki dan keabsahan tanda tangan penguji

Palembang, 27 Februari 2019
Program Studi Teknik Informatika- S2
Ketua,

Darius Antoni, S.Kom., M.M., Ph.D.

Universitas Bina Darma ISO 9001 : 2000	**FORMULIR** **Berita Acara Ujian Tesis**	Nomor Dok :	FRM/TA-MM/01
		Nomor Revisi :	01
		Tgl. Berlaku :	01 Juli 2007
		Klausa ISO	7.5.1 dan 8.2.3

LAMPIRAN II : CATATAN TIM PENGUJI UJIAN TESIS

Nama	:	ARLIN NURLIYANI
Nim	:	162420001
Konsentrasi	:	ENTERPRISE IT INFRASTRUCTURE
Judul	:	ASSESMENT IT RISK MANAGEMENT PADA LABORATORIUM TEKNIK KOMPUTER JARINGAN SMK NEGERI 3 OKU

Nama Dosen Penguji :	Tanda Tangan	Catatan
Dedy Syamsuar, Ph.D. (.....)		
A. Haidar Mirza, S.T., M.Kom. (.....)		
Dr. Widya Cholil, S.Kom., M.IT. (.....)		
Dr. Edi Surya Negara, M.Kom. (.....)		

Palembang , 27 Februari 2019
Program Studi Teknik Informatika – S2
Ketua,

Darius Antoni, S.Kom., M.M., Ph.D.

Universitas Bina Darma
PASCASARJANA

SURAT KETERANGAN

Nomor: 065/PPs-UBD/II/2019

Direktur Program Pascasarjana Universitas Bina Darma, menerangkan bahwa:

Nama : Arlin Nurliyani

Nim : 162420001

Konsentrasi : Enterprise IT Infrastructure

telah menyelesaikan studinya di Program Pascasarjana Program Studi Teknik Informatika – S2 dan dinyataka **LULUS** pada hari Rabu , tanggal 27 Februari 2019 dengan judul Tesis :

***Assesment IT Risk Management* Pada Laboratorium Teknik Komputer Jaringan SMK Negeri 3 OKU**

dan yang bersangkutan juga telah berhak untuk menggunakan gelar akademik Strata 2 (S2) dengan sebutan **MAGISTER KOMPUTER (M.KOM)**

Demikian Surat Keterangan ini dibuat untuk dipergunakan sebagaimana mestinya.

Dikeluarkan di : Palembang
Pada Tanggal : 27 Februari 2019
Program Pascasarjana,
Direktur

Dr. Ir. Hj. Hasmawaty AR, M.M., M.T.

Universitas Bina Darma *ISO 9001 :2001*	**FORMULIR KELAYAKAN PENJILIDAN**	Nomor Dok :	IK/TA-MM/01
		Nomor Revisi :	01
		Tgl. Berlaku :	01 Juli 2017
		Klausa ISO :	7.5.1 dan 8.2.3

Nama : ARLIN NURLIYANI
NIM : 162420001
KONSENTRASI : ENTERPRISE IT INFRASTRUCTURE
JUDUL TESIS : ***ASSESSMENT IT RISK MANAGEMENT*** **PADA LABORATORIUM TEKNIK KOMPUTER DAN JARINGAN SMK NEGERI 3 OKU**
Dosen Pembimbing I : Dedy Syamsuar, Ph.D.
Dosen Pembimbing II : A. Haidar Mirza, S.T., M.Kom.
Tanggal Ujian : 27 Februari 2019

Point Chek :

1. COVER TESIS	✓
2. HALAMAN DEPAN	✓
3. HALAMAN PENGESAHAN PENGUJI	✓
4. HALAMAN PENGESAHAN PEMBIMBING	✓
5. SURAT PERNYATAAN	✓
6. ABSTRAK (BAHASA INDONESIA)	✓
7. ABSTRACT (BAHASA INGGRIS)	✓
8. MOTTO DAN HALAMAN PERSEMBAHAN	✓
9. KATA PENGANTAR	✓
10. DAFTAR ISI	✓
11. DAFTAR TABEL	✓
12. DAFTAR GAMBAR	✓
13. DAFTAR LAMPIRAN	✓
14. ISI TESIS (BAB I S/D BAB VI)	✓
15. DAFTAR PUSTAKA	✓
16. DAFTAR RIWAYAT HIDUP	✓
17. LAMPIRAN-LAMPIRAN	✓
➢ SK PEMBIMBING	✓
➢ SURAT IZIN PENELITIAN	✓
➢ LEMBAR KUESIONER	✓
➢ HASIL PENGELOLAHAN DATA	✓
➢ JURNAL DAN SERTIFIKAT SEMINAR	✓
➢ LEMBAR PERBAIKAN TESIS	✓

Dengan ini dinyatakan **layak** untuk dijilid sesuai dengan format yang berlaku dilingkungan Program Pascasarjana Program Studi Teknik Informatika – S2 Universitas Bina Darma

Pemeriksa Kelayakan,
Pembimbing I,

Dedy Syamsuar, Ph.D