MANAJEMEN INSIDEN DALAM PENGELOLAAN INFRASTRUKTUR TEKNOLOGI INFORMASI (Studi Kasus UPT Laboratorium STMIK AMIKOM YOGYAKARTA)

Tri Susanto
Program Studi Teknik Informatika
Program Pascasarjana, STMIK AMIKOM Yogyakarta
M3susanto@gmail.com

Abstrak

Membangun kontrol internal yang kuat dalam Teknologi Informasi (TI) dapat membantu organisasi untuk meningkatkan pemahaman tentang TI di kalangan eksekutif, membuat keputusan bisnis yang lebih baik dalam kualitas yang lebih tinggi dan informasi lebih tepat waktu, menyelaraskan berbagai inisiatif proyek dengan kebutuhan bisnis, mencegah hilangnya sumber daya dan kemungkinan pelanggaran sistem. Pengukuran layanan IT dengan menggunakan maturity level pada insiden, dengan menggunakan metode deskriptif dan metode kuantitaif (kusioner). Dilakukan sebagai langkah untuk melihat tingkatan kematangan dari divisi Technical support. Dengan diketahuinya tingkatan/level tersebut akan mudah menentukan proses selanjutnya guna meningkatkan layanan TI tersebut. Pengukuran difokuskan pada manajeman insiden pada divisi Technical Support. Pembuatan dokumen tatalaksana dikembangkan sebagai tujuan utama untuk membantu divisi helpdesk dalam melakukan pendokumentasian dan mendukung layanan IT yang terdiri dari 10 aktifitas,yang dibangun untuk menjadi kesimpulan keseluruhan proses program. Matriks dalam dokumen tatalaksanan yang dibuat berisikan masing-masing aktifitas dalam program berikut dengan tujuan, indicator kinerja, formulir dan dokumen yang diperlukan untuk pelaksanaan aktifitas,yang digunakan untuk menilai terhadap setiap prosedur dalam pelaksanaan manajemen insiden di UPT STMIK AMIKOM Yogyakarta.

Keywords: *ITIL, Manajemen insiden.*

A. PENDAHULUAN

Membangun kontrol internal yang kuat dalam Teknologi Informasi (TI) dapat membantu organisasi untuk meningkatkan pemahaman tentang TI di kalangan eksekutif, membuat keputusan bisnis yang lebih baik dalam kualitas yang lebih tinggi dan informasi lebih tepat waktu, menyelaraskan berbagai inisiatif proyek dengan kebutuhan bisnis, mencegah hilangnya sumber daya dan kemungkinan pelanggaran sistem (Fox dan Zonneveld, 2003). Semua itu digunakan untuk mengoptimalkan teknologi informasi dalam meningkatkan

kompetensi manajemen insiden dalam perusahaan yang sasaran strategisnya pada bidang Pengukuran, Analisis, dan Pengelolaan Pengetahuan, yaitu membangun infrastruktur teknologi informasi yang handal dan aman yang diselaraskan dengan kebutuhan dan arah organisasi (BPK, 2006). Agar penanganan insiden dapat semakin baik dan mengurangi ketergantungan terhadap staf tertentu, diperlukan sebuah dokumen tata laksana mengenai manajemen insiden yang berdasarkan framework tata kelola TI. Dengan adanya dokumen tata laksana manajemen insiden, semua karyawan di UPT STMIK AMIKOM Yogyakarta dapat mengetahui fungsi dan tanggungjawabnya serta juga langkah-langkah yang harus diambilnya dalam penanganan suatu insiden, untuk mengurangi terjadinya kesalahan atau kekacauan dalam infrastruktur teknologi informasi yang digunakan.

Untuk pengelolaan eksploitasi layanan Teknologi Informasi dan Komunikasi (TIK) organisasi dapat menggunakan ITIL (*Information Technology Infrastructure Library*).Metode ITIL muncul ketika di Inggris sektor publik mulai memprivatisasi eksploitasi ICT dan kepala sekolah ingin memiliki pegangan pada layanan disediakan oleh departemen ini TIK diprivatisasi.Ini disebut untuk memperoleh wawasan dalam tugas-tugas yang harus ditangani oleh sebuah TIK organisasi. Tidak hanya deskripsi tugas dilihat terpisah adalah penting, tetapi juga hubungan antara berbagai tugas dan jalannya proses dalam berbagai tugas harus jelas. Implementasi ITIL harus mengarah kepada pelaksanaan manajemen proses penyediaan layanan pertemuan tingkat layanan tertentu (Thiadens et al., 2000). Meskipun ITIL mencakup sejumlah bidang, fokus utamanya adalah pada IT *Service Management* (ITSM), yang dengan sendirinya umumnya dibagi menjadi dua bidang utama: Layanan Dukungan dan Pelayanan. Bersama-sama, kedua bidang terdiri dari disiplin yang bertanggung jawab untuk penyediaan dan pengelolaan layanan TI yang efektif (http://www.itil-itsmworld.com/ what.htm).ini merupakan salah satu penggunaan *Framework* ITIL dalam penelitian ini, dimana ITIL memiliki fokus pengembangan tata kelola TI khususnya dalam hal layanan (*IT service*). Selain itu *framework* ITIL sangat tepat digunakan sebagai panduan dalam mengembangkan sebuah tata laksana karena

sifatnya *best practice* dan memiliki *library* yang terinci untuk mengembangkan langkah-langkah dalam prosedur.

B. METODOLOGI PENELITIAN

Metode penelitian yang dilakukan dalam pengelolahan dan menganalisa data meliputi langkah berikut:

1. Studi Literatur dan Identifikasi Permasalahan.

   Pada tahap ini dilakukan pencarian literatur berupa buku, jurnal, artikel, ataupun sumber ilmiah lainnya yang membahas mengenai panduan audit IT, ITIL, manajemen insiden, serta metode penilaiannya. Tahap ini dilakukan untuk memahami kriteria serta metode dan prosedur untuk mengaudit.

2. Pengumpulan Informasi dan Analisa.

   Dalam tahap ini dilakukan aktifitas penelaahan dokumen tata kelola Teknologi Informasi UPT Laboratorium STMIK AMIKOM.Selain itu juga dilakukan studi literatur framework ITIL v3. Mengolah informasi dan data internal UPT, khususnya pelaksanaan manajemen insiden pada Bagian Operasional dan Dukungan Teknologi Informasi, bagian Teknologi Informasi, serta prosedur auditinternal yang berlaku. Pengumpulan informasi dilakukan dengan metode observasi dokumen dan wawancara dengan pihak terkait.

3. Analisa Informasi Teridentifikasi

   Dalam tahap ini akan dilakukan verifikasi masing-masing bagian dari dokumen tata laksana untuk mengetahui apakah masing-masing aktifitas dalam dokumen sudah sesuai dengan tujuannya dan dapat dilaksanakan. Selain lampiran-lampiran.Dari informasi yang sudah diidentifikasikan tersebut, dilakukan analisa tiap aktivitas untuk mendapatkan alur aktivitas dalam proses manajemen insiden. Hasil analisa tersebut akan digunakan sebagai bahan pengembangan panduan audit.

4. Pengembangan Panduan Audit

   Tahapan ini adalah memetakan proses manajemen insiden ITIL ke dalam prosedur audit manajemen insiden IT yang berjalan di UPT Laboratorium STMIK AMIKOM. Dalam tahap ini dilakukan langkah-langkah:

   a. Pendahuluan; Dalam tahap ini dilakukan pendefinisian mengenai latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian serta metodologi yang digunakan untuk memecahkan permasalahan, yaitu pembuatan dokumen tata laksana proses manajemen insiden.
   b. Pengumpulan Informasi dan Analisa; Dalam tahap ini dilakukan aktifitas penelaahan dokumen tata kelola UPT STMIK AMIKOM. Selain itu juga dilakukan studi literatur *framework* ITIL.
   c. Pengukuran layanan IT dengan menggunakan *maturity level* pada insiden, dengan menggunakan metode deskriptif dan metode kuantitaif (kusioner). Dilakukan sebagai langkah untuk melihat tingkatan kematangan dari divisi *Technical support*. Dengan diketahuinya tingkatan/*level* tersebut akan mudah menentukan proses selanjutnya guna meningkatkan layanan TI tersebut. Pada tahapan ini akanmenggunakan matrik manajemen insiden (Dugmore, Ivor Macfarlane and Jenny, 2006). Pengukuran difokuskan pada manajeman insiden pada divisi *Technical Support*. Dengan menggunakan komponen tersebut diharapkan dapat melihat :
      1) Untuk mengembalikan layanan kepada pengguna/user secepat mungkin.
      2) Untuk meminimalkan dampak negatif terhadap kegiatan operasional.
      3) Untuk menjamin penggunaan sumber daya terbaik.
      4) Untuk menjaga dan menerapkan pendekatan yang konsisten untuk mengelola insiden.
      5) Untuk mengidenfitikasi masalah yang sering terjadi.

d. Pengukuran kinerja pada manajemen insiden (tahap I)

Adalah langkah yang dilakukan untuk melihat posisi tata kelola *technical support* terhadap pencapaian SLA yang dipengaruhi dari tata kelola insiden dan problem. Pengukuran performa menggunakan matrik ITIL v3 pada komponen manajemen insiden dan problem. Dalam mengukur kinerja salah satunya menggunakan matrik manajemen insiden (Taylor, 2007) dengan melakukan *questioner* dalam wawancara dan pembacaan log meliputi:

1) Total jumlah insiden (sebagai *control*).
2) Rincian insiden dalam setiap tahapan (*logged, process, closed*).
3) Ukuran dari *backlog* kejadian saat itu.
4) Jumlah dan persentase insiden utama.
5) Rata-rata waktu untuk menyelesaikan insiden.
6) Persentase Insiden yang ditangani berdasarkan waktu yang disepakati (sesuai yang ada di SLA, misal: berdasarkan dampak dan kode urgensi).
7) Jumlah insiden yang dibuka kembali terhadap persentase total insiden.
8) Jumlah dan persentase insiden yang salah penangganan.
9) Jumlah dan persentase insiden yang salah kategori.
10) Persentase insiden ditutup oleh *service desk/technical support* tanpa referensi ke level support lainnya.
11) Jumlah dan persentase insiden di proses per *service desk/technical support* staf.
12) Jumlah dan persentase insiden berhasil di tangani tanpa datang ke lokasi (remote desktop).
13) Jumlah insiden ditangani oleh masing-masing insiden model.
14) Rincian insiden berdasarkan waktu dalam sehari untuk melihat dan menemukan puncak waktu insiden.

Dengan adanya penangganan manajemen insiden maka diharapkan faktorfaktor kritis dapat diatasi, meliputi:

1) Sebuah *service desk/technical support* yang baik adalah kunci sukses untuk manajemen insiden.
2) Target pekerjaan yang jelas sesuai dengan SLA.
3) Pelatihan yang memadai berorientasi pelanggan dan secara teknis mendukung staf dengan tingkat keterampilan yang benar, pada semua tahap proses.
4) Alat-alat pendukung yang terintegrasi untuk mendorong dan mengendalikan proses.
5) OLA (*Operational Level Agreement*) dan UC (*Underpinning Contracts*) mampu membentuk dan mempengaruhi perilaku staf support.

e. Pembuatan Dokumen Tata Laksana; Dalam tahap ini dilakukan pembuatan dokumen tata laksana berdasarkan hasil analisa di langkah sebelumnya. Dokumen prosedur yang dibuat akan terdiri dari rincian aktifitas manajemen insiden, dan lampiran-lampiran kategori insiden, prioritas insiden, metrik dan CSF (*Critical Success Factor*), SLA (*Service Level Agreement*) serta diagram RACI. Selain lampiran-lampiran diatas, akan dibuat juga diagram flow chart yang menggambarkan tiap aktifitas yang dilakukan.
f. Verifikasi Dokumen Tata Laksana; Dalam tahap ini akan dilakukan verifikasi masing-masing bagian dari dokumen tata laksana untuk mengetahui apakah masing-masing aktifitas dalam dokumen sudah sesuai dengan tujuannya dan dapat dilaksanakan.
g. Validasi Dokumen Tata Laksana; Dalam tahap ini akan dilakukan validasi terhadap dokumen tata laksana untuk mengetahui apakah tujuan utama dari proses manajemen insiden sudah terpenuhi dengan dokumen ini.
h. Kesimpulan; Dalam tahap ini akan dilakukan perumusan kesimpulan dari keseluruhan langkah yang dilakukan dan hasil yang didapat.

5. Pembuatan dokumen

   Membuat dokumen-dokumen yang diperlukan dalam proses pelaksanaan audit yang meliputi *Audit Checklist* dan form penilaian, serta template laporan dan formulir lainnya yang dapat memudahkan kerja auditor dalam mengaudit manajemen insiden IT di UPT. STMIK AMIKOM Yogyakarta.

C. PEMBAHASAN

1. Deskripsi Kasus

Dalam penelitian ini, peneliti pada kesempatan awal melakukan observasi serta interview kepada kepala bagian UPT dan staff pada bagian tersebut, yang digunakan untuk memperoleh data awal untuk menganalisis suatu insiden dalam manajemen tersebut sertauntuk mengetahui apa saja yang menjadi konsentrasi dalammenjalankan operasional organisasi TI dalam UPT. Dari hasil diskusi tersebut, bahwa pengaruh insiden dalam layanan IT yang akan dianalisis menggunakan data laporan insiden, yang terjadi dari bulan januari 2011 sampai dengan april 2012. Yang meliputi dari insiden yang terjadi serta penanganan insiden tersebut. Proses manajemen insiden (*incident management*) dimulai dengan identifikasi. Identifikasi yang paling umum dilakukan adalah melalui layanan *service desk* dan laporan dari staf teknisi.Selain itu identifikasi insiden dapat dilakukan secara otomatis oleh *tool event management* yang dipasang pada perangkat-perangkat utama.Kondisi ideal dari langkah identifikasi adalah insiden dapat teridentifikasi sebelum terjadi implikasi terhadap user.Dimana manajemen insiden adalah semua kejadianyang bukan bagian dari operasional standar layanan dan yang menyebabkanatau dapat menyebabkan sebuah gangguan, penurunan kualitas dari layanantersebut (Taylor, 2007).Dalam membuat kategori insiden dibutuhkan sebuah proses khusus antara pengelola IT dan pihak manajemen organisasi. Hal ini bertujuan untuk menghasilkan kategori insiden dan prioritas penanganannya sejalan dengan proses bisnis organisasi. Kategori insiden dapat dibuat berdasarkan perkiraan lamanya penanganan, implikasi terhadap proses bisnis organisasi, dan jumlah staf teknis terkait.

Maka dari kedua definisi tersebut dan hasil pengamatan dilapangan dan laporan harian masalah (lihat pada lampiran), dapatdikelompokkan faktor-faktor penyebab insiden diantaranya adalah sebagai berikut:

1. *Software* (misal: terkena virus, *software* bajakan, *request software*dan sebagainya).
2. *Hardware* (misal: permintaan barang, perbaikan/*service* yang tidaksesuai dengan SOP).
3. *User*/pengguna (misal: salah hapus program atau pemakaian*hardware* yang tidak seharusnya atau pengerusakan *hardware*).
4. Network (misalnya kerusakan jaringan, *not conneteced*)
5. Staf TI (misal: staf IT kesalahandalam penangganan gangguan).

2. Analisa Sistem

a. *Event Management*

1) Konfigurasi Sistem : Laboratorium (UPT) STMIK AMIKOM Yogyakarta telah menggunakan sistem informasi yang telah terintregrasi dengan baik, dimana segala kegiatan operasional telah terintegrasi dengan baik oleh system komputer. Yang tujuannya dari pembuatan sistem sebagai wujud pihak manajemen yang berbasis IT dengan cara penerapan segala sesuatu untuk mempelancar proses operasional sehingga dapat mengefesienkan waktu. Sehingga direkomendasikan bahwa dalam penerapan sistem selama ini telah berjalan lancar hanya ada kekurangan sistem bila dilihat dari sisi *user*, serta mengadakan *training* karyawan sebelum karyawan bekerja, atau mengadakan *training* untuk memanage sebelum/sesudah terjadi kesalahan, atau melakukan sertifikasi terhadap para laboran untuk meningkatkan skill/kemampuan dalam menangani kesalahan yang akan terjadi di laboratorium.
2) Konfigurasi sistem operasi yang dipakai oleh Laboratorium UPT STMK AMIKOM Yogyakarta yaitu *Windows, Linux, Ubuntu* Dan *Machintosh* : Konfigurasi system selama ini akan dilakukan, apabila terjadi sesuatu kesalahan/*error* saja, ini yang membedakan antara insiden manajemen

dengan manajemen masalah, dimana insiden manajemen dilakukan apabila terjadi kesalahan/kerusahan, sedangkan manajemen masalah membuat suatu aturan sebelum terjadi suatu masalahan. Kesalahan/error pada sistem operasi selama ini sangat jarang terjadi, apabila terjadi pun hanya masalah yang tidak sampai merusak aplikasi dalam *software*. Direkomendasikan untuk :untuk para manajemen untuk lebih merespon konfigurasi dengan proaktif, yang tujuannya adalah agar tidak terjadi *error* tiap waktu, dengan melakukan kontrol sistem operasi setiap hari baik sebelum penggunaan laboratorium maupun sesudah menggunakan laboratorium, serta penghindaran dari penggunaan *software* bajakan. Periksa HCL untuk menentukan apakah ada *driver* yang kompatibel dengan *Windows* dan tersedia untuk adaptor nirkabel

3) Konfigurasi *database :*UPT Laboraturium selama ini menggunakan *database ORACLE.* Dimana pihak UPT sering melakukan konfigurasi pada sistem operasi dan aplikasi, dilakukan secara berkala dan kontinu sesuai kebutuhan.Agar dapat memanage semua kegiatan opersional di sarankan untuk Menambahkan jumlah *server database* pada UPT laboratorium. Dalam penangan kesalahan/mengurangi kesalahan dalam database, disarankan bagian laboran harus proaktif dalam melakukan pengecekan database, dengan cara selalu mengontrol konfigurasi secara rutin, sehingga apabila terjadi masalah dapat di deteksi lebih awal. Dan selalu melakukan kontrol terhadap data apa saja yang keluar atupun masuk sistem. Sehingga tidak terjadi penyalah gunaan terhadap sistem.Selain itu rutin melakukan *back up* harian untuk *database.*

4) Konfigurasi *server :*Untuk pengaturan *server ORACLE* dilakukan secara rutin tiap tahunnya atau berkala untuk mengetahui kondisi dari *server ORACLE*. Server akan di-*shutdown* dan di cek sesuai kebijakan perusahaan, jika *server* memang berjalan normal, tidak perlu di konfigurasi ulang. Direkomendasikan untuk lebih merespon suatu kejadian/*event* lebih proaktif, pastikan juga strategi keamanan sudah terjamin untuk melakukan pemonitoran berkala, tidak hanya melakukan

back up harian, tapi juga melakukan kontrol pemakaian setiap harian, untuk menangani masalah menurut kriterianya.

5) Konfigurasi *network :*UPT dalam menangani suatu jaringan mempunyai system prosedur yaitu dengan *Change Application* (semua kegiatan terekam dalam *server*), sehingga konfigurasi jaringan bisa dilakukan dengan mudah. Direkomendasikan untuk lebih cepat tanggap atau merespon dengan cepat, apabila terjadi suatu kerusakan/*error* yang menyebabkan *offline* pada sistem komputer di laboratorium. Pengecekan dapat dilakukan secara berkala dengan pengecekan keadaan/kondisi kabel LAN, keteraturan pemasangan dan pengurutan, semua ini akan bergunakan apabila terjadi kerusakan maka pihak laboran dengan cepat memperbaiki/menanggulangi suatu kerusakan. Dimana dalam melakukan pemasangan jaringan dalam laboratorium telah teratur dan sesuai dengan prosedur yang berlaku, sehingga lebih mudah dalam pengkontrolan/pengecekan. Pendeteksian yang dilakukan, dapat berguna apabila jaringan ada pengembangan kearah penambahan *Bandwidth Management* yang ber-*continue,* dan selalu terkontrol, lalu administrator jaringan wajib mendiagnosis permasalahan perangkat yang tersambung dengan jaringan secara teratur.
6) *Software License Monitoring :*yaitu bagian UPT melakukan pemantau terhadap penggunaan *software* yang dilakukan secara berkala dan kontinu, untuk mengetahui apabila terjadi kerusakan/*error* terhadap *software* dengan kebijakan yang berlaku di dalam penggunaan dan perawatan *software*.
7) Monitoring Hardware : yaitu pengecekan atau perawatan yang dilakukan oleh pihak UPT terhadap perangkat *hardware* yang berada di laboratorium STMIK AMIKOM, agar pada saat penggunaan komputer tidak terjadi kerusakan atau komputer bisa digunakan sebagaimana mestinya, serta melakukan *update* terhadap perangkat hardware sesuai dengan kebutuhan, dan pemantau terhadap data yang masuk maupun yang keluar agar tidak terjadi *over* pada penyimpanan data.

Direkomendasikan agar penjaga terhadap tiap laboratorium selama terlaksananya proses pembeajaran di laboratorium, supaya pada saat terjadi kesalahan langsung bisa ditanggani dengan cepat.

8) Kegiatan normal perusahaan : yaitu kegiatan yang menunjang dalam operasional sehari-hari dalam UPT laboratorium, ada beberapa item yaitu:
   a) Monitoring laboratorium, seperti pemantauan dengan menggunakan camera CCTV untuk kegiatan di semua laboratorium tanpa harus diawasi terus-menerus dimana semua kegiatan terrekam dan ter-*record*, *remote desktop*, line telepon dan HT (komunikasi), yang digunakan sebagai sarana komunikasi antara user dan pihak teknisi bagian UPT, apabila terjadi kerusakan/error di laboratorium, yang bertugas untuk menanggani kerusakan. Dan juga untuk menangani masalah pada *hardware, software*, kegiatan praktikum dan penanganan asset (ac, sound, meja, kursi, lemari dll).
   b) *Maintenace*/perawatan rutin, seperti *hardware*, *software*, kegiatan praktikum dan penanganan asset, apabila terjadi kerusakan maka akan langsung ditanggani agar tidak terjadi kerusakan yang makin parah.
   c) Instalasi dan konfigurasi, seperti untuk aplikasi software yang digunakan pada masing-masing laboratorium.
   d) *Backup* dan *restore*, seperti untuk data-data (materi dosen untuk kegiatan pembelajaran) dan memantau data yang masuk atau pun yang keluar, agar tidak terjadi penumpukan data/kelebihan kapasitas dalam penyimpanan data.
   e) Administrasi laboratorium, seperti kegiatan surat menyurat dan pembuatan anggaran yang masuk/keluar, serta dokumentasi kegiatan di laboratorium..

Dalam penangganan *event* yang terjadi di UPT laboratorium sudah terdokumentasi dan terstruktur dengan baik.Dimana *event* yang terjadi hanya di deteksi secara umum saja, serta untuk penangganannya dilakukan secara simpel dan sederhana apabila terjadi suatu kerusakan yang tidak terlalu serius.

Untuk penanganannya hanya dilakukan apabila terjadi suatu masalah saja, selebihnya hanya dilakukan monitoring secara rutin untuk mencegah terjadinya kesalahan. Serta belum tersedianya aplikasi yang dapat mencegah sebelum terjadinya kerusakan. Jadi untuk penangannya hanya didukung dengan peralatan yang sudah memenuhi standar teknologi, seperti :

1) Camera CCTV, yang digunakan untuk memantau kegiatan atau kejadian yang terjadi selama proses pembelajaran, seperti kerusakan yang diperbuat oleh siswa, pencurian alat dan sebagainya.
2) *Remote desktop*, yang digunakan untuk memantau kegiatan dalam aplikasi komputer selama proses pembelajaran.
3) Line telepon, yang digunakan untuk pelaporan apabila terjadi kerusakan pada sistem baik *software* maupun *hardware* di laboratorium.
4) HT, yang digunakan sebagai komunikasi antar bagian teknisi laboratorium untuk monitoring kegiatan.

***b. Incident Manajement*(manajemen insiden)**

Incident Management adalah sebuah penanganan dan pencegahan suatu kejadian / masalah yang akan mempengaruhi IT *Service* suatu organisasi. Hal ini meliputi memastikan bahwa suatu masalah diperbaiki, setelah terjadinya kesalahan/kerusakan tetapi harus dengan cara*responsivenees* atau secara cepat sehingga dapat memberikan pelayanan yang baik bagi *user*. Serta mencegah terjadinya kembali masalah yang sama, dan melakukan perawatan dan pencegahan untuk mengurangi masalah-masalah ini muncul pada saat pertama kali. Perbedaan antara *Incident Management* dan *Problem Management* adalah dari cara penyelesaiannya. *Incident Management* akan menyelesaikan masalah apabila terjadi masalah. Sedangkan *Problem Management* akan menyelesaikan sebelum masalah terjadi, dan hal tersebut dilakukan secara permanen.

Tugas pokok dari penangan incident di laboratorium adalah bagian utama dari bagian helpdesk.Yang mencakup pada proses manajemen insiden yaitu: Memberikan pelayanan dan solusi kepada pengguna di

laboratorium selama proses pembelajaran terkait dengan permasalahan TI; dan Menerima keluhan dari pengguna dan menyelesaikan keluhan tersebut. Dalam operasionalnya Sub Bagian Dukungan TI terdiri dari 2 bagian helpdesk yaitu pada operator dan teknisi. Dimana bagian helpdesk operator merupakan bagian utama yang menerima terjadinya keluhan atau permasalahan pada laboratorium, serta memberikan solusi dalam penanganan pertama, apabila tidak bisa baru kemudian disampaikan ke bagian helpdesk teknisi yang akan menanggani terjadinya kerusakan/masalah-masalah yang terjadi langsung ketempat terjadinya kerusakan.

Deskripsi manajemen insiden yang terjadi, antara lain :

a) *Easy file server* : User tidak bisa mengakses *file*dikarenakan *server down*, serta tidak bisa digunakan sebagai *sharing file* yang disebabkan oleh *sistem easy file server* mengalami error. Beberapa hal yang bisa memicu *server error* adalah *server* terkena virus, banyak nya *user* yang mengdownload atau *upload* melebihi kapasistas memory yang menyebabkan terjadinya kerusakan atau tersambar petir.Dari semua permasalahan yang terjadi yang menyebabkan *server error* bukan suatu masalah bagi pihak UPT, karena selama ini pihak UPT sudah memperhitungkan efek nya dan dapat mem-*back up* data-data yang tersimpan. Direkomendasikan untuk lebih meningkatkan keamanan data, melakukan pengecekan setiap saat serta pemantau terhadap sistem *easy file server* secara berkala, dengan penenpatan SDM yang memadai dalam mengatasi permasalahan.
b) Insiden tehadap perangkat *Hardware* : dalam penanganan terjadinya kerusakan yang berhubungan dengan perangkat keras harus melalui penanganan yang khusus. Insiden yang sering terjadi berdasarkan laporan harian yang diterima pihak UPT adalah masalah kerusakan *mouse*, kerusakan *keyboard*, layar monitor rusak atau jaringan ke *server offline*.Dalam masalah ini direkomendasikan apabila ada kerusakan langsung segera ditangani setelah terjadinya laporan kerusakan, untuk

mencegah terjadi kerusakan yang lebih fatal lagi. Serta meningkatkan pelayanan terhadap *user* selama proses belajar.

c) Insiden pada *software* :dimana kejadian insiden pada sistem operasi dan *software* aplikasi yang digunakan sebagai praktikum mahasiswa. Untuk sistem operasi yang digunakan selama ini adalah *windows XP, windows seven, linux, ubuntu* dan aplikasi *software* yang digunakan adalah *office, SPSS, POM for windows, C++, 3D max, dreamweaver, photoshop, coreldraw,* dsb. Dimana incident yang sering terjadi adalah aplikasi *software* belum terinstal atau aplikasi *software* terjadi *error*.Yang diindikasi kerusakan karena virus atau *human error* pada saat penggunaan. Direkomendasikan untuk *responsiveness* hal ini, sebaiknya UPT mengotomatisasikan proses *problem management* untuk menetapkan prosedur-prosedur yang berulang, yang melakukan identifikasi, mencatat dan mendiagnosa masalah, Perusahaan harus memiliki analisis proaktif dan pemrosesan, kinerja, ketersediaan, dan tren tingkat layanan untuk menangani masalah-masalah potensial, serta menghindari penggunaan *software* bajakan atau antivirus bajakan. Sehingga bisa meningkatkan kinerja dan pelayanan selama ini.

Berikut penjelasan bagian-bagiannya :

1) *Help Desk :*Mempunyai tugas menerima keluhan-keluhan *user* terhadap penggunaan sistem selama proses praktikum berlangsung. Setelah laporan diterima, maka pihak helpdesk operator memberikan atau melaporan keluhan tadi kepada helpdesk teknisi untuk menindaklanjuti permasalahan yang dilaporkan, sehingga masalah tersebut bisa di selesaikan dengan cepat dan effektif.

2) Bagian teknisi :Bertugas menganalisis masalah yang dialami *user* yang dilaporkan dari pihak operator.

3) *Hardware* dan *Software Maintenance :*Bertugas untuk menangani masalah pada *hardware* maupun *software* pada laboratorium. Atau melakukan perawatan atau pengecekan secara berkala terhadap fasilitas yang tersedia di laboratorium.

3. Pengukuran *Maturity Level* Pada Manajemen Insiden

Pada penelitian ini akan dilakukan pengukuran menggunakan metode wawancara kepada karyawan UPT secara keseluruhan terhadap kerja layanan IT yang digunakan untuk acuan mengetahui tolak ukur kesusksesan terhadap layanan IT yang diberikan selama ini. Dalam pengukuran ini, akan dilakukan dua kali pengukuran yaitu menggunakan pengukurandeskriptif (studi pustaka) dan pengukuran kuantitatif (kuesioner).Studi pustaka dilakukan sebagai dasar dalammelakukan analisis deskriptif melalui pemetaan atas kriteria dari masing-masing*maturity level*, sedangkan pada kusioner untuk mengetahui terhadap tingkat layanan IT dari masing-masing karyawan di UPT laboratorium.

a. Pengukuran deskriptif

Pengukuran deskriptif yang dilakukan pada penelitian ini dengan cara melakukan pemetaan ataskriteria dari masing-masing level kepada kondisi di divisi *technical support*.Dengan melakukan studi referensi atas kriteria dari masing-masing*maturity level*.Dari *maturity level* tersebutdijelaskan sebagai berikut:

1. *Initial*

Pada tingkatan initial ini, bahwa kondisi lingkungan organisasi yang sangat belum kestabilan dalam organisasi.Dimana individu telah mengenali kebutuhan untuk mengelola permasalahan dan mengetahui penyebabnya secara individu karena belum ada pembagian kerja yang jelas. Proses mengelola permasalahan merupakan issue yang belum dibahas secara serius. Belum ada proses dan kebijakan standar untuk mengelola permasalahan. Belum ada rencana pelatihan dan belum pernah diadakan pelatihan penanggulangan masalah secara formal. Belum ada rencana menggunakan *tools* khusus untuk mengelola insiden. Penanganan masalah dilaksanakan secara reaktif dan atas inisiatif sendiri.Tanggung jawab manajemen masalah tidak ditugaskan.Target tidak jelas dan belum ada pengukuran yang

dilakukan.Pada tingkat ini struktur organisasi masih kacau, dan belum ada nya pencatatan ataupun dokumentasi.

2. *Managed*

Pada tingkatan ini, dimana sebuah organisasi telah mencapai semuatujuan yang spesifik dan umum secara keseluruhan.Organisasi telah memastikan bahwa persyaratan yang dikelola dan prosesyang direncanakan, dilakukan, diukur dan dikendalikan. Disiplin prosestercermin dari tingkat *managed* ini membantu untuk memastikan bahwapada prakteknya semua proses dipertahankan pada saat terjadinyainsiden.Serta semua praktek dikelola dan didokumentasikandengan baik.Pada tingkat ini semua kegiatan telah terdokumentasi dengan baik.

3. *Defined*

Pada tingkatan ini, sebuah organisasi telah mencapai semua tujuan yangspesifik dan umum. Proses yang baik ditandai dan dipahami, dandijelaskan dalam standar, prosedur, alat, dan metode serta rencanamereka didokumentasikan secara terstruktur.Kebijakan dan peningkatan proses-proses pengelolaan insiden mulai distandardisasi dan didokumentasikan Kebutuhan*skill* yang diperlukan untuk pengelolaan permasalahan telah didefinisikan dan didokumentasikan secara menyeluruh. Rencana pelatihan formal telah disusun, tetapi pelaksanaannya masih tergantung kepada inisiatif individu.Kebutuhan adanya integrasi sistem pengelolaan permasalahan sudah disepakati dan dibuktikan dengan adanya dukungan pihak manajemen, serta alokasi anggaran untuk staf pengelola dan pelatihan. Rencana pengelolaan masalah siap digunakan dan sudah ada rencana otomatisasi proses. Penanggungjawab proses telah ditetapkan, tetapi kewenangannya masih terbatas. Perekaman, penelusuran masalah, dan penyelesaiannya telah disebar di antara tim penanggungjawab, menggunakan peralatan yang tersedia tanpa pemusatan. proses yang dikelola lebih proaktif menggunakan suatu pemahamantentang keterkaitan dari suatu kegiatan proses dan langkah-langkah rincidari dari suatu proses, produk kerja dan layanan.pada tingkat ini, proses hanya Kwantitatif diprediksi.

4*. Quantitatively Managed*

Prosesyang dipilih yang secara signifikan berkontribusi terhadap kinerja prosessecara keseluruhan. Dalam proses ini dipilih, dikontrol denganmenggunakan statistik dan teknik kuantitatif secara terstruktur.Tujuan kuantitatif untuk kualitas dan kinerja proses yangdijalankan dan digunakan sebagai kriteria dalam proses pengelolaan.Tanggungjawab dan kepemilikan proses sudah jelas dan terorganisir. Memberikan bantuan kepada para pengguna termasuk dalam hal pengelolaan data, fasilitas, dan operasional.Adanya pemberian reward/penghargaan pada karyawan yang diterapkan untuk meningkatkan motivasi kerja.Metode-metode dan prosedur-prosedur sudah didokumentasikan, dikomunikasikan dan diukur untuk menjamin efektifitas.Pengelolaan permasalahan diintegrasikan dengan proses-proses terkait lainnya.Pengetahuan dan tenaga ahli sudah memadai, dikelola dengan baik dan dikembangkan ke tingkat yang lebih tinggi.Dengan adanya pelatihan secara berkala untuk peningkatan skill dalam mengatasi masalah.Fungsi telah dianggap sebagai aset dan kontributor utama bagi keberhasilan pencapaian tujuan-tujuan TI, serta peningkatan layanan TI.Seluruh tenaga ahli yang ada dilibatkan dan efektivitas pelatihan dinilai.Tujuan kuantitatif didasarkan pada kebutuhan pelanggan, penggunaakhir, organisasi, dan proses pelaksana. Kualitas dan proses kinerja yangdipahami dalam istilah statistik dan dikelola sepanjang proses. Pada tingkat ini, kinerja proses dikontrol menggunakanstatistik dan lainnya kuantitatif teknik, dan secara kuantitatif diprediksi.

5. Optimizing

Pada tingkat ini, telah fokus pada meningkatkan kinerja proses, baik melaluitambahan dan perbaikan teknologiinovatif. Perekaman, pelaporan, analisis permasalahan dan penetapan hasilnya dilakukan secara otomatis dan terintegrasi dengan pengelolaan konfigurasi data.Proses, kebijakan dan prosedur sudah distandardisasi.Secara formal diadakan peningkatan keahlian sesuai kebutuhan personil dan tujuan organisasi. Penanggungjawab proses memiliki kewenangan penuh untuk mengambil keputusan. Tanggungjawab

pengelolaan permasalah sudah diturunkan ke masing-masing unit kerja.Berbagai permasalahan sudah dapat diantisipasi dan dicegah.Tujuan perbaikan kuantitatifproses bagi organisasi adalah terus menjalankan revisi untuk tujuansebagai kriteria dalam mengelolaproses perbaikan. Efek dari proses perbaikan digunakan, diukur dandievaluasi terhadap proses perbaikan - tujuan kuantitatif.Meskipun proses mungkin menghasilkan hasilyang diprediksi, hasil mungkin tidak cukup untuk mencapai tujuan. Target dan metrik sudah ditentukan dan mengikuti best practice dari perusahaan-perusahaan lain yang menjadi terkemuka. Perbaikan secara berkesinambungan sudah membudaya dalam organisasi untuk mencapai standard *best practice* tersebut. Proses pengelolaan permasalahan sudah maju, diterapkan dan dikomunikasikan secara proaktif, serta memberikan kontribusi terhadap tujuan-tujan TI. Padatingkat telah mencapai kematangan dalam proses kerja, untuk meningkatkan kinerja (sambilmempertahankan statistik prediktabilitas) untuk mencapai proses*improvement* kuantitatif.

4. Pengukuran Kinerja Manajemen Insiden

Pada tahapan pengukuran ini dalam manajemen insiden menggunakan matrik ITIL v3 (Taylor, 2007), yang terlampir pada Appendix B. Dalam metode pengukuran ini, mengunakan metode Survey dan wawancara hanya dilakukan kepada bagian dan wakil TI pada UPT laboratorium.Dalam memperoleh suatu informasi yang dibutuhkan untuk pengukuran kinerja secara survey dan wawancara, maka dibuatlah matrik yang bertujuan untuk melihat sudah sejauh mana pengelolaan insiden dalam operasional TI guna mencapai SLA.Berikut ini merupakan matrik manajemen insiden yang disajikan pada tabel3.1.

Tabel 3.1 Matrik manajemen insiden

Goal	*Purpose*	Meningkatkan pengelolaan insiden
	Issue	Mengetahui tingkat layanan insiden
	Object	Tim *helpdesk*
	Viewpoint	Dari sudut pandang IT
Questions	Q1	Berapa jumlah dan persentase insiden diproses per *service desk*/technical support staff
Metrics	M1	Persentase insiden yang diselesaikan oleh first line

		support (tim *helpdesk*)
Questions	Q2	Berapa Persentase insiden ditutup oleh *service desk/technical support* tanpa referensi ke level support lainnya.
Metrics	M2	Berapa persen insiden yang salah dalam kategori?

a. Matrik 1(M1). Persentase insiden yang diselesaikan oleh 1st *line support* (tim helpdesk).

Deskripsi : Berapa Jumlah dan persentase insiden di proses per*service desk/technical support* staf.

Spesifikasi $\frac{Jumlah\ Insiden}{Total\ insiden\ dalam\ 1\ tahun}\ x\ 100\%$

Dengan jumlah insiden yang terjadi setiap harinya rata-rata sebanyak 10 kali insiden yang terjadi, maka dalam sebulan jumlah insiden sebanyak 260 kali untuk rata-ratanya.

$Spesifikasi : \frac{260}{3170}\ x\ 100\% = 8.2\%$

Justifikasi : Setiap staf helpdesk memiliki outputan dalam menerima laporan dari user/pengguna. Selama timbagian helpdesk mampu mengatasi insiden yang terjadi dilaboratorium, maka laporan complain dari user akan dinyatakan di tutup/selesai. Jika tim helpdesk mengetahui dengan baik suatu kerusakan/error yang terjadi dengan melakukan monitoring secara berkala maka semakin berkurang jumlah insiden yang diselesaikan, maka pihak manajemen akan dapat melakukan peningkatan terhadap layanan IT pada*user*. Nilai dibawah batasan bahaya maka menandakan bahwa manajemen insiden perlu penangganan serius.

Nilai Bahaya :<65
Nilai tercapai : 8.2 %
Rentang nilai : 0-100%

Dari perhitungan yang dihasilkan maka pihak UPT pada bagian penangan insiden dengan hasil dalam keadaan bahaya.

b. Matrik 2(M2). Persentase insiden yang salah dalam penangganan

Deskripsi : Jumlah dan persentase insiden yang salah penangganan.

Spesifikasi :$\frac{Jumlah\ Insiden}{Total\ insiden\ dalam\ 1\ tahun}\ x\ 100\%$

Dengan jumlah insiden yang terjadi setiap bulannya rata-rata sebanyak 5 kali insiden yang terjadi.

$Spesifikasi : \frac{5}{60}\ x\ 100\% = 8.3\%$

Justifikasi : Hal ini digunakan untuk mengukur laporan/telepon yang masuk yang salah dalam pendelegasian maupun kategori insiden. Yang biasa terjadi karena adanya *misscomunication* atau ketidaktahuan/penguasaan atas kerusakan yang terjadi, serta kurangnya pemahaman akan pengetahuan yang menyebabkan berkurangnya kualitas layanan yang akan diberikan. Semakin besar persentase semakin bahaya kondisi pengelolaan manajemen insiden.

Nilai Bahaya :>30
Nilai tercapai : 8.3%
Rentang nilai : 0-100%

Dari perhitungan yang dihasilkan maka pihak UPT pada bagian penangan insiden dengan hasil dalam keadaan bahaya.

c. Analisis Proses pre implementasi

Berdasarkan hasil pengukuran kinerja dan pengamatan yang terjadi dilokasi penelitian ini, maka beberapa analisis dapat dilakukan atas proses yang terjadi di bagian technical support yaitu :

a. Belum adanya aplikasi *helpdesk* sehingga tidak ada suatu proses mulai dari penerimaan laporan, eskalasi, penugasan dan reporting secara jelas.
b. *Standart operating prosedur* (SOP) penangganan insiden dan problem yang ada tidak efisien dan efektif. Kesalahan penugasan terjadi karena informasi insiden dan problem sangat minim atau berbeda dengan kejadian sesungguhnya, sehingga terjadi multi presepsi atas suatu kejadian. Semua staf TI bukan hanya dari divisi technical support seringkali menerima laporan gangguan dari pengguna/user sehingga memakan waktu dan proses Verifikasi yang lama.
c. Tidak adanya Sosialisasi SLA, hal ini penting agar semua staf technical support benar-benar memahami layanan yang akan dinilai oleh manajemen dan pengguna sebagai dasar pengukuran kinerja divisi technical support.
d. Personil/SDM dari divisi technical support masih minim dan kurang dalam pengetahuan dalam bidang IT, yang menyebabkan kesulitan dalam penyelesaian insiden atau pemantauan yang terjadi. Selain itu tidak adanya training di internal TI menyebabkan pekerjaan ditanganiberdasarkan kemampuan atau keahlian pribadi.

e. Selain itu lingkungan kerja, sangat resisten terhadap adanyaperubahan terutama yang bersifat kebijakan dari pimpinan. Hal ini karenaketika memulai bisnis perusahaan tidak melihat IT sebagaipendukung dasar dari suatu operasional sehingga SDM yang direkrutmasih memiliki kemampuan yang minim dan semua pelaporan dibuatdalam bentuk manual. Ketika adanya suatu proses training, semuastaf disibukkan dengan jadwal kerja yang padat sehinggapengembangan diri atau pengetahuan tidak berhasil dijalankan olehperusahaan.

d. Analisa Permasalahan Dan Pembuatan Dokumentasi Tata Laksana Program.

Hasil analisis dan evaluasi pada dokumen tata kelola pada UPT, selama ini menunjukkan bahwa belum seluruh program dalam dokumen Rencana Strategis TI memiliki dokumen pendukung tata laksana yang memiliki standarisasi dalam pelaporan maupun pembuatan dokumen.Dimana pembuatan dokumen pengembangannya dilakukan secara individual.Hal ini mengakibatkan dalam pelaksanaan program sering tidak maksimal dan kinerjanya tidak dapat diukur.Pada sub bab ini akan dibahas mengenai permasalah yang terjadi serta penyusunan strateginya dalam menanggani permasalahan tersebut, apabila sudah tersusun secara structural akan dibuat dokumen tat laksana program yang sesuai dengan standar SOP.

Ada beberapa tahapan aktivitas yang harus disediakan dalam pembuatan dokumen tata laksana, serta untuk merancang strategi kebutuhan dan keberlangsungan IT.Salah satunya adalah menjabarkan tahapan analisa dan permasalahan yang terjadi.Berikut ini merupakan tahapan analisa terjadinya suatu insiden.

1. Inisialisasi.

a. Penentuan Kebijakan

Didalam pembuatan atau perumusan suatu kebijakan dalam suatu instansi, peran seorang pimpinan sangat penting sekali dalam mengambil

suatu keputusan berdasarkan kesepakatan bersama antar pimpinan dan bawahan.Untuk itu dalam penentuan suatu kebiakan hal ini harus dibangun dan diputuskan secara bersama-sama dalam suatu organisasi, atau setiap bagian terlibat dalam menentukan suatu kebijakan. Penentuan suatu kebijakan dalam suatu organisasi harus sejalan dengan visi dan misi yang diterapkan dalam organisasi, agar tepat sasaran dalam mengambil suatu keputusan dan fokus terhadap permasalahan yang akan dihadapinya. Dimana suatu kebijakan yang sudah disepakati harus dipatuhi dan dijalankan secara baik dalam suatu organisasi.Dalam kebijakan yang dibuat tidak bersifat fleksibel tetapi mengikat seluruh anggota dalam oganisasi tanpa terkecuali.

b. Lingkup

Pada tahap selanjutnya, akan ditentukan lingkup serta tanggungjawab dari masing-masing staf yang ada dalam suatu organisasi sesuai dengan jabatan dalam struktural organisasi, agar dapat menjalankan tugas dan tanggung jawabnya sesuai dengan apa yang ditugaskan atau diemban. Kewenangan dan tanggungjawab dari setiap staf disesuaikan dengan kemampuan dan kapabilitas yang dimilikinya, agar mendukung terhadap setiap kegiatan yang akan dilaksanakan. Dalam meningkatkan suatu kapabilitas staf maka harus selalu diadakan suatu pelatihan dalam meningkatkan skill/kemampuan staf.

c. Alokasi sumberdaya

pada tahap ini ditentukan lingkup serta tanggungjawab dari setiap staf yang ada diorganisasi. Kewenangan dan tanggungjawab dari setiap staf disesuaikan dengan kemampuan dan kapabilitas yang dimilikinya, agar mendukung terhadap setiap kegiatan yang akan dilaksanakan.Sehingga perlu dilakukan pembagian tugas, agar kegiatan berjalan dengan lancar.keberlangsungan dari bisnis membutuhkan sumberdaya diantaranya uang dan sumberdaya manusia. Hal ini sangat penting untuk mendukung kelangsungan dari proses. Penentuan alokasi sumberdaya dengan tepat dapat mengefisiensikan kinerja yang dilakukan.

d. Struktur organisasi

Berjalannya suatu organisasi yang baik harus tersusun secara sistimatis dan komplek dimana pembagian dalam tata laksana tugas sudah jelas dan sesuai dengan SOP. Didalam organisasi yang terstruktur dengan baik dapat dengan cepat menyelesaikan suatu permasalahan yang terjadi. Karena proses penanganan dan pelaporan sudah dibuat SOP nya, sehingga langsung menjalankannya berdasarkan pembagian deskripsi pekerjaannya.

Dari penjelasan diatas maka, peneliti membuat suatu kajian terhadap masalah ancaman atau kerusakan pada layanan IT yang diberikan pihak UPT pada user, yang disajikan dalam tabel3.2.

Tabel 3.2 Ancaman dalam layanan IT

No	Resiko	Ancaman
1	Kerusakan internal/eksternal sistem atau jaringan	Listrik padam, cuaca alam, kualitas software rendah/bajakan, hacker, sabotase oleh pihak lain, kerusakan tidak sengaja
2	Kerusakan hardware/perangkat computer	Hilangnya perangkat utama atau accesoris komputer, kerusakan teknis dalam hardware, kebakaran/konsleting
3	Kehilangan data	Virus, Trojan, kerusakan teknis yang tidak disengaja, human error, hacker
4	Ketidaktersediaan staf teknik	Sakit, permintaan cuti, terjadi kerusakan dalam beberapa tempat untuk satu waktu, staf yang lagi ngajar
5	Kegagalan dalam penyediaan layanan	Tidak bisa memenuhi permintaan user, keterlambatan dalam menangani kerusakan, tidak responsive, keterbatasan staf/teknisi

5. Tahap Kebutuhan dan Strategi

a. Analisis Resiko

Pada tahap ini menilai level resiko dan membuat ranking resiko dengan mempertimbangkan faktor kecenderungan (*likelihood*) dan besarnya dampak resiko (*impact*). Pada proses penilaian ini dengan pendekatan analisa insiden dapat secara kualitatif atau kuantitatif. Level kecenderungan dan dampak dapat dikategorikan sesuai variasi yang ada, misalnya menjadi tinggi, sedang dan rendah.

b. Strategi Keberlangsungan Layanan TI

Setelah mengetahui resiko-resiko yang terjadi serta prioritas yang harus dilakukan dari hasil analisis resiko maka dapat dirancang strategi-strategi untuk keberlangsungan layanan TI.Pada tabel 3.3 dapat diperlihatkan strategi-strategi yang dapat dilakukan dalam rangka keberlangsungan layanan.

Tabel 3.3 Strategi layanan IT

No	Sumber Insiden	Insiden	Keberlangsungan Layanan IT
1	Alami	Kerusakan yang terjadi pada software, hardware dan aplikasi, yang disebabkan karena gejala alamiah, seperti kebakaran, gempa dll	Melakukan pemantauan terhadap sistem secara berkala dan back up data berdasarkan pensisteman berkala
2	Manusia	Kesalahan yang terjadi karena human error, seperti kesalahan operasional, terkena virus, intended attack dan akses tidak terautorisasi.	• Melakukan pembagian tugas/deskripsi tugas berdasarkan kemampuan/skill, pelatihan secara berkala, tanggungjawab terhadap masing-masing tugas, pengetahuan tentang sistem itu sendiri. • Peningkatan keamanan jaringan dengan melihat titik-titik yang rawan untuk diserang, maintenance dan perbaikan, serta menggunakan enskripsi data. • Pengecekan terhadap keamanan dengan menggunakan password atau user name secara dinamis, penghapusan account/user yang tidak berhak mengakses, pengecekan terhadap pengguna atau yang melakukan download materi atao software. • Pembelian antivirus yang asli/tidak bajakan,

			melakukan update antivirus secara berkala, restorasi dan back up data, serta pemantauan terhadap pengguna.
3	Lingkungan	Kerusakan yang terjadi karena adanya pemadaman listrik dan kerusakan jaringan	Pemasangan sistem jaringan secara paralel/membuat duplikat apabila terjadi kerusakan masih memiliki cadangan, memasang sistem tenaga listrik cadangan, melakukan back up dan pengendalian secara remote.
4	Spesifikasi sistem	Kerusakan pada sistem bisa berupa penggunaan sistem bajakan	Melakukan pelatihan dan pelajari tentang sistem serta melakukan pengujian terhdapa penggunaan sistem tersebut.
5	Proses layanan IT	Kesalahan yang terjadi, karena kurangnya pengetahuan/latihan, backup yang kurang, komunikasi penyediaan layanan yang kurang terorganisir	Pembuatan dokumen tat kelola IT secara teratur, mengadakan pelatihan untuk para staf teknis, peningkatan terhadap kualitas layanan terhadap user, melakukan back up dan penanganan masalah secara cepat dan effisien.

Dari dokumen ini, diketahui beberapa aktifitas yang tidak sesuai dengan tujuan program juga dimasukkan ke dalam dokumen.Dalam upaya penyempurnaan pembuatan dokumen tersebut yang berfokus pada insiden manajemen.Dimana dalam pembuatan dokumen ini, peneliti mengacu pada dasar yang tercantum dalam framework ITIL.Selain itu dokumen ini juga memiliki aktifitas tambahan untuk keperluan pelaporan, dan evaluasi sebagai kebutuhan manajemen untuk mengukur kinerja program.Dalam membangun dokumen tata laksana tersebut, penulis terlebih dahulu mendefenisikan tujuan utama keseluruhan dokumen. Selain itu penulis juga menelaah dan memasukkan kebijakan yang dikeluarkan manajemen terkait dengan proses manajemen insiden, sebagai bagian daripada dokumen berdasarkan pembagian tugas atau jabatan. Kebijakan-kebijakan tersebut antara lain kebijakan mengenai fungsi dan tanggungjawab pelaksana program, kebijakan mengenai kategori insiden,

kebijakan mengenai prioritas insiden, kebijakan mengenai waktu penanganan insiden, dan kebijakan mengenai pengukuran kinerja penanganan insiden. Setelah itu penulis menyempurnakan dokumen tata laksana dengan membangun ulang rincian masing-masing aktifitas dalam program. Rincian tersebut antara lain mendefenisikan masing-masing tujuan aktifitas dari program, indikator kinerja untuk tujuan tersebut, formulir dan dokumen yang diperlukan untuk melaksanakan aktifitas tersebut, rincian langkah-langkah pelaksanaan aktifitas, diagram RACI aktifitas dan diagram alir pelaksanaan aktifitas. Rincian dokumen tata laksana yang penulis bangun dapat dilihat pada tabel 3.4.Yang menampilkan rincian aktifitas dalam dokumen tata laksana program setelah penyempurnaan.

Tabel 3.4 Dokumen tata laksanan setelah penyempurnaan

No	Aktifitas	Tujuan
1	Identifikasi insiden (*incident identification*)	▪ Memastikan insiden yang akan terjadi dapat diidentifikasikan sebelum menimbulkan implikasi negative pada proses bisnis yang sedang berlangsung, sehingga akan berkurangnya *good will user* terhadap palayanan IT. Sehingga dapat mencegah sebelum terjadinya insiden. Dan Pembuatan laporan penanganan insiden yang sesuai dengan SOP baik pada saat terjadi maupun pada saat insiden telah terselesaikan.
2	Pencatatan insiden (*incidentlogging*)	▪ Memastikan dalam melakukan pencatatan informasi terhadap laporan insiden yang masuk secara detail dan sumbernya dapat diverivikasi sebagai dasar pelaksanaan proses penanganan insiden. ▪ Memastikan dibuatnya ringkasan insiden dan kata kunci pencarian kartu insiden. ▪ Menjamin adanya layanan IT yang ada mampu mendukung peningkatan kualitas program akademik
3	Kategorisasi insiden (*incidentcategorization*)	▪ Mengkelompokan jenis-jenis insiden yang terjadi berdasarkan kerusakannya untuk pemilahan penanganan dengan cepat dan effisien,serta memastikan kategorisasi laporan insiden tepat dan dilakukan dalam waktu singkat.
4	Prioritas insiden (*incident*	▪ Memastikan laporan insiden yang masuk pada helpdesk operator langsung

	priorization)	mendapatkan penanganan prioritas yang tepat dan cepat, sehingga tidak menggangu proses belajar. ▪ Memastikan pendelegasian penanganan insiden mendapat staf yang tepat untuk menanganinya berdasarka kemampuan dan pengetahuan yang dimiliki untuk menghindari terjadinya kesalahan penanganan insiden atau memakan waktu yang cukup lama dalam pelayanan IT.
5	Diagnosa awal (*initial diagnosis*)	▪ Memastikan tindakan diagnose awal dilakukan pada level Helpdesk Operator dalam waktu singkat Memastikan user mendapatkan penagganan yang prioritas. Dan memastikan dapat memberi masukan bagi penanganan insiden keseluruhan dan kalau dimungkinkan dapat memberi solusi atas insiden. ▪ Menyediakan kebijakan, prosedur, panduan dan dokumen lain yang akurat, mudah dipahamidan disetujui serta terdokumentasi dalam suatu kerangka kontrol teknologi Informasi. ▪ Mengontrol dampak pengukuran, authorisasi serta implementasi akibat adanya perubahan yang terjadi terhadap infrastruktur IT, aplikasi dan solusi teknis. • Meminimasi kesalahan berkaitan dengan permintaan spesifikasi yang tidak lengkap dan penghentian impelentasi akibat perubahan yang tidak terauthorisasi
6	Investigasi dan diagnosa (*investigation and diagnosis*)	▪ Memastikan investigasi dilakukan menyeluruh dan mendalam untuk menemukan sumber permasalahan insiden. ▪ Memastikan aktifitas investigasi dan diagnosa dilakukan berdasarkan standar dan memenuhi SLA target waktu penanganan. ▪ Memastikan solusi yangditemukan adalah tepat untuk insiden yang dimaksud.
7	Resolusi (*resolution and recovery*)	▪ Memastikan solusi dalam menanganai terjadinya insiden sudah teruji/terbukti dan dapat diimplementasikan secara terstruktur, serta memiliki dokumentasi dalam penangganan insiden.

8	Penutupan (*incident closure*)	▪ Memastikan setelah melakukan penangganan terjadinya insiden maka melakukan tindakan aktifitas penutupan dan memastikan komplain dari user diterima, sert insiden dapat ditanggani dengan baik, sehingga katifitas dapat berjalan dengan baik.
9	Pelaporan penanganan insiden (*incident management report*)	▪ Memastikan dilakukannya rekapitulasi harian secara berkala dan melakukan evaluasi sebagai acuan buat penaganan pada saat terjadinya lagi insiden dimasa yang akan datang.
10	Evaluasi penanganan insiden (*incident management evaluation*)	▪ Memastikan evaluasi dilakukan secara setiap bulan untuk meningkatkan kualitas penanganan insiden dengan melakukan back up data serta memastikan hasil evaluasi ditindaklanjuti oleh masing-masing pihak dalam penangganan insiden yang terjadi. ▪ Menyelaraskan manajemen IT dan bisnis dalam hal mengartikan kebutuhan bisnis menjadi layanan, serta dalam hal pengembangan strategi penyampaian layanan secara transparan dan efektif

D. KESIMPULAN

Dari pokok pembahasan yang diatas, maka peneliti akan mengambil kesimpulan dari penelitian ini sebagai berikut: Pembuatan dokumen tatalaksana dikembangkan sebagai tujuan utama untuk membantu divisi helpdesk dalam melakukan pendokumentasian dan mendukung layanan IT yang terdiri dari 10 aktifitas,yang dibangun untuk menjadi kesimpulan keseluruhan proses program. Matriks dalam dokumen tatalaksanan yang dibuat berisikan masing-masing aktifitas dalam program berikut dengan tujuan, indicator kinerja, formulir dan dokumen yang diperlukan untuk pelaksanaan aktifitas,yang digunakan untuk menilai terhadap setiap prosedur dalam pelaksanaan manajemen insiden di UPT STMIK AMIKOM Yogyakarta yang merupakan suatu solusi sesuai dengan praktek-praktek terbaik manajemen insiden menurut ITIL dan menghasilkan kinerja sesuai dengan tujuan manajemen insiden dalam ITIL.

DAFTAR PUSTAKA

Badan Pemeriksa Keuangan RI, 2006, Rencana Strategis Badan Pemeriksa Keuangan RI 2006-2010, Jakarta.

Baschap, Jon, "The Executive's guide to information technology", John willey and sons, 1st edition, 2003.

Brooker, Sherly., Jerome R. Gardner, Leva Zumbakyte. 2004. What Is Your Risk Appetite? The Risk IT Model. Information System Control Juornal Volume 2. ISACA.

Cilli, Claudio., (2003), IT Governance : Why a Guideline ?. Information System Control Juornal Volume 3. ISACA.

COBIT 4.0. 2005.IT Governance Institute.

De Haes, Steven., Wim Van Grembergen. 2004. IT Governance and Its Mechanism, Information System Control Juornal Volume 1.ISACA.

Dr. D. Akira Robinson, (2006)"An ITIL Perspective on Storage Management", Department of The NAVY.

Duncan, N.B. 1995. Capturing Flexibility of Informations Technology Infrastructure: A Study of Resources Characteristic and Their Measure.Journal of Information System.Vol 12. No 2. pp. 37-57.

Goodhue, D. L. Understanding User Evolution of Information Systems, Journal of Management Science. 1995.

http://call4tech.com/itil/upload/intro_itil.pdf.

http://gicara.com/uncategorized/apa-yang-dimaksud-dengan-incident-management.html diakses tgl 2 Februari 2012 jam 23.25

http://itilindo.wordpress.com/2008/11/21/apa-itu-itil/ diakses tgl 1 Februari 2012 jam 21.42

Introduction to The IT Infrastructure Library (ITIL), Fox IT, LLC., 2004,

IS Auditing Procedure P1 IS Risk Assessment Measurement .April 2002.ISACA.

IS Standards, Guidelines and Procedures for Auditing and Control Professionals.May 2003.ISACA.

ISACA (2005), IS Standards, Guidelines and Procedures for Auditing and Control

ISO/IEC, ISO 38500 (2008):Corporate Governance of Information Technology, ISO/IEC, Switzerland.

ISO/IEC, ISO 9001 (2008):Quality Management System, ISO/IEC, Switzerland.

IT Service Management Forum, An Introductory Overview of ITIL V3, USA

ITIL (2007a), The Official Introduction to the ITIL Service Lifecycle, Published by TSO, Belfast.

ITIL (2007b), Service Operation, Published by TSO, Belfast.

Linpei Zhang, (2006). "ITIL Introduction Presentation",ADP Small Business Services, April 2006.

Martin, E. Wainright. 2005. Managing Information Technology. Fifth Edition. Pearson Prentice Hall

Office of Government Commerce, ITIL V3:Service Operation, England.

Profeessionals, Information Systems Audit and Control Association, Illinois,

Schiesser, Rich," IT Systems Management", Prentice Hall, 1st edition, 2002.

Siswanto. (2007). Memanfaatkan Teknologi Informasi untuk Strategi Keunggulan Bersaing Industri di Perguruan Tinggi Swasta. Makalah Seminar Perguruan Tinggi di Indonesia dalam Transisi Perguruan Tinggi Era Industrialisasi ke Era Informasi. Yogyakarta: Universitas Atma Jaya.

Tjokronegoro, Arjatmo. (2000). Mutu dan Profesionalisme Dosen (Tenaga Pendidik) dalam Perspektif Abad 21, Makalah Seminar Nasional Asosiasi Perguruan Tinggi Swasta Indonesia. Jakarta. 2000.

Weill, P., Broadbent, M., & Butler, C. 1996. Exploring How Firm View IT Infrastructure.Work Paper at the Sixteenth International Converence on Information System,Amsterdam.

www.itil-officialsite.com/home/home.asp.

www.softlanding.com. SOX Compliance: Burden or Opportunity?. diakses pada 20 februari 2012.

Zuhal. (2000). Kecenderungan Perkembangan IPTEK dalam Perspektif Global. Makalah Seminar Nasional Asosiasi Perguruan Tinggi Swasta Indonesia. Jakarta. 2000.