PENERAPAN ITSM DENGAN *FRAMEWORK* ITIL V3 STUDI KASUS: STMIK MIKROSKIL

Riche[1]
STMIK Mikroskil, Jl. Thamrin No. 112, 124, 140, Telp. (061) 4573767, Fax. (061) 4567789
[1]Jurusan Sistem Informasi, STMIK Mikroskil, Medan
[1]richesuwandy@gmail.com

ABSTRAK

Latar belakang dari penulisan ini adalah organisasi dalam IT tidak memiliki pendekatan terstruktur untuk menerapkan pengelolaan akses dan proses pengelolaan layanan. Kemudian Information Technology Service Management (ITSM) standar dan kerangka tidak menyediakan contoh secara praktik, bagaimana menerapakan layanan IT dalam proses bisnis dalam organisasi. Dan yang terakhir adalah terdapat banyak opini bahwa perlu adanya diterapkan layanan IT untuk meningkatkan kualitas layanan. Tujuan penulisan adalah meningkatkan kualitas layanan IT dalam STMIK – Mikrsoksil dan merincikan langkah – langkah dalam menerapkan ITSM dengan framework ITIL V3 dalam STMIK – Mikroskil. Dimana dalam penulisan ini ruang lingkup dibatasi untuk area akademis seperti mahasiswa dan dosen serta pada layanan operasionalnya secara umum dan pengelolaan terhadap akses secara khususnya. Permasalahan yang ditemukan saat ini adalah ITSM merupakan sebuah sistem pengelolaan layanan yang digunakan untuk area IT. Oleh karena itu, untuk meningkatkan kualitas dari IT dalam STMIK – Mikroskil maka dibutuhkan adanya sebuah metode layanan IT. Metode pengelolaan IT yang akan digunakan adalah ITSM dengan framework ITIL V3. Metode penelitian dilakukan dengan melakukan pendefinisian masalah, kemudian melakukan analisa kebutuhan terhadap sistem lama dan merekomendasikan sistem baru yang seusai dengan analisa kebutuhan.

Kata kunci*— ITSM, ITIL V3, Service, IT Service*

1. PENDAHULUAN

Dalam lingkungan bisnis yang begitu kompetitif dan cepat berubah, perusahaan semakin menyadari manfaat potensial yang dihasilkan oleh Teknologi Informasi (TI). Banyak manfaat yang dapat diambil oleh perusahaan ketika mampu mengimplementasikan TI dalam proses bisnisnya. Pengurangan waktu dalam menyampaikan layanan, peningkatan kualitas, fungsional dan kemudahan penggunaan serta perbaikan secara terus menerus yang dilakukan dengan biaya yang seminimal mungkin merupakan keuntungan yang pada akhirnya mampu membantu perusahaan untuk mencapai visi dan misinya. Besarnya keuntungan yang didapat oleh perusahaan kemudian mendorong terjadinya peningkatan ekspektasi terhadap peran TI, sehingga kini TI tidak lagi sebagai pendorong dan pendukung strategi perusahaan melainkan sebagai bagian yang terintegrasi dari strategi bisnis. Para pimpinan perusahaan sepakat bahwa keselarasan antara Tujuan Bisnis dan TI merupakan *Critical Success Factor* (CSF) di perusahaan [1].

Pengelolaan yang sesuai standar perlu dilakukan, hal ini terlihat dari fakta di lapangan. Departemen TI pada perusahaan yang sudah mapan seringkali dihadapi permasalahan rumit. Permasalahan-permasalahan yang sering muncul adalah disalokasi anggaran perusahaan dalam memenuhi infrastruktur TI, infrastruktur yang ada tidak sesuai dengan bisnis perusahaan sehingga infrastruktur TI menjadi sumber masalah yang baru, minimnya *maintenance* infrastruktur TI pada perusahaan dikarenakan anggaran yang terbatas, minimnya *maintenance* menyebabkan infrastruktur yang ada tidak dapat digunakan dalam jangka waktu yang lama.

Untuk mereduksi permasalahan-permasalahan tersebut di atas maka diperlukan adanya suatu tata kelola TI pada perusahaan yang mampu menjamin perbaikan secara efektif dan efisien dari proses bisnis yang berkaitan dengan TI. Keberadaan tata kelola TI mampu mengembangkan pengaplikasian teknologi dan pemenuhan kebutuhan akan informasi yang dapat diandalkan dan terjamin. Tata Kelola TI pada dasarnya merupakan serangkaian proses untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis dapat dicapai melalui penambahan nilai sekaligus penyeimbangan resiko terkait dengan pengelolaan proses TI, termasuk dukungan secara optimal yang diberikan oleh sumber daya TI terhadap pemenuhan tujuan bisnis [1].

Layanan didefinisikan sebagai *time-perishable*, pengalaman yang tidak berwujud yang dilakukan untuk pelanggan yang bertindak sebagai seorang Co-Produser [2]. ITSM berperan sebagai pengukur pelayanan yang penting dalam ilmu komputasi [3]. Berdasarkan latar belakang yang telah dipaparkan di atas, peneliti termotivasi untuk menerapakan ITSM dengan *framework* ITIL V3 sebagai *framework* penulisan ini. *Framework* dipilih karena berdasarkan Peraturan Mentri BUMN No. PER – 02/MBU/2013 mengenai tata kelola TI seluruhnya mengacu kepada ITIL V3.

2. METODE PENELITIAN

2.1 Model Penelitian

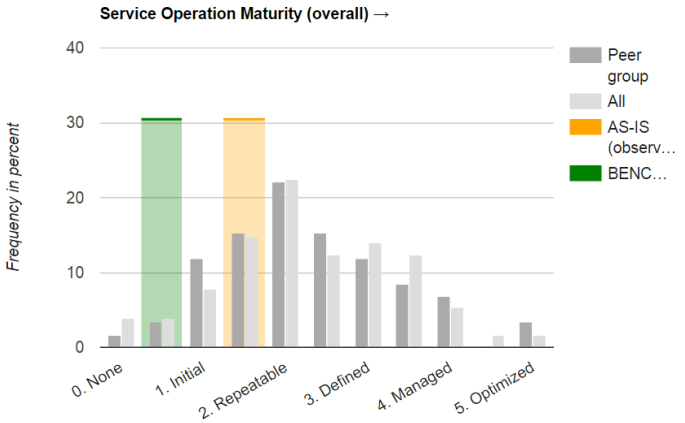
Penelitian ini menggunakan *framework* atau kerangka kerja ITIL V3, dengan harapan dapat memberikan solusi terhadap permasalahan yang ditemukan. Berikut adalah tahapan yang akan dilakukan.

- *Service Strategy*
  Dalam fase *service strategy* yang akan dilakukan antara lain:
  - Melakukan identifikasi terhadap layanan yang harus diberikan
  - Melakukan identifikasi kepada siapa layanan harus diberikan
  - Melakukan identifikasi terhadap kompetisi – kompetisi yang mungkin muncul.
  - Melakukan identifikasi hal – hal yang membedakan terhadap kompetitor
- *Service Design*
  Dalam fase *service design* yang akan dilakukan adalah:
  - Melakukan perancangan terhadap layanan agar dapat memberikan solusi kepada hasil identifikasi pada fase sebelumnya.
  - Melakukan perancangan infrasturktur TI yang aman.
  - Mengembangkan kemampuan dalam TI
- *Service Transistion*
  Dalam fase *service transition* yang akan dilakukan adalah:
  - Melakukan identifikasi terhadap pihak yang berkepentingan dalam hal ini dosen dan mahasiswa.
  - Melakukan pengaplikasian dan adaptasi dari fase sebelumnya.
- *Service Operation*
  Dalam fase *service operation* yang dilakukan adalah:
  - Melakukan penyaringan terhadap kejadian – kejadian, agar dapat memutuskan tindakan yang tepat.
  - Melakukan pengelolaan seluruh siklus, agar dapat mengembalikan layanan TI secapat mungkin apabila terjadi insiden
  - Memenuhi permintaan pelanggan pada layanan TI
  - Menentukan hak akses
  - Melakukan pengelolaan semua siklus masalah yang terjadi
  - Melakukan kontrol terhadap layanan TI
  - Melakukan pengelolaan lingkungan fisik dari infrastruktur TI.
  - Melakukan pengelolaan siklus hidup aplikasi layanan TI
  - Menyediakan tenaga kerja spesialisasi untuk mendukung pengelolaan infrastruktur TI
- *Continual Service Improvement*
  Dalam fase *continual service improvement* yang dilakukan adalah:
  - Melakukan tinjauan ulang terhadap layanan
  - Melakukan evaluasi proses
  - Melakukan pengecekan apakah layanan TI berjalan sesuai dengan rencana dan perlu dilakukan tindakan korektif apabila diperlukan

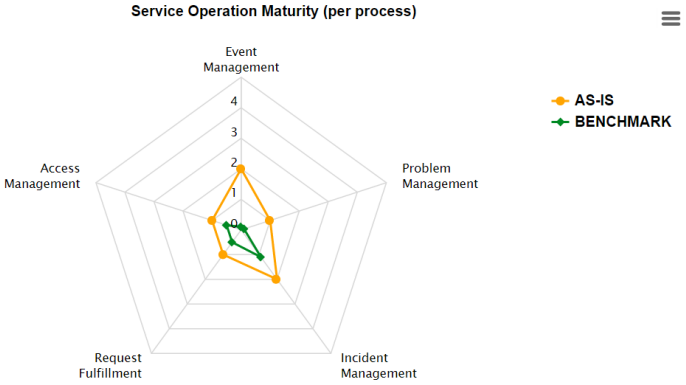
3. HASIL DAN PEMBAHASAN

3.1 Pengukuran Maturity Level

Pengukuran *maturity* level menggunakan ITIL *Self Assessment Study* [4], yang merupakan dasar pemilihan *access management* sebagai bagian yang diteliti oleh peneliti. Pengukuran maturity level ini menggunakan kuesioner *online* yang diakses oleh Kepala Pusat Sistem Informasi dalam menilai kondisi saat ini dalam menangani hak akses. Hasil dari pengukuran dapat dilihat pada gambar 1 dibawah ini.



Gambar 1. *Service Operation Maturity*



Gambar 2. *Service Operation Maturity (per process)*

ITIL Processes	Deviation from Benchmark (in maturity levels)
Change Management	-0,5
IT Service Management	-0,5
Financial Management for IT Services	-0,2
Service Asset and Configuration Management	-0,1
Information Security Management	-0,1
Release and Deployment Management	0
Business Relationship Management	0,1
Service Portfolio Management	0,1
Demand Management	0,1
Service Validation and Testing	0,1
Change Evaluation	0,3
Service Level Management	0,3
Transition Planning and Support	0,3
IT Service Continuity Management	0,4
Access Management	0,5
Availability Management	0,5
Request Fulfillment	0,5
Supplier Management	0,5
Service Catalogue Management	0,5
Knowledge Management	0,5
Capacity Management	0,6
Design Coordination	0,9
Incident Management	0,9
Problem Management	0,9
Event Management	1,9

Gambar 3. *Roadmap Process Indicating*

3.2 Analisa Kebutuhan

Berdasarkan hasil analisa yang diperoleh dari peneliti, maka peneliti merekomendasikan kepada pihak Departemen Pusat Sistem Informasi untuk melengkapi beberapa poin yang dianggap peneliti sebagai sebuah kebutuhan antara lain:

- Kebijakan TI
- Verifikasi kerahasiaan data
- Pengendalian hak akses

3.3 Kebijakan Teknologi Informasi

Menurut David Eatson Kebijakan Publik diartikan sebagai pengalokasian nilai – nilai kekuasaan untuk seluruh masyarakat yang keberadaannya mengikat. Dalam hal ini hanya pemerintah yang dapat melakukan suatu tindakan kepada masyarakat dan tindakan tersebut merupakan bentuk dari sesuatu yang dipilih oleh pemerintah yang merupakan bentuk dari pengalokasian nilai – nilai kepada masyarakat. Berikut adalah beberapa kebijakan teknologi informasi yang dapat diuraikan berdasarkan kebutuhan Departemen Pusat Sistem Informasi STMIK Mikroksil:

- Penggunaan Kebijakan Yang Diterima
  Kebijakan ini menetapkan kebijakan yang diterima untuk seluruh sumber daya teknologi yang dimiliki STMIK Mikroskil.
  Beberapa prosedur yang direkomendasikan peneliti dalam kebijkan ini antara lain:
  - Setiap kata sandi yang digunakan untuk mengakses sistem STMIK Mikroskil harus tetap aman dan terlindungi dari penggunaan yang tidak sah.
  - Akun pengguna tidak dapat dibagi antar individu. Pengguna harus bertanggung jawab terhadap keamanan sandi dan akun mereka sendiri
  - Setiap komputer yang berada pada jaringan internal STMIK Mikroskil, baik yang merupakan milik pribadi maupun STMIK Mikroskil, harus secara terus – menerus melakukan *virus-scanning* dan melakukan pembaharuan terhadap *database* anti-virus
  - Staf dan mahasiswa harus secara hati – hati dalam membuka pesan elektronik (*e-mail*) yang diterima dari pengirim yang tidak dikenal (*spam mail*).
  - Informasi pribadi tidak dapat dikirim melalui sarana elektronik secara langsung, tetapi dikirim dalam jaringan internal STMIK Mikroskil
  - Keseluruhan *workstation* harus tersimpan secara aman. Dalam hal ini pengguna harus mengunci komputer ketika tidak berada ditempat, untuk melindungi pengguna yang tidak sah untuk melakukan akses terhadap *file* yang penting.
- Kebijakan Pengaksesan
  Kebijakan ini menetapkan pedoman pengaksesan untuk semua sumber daya teknologi yang dimiliki STMIK Mikroskil. Tujuan dari kebijakan ini adalah untuk memastikan bahwa setiap mahasiswa STMIK Mikroksil disajikan dengan fasilitas yang sama untuk belajar dan semua staf secara memadai dapat menggunakan peralatan teknologi yang dibutuhkan untuk mencapai tujuan bersama.
  Beberapa prosedur yang direkomendasikan peneliti dalam kebijakan ini antara lain:
  - Pusat Sistem Informasi STMIK Mikroskil harus memastikan setiap mahasiswa dan staf disajikan dengan lingkungan sistem yang sama atau sebanding.
  - Pusat Sistem Informasi STMIK Mikroskil harus memberikan solusi teknologi yang membantu meningkatkan lingkungan belajar dan mengajar serta bekerja untuk mahasiswa dan staf.
  - Pusat Sistem Informasi STMIK Mikroskil harus menjawab seluruh kebutuhan penting yang berkaitan dengan sistem yang diminta oleh pengguna
  - Pusat Sistem Informasi STMIK Mikroskil harus terus berusaha untuk memastikan bahwa lingkungan STMIK Mikroskil memiliki teknologi yang diperlukan, memadai dan terstruktur.
- Kebijakan Backup
  Departemen Pusat Sistem Informasi STMIK Mikroskil memastikan tata cara penyimpanan data penting untuk setiap departemen atau individu. Daerah penyimpanan, atau kelompok pemakai tertentu, digunakan untuk menyimpan semua data dengan aman serta
  Beberapa prosedur yang direkomendasikan peneliti terhadap kebijakan backup antara lain:
  - Setiap staf masing – masing departemen maupun mahasiswa harus menyimpan data sensitif, data penting dan data rahasia dimasing – masing tempat penyimpanan kelompok, karena Pusat Sistem Informasi STMIK Mikroskil tidak bertanggung jawab atas kehilangan data yang tersimpan ditempat lain.
  - Jadwal *backup* secara umum berada pada setiap tempat penyimpanan kelompok. Dalam hal ini, untuk memastikan bahwa backup terjadi secara berkala dan selama rentang waktu tertentu. Pusat Sistem Informasi

STMIK Mikroskil tidak perlu memberitahukan langsung apabila terdapat *file* dan *folder* yang hilang maupun rusak, karena dalam hal ini Pusat Sistem Informasi STMIK Mikroskil akan melakukan *restoring* atau pengembalian *file* dan *folder* yang rusak secara otomatis.

- Pusat Sistem Informasi STMIK Mikroskil harus melakukan pengujian terhadap integritas data yang telah di-*backup*. Pengujian dapat dilakukan pada interval waktu yang telah dijadwalkan secara rutin dan dilakukan secara acak dan manual untuk memastikan keabsahan, keakuratan dan keaslian *backup*.

- Kebijakan Komunikasi Elektronik
  Komunikasi elektronik diperlukan untuk memenuhi peran ganda dan kegiatan di STMIK Mikroskil, karena berbagai jenis komunikasi elektronik akan berfokus pada yang digunakan STMIK Mikroskil, antara lain:
  - *Email*
    Email adalah metode komunikasi resmi di STMIK Mikroskil, baik bagi mahasiswa dan staf. Bisnis dilakukan setiap hari melalui email. Sejak email memiliki baik konotasi positif dan negatif, sangat penting bahwa kita mengakui bahwa aspek - aspek positif sangat lebih besar daripada aspek - aspek negatif. Namun, kita harus juga menyadari bahwa aspek - aspek negatif ada dan memastikan bahwa metode komunikasi yang digunakan efektif, efisien, dan untuk tujuan yang telah ditetapkan.
  - *Video Conference*
    Video conference digunakan terutama untuk kelas instruksional. Video conference digunakan untuk memfasilitasi konferensi dan pertemuan dengan lembaga lain, lembaga negara, atau badan pihak ketiga lainnya.
- Kebijakan Informasi Sensitif
  Sensitivitas informasi adalah fokus utama di STMIK Mikroskil. Karena kita adalah entitas pendidikan, kita berurusan dengan banyak berbagai jenis informasi, beberapa untuk keperluan umum, beberapa tidak. Kebijakan ini dimaksudkan untuk membantu karyawan menentukan informasi apa yang dapat diungkapkan untuk non staf, serta kepekaan relatif dari informasi yang tidak boleh diungkapkan di luar STMIK Mikroskil tanpa otorisasi yang tepat. Beberapa prosedur yang direkomendasikan oleh peneliti terhadap kebijakan informasi sensitif, antara lain:
  - Informasi yang bersifat minimal sensitif.
    - Deskripsi : informasi umum, beberapa individu, informasi teknis
    - Hak akses : staf, mahasiswa STMIK Mikroskil yang memiliki hak akses
    - Distribusi internal : disetujui dengan surat elektronik (e-mail), *hardcopy*
    - Distribusi eksternal : disetujui dengan surat elektronik (e-mail), *hardcopy*
    - Penyimpanan : hanya dapat diakses oleh pengguna yang sah.
    - Pembuangan / Pemusnahan : data elektronik harus dihapus secara permanen. Terhadap pemusnahan *hardcopy* dapat dilihat berdasarkan kebijakan retensi data.
  - Informasi yang bersifat lebih sensitif
    - Deskripsi : bisnis, keuangan, teknis
    - Akses : staf STMIK Mikroskil yang memiliki hak akses
    - Distribusi internal : disetujui dengan surat elektronik (e-mail), *hardcopy*
    - Distribusi eksternal : disetujui dengan surat elektronik (e-mail), *hardcopy*
    - Penyimpanan : kontrol akses individu lebih disarankan untuk informasi yang lebih sensitif
    - Pembuangan / Pemusnahan : data elektronik harus dihapus secara permanen. Terhadap pemusnahan *hardcopy* dapat dilihat berdasarkan kebijakan retensi data.
  - Informasi yang bersifat paling sensitif
    - Deskripsi : opersional, individu, keuangan, *source code*, informasi teknis keamanan organisasi
    - Akses : individu yang ditunjuk dengan menandatangani surat perjanjian untuk mendapatkan akses
    - Distribusi internal : disetujui dengan surat elektronik (e-mail), *hardcopy*
    - Distribusi eksternal : disetujui dengan surat elektronik (e-mail), *hardcopy*
    - Penyimpanan : kontrol akses individu sangat dianjurkan untuk informasi elektronik.
    - Pembuangan / Pemusnahan : data elektronik harus dihapus secara permanen. Terhadap pemusnahan *hardcopy* dapat dilihat berdasarkan kebijakan retensi data.
- Kebijakan Pengendalian Hak Akses
  Kebijakan ini menetapkan aturan resmi yang ditetapkan untuk memungkinkan pengguna untuk mengakses dan memanipulasi jarak jauh informasi pribadi, aplikasi jaringan, dan data lainnya dari luar kampus.
- Kebijakan Peraturan dan Tanggung Jawab Mahasiswa

Ini adalah pemahaman semua mahasiswa, bahwa sumber daya teknologi dan peralatan yang disediakan adalah untuk kepentingan semua mahasiswa. Kebijakan ini menjelaskan apa yang harus siswa hak sehubungan dengan teknologi ini dan juga tanggung jawab apa yang diharapkan dari masing-masing mahasiswa.

3.4 Verifikasi Kerahasiaan Data

Data rahasia merupakan data memegang nilai paling penting dan membawa risiko yang besar dalam sebuah organisasi maupun individu tertentu. Berdasarkan rincian tersebut perlu adanya melakukan verifikasi kerahasian data yang memiliki kaitan khusus terhadap kerahasiaan data tersebut. Data rahasia yang ditujukan mencakup seluruh organisasi dan *hard copy* data organisasi. Tujuan dari verifikasi kerahasiaan data itu perlu dikarenakan untuk menangani tantangan terhadap mempertahankan data pribadi atau data tertentu yang bersifat rahasia. Dalam hal ini, risiko yang ditemukan adalah pencurian data identitas, perubahan data yang tidak disetujui atau bersifat ilegal, memanipulasi data keuangan yang terkait dengan akses informasi elektronik dan kerahasiaan data terhadap proses pengumpulan data.

Verifikasi kerahasiaan dapat juga dengan melakukan pengendalian terhadap hak akses dimana pengendalian dilakukan dengan menetapkan aturan resmi yang memungkinkan kepada pengguna untuk mengakses dan memanipulasi jarak jauh informasi pribadi, aplikasi jaringan, dan data lainnya dari luar kampus.

Berikut adalah pengklasifikasian data yang diuraikan dalam Tabel 1, antara lain:

Tabel 1 Klasifikasi Data [5]

Kelas Data	**Dampak Terhadap Bisnis**	**Contoh**
Perlindungan Tingkat 3	Extrim	*enterprise credential stores*, *backup data systems*, konsol pengelolaan data pusat
Perlindung Tingkat 2	Tinggi	Data nomor identitas (KTP, SIM), Nomor rekening bank, nomor kartu kredit, informasi medis, informasi asuransi kesehatan, dan lain - lain
Perlindungan Tingkat 1	Sedang	Nomor id mahasiswa, nomor id staf, perpustakaan berbayar, lisensi dari perangkat lunak
Perlindungan Tingkat 0	Terbatas atau Tidak ada sama sekali	Data halaman web, informasi direktori publik, daftar syarat dan prasyarat

4.5 Pengendalian Hak Akses

Pengendalian akses (*access control*) menjadi pertimbangan pertama saat seorang profesional Sistem Keamanan Informasi akan membuat program keamanan informasi. Keistimewaan dan variasi mekanisme *access control* baik secara fisik, teknik dan administrasi akan membangun arsitektur keamanan informasi yang praktis untuk melindungi informasi penting dan sensitif yang menjadi aset organisasi.

Privasi (secara individu) adalah salah satu alasan penerapan *access control* dalam organisasi. Saat ini teknologi telah membuat pertukaran informasi menjadi semakin mudah dan semakin luas, sehingga usaha-usaha perlindungan informasi menjadi semakin kompleks dan sulit [6].

Pengendalian hak akses selalu mengarah kepada kerahasiaan data, beberapa macam pengendalian hak akses dalam keamanan informasi, antara lain :

- Pencegahan dengan pengendalian secara fisik. Pencegahan yang dimaksud disini adalah usaha mencegah pihak-pihak yang tidak berhak agar tidak memasuki / menggunakan sumberdaya komputer dan juga melindunginya dari bahaya bencana alam. Hal yang termasuk di dalamnya, antara lain :
  - *Back-up file*/dokumentasi yaitu untuk mencegah agar apabila terjadi kecelakaan terhadap sistem komputer, file/dokumen penting tetap ada. Dokumen back-up ini sebaiknya disimpan ditempat yang berjauhan dan dengan tindakan keamanan yang setara dengan dokumen aktifnya.
  - Pemagaran yaitu untuk membatasi agar hanya orang – orang yang berhak saja yang dapat memasuki sistem. Termasuk dalam sistem pemagaran adalah CCTV, *alarm*, dan lain – lain.
  - Sistem tanda pengenal yaitu untuk mengenali bahwa orang tersebut adalah pihak yang memang diberikan akses tertentu.
  - *Back-up power* yaitu untuk memastikan tidak ada pemutusan power/listrik secara mendadak yang akan mengakibatkan kerusakan pada sistem. Back-up power biasanya berupa baterai cadangan atau generator diesel. Perangkat yang paling populer adalah ups (*uninterruptible power supply*).
  - Pemilihan lokasi adalah faktor yang sangat penting untuk menghindari resiko yang mungkin timbul akibat bencana banjir, kebakaran, radiasi gelombang elektromagnetik atau yang lainnya.
  - Pemadam kebakaran. Kebakaran akan merusak sistem. Selain lokasi sistem harus jauh dari tempat yang menjadi pemicu kebakaran, material yang digunakan pun sebaiknya yang tidak mudah terbakar. Alat

pemadam kebakaran perlu diletakkan ditempat yang tepat dan mudah dijangkau dengan bahan yang baik, sebab bahan pemadam yang buruk akan merusak sistem bagaikan api itu sendiri.

- Pendeteksian dalam pengendalian secara fisik.
  Pendeteksian sebagai pengendalian secara fisik merupakan perlindungan atas pelanggaran yang telah terlanjur terjadi.
  - Detektor gerak yaitu area ruang server komputer umumnya tidak dipakai sebagai lalu-lintas aktifitas manusia, sehingga pemasangan alat deteksi gerak akan sangat berguna untuk mencegah penyusupan.
  - Detektor asap dan api yaitu apabila diletakkan ditempat yang tepat akan sangat berguna sebagai alat pemberitahu yang tercepat bila terjadi kebakaran.
  - CCTV (*Closed-Circuit Television*) yaitu digunakan untuk memantau kawasan dimana sistem berada/diletakkan.
- Pengendalian secara teknis
  Pengamanan secara teknis ini meliputi penggunaan penjaga keamanan, yang mana termasuk didalamnya adalah hardware komputer, sistem operasi dan software aplikasi, komunikasi serta peralatan lain yang berhubungan. Hal yang termasuk di dalam pengendalian secara teknis, antara lain :
  - Pencegahan dalam pengendalian secara teknis. Pencegahan yang secara teknis digunakan untuk mencegah pihak yang tidak berhak mengakses sumber daya komputer. Yang termasuk dalam pencegahan secara teknis antara lain :
    - *Software Access Control* yaitu digunakan untuk mengendalikan pertukaran data dan program antar user. Biasanya diimplementasikan dalam bentuk daftar access control yang mendefinisikan hak akses setiap user.
    - *Software Antivirus*. Virus merupakan program yang mewabah dalam komputer serta dapat merusak sistem dan data yang pada akhirnya menghambat produktifitas. Virus baru bermunculan dengan cepat, sehingga pemasangan software antivirus yang selalu up-date dan selalu aktif dalam komputer merupakan suatu keharusan.
    - Sistem pengendalian pustaka mengharuskan semua perubahan program yang diimplementasikan oleh personil pengendali pustaka ini, hal ini untuk menghindari pihak yang tidak berhak melakukan perubahan.
    - *Password* digunakan untuk membuktikan bahwa pengguna atau pemilik ID adalah orang yang memang memiliki hak akses tertentu terhadap sistem.
    - *Smartcard*. Umumnya berbentuk seperti kartu kredit dan dilengkapi chip yang telah diprogram. Informasi didalamnya dapat dibaca di tempat-tempat yang disediakan untuk itu yang dapat mengidentifikasikan hak-hak user. Dalam penggunaannya biasanya dikombinasikan dengan pengendalian akses lainnya seperti password, biometrik, atau ID.
- Pengendalian secara administratif
  Administratif atau personel keamanan terdiri dari pembatasan manajemen, prosedur operasional, prosedur pertanggung jawaban, dan pengendalian administratif tambahan untuk menyediakan tingkat perlindungan yang memadai pada sumber daya komputer. Pengendalian administratif termasuk juga prosedur untuk menyakinkan bahwa semua personel yang mendapatkan akses pada sumber daya komputer, mendapatkan otorisasi dan security clearance yang tepat. Pengendalian yang termasuk di dalamnya antara lain :
  - Pencegahan dalam pengendalian administratif. Teknik yang sangat personal untuk melatih kebiasaan orang-orang untuk menjaga kerahasiaan, integritas dan ketersediaan data dan program. Yang termasuk dalam pencegahan ini adalah :
    - Kesadaran keamanan informasi dan pelatihan teknis. Pelatihan untuk menanamkan kesadaran keamanan informasi adalah suatu langkah pencegahan dengan membuat user mengerti keuntungan menerapkan keamanan informasi tersebut. Sehingga diharapkan user dapat menciptakan iklim yang mendukung.
    - Pelatihan teknis kepada user dapat menolong untuk mencegah terjadinya masalah-masalah keamanan yang biasanya terjadi akibat kesalahan dan kelalaian user dan memberikan pemahaman/pelatihan mengenai keadaan darurat, agar user dapat mengambil tindakan tepat saat terjadi bencana.
    - Pemisahan/pembagian tugas. Yang dimaksud adalah user yang berbeda mendapatkan bertanggung jawab yang berbeda atas tugas-tugas yang berbeda yang merupakan bagian dari keseluruhan proses. Hal ini dilakukan untuk menghindari seorang user menguasai seluruh proses yang membuka peluang bagi kolusi dan manipulasi.
    - Prosedur rekruitmen dan pemberhentian karyawan TI. Prosedur rekruitmen yang tepat akan mencegah organisasi mempekerjakan orang yang berpotensi merusak sistem. Prosedur pemberhentian karyawan TI perlu dibuat dengan cermat agar aset/sumber daya organisasi tidak ikut terbawa keluar, dengan cara

menarik seluruh kewenangan atas akses sistem informasi yang dimiliki, misalnya menghapus password log-on ID atau mengganti semua kunci aksesnya.

- ❖ Pengawasan harus sejalan dengan kebijakan dan prosedur yang telah ditetapkan oleh organisasi, terutama pada sumber daya organisasi yang sensitif dan rentan terhadap penyalahgunaan wewenang.
- ❖ Perencanaan keadaan darurat dan pemulihan dari bencana adalah sebuah dokumen yang berisi prosedur untuk menghadapi keadaan darurat, back-up operasional, dan pemulihan instalasi komputer baik sebagian atau seluruhnya yang rusak akibat bencana. Yang paling penting dalam perencanaan ini adalah membuat instalasi komputer bekerja normal kembali dalam waktu yang sesingkat-singkatnya.
- ❖ Registrasi. User perlu melakukan registrasi untuk mendapatkan akses komputer dalam organisasi dan user harus bertanggung jawab atas semua sember daya komputer yang digunakannya.

4. KESIMPULAN

Berdasarakan hasil dan pembahasan pada bab sebelumnya, maka peneliti membuat kesimpulan mengenai hasil dan pembahasan, antara lain :

a. Berdasarkan hasil analisa perkembangan infrastruktur maupun teknologi yang terdapat di STMIK Mikroskil sudah mampu mengikuti teknologi yang berkembang saat ini.
b. Kelemahan yang dimiliki oleh STMIK Mikroskil sudah mampu teratasi dengan baik dari sisi eksternal dan internal
c. Penerapan ITSM dengan *framework* ITIL V3 sangat tepat, karena *framework* ITIL V3 memiliki tahapan yang jelas dalam mengimplementasikan layanan TI di STMIK Mikroksil dan dapat meningkat kualitas layanan TI
d. Hal yang perlu diperhatikan oleh STMIK Mikroskil adalah dalam pengelolaan akses. Secara umum pengelolaan akses sudah ada namun tidak memiliki tahapan yang baik dan tidak dibuat secara tertulis atau terdokumentasi.
e. Kebijakan TI yang dibuat berdasarkan hasil analisa, meruapakan kebijakan yang dapat membantu dalam pengambilan keputusan dan membuat prosedur.
f. Verifikasi terhadap kerahasiaan data itu penting sekali, tingkat kerahasiaan data sudah diklasifikasikan menurut kelas – kelasnya, sehingga memudahkan membedakan data mana yang paling dan berpengaruh terhadap STMIK Mikroskil
g. Pengendalian hak akses telah diuraikan dengan langkah yang jelas, sehingga memudahkan STMIK Mikroskil mengimplementasikan ITIL V3 disisi pengelolaan akses

5. SARAN

Beberapa saran yang dapat dikemukan oleh peneliti menurut hasil penelitian, antara lain :

a. ITIL merupakan *best practice* dalam menyelaraskan proses TI operation dengan kepentingan bisnis, oleh karena itu diharapkan penerapan metode ITIL berserta fungsi – fungsi yang terdapat didalamnya dapat dimaksimalkan untuk mendapatkan hasil yang maksimal.
b. Mengingat keterbatasan waktu, maka diharapkan dapat dijadikan pertimbangan untuk penelitian selanjutnya.
c. Untuk organisasi yang biasanya tergantung dari operasional TI, dapat menerapkan ITSM dengan framework ITIL V3 sebagai *best practice* dalam menyelaraskan proses TI dengan kepentingan bisnis.
d. STMIK Mikroskil akan menjalankan ISO 9001:2008, dimana apabila STMIK Mikroskil menerapkan konsep ITIL V3 secara penuh dengan ISO 9001:2008 secara bersamaan, maka kualitas dari layanan TI di STMIK Mikroksil akan meningkat.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada STMIK Mikroskil, khususnya Departemen Pusat Sistem Informasi yang bersedia untuk memberikan data yang dibutuhkan selama melakukan penelitian.

DAFTAR PUSTAKA

[1] Sarno, R. (2009). *Audit Sistem dan Teknologi Informasi.* Surabaya: ITS Press.
[2] Sasser, E. W., Olsen, R. P., & Wyckoff, D. D. (1978). *Management of Service Operations : Text, Cases, and Readings.* Boston: Allyn and Bacon.
[3] Zhang, L. J., Zhang, L. J., & Cai, L. H. (2007). *Services Computing.* Berlin Heidelberg: Springer-Verlag.
[4] Winkler, T., Wulf, J., Brenner, W., & Andersen, N. B. (2011). *ITIL Self-Assessment*. Retrieved from ITIL Self-Assessment: http://itil.selfsurvey.org/
[5] California, B. U. (2016). *Data Classification Standard | Information Security and Policy*. Retrieved from https://security.berkeley.edu/data-classification-standard.
[6] Tipton, H. F., & Krause, M. (2004). *Information Security Management Handbook Fifth Edition.* Boca Ranton London New York Washington, D. C.: Auerbach Publication.