

MANAJEMEN TEKNOLOGI INFORMASI



MODUL - Sesi 8 – BAB 8 PENGOPERASIAN DAN PELAYANAN

ISMAIL, S.KOM, M.KOM

BAB 8

PENGOPERASIAN DAN PELAYANAN

Capaian Pembelajaran (Learning Outcomes):

1. Menetapkan dan Mengelola Kinerja Teknologi Informasi
2. Mengelola Layanan Pihak Ketiga
3. Mengelola Kinerja dan Kapasitas
4. Memastikan Keberlangsungan Layanan
5. Memastikan Keamanan Sistem
6. Mengidentifikasi dan Mengalokasikan Biaya
7. Mengedukasi dan Melatih Pengguna
8. Mengelola Pusat Layanan dan Insiden
9. Mengelola Konfigurasi
10. Mengelola Data
11. Mengelola Lingkungan Fisik
12. Mengelola Operasional Sistem



8.1 MENETAPKAN DAN MENGELOLA KINERJA TEKNOLOGI INFORMASI

Setiap domain atau kelompok pengguna sistem memiliki harapan dan ekspektasinya masing-masing terhadap kinerja aplikasi yang dipergunakan. Target atau obyektif harapan tersebut haruslah ditetapkan dan didokumentasikan secara formal dalam bentuk kontrak kerja/kinerja antara organisasi dengan vendor pemasok atau penyediaanya. Kinerja tersebut selain harus dicapai harus pula dipantau dari waktu ke waktu, untuk memastikan agar sistem yang dipergunakan benar-benar bermanfaat memenuhi kebutuhan organisasi atau bisnis perusahaan.

Ada delapan langkah aktivitas yang perlu dilakukan dalam mengelola manajemen kinerja layanan teknologi informasi di organisasi, yaitu:

- Mengembangkan kerangka konseptual yang memperlihatkan jenis-jenis layanan teknologi informasi beserta peranannya dalam konteks organisasi.
- Menyusun daftar atau katalog jenis layanan teknologi informasi yang ada pada organisasi.
- Menetapkan Service Level Agreement (SLA) atau kesepakatan tingkat layanan terhadap jenis layanan teknologi informasi yang dianggap sangat penting atau kritis bagi kelangsungan hidup organisasi.
- Menetapkan Operating Level Agreement atau kesepakatan model kinerja operasional yang harus dipenuhi agar SLA yang telah ditetapkan sebelumnya dapat dicapai.
- Memantau dan melaporkan tingkat kinerja layanan teknologi informasi dari

waktu ke waktu - baik secara periodik maupun ad-hoc.

- Mengkaji hasil pemantauan terhadap SLA dan membandingkannya dengan kesepakatan pada kontrak.

Terkait dengan proses dan aktivitas di atas, sejumlah entitas pengendali yang harus dimiliki antara lain:

- Kerangka Manajemen Tingkat Layanan yang memperlihatkan kelompok-kelompok layanan teknologi informasi yang ada pada organisasi beserta karakteristik dan konteks keberadaannya.
- Definisi Pelayanan Teknologi yang dianut atau diadopsi oleh organisasi untuk dipergunakan sebagai panduan dalam menentukan proses yang terkait dengannya.
- Kesepakatan Tingkat Layanan yang didefinisikan dan tercantum dalam berbagai dokumen kontrak internal maupun eksternal sebagai indikator kinerja yang harus dicapai oleh sistem.
- Kesepakatan Tingkat Operasional yang merupakan ukuran teknis implementasi proses di lapangan untuk mencapai SLA yang telah didefinisikan.
- Laporan Pemantauan Kinerja Sistem yang telah dicapai dalam titik atau masa kurun tertentu.

- Hasil Kajian Tingkat Layanan Sistem yang berhasil dicapai dengan disandingkan pada kontrak perjanjian yang telah disepakati dan ditandatangani sebelumnya.

Adapun indikator yang dapat dipergunakan untuk menilai efektivitas pelaksanaan proses ini antara lain adalah: (i) persentase kinerja layanan yang sesuai dengan SLA; (ii) jumlah layanan yang diberikan namun tidak terdapat dalam katalog; (iii) frekuensi pertemuan per tahun yang membahas pencapaian SLA; dan lain sebagainya.

Pada dasarnya tingkat layanan teknologi informasi diukur secara berkesinambungan. Dari hari ke hari, tingkat layanan ini seyogyanya ditingkatkan, sejalan dengan ketatnya persaingan dan harapan pelanggan. Tentu saja untuk membuat aktivitas ini berlangsung dengan baik, harus diintegrasikan dengan sistem kompensasi dan penghargaan karyawan termasuk pemberian insentif yang sesuai dengan kinerjanya.

8.2 MENGELOLA LAYANAN PIHAK KETIGA

Organisasi selaku pihak pertama menggunakan teknologi informasi untuk memberikan layanan kepada pelanggannya selaku pihak kedua - baik yang merupakan pelanggan internal maupun eksternal. Karena kebanyakan produk dan layanan teknologi informasi berasal dari berbagai perusahaan lain di luar organisasi yang ada - katakanlah berasal dari vendor, pemasok, atau mitra -maka perlu dimiliki model pengelolaan efektif kepada para pihak ketiga ini untuk memastikan terselenggaranya manajemen teknologi informasi sesuai kebutuhan. Disamping itu organisasi perlu pula melakukan pemantauan atau monitoring terhadap mitra kerjanya sehari-hari, terutama terkait dengan pembagian tugas

dan tanggung jawab agar layanan teknologi informasi dapat berjalan sebagaimana yang disepakati pada kontrak kerja.

Ada enam aktivitas yang harus dilakukan terkait dengan proses ini yaitu masing-masing adalah:

- Mengidentifikasi dan mengklasifikasikan jenis-jenis dan model layanan dari pihak ketiga berdasarkan konteks dan kontrak kerja yang disepakati.
- Mendefinisikan dan menyusun proses serta struktur kerja pengelolaan teknologi informasi dengan pihak ketiga.
- Mengembangkan instrumen untuk menyeleksi dan menilai/mengevaluasi kinerja pihak ketiga
- Mengidentifikasi, menganalisa, dan memitigasi berbagai risiko terkait dengan keberadaan pihak ketiga selaku pemasok produk dan/atau layanan teknologi informasi.
- Memantau secara rutin proses kerja yang dilakukan oleh pihak ketiga dari masa ke masa.
- Mengevaluasi kinerja pihak ketiga secara keseluruhan dan pengembangan kemitraan untuk memenuhi obyektif organisasi jangka panjang.

Adapun alat kendali atau kontrol yang harus diperhatikan secara sungguh-sungguh oleh organisasi adalah:

- Model dan Struktur Kerjasama Pihak Ketiga - yang biasanya dibagi berdasarkan karakteristik dan model bisnisnya masing-masing seperti: sewa menyewa, beli putus, outsourcing, insourcing, layanan berbasis kuota, cloud computing, dan lain sebagainya.
- Manajemen Kontrak Kerja Pemasok - yang berisi detail perjanjian tugas, kewajiban, hak, dan wewenang pihak ketiga dalam peranannya selaku mitra kerja organisasi atau perusahaan.
- Manajemen Risiko Pemasok - yang secara khusus menangani berbagai model mitigasi risiko yang harus dilakukan oleh organisasi dan pemasoknya untuk memastikan tidak terganggunya proses pengelolaan produk dan layanan teknologi informasi yang diberikan.
- Model Pemantauan Kinerja Pemasok-yang terdiri dari pendekatan, mekanisme, dan rangkaian proses pemantauan akan kinerja pihak ketiga dari waktu ke waktu untuk memastikan dipenuhinya kebutuhan organisasi sesuai dengan kontrak kerja yang berlaku.

Efektif tidaknya pelaksanaan proses ini dapat dilihat dengan memperhatikan sejumlah indikator seperti: (i) jumlah keluhan pihak organisasi terhadap kinerja pemasok atau vendor; (ii) terpenuhi tidaknya tingkat layanan yang disepakati bersama; (iii) periode atau frekuensi pemantauan per masing-masing pemasok; dan lain sebagainya.

Setiap kontrak antara organisasi dengan pemasok teknologi informasinya harus direviu secara rutin dan berkala. Secara prinsip, organisasi mengharapkan terjalinnya kemitraan strategis jangka panjang dengan para pemasok kuncinya, bukan sekedar kontrak jangka pendek yang mengalami perpanjangan setiap akhir masa berlakunya. Oleh karena itulah dalam melakukan evaluasi kontrak, harus dilakukan dengan semangat kerjasama yang dilandasi dengan niat baik dan data hasil evaluasi menyeluruh terhadap kualitas pelayanan yang telah diberikan selama ini. Dengan adanya indikator dan instrumen penilaian yang disepakati bersama, maka proses revisi dan pembaharuan kontrak dapat dilakukan dengan efektif dan berdampak strategis bagi kedua belah pihak. Pihak pemasok harus secara terbuka menerima berbagai masukan dari para pemangku kepentingan yang ada di organisasi, demikian pula sebaliknya organisasi harus mau mendengarkan penjelasan dari mitra kerjanya berdasarkan hasil evaluasi yang dilakukan. Hanya dengan semangat win-win solution atau saling menguntungkan sajalah maka proses pengelolaan pihak ketiga ini dapat berjalan dengan baik.

8.3 MENGELOLA KINERJA DAN KAPASITAS

Bisnis atau aktivitas organisasi berkembang secara dinamis dan pesat dari hari ke hari. Meningkatnya volume dan transaksi interaksi antara organisasi dengan pelanggannya secara langsung akan berdampak pada utilisasi dan kebutuhan penggunaan sumber daya teknologi informasi dan komunikasi. Untuk mencegah terganggunya sistem karena keterbatasan sumber daya yang ada, maka organisasi harus senantiasa melakukan pemantauan terhadap kinerja dan ketersediaan sumber daya teknologi yang dimiliki, seperti: ketersediaan media penyimpanan (siswa kapasitas), kehandalan atau kinerja sistem termutakhir, dan hal-hal terkait lainnya.

Terdapat enam aktivitas yang harus dilaksanakan oleh organisasi, yaitu:

- Mengembangkan rencana pengkajian dan penghitungan kapasitas serta kapabilitas sumber daya teknologi informasi berdasarkan kemajuan dan perkembangan bisnis atau organisasi.
- Menganalisa kinerja dan kapasitas terkini/termutakhir dari berbagai komponen teknologi informasi yang ada.
- Melaksanakan perhitungan kebutuhan kapasitas dan kinerja teknologi informasi untuk masa mendatang dalam konteks jangka pendek, menengah, dan panjang.
- Mengkaji gap antara kebutuhan dan ketersediaan sumber daya teknologi informasi untuk kondisi termutakhir dan demi kebutuhan beberapa tahun ke depan.
- Mempersiapkan rencana cadangan (contingency planning) seandainya gap keterbutuhan komponen teknologi informasi tidak dapat segera terpenuhi.
- Memantau dan menyusun laporan secara berkala terkait dengan kinerja dan kapasitas termutakhir komponen teknologi informasi.

Sejumlah entitas pengendali yang harus dipersiapkan oleh organisasi sehubungan dengan implementasi proses ini antara lain adalah:

- Rencana dan Perhitungan Kapasitas serta Kinerja teknologi informasi yang dibutuhkan organisasi dalam perspektif jangka pendek, menengah, dan panjang

- Hasil Kajian Perhitungan Kapasitas dan Kinerja Termutakhir yang menggambarkan keadaan terkini dari organisasi beserta analisa dampak dan risikonya.
- Target Kapasitas dan Kinerja yang telah ditetapkan untuk masing-masing kurun waktu di masa mendatang, yang telah disepakati oleh segenap pimpinan organisasi untuk dipenuhi dan dijadikan obyektif strategis.
- Gap Keterbutuhan Komponen Teknologi Informasi yang didapatkan dari hasil perhitungan keterbutuhan dan ketersediaan sistem dari waktu ke waktu.
- Profil Ketersediaan Komponen Teknologi Informasi dalam setiap satuan atau durasi waktu.
- Hasil Pemantauan dan Laporan Formal Kapasitas serta Ketersediaan Sistem teknologi informasi secara lengkap dan detail untuk kebutuhan evaluasi dan perencanaan.

Adapun sejumlah indikator yang dapat dipakai untuk menilai tingkat efektivitas pelaksanaan proses ini antara lain: (i) waktu jeda atau tidak bekerjanya sistem karena kekurangan sumber daya; (ii) profil utilisasi dari masing-masing komponen teknologi informasi yang krusial; (iii) persentasi SLA yang tidak tercapai; dan lain sebagainya.

Tingkat kinerja dan kapasitas sistem teknologi informasi harus selaras dan sinkron dengan dinamika bisnis dari waktu ke waktu. Untuk itulah maka perencanaan dan perancangan sistem harus mengacu pada hasil prediksi atau ramalan perkembangan

bisnis di masa mendatang. Analisa terhadap tren dan kajian eksternal merupakan hal penting dan utama yang harus dikerjakan oleh organisasi secara sungguh-sungguh agar sumber daya teknologi informasi dapat dijaga tingkat optimalisasinya. Beberapa organisasi yang telah maju menerapkan sistem pemantauan berbasis kinerja atau indikator empiris seperti performance scorecards dan lain sebagainya. Instrumen ini secara otomatis dihubungkan melalui tool/software dengan kinerja, kehandalan, dan kapasitas sistem yang dimiliki dan dioperasikan oleh organisasi. Secara terus menerus berkesinambungan dilakukan penyesuaian dan revisi perencanaan berdasarkan hasil evaluasi kinerja dan kapasitas yang ada.



8.4 MEMASTIKAN KEBERLANGSUNGAN LAYANAN



Untuk memastikan senantiasa tersedianya layanan teknologi informasi dan komunikasi yang tak terputus (continuous service) membutuhkan serangkaian proses perencanaan, pemeliharaan, pengujian, dan pemantauan sistem yang serius. Memilih pendekatan dan metoda layanan yang pas dan sesuai dengan kebutuhan organisasi merupakan kunci pengelolaan yang prima - dimana secara simultan terjadi usaha meminimalisasi probabilitas terganggunya sistem serta mengurangi dampak kerugian negatif akibat terganggunya sistem yang berpengaruh langsung terhadap proses dan aktivitas organisasi atau perusahaan.

Paling tidak terhadap sebelas aktivitas yang harus diperhatikan secara sungguh-sungguh oleh organisasi seperti yang dijelaskan dalam paparan ringkas berikut ini:

- Mengembangkan kerangka layanan teknologi informasi yang berkesinambungan, yaitu suatu gambaran mengenai peranan dan fungsi sistem dimana saja (dalam

konteks organisasi) yang tidak boleh mengalami gangguan atau interupsi sama sekali.

- Melaksanakan kajian risiko dan dampak pada bisnis seandainya terjadi gangguan pada sejumlah sistem teknologi informasi yang dimiliki oleh organisasi atau perusahaan terkait.
- Menyusun dan memelihara prosedur baku perencanaan pelaksanaan proses layanan teknologi informasi yang berkesinambungan dan tak terputus.
- Mengidentifikasi dan mengkategorisasikan jenis-jenis komponen teknologi informasi berdasarkan konteks pemulihannya berdasarkan tingkat kepentingannya bagi organisasi atau perusahaan.
- Menyusun dan menerapkan prosedur perubahan atau revisi terkait dengan strategi layanan untuk memastikan keterkinian atau kemutakhiran dokumen yang dipergunakan sebagai panduan teknis.
- Melakukan tes atau uji coba terhadap prosedur pemulihan layanan secara berkala untuk menilai tingkat efektivitasnya dan membiasakan para pemangku kepentingan menerapkannya.
- Melaksanakan sejumlah rencana aksi dan revisi berdasarkan hasil dari tes atau uji coba terhadap prosedur pemulihan layanan yang dilaksanakan secara periodik tersebut.

- Merencanakan dan menyelenggarakan pelatihan penyediaan layanan berkesinambungan kepada seluruh pihak yang secara langsung maupun tidak langsung terkait dengan hal ini.
- Merencanakan pendekatan yang akan dipergunakan dalam memulihkan layanan teknologi informasi yang mengalami gangguan.
- Merencanakan dan menerapkan model proteksi dan pencadangan komponen maupun sumber daya teknologi informasi yang penting dan krusial bagi keberlangsungan operasional organisasi atau perusahaan.
- Mengembangkan prosedur untuk menilai serta mengavaluasi hasil proses yang terkait langsung dengan penyediaan layanan teknologi informasi serta mekanisme pemulihannya jika terdapat gangguan yang tidak diinginkan.

Ada cukup banyak entitas yang harus dimiliki oleh organisasi sebagai alat pengendali terlaksananya proses ini secara efektif, yaitu:

- Kerangka Keberlangsungan Layanan Teknologi Informasi - yang memperlihatkan berbagai jenis layanan teknologi yang terdapat pada organisasi, hubungan keterkaitannya dengan bisnis, serta karakteristik uniknya.
- Rencana Keberlangsungan Layanan Teknologi Informasi - yang merupakan dokumen prosedur layanan teknologi informasi secara berkesinambungan untuk mendukung organisasi dan perusahaan tanpa henti.

- Daftar Sumber Daya Teknologi Informasi yang Renting - yang memperlihatkan daftar sumber daya teknologi informasi mana saja yang sangat penting dan krusial keberadaannya bagi organisasi sebagai dasar prioritas penerapan layanan yang prima.
- Rencana Pemeliharaan dan Penjaminan Layanan Teknologi Informasi - yang menggambarkan model pendekatan untuk memastikan terpeliharanya dan terjaminnya aktivitas penanganan pelayanan secara terus-menerus tanpa interupsi sesuai dengan kebutuhan bisnis.
- Uji Coba Prosedur Pemulihan Layanan Teknologi Informasi - yang memperlihatkan jadwal serta kegiatan tes atau uji coba prosedur layanan dan pemulihannya yang dilakukan secara rutin dan berkala untuk menjamin kualitas pelayanan.
- Pelatihan Layanan dan Pemulihan Teknologi Informasi - yang memperlihatkan jadwal serta jenis pelatihan terkait dengan tata cara atau prosedur melaksanakan layanan teknologi informasi yang berkesinambungan serta mekanisme pemulihan jika terdapat gangguan yang tidak diinginkan.
- Distribusi Rencana Layanan Teknologi Informasi - yang memastikan bahwa seluruh rencana memberikan layanan prima dimengerti dan siap dijalankan oleh seluruh unit organisasi.
- Mekanisme Pemulihan Layanan Teknologi Informasi - yang menggambarkan prosedur serta mekanisme teknis berisi tata cara memulihkan kembali layanan teknologi informasi setelah atau pasca terjadinya gangguan maupun berbagai

interupsi.

- Cadangan Simpanan Eksternal - yang memperlihatkan bagaimana dikelolanya situs di luar organisasi yang berisi cadangan dari aset data, informasi, maupun sumber daya teknologi informasi lainnya untuk mengantisipasi jika terjadi kegiatan yang tidak diinginkan.
- Kajian Pasca Pemulihan Layanan - yang menggambarkan tata cara evaluasi yang harus dilakukan secepat pemangku kepentingan terkait dengan kinerja layanan maupun pemulihan terhadap layanan dari organisasi yang bersangkutan.

Efektivitas pelaksanaan proses ini dapat pula dipantau dan dimonitor dengan menggunakan indikator seperti: (i) jumlah waktu yang terbuang percuma ketiga terjadi gangguan; (ii) persentase aplikasi atau sistem teknologi penting yang tidak terdapat prosedur proteksi maupun pemulihannya; (iii) dampak kerugian bisnis yang terjadi akibat adanya gangguan terhadap sistem; dan lain sebagainya.

Pada dasarnya, proses layanan terhadap teknologi informasi haruslah dilihat secara holistik dan terintegrasi dengan sistem bisnis atau organisasi yang ada. Secara rutin dan kontinyu setiap layanan teknologi informasi dipantau, dimonitor, dan dijaga kinerjanya dengan menggunakan indikator empirik (metrik). Adapun cara menyelaraskan antara kebutuhan bisnis dengan performa teknologi informasi dalam kaitannya dengan ketersediaan sistem adalah melalui mekanisme analisa risiko. Paling tidak, sistem yang sangat krusial bagi kelangsungan hidup organisasi, dan memiliki profil ancaman dengan

probabilitas tinggi haruslah dijaga benar eksistensinya agar senantiasa dapat beroperasi secara penuh.

8.5 MEMASTIKAN KEAMANAN SISTEM

Kebutuhan untuk menjaga validitas dan integritas data maupun informasi serta memproteksi berbagai aset teknologi informasi memaksa organisasi untuk menerapkan sejumlah proses terkait dengan manajemen keamanan sistem. Organisasi perlu mengembangkan sejumlah kebijakan, standar, maupun prosedur untuk mengelola aspek keamanan dimaksud. Keseluruhan peraturan tersebut haruslah dipantau implementasinya dan dipastikan efektivitasnya - terutama dalam hubungannya dengan usaha untuk menanggapi berbagai ancaman keamanan maupun menghadapi kelemahan/kerawanan sistem yang dimiliki organisasi. Secara prinsip terdapat tiga cara dalam menghadapi isu keamanan sistem, masing-masing melalui usaha preventif, reaktif, maupun perbaikan kualitas secara kontinyu.

Paling tidak terdapat tujuh aktivitas yang harus dilaksanakan organisasi dalam melaksanakan proses tersebut, yaitu:

- Mendefinisikan dan memelihara prosedur keamanan sistem yang harus disusun dan diadopsi oleh seluruh lapisan organisasi.
- Mendefinisikan, mengembangkan, dan menerapkan proses terkait dengan pengelolaan manajemen identitas individu.
- Memantau dan mengidentifikasi insiden maupun ancaman yang mungkin terjadi menimpa organisasi.

- Mengkaji dan memvalidasi secara periodik hak akses individu yang beraktivitas dalam linekunean oreanisasi.
- Menyusun dan mengernbangkan berbagai standar dan prosedur terkait dengan manajemen penyandian (kriptografi).
- Mengimplementasikan dan menerapkan berbagai prosedur teknis untuk mengamankan lalu lintas data pada jaringan komputer lokal maupun internet.
- Melaksanakan kajian kerawanan dan kelemahan sistem secara berkala dan periodik.

Terdapat cukup banyak ehtitas pengendali yang harus dimiliki dan dikembangkan oleh organisasi, yaitu:

- Manajemen Keamanan Data - suatu bentuk mekanisme pengamanan data yang telah disepakati pimpinan dan segenap pemangku kepentingan organisasi.
- Model Keamanan Teknologi Informasi - translasi kebutuhan organisasi atau bisnis terhadap keamanan data ke dalam bentuk prinsip dan prosedur teknis yang harus dipatuhi serta diadopsi oleh seluruh organisasi.
- Manajemen Identitas Individu - model alokasi tanda pengenal unik berbasis digital terhadap masing-masing individu yang beraktivias di organisasi.
- Manajemen Akun Individu - prosedur pengambilan, pengalokasian, pemakaian, pemutakhiran, pemantauan, dan pengakhiran identitas individu yang telah

diberikan organisasi kepada masing-masing karyawannya berdasarkan hak wewenang, tugas, serta tanggung jawabnya.

- Model Pemantauan dan Surveilans - tata cara melakukan pengawasan terhadap keadaan keamanan setiap aset dan sumber daya teknologi informasi yang berada dalam perimeter organisasi.
- Daftar Potensi Insiden Keamanan - sejumlah kejadian tidak diinginkan yang mungkin terjadi dan menimpa organisasi sehingga mendatangkan dampak kerugian material maupun immaterial.
- Proteksi terhadap Teknologi Keamanan - teknik mengamankan seluruh model pengamanan yang diterapkan oleh organisasi untuk menjaga aset berharganya.
- Manajemen Kunci Kriptografi - prosedur baku dan standar untuk mengelola kunci publik maupun privat demi kebutuhan penyandian data maupun pesan.
- Model Pencegahan, Deteksi, dan Koreksi Program Jahat - teknik dan peralatan yang dibutuhkan untuk mencegah tereksekusinya program tertentu yang bertujuan tidak baik (malicious software), seperti: virus, trojan, botnet, spyware, dan lain sebagainya.
- Standar Keamanan Jaringan - kriteria yang harus dipenuhi organisasi untuk mengamankan jaringan komputer dan telekomunikasi yang dipergunakan.

- Mekanisme Pertukaran Data Penting - tata cara pertukaran data digital yang harus dipatuhi untuk menjamin keamanan data yang ada.

Adapun sejumlah indikator yang bisa dipergunakan adalah sebagai berikut: (i) jumlah insiden yang berakibat buruk terhadap organisasi; (ii) jumlah sistem atau aplikasi yang tidak memenuhi standar keamanan yang telah ditetapkan; (iii) hasil audit kerawanan atau kelemahan sistem yang ada pada organisasi; dan lain sebagainya.

Aspek keamanan data adalah merupakan tanggung jawab seluruh pemangku kepentingan dalam organisasi - baik dalam level manajemen maupun karyawan/ staf. Bahkan dari waktu ke waktu, sejalan dengan perkembangan teknologi yang ada, tanggung jawab setiap individu dalam organisasi terhadap keamanan data menjadi bertambah penting dan berat. Tidak semua model pengamanan dapat dilakukan secara otomatis dengan memanfaatkan teknologi, mengingat sebagian besarnya terkadang masih harus ditangani secara manual. Adapun serangkaian tugas rutin yang harus dilakukan organisasi adalah memastikan setiap kerawanan dan kelemahan yang ada dimitigasi risiko eksploitasinya, dan secara simultan melakukan pemantauan dan monitoring terhadap berbagai cobaan, ancaman, maupun potensi insiden yang mungkin terjadi. Sebagai tambahan, indikator telah tercapainya target keamanan data perlu pula dikomunikasikan dan dipelajari oleh seluruh pihak yang memegang tanggung jawab kunci dalam mengamankan data organisasi.

8.6 MENGIDENTIFIKASIKAN DAN MENGALOKASIKAN BIAYA

Demi memperoleh layanan teknologi informasi yang andal dan prima, dibutuhkan biaya atau sumber daya finansial dengan jumlah yang sesuai dengan fitur serta kualitas yang diinginkan. Oleh karena itulah maka setiap kebutuhan biaya harus dihitung secara cermat dan mendapatkan komitmen persetujuan pimpinan organisasi untuk dialokasikan atau dibayarkan kepada penyedia jasa layanan teknologi informasi.

Ada empat hal pokok yang harus dilakukan sebagai serangkaian aktivitas untuk menjalankan proses ini, yaitu:

- Memetakan komponen sumber daya dan infrastruktur yang diperlukan untuk menjalankan masing-masing layanan teknologi informasi yang dibutuhkan organisasi.
- Mengidentifikasi komponen kebutuhan biaya per-masing-masing layanan teknologi informasi dan total alokasi yang dibutuhkan per unit biaya dan per satuan waktu.
- Mengembangkan dan menjalankan model akuntansi berbasis biaya dan mengendalikannya.
- Mengembangkan dan mengoperasikan model pencairan dana dalam bentuk kebijakan dan prosedur yang harus ditaati bersama.

Terkait dengan proses ini, terdapat empat entitas pengendali yang dibutuhkan, yaitu masing-masing:

- Definisi Layanan Teknologi Informasi - untuk dipergunakan dalam menentukan jenis-jenis pekerjaan mana saja yang perlu secara sungguh-sungguh dialokasikan biaya pengadaannya (capex maupun opex).
- Sistem Akuntansi dan Keuangan untuk Alokasi Teknologi Informasi - untuk dipakai sebagai acuan dalam melakukan perhitungan maupun pengalokasian seluruh biaya teknologi informasi yang dibutuhkan.
- Model Pembiayaan dan Pencairan - untuk dipergunakan sebagai syarat pengalokasian dan pencairan dana yang dibutuhkan untuk dibayarkan kepada pihak pemasok layanan teknologi informasi.
- Pemutakhiran Model Pembiayaan - untuk dipakai sebagai acuan perbaikan sistem pembiayaan dari masa ke masa sesuai dengan kebutuhan jaman dan hasil evaluasi tingkat efektivitas dan efisiensi.

Untuk memastikan proses ini dilaksanakan dengan baik dan konsisten, indikator yang dapat dipergunakan antara lain adalah: (i) jumlah tagihan yang langsung dibayarkan organisasi; (ii) rata-rata jeda waktu antara penagihan dan pembayaran; (iii) jumlah "dispute" atau ketidaksepahaman akan model pembayaran antara organisasi dengan pemasoknya; dan lain sebagainya.

Jenis-jenis komponen biaya yang harus dialokasikan untuk mendapatkan layanan teknologi informasi diidentifikasi, dikelola, dan dilaporkan ke pimpinan organisasi untuk

dipelajari kewajaran dan strategi pengelolaannya. Secara esensial, pimpinan organisasi akan melakukan perhitungan atau analisa cost-benefit untuk mengevaluasi tingkat optimalisasi dari masing-masing komponen pembiayaan yang dikeluarkan. Hasil evaluasi ini akan dipergunakan sebagai basis dalam menentukan revisi model sesuai kebutuhan di masa mendatang. Adapun salah satu cara yang dapat dipergunakan untuk menilai wajar tidaknya biaya yang dikeluarkan adalah melalui proses perbandingan dengan organisasi sejenis lainnya atau yang dikenal sebagai istilah "benchmarking". Perlu diperhatikan bahwa dalam konteks pembiayaan berlaku pula istilah perbaikan yang berkesinambungan (continous improvement), terlebih-lebih dengan melihat kenyataan bahwa target akhir dari kerjasama antara organisasi dengan pemasok layanannya adalah kemitraan strategis berjangka panjang - bukan sekedar kontrak tahunan yang berulang belaka.



8.7 MENGEDUKASI DAN MELATIH PENGGUNA

Sudah seyogyanya setiap individu yang menggunakan beragam aplikasi teknologi informasi di organisasi mendapatkan kesempatan untuk mendapatkan bimbingan atau pelatihan secukupnya. Biasanya setiap kelompok pengguna atau user group memiliki kebutuhan uniknya sendiri-sendiri - walaupun dalam kenyataannya setiap individu memiliki karakteristik yang berbeda sehingga berakibat pada berbeda-bedanya kebutuhan pelatihan dari masing-masing orang atau pengguna. Organisasi harus dengan baik mengidentifikasikan dan memetakan kebutuhan ini agar dapat dipersiapkan program pelatihan yang tepat dan sesuai dengan kebutuhan. Dengan dimilikinya karyawan yang kompeten dalam menggunakan sistem, maka diharapkan manfaat yang dijanjikan dengan adanya sistem dapat segera terwujud, seperti: semakin cepatnya proses (efisiensi), semakin

transparannya laporan, semakin terkendalinya eksekusi kebijakan, semakin meningkatnya produktivitas kerja, dan lain sebagainya.

Terdapat lima aktivitas yang harus dilakukan terkait dengan hal ini, yaitu:

- Mengidentifikasi kebutuhan pelatihan dari para pengguna - dengan cara melakukan analisa jenis-jenis aplikasi dan kewajiban user dalam mengoperasikan sistem tertentu serta mengukur tingkat penguasannya.
- Menentukan, menyusun, dan mengembangkan program pelatihan – yang dibuat berdasarkan hasil kajian terhadap kelompok pengguna masa saja yang membutuhkan keahlian apa saja dalam hal pemanfaatan sistem maupun aplikasi teknologi informasi dan komunikasi yang dibutuhkan organisasi.
- Meningkatkan keperdulian dan menyelenggarakan pelatihan-yaitu pelaksanaan serangkaian program pelatihan bagi mereka yang telah ditargetkan untuk menjadi pengguna dengan kompetensi dan keahlian tertentu.
- Mengevaluasi hasil pelatihan - melalui berbagai cara efektif seperti pemantauan terhadap kinerja individu maupun kelompok pasca pelatihan diberikan kepada kelompok pengguna dimaksud.
- Menilai dan menetapkan metoda pelatihan yang terbaik untuk diadopsi - berupa perbaikan model dan pendekatan pelatihan berdasarkan hasil evaluasi peserta didik maupun penyelenggara untuk peningkatan kualitas pelatihan dan pengembangan di kemudian hari.

Terkait dengan hal ini ada beberapa entitas pengendali yang harus dimiliki oleh organisasi yaitu:

- Tata Cara Pengidentifikasian Kebutuhan Pelatihan dan Edukasi - yang merupakan panduan pelaksanaan proses identifikasi kebutuhan secara rutin dan berkala untuk memastikan setiap individu dalam organisasi memiliki kompetensi dan keahlian (literasi) sebagaimana dibutuhkan dari masa ke masa.
- Standar Penyelenggaraan Pelatihan dan Edukasi - yang merupakan kriteria yang harus wajib diikuti oleh seluruh pihak penyelenggara dan pelaksana program pelatihan maupun proses lain yang berbau edukasi/pendidikan peningkatan kompetensi atau keahlian.
- Instrumen Evaluasi Pelatihan dan Edukasi - yang merupakan alat atau cara untuk mengukur efektivitas penyelenggaraan dan pelaksanaan model pelatihan dan edukasi untuk memastikan tercapainya obyektif yang dicanangkan organisasi.

Dengan mudah organisasi dapat mengukur tingkat keberhasilan atau efektivitas pelaksanaan pelatihan ini seperti misalnya dengan menggunakan indikator seperti: (i) jumlah telepon ke help desk dari para pengguna yang mengalami kesulitan menggunakan sistem; (ii) tingkat kepuasan pimpinan terhadap kinerja anak buahnya; (iii) durasi waktu antara tahap identifikasi hingga pelaksanaan pelatihan yang terkait dengannya; (iv) hasil evaluasi pelaksanaan program pelatihan; (v) rata-rata jumlah pelatihan yang diterima per masing-masing karyawan; dan lain sebagainya.

Setiap program pelatihan bertujuan untuk meningkatkan kinerja individu dimana secara kolektif akan berdampak terhadap meningkatnya performa organisasi atau perusahaan. Oleh karena itulah maka keberadaan aktivitas pelatihan dan edukasi sangat krusial bagi keberlangsungan organisasi. Setiap tahunnya, setiap organisasi moderen melakukan perencanaan dan penganggaran alokasi keuangan untuk kebutuhan pelatihan manajemen serta karyawannya. Proses pelatihan yang tidak efektif atau buruk akan mempengaruhi kinerja organisasi secara signifikan sehingga sudah merupakan kewajiban bagi seluruh pemangku kepentingan untuk mengelola proses ini dengan sebaik-baiknya.



8.8 MENGELOLA PUSAT LAYANAN DAN INSIDEN

Menjawab pertanyaan secara cepat dan tepat mengenai permasalahan penggunaan atau pemanfaatan teknologi dalam organisasi akan sangat mempengaruhi kinerja organisasi. Oleh karena itulah setiap organisasi harus memiliki fungsi "help desk service" yaitu suatu pusat pelayanan informasi yang akan membantu berbagai persoalan teknis maupun administratif operasional yang dihadapi para pengguna sistem dan aplikasi. Terkait dengan hal ini, organisasi harus mengembangkan pusat tersebut, membuat prosedur penanganan dan eskalasi insiden, mempelajari tren atau isu keluhan, mencari akar permasalahan, serta menetapkan resolusi atau pemecahan masalahnya. Ada enam aktivitas yang harus dilaksanakan secara sungguh-sungguh, yaitu:

- Mengembangkan struktur kategori dan klasifikasi jenis permasalahan berdasarkan tingkat kepentingan dan dampaknya terhadap organisasi serta prosedur eskalasi pengambilan keputusannya berbasis struktur dan fungsi organisasi.
- Mendeteksi dan merekam berbagai laporan insiden serta isu/masalah yang dihadapi para pengguna sistem dan teknologi informasi berdasarkan jenis permintaan atau permohonan layanan pemecahan masalahnya.
- Mengklasifikasikan, menginvestigasi, dan mendiagnosa permasalahan yang dilaporkan oleh lapangan melalui para pengguna yang menghadapi problema terkait.
- Menyelesaikan masalah, mengembalikan sistem/aplikasi ke fungsi normalnya, dan menutup atau mendeklarasikan telah selesainya insiden ditangani.
- Menginformasikan para pengguna terkait sehubungan cara penanganan masalah atau insiden sejenis sebagai bagian dari proses pembelajaran.
- Menyusun laporan untuk dipelajari para pemangku kepentingan untuk memperbaiki sistem dan aplikasi sesuai dengan hasil evaluasi yang dilakukan bersama.

Adapun entitas yang harus dimiliki organisasi terkait dengan implementasi proses ini adalah sebagai berikut:

- Pusat Layanan (Service Desk) - yang berfungsi selama 24/7 untuk menjawab berbagai pertanyaan dan menyelesaikan sejumlah masalah teknis/praktis yang dihadapi secara langsung oleh pengguna sistem dan aplikasi teknologi.
- Daftar Pertanyaan Pengguna - yang berisi seluruh kemungkinan pertanyaan yang berpotensi ditanyakan oleh pengguna terkait dengan permasalahan lapangan yang kerap terjadi beserta jawaban serta cara menghadapi/menyelesaikan masalah tersebut.
- Skema dan Prosedur Eskalasi Insiden - yang merupakan tahapan cara menangani masalah dengan melibatkan pihak yang lebih tinggi otoritasnya berdasarkan karakteristik dan profil masalah yang dihadapi oleh pengguna (biasanya memerlukan sumber daya tambahan untuk menyelesaikan masalahnya atau membutuhkan keputusan dengan tingkat otoritas yang lebih tinggi).
- Penetapan Akhir Penyelesaian Insiden - yang pada dasarnya adalah suatu pernyataan bahwa insiden yang dihadapi telah diselesaikan dengan baik dan memberikan manfaat bagi pemakai yang berhadapan langsung dengan insiden yang terjadi.
- Laporan Analisa Tren - yang berupa ringkasan terhadap jenis dan tipe insiden yang terjadi dalam suatu kurun waktu untuk dilihat tren atau kecenderungan

kejadiannya sebagai suatu pembelajaran untuk pembenahan dan pengembangan sistem di kemudian hari.

Indikator relevan yang dapat dipergunakan untuk memonitor dan memantau efektivitas pelaksanaan proses ini antara lain adalah: (i) tingkat kepuasan pelanggan atas pelayanan yang diberikan; (ii) rata-rata durasi penyelesaian insiden yang dihadapi; (iii) jumlah eskalasi yang terjadi; dan lain sebagainya.

Help desk yang baik biasanya ditangani oleh individu-individu yang kompeten dengan dilengkapi teknologi yang memadai. Tidak ada masalah yang tidak dapat diatasi jika memang fungsi ini direncanakan dan dikembangkan secara sungguh-sungguh. Perlu diperhatikan bahwa dalam kenyataannya, setiap detik bagi organisasi komersial semacam perusahaan sangat bernilai harganya. Insiden yang menyebabkan sistem dan aplikasi tidak berfungsi akan berakibat secara langsung terhadap kinerja perusahaan. Oleh karena itulah maka fungsi help desk harus dapat menangani berbagai masalah atau insiden yang terjadi dalam rentang waktu yang telah ditetapkan oleh organisasi.

8.9 MENGELOLA KONFIGURASI

Memastikan integritas konfigurasi piranti keras dan piranti lunak yang berada dalam teritori organisasi merupakan fungsi penting yang harus dimiliki untuk memastikan beroperasionalnya sistem secara baik. Seperti diketahui bersama, organisasi berkembang secara sangat pesat, dimana menyebabkan teknologi informasi harus senantiasa mampu untuk menyesuaikan dirinya. Konfigurasi berbicara mengenai "keseimbangan" kondisi atau profil antara komponen sistem seperti hardware,

software, database, infrastruktur, fasilitas, maupun sumber daya manusia agar senantiasa dapat memiliki kinerja yang diharapkan dan telah ditetapkan sebelumnya.

Terdapat empat aktivitas yang harus dilakukan terkait dengan pelaksanaan proses ini, yaitu:

- Mengembangkan prosedur perencanaan dan pengelolaan konfigurasi yang akan menjadi panduan dan referensi utama bagi divisi sistem dan teknologi informasi.
- Mengumpulkan informasi dan memverifikasi kondisi konfigurasi terkini sebagai bahan pengkajian mengenai situasi kinerja serta risiko yang dihadapi oleh organisasi.
- Mengkaji serta mengevaluasi kondisi konfigurasi untuk melihat ada tidaknya dampak negatif maupun positif bagi organisasi sesuai dengan perkembangan kebutuhan termutakhir.
- Memutakhirkan konfigurasi sistem dan teknologi sebagai jawaban terhadap kajian dan evaluasi kebutuhan kinerja dengan kondisi sistem yang dimiliki pada saat tertentu.

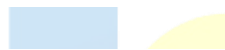
Untuk itu dibutuhkan tiga entitas pengendali terkait dengan manajemen konfigurasi masing-masing adalah:

- Repositori Standar Baseline Konfigurasi - yang berisi seluruh informasi terkait dengan parameter konfigurasi yang harus dipenuhi dalam berbagai situasi dan kondisi untuk menjamin kinerja yang diharapkan.
- Manajemen Identifikasi dan Pemeliharaan Konfigurasi - yang memuat prosedur untuk mengidentifikasikan, mencatat, merubah, dan memutakhirkan situasi dan kondisi konfigurasi per satuan waktu yang telah ditetapkan sebagai catatan dan rekam jejak untuk bahan pemantauan, evaluasi, pengamatan, dan penilaian.
- Kajian Integritas Konfigurasi - yang berisi prinsip-prinsip dan prosedur baku penilaian situasi dan kondisi (integritas) konfigurasi pada satu satuan waktu tertentu yang dilaksanakan prosesnya secara periodik/berkala.

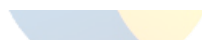
Dalam kaitannya dengan pemantauan efektivitas pelaksanaan proses ini dapat dipergunakan ukuran atau indikator seperti: (i) jumlah kasus konfigurasi yang ditemukan berada diluar aturan teknis yang berlaku (compliance); (ii) jumlah kasus deviasi antara rencana konfigurasi dengan keadaan aktual sebenarnya; (iii) waktu yang diperlukan untuk melakukan penyesuaian terhadap konfigurasi; dan lain sebagainya.

Organisasi yang moderen biasanya memiliki sistem konfigurasi yang tersentralisasi dan berfungsi secara otomatis penuh, dalam arti kata terdapat suatu pusat (server) yang menangani manajemen konfigurasi seluruh aset

sistem dan teknologi yang ada dalam organisasi. Tentu saja sistem terpusat ini dibangun dengan konsep yang sangat holistik, dimana seluruh sistem dan aplikasi yang ada di organisasi secara terpadu dan terintegrasi dihubungkan dengan sistem utama konfigurasi tersebut sehingga bisa senantiasa dipantau, dinilai, dievaluasi, dan dimutakhirkan. Mengingat bahwa berbagai sistem yang ada berasal dari beraneka ragam vendor teknologi, maka sistem yang ada dibangun dan dikembangkan secara bersama-sama oleh seluruh penyelenggara teknologi - baik secara langsung maupun tidak langsung. Obyektif utama sebagai muaranya adalah terciptanya dan terjaganya kinerja sistem dari hari ke hari sesuai dengan kebutuhan organisasi.



8.10 MENGELOLA DATA



Data digital atau data elektronik adalah aset organisasi yang tak ternilai harganya. Oleh karena itulah maka keberadaannya harus dirawat dan dikelola sungguh-sungguh agar senantiasa utuh, valid, dan berkualitas (dijaga integritasnya). Perawatan yang dimaksud antara lain melakukan pencadangan (backup), pemeliharaan media penyimpanan, pemutakhiran data, penghapusan atau pemusnahan data, dan lain sebagainya. Dalam kaitan dengan proses ini, terdapat lima aktivitas yang harus dilakukan, yaitu:

- Mentranslasikan berbagai kebutuhan penyimpanan, pencadangan, dan pemeliharaan data ke dalam sebuah prosedur yang harus dipatuhi oleh seluruh penanggung jawab berbagai aset data yang ada dalam sebuah organisasi.

- Mendefinisikan, memelihara, dan menerapkan prosedur untuk mengelola pustaka media penyimpan data - agar terhindar dari berbagai hazard atau kondisi yang dapat membahayakan keberadaan dan memori data yang terkandung di dalamnya.
- Mendefinisikan, memelihara, dan menerapkan prosedur terkait dengan pemusnahan pustaka data serta peralatan terkait dengannya secara aman dan terkendali.
- Melakukan pencadangan data sesuai dengan skema dan prosedur yang berlaku.
- Mendefmsiikan, memelihara, dan menerapkan prosedur untuk melakukan proses restorasi data sebagai bagian penting dari kegiatan pengelolaan data.

Ada enam entitas pengendali yang harus diperhatikan keberadaannya oleh sebuah organisasi, yaitu masing-masing sebagai berikut:

- Kebutuhan Organisasi mengenai Pengelolaan Data - berisi kebutuhan dan harapan para pemangku kepentingan akan terkelolanya data organisasi secara sebaik-baiknya.
- Mekanisme Penyimpanan dan Pemutakhiran Data - berisi tata cara dan prosedur mengelola data secara efektif dan efisien agar sejalan dengan kebijakan organisasi dan aturan perundang-undangan yang berlaku.

- Sistem Manajemen Pustaka Media Penyimpan - berisi mekanisme pengelolaan media penyimpan elektronik maupun digital agar senantiasa terpelihara dan dapat berfungsi dengan sebaik-baiknya.
- Prosedur Pemusnahan dan Pemutakhiran Data dan Sumber Daya Teknologi berisi prinsip-prinsip dan detail teknis manajemen atau pengelolaan sumber daya teknologi yang dipergunakan sebagai penyimpan data/informasi sebagai aset organisasi yang tak ternilai harganya.
- Manajemen Pencadangan dan Restorasi Data - berisi mekanisme rutin maupun adhoc berkaitan dengan kewajiban membuat data cadangan (backup) sebagai bagian dari mitigasi risiko serta merestorasinya seandainya terjadi peristiwa atau kejadian yang membutuhkannya.
- Manajemen Keamanan Data dan Informasi - berisi panduan yang harus diadopsi oleh organisasi dan seluruh pemangku kepentingan yang ada di dalamnya dalam hal mengelola dan mengamankan data maupun informasi yang dipergunakannya agar terhindar dari kejadian yang tidak diinginkan, seperti: perusakan data, pengaksesan data oleh pihak tak berwenang, penghilangan data, penyadapan data, dan lain sebagainya.

Dalam konteks itulah maka cukup banyak indikator yang dapat dikembangkan untuk melihat tingkat efektivitas pelaksanaan proses ini, seperti: (i) tingkat kepuasan pengguna data; (ii) kecepatan restorasi data pada saat dibutuhkan; (iii) validitas dan reliabilitas data; dan lain sebagainya.

Manajemen data pada organisasi maju tidak saja ditandai dengan adanya kebijakan, aturan, dan panduan teknis yang lengkap terkait dengan proses pengelolaan data dan informasi, namun telah masuk lebih jauh menjadi budaya organisasi yang secara tertib, disiplin, dan konsisten dijalankan oleh segenap individu dan para pemangku kepentingan yang ada. Seluruh jajaran organisasi sadar sepenuhnya akan pentingnya memelihara dan menjaga data selaku aset berharga dan memanfaatkannya dengan sebaik-baiknya.

8.11 MENGELOLA LINGKUNGAN FISIK



Sumber daya teknologi informasi seperti server, infrastruktur, data center, komputer, dan piranti keras maupun lunak lainnya berada dalam sebuah teritori lingkungan fisik yang harus dijaga kondisinya. Buruknya instalasi atau kondisi fisik lingkungan dapat mengakibatkan terjadinya insiden yang dapat mengganggu operasional sistem, seperti: kebakaran karena arus pendek, kerusakan karena banyaknya debu, malfungsi karena medan magnet, sistem rusak karena suhu terlampaui panas, dan lain sebagainya. Disamping itu desain lingkungan yang baik harus pula memperhatikan faktor-faktor risiko lain seperti keamanan data, kemudahan akses, maupun ketersediaan biaya pemeliharaan serta pengelolaan.

Ada lima aktivitas utama yang harus dijalankan secara sungguh-sungguh oleh organisasi, masing-masing adalah:

- Menetapkan tingkat kebutuhan proteksi lingkungan fisik sistem teknologi informasi berdasarkan karakteristik dan situasi kondisi yang ada.

- Memilih dan menetapkan situs atau fasilitas yang akan dijaga kondisi lingkungannya agar kondusif dan aman bagi kegiatan operasional.
- Menerapkan ukuran-ukuran atau indikator situasi dan kondisi lingkungan fisik sebagai cara untuk mengawasi serta memantau keadaannya.
- Mengelola lingkungan fisik melalui aktivitas pemeliharaan, pemantauan, pengawasan, dan pelaporan dari pihak-pihak yang diberi tanggung jawab kepada pimpinan organisasi.
- Mendefinisikan dan menerapkan prosedur pemeliharaan kondisi lingkungan fisik oleh pihak-pihak yang diberi tugas sesuai dengan otoritas dan wewenangnya masing-masing.

Adapun entitas sebagai pengendali pelaksanaan proses yang harus diperhatikan oleh organisasi adalah sebagai berikut:

- Peta Situs dan Fasilitas - memperlihatkan tata letak berbagai fasilitas yang dimiliki organisasi beserta karakteristiknya yang dikaitkan dengan tingkat kepentingan dan perlindungan yang harus diberikan padanya.
- Ukuran dan Indikator Kondisi Fasilitas - membantu manajemen dalam memantau kondisi fasilitas yang ada untuk kebutuhan pencegahan, pendeteksian, maupun mitigasi risiko terhadap kemungkinan terjadinya kerusakan fasilitas karena hal-hal yang berhubungan dengan kebakaran, suhu, bencana alam, serangan teroris, vandalisme, beban listrik berlebihan, ledakan, kebocoran zat kimia, dan lain sebagainya.

- Model Akses Fisik terhadap Fasilitas - merupakan kebijakan yang diambil organisasi terhadap berbagai hak akses pemanfaatan fasilitas baik untuk kebutuhan operasional maupun pemeliharaan, dimana masing-masing individu dalam organisasi diberikan tingkat otoritas yang berbeda-beda sesuai dengan hak, tugas, dan tanggung jawabnya.
- Proteksi terhadap Faktor Lingkungan - memastikan dilindunginya aset fasilitas dari kemungkinan kerusakan atau hal negatif lainnya yang ditimbulkan oleh lingkungan sekitar, seperti: korosi, medan magnet, suhu, kelembaban, dan lain sebagainya.
- Mekanisme Pengelolaan Fasilitas Fisik - memberikan wewenang dan menugaskan pihak tertentu untuk secara aktif dan rutin melakukan pemeliharaan dan pengelolaan terhadap seluruh fasilitas fisik yang dimiliki organisasi agar dijaga kondisinya.

Sementara itu indikator yang dapat dipergunakan untuk melihat efektif tidaknya pelaksanaan proses ini adalah sebagai berikut: (i) jumlah insiden fisik yang mengakibatkan lumpuhnya fasilitas yang dibutuhkan; (ii) jumlah insiden yang terjadi karena rapuhnya model pengamanan yang diterapkan; (iii) frekuensi kajian atau audit terhadap kondisi fasilitas fisik di lapangan, dan lain sebagainya.

Memelihara kondisi fisik fasilitas agar senantiasa layak pakai adalah obyektif organisasi yang harus dilihat dari perspektif jangka panjang. Organisasi harus memiliki prosedur rutin dan tetap untuk mengelola berbagai aset fisik yang dimiliki untuk memastikan lancarnya kegiatan operasional yang menggunakannya. Untuk memastikan kualitas pelayanan, harus dikembangkan dan diadopsi beragam

standar dan ukuran/indikator pelaksanaan oleh segenap pemangku kepentingan. Sementara fasilitas yang sudah dianggap harus diperbaiki karena termakan usia perlu dideteksi dan dimutakhirkan agar tidak terjadi penurunan terhadap kinerja operasional organisasi.

8.12 MENGELOLA OPERASIONAL SISTEM

Sistem teknologi informasi harus bekerja selama 24/7 tanpa henti dengan kinerja atau performa yang telah ditentukan oleh bisnis atau organisasi penggunanya. Untuk memastikan bahwa selama waktu tersebut seluruh perangkat hardware bekerja dengan baik, segenap aplikasi berjalan sebagaimana mestinya, semua infrastruktur beroperasi secara prima, dan beragam database terjaga integritasnya, diperlukan manajemen atau pengelolaan operasional yang andal.

Ada tujuh aktivitas inti yang harus dikerjakan secara sungguh-sungguh, yaitu:

- Menyusun prosedur operasional yang harus dipatuhi oleh seluruh penyelenggara sistem, terutama terkait dengan mekanisme dan langkah-langkah teknis rutin yang harus dilakukan pada saat-saat yang telah ditentukan.
- Menjadwalkan program yang harus berjalan secara otomatis terkait dengan operasional dan pemeliharaan perangkat, demi menjaga integritas sistem dari masa ke masa.

- Memantau situasi dan kondisi sistem secara terus menerus, rutin, dan periodik serta menangani berbagai permasalahan kinerja operasional yang terjadi.
- Mengelola dan menjaga keamanan berbagai entitas keluaran atau output seperti laporan, media penyimpan, statistik, dan lain sebagainya.
- Mengimplementasikan perubahan-perubahan yang terkait dengan operasional sistem dalam bentuk penyesuaian parameter dan konfigurasi program maupun perangkat teknologi yang dipergunakan.
- Menjalankan prosedur keamanan data, informasi, dan sistem yang dipergunakan agar sumber daya operasional terhindar dari mereka yang tidak berwenang untuk mengaksesnya.
- Mengembangkan prosedur pemeliharaan sistem dan operasional otomatis dan dapat mencegah terjadinya hal-hal yang tidak diinginkan dalam keseharian.

INAKA

Paling tidak ada lima buah entitas pengendali yang harus dikembangkan oleh organisasi, yaitu masing-masing adalah:

- Prosedur Operasional dan Instruksi Kerja - merupakan dokumen yang harus diikuti dan ditaati oleh para penyelenggara operasional sistem dan teknologi informasi.
- Daftar Penjadwalan Pekerjaan - merupakan jadwal operasional sejumlah program aplikasi (job processing) maupun pemeliharaan sumber daya terkait

dengannya yang harus dijalankan secara otomatis maupun manual.

Perangkat Pemantau Operasional - merupakan teknologi atau tool yang dipergunakan untuk memantau seluruh komponen penting dalam operasional sistem dan teknologi untuk memastikan berjalannya perangkat sesuai dengan fungsinya.

- Daftar Dokumen dan Entitas Penting - merupakan entitas keluaran (output) dari aktivitas operasional yang harus dijaga kondisi dan kerahasiaannya.
- Panduan Pemeliharaan Perangkat Teknologi - merupakan kompulan prosedur untuk menjamin terjaganya kondisi seluruh perangkat teknologi sebagaimana mestinya.

Secara mudah dapat dikembangkan berbagai indikator untuk memastikan agar proses ini berjalan dengan baik, seperti: (i) dampak insiden yang terjadi karena masalah operasional; (ii) durasi rata-rata sistem tidak bekerja karena adanya insiden atau masalah operasional; (iii) periode pemeliharaan rutin perangkat-perangkat penting; dan lain sebagainya.

Pada dasarnya, diupayakan agar kegiatan operasional sistem dapat berjalan secara otomatis - dimana secara simultan diawasi dan dipantau oleh manusia dengan menggunakan sejumlah tool atau perangkat pembantu. Dengan diberlakukannya standar pengelolaan dan pemeliharaan yang konsisten, maka niscaya tingkat layanan yang diinginkan dari operasional sistem dapat senantiasa terjaga dengan baik.