IKI – 83408T
Proteksi dan Teknik Keamanan Sistem Informasi

Operations Security dan Penerapannya di Usaha Kecil Menengah (UKM)

Kelompok 6:
Pranarendra Wibowo (7204000322)
Timor Setiyaningsih (7204000381)

Magister Teknologi Informasi
Fakultas Ilmu Komputer
Universitas Indonesia
Jakarta
2005

Daftar Isi

Operations Security
dan
Penerapannya di Usaha Kecil Menengah (UKM)

1. Pendahuluan

Pada domain Keamanan Operasi (Operations Security) akan dibahas mengenai kontrol-kontrol apa saja yang diperlukan pada lingkungan operasi yang berhubungan dengan komputasi. Hal-hal tersebut harus mencakup tiga pilar dari keamanan informasi yaitu Kerahasiaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability). Pada tiap-tiap pembahasan akan disertai pula dengan ilustrasi tentang bagaimana Penerapannya di UKM.

1.1 Tujuan

Pendekatan yang akan dilakukan meliputi:
1. Kontrol dan Proteksi (Controls and Protections)
2. Pengawasan dan Pengauditan (Monitoring and Auditing)
3. Ancaman dan Kerawanan (Threats and Vulnerabilities)

1.2 Definisi Domain

Keamanan Operasi bermakna suatu tindakan untuk mengerti hal-hal yang menjadi ancaman dan hal-hal yang menjadi kerawanan dari operasi-operasi komputer yang bertujuan untuk secara rutin mendukung aktivitas operasional dari suatu sistem komputer agar dapat berfungsi dengan benar.

1.2.1 Tiga Hal Utama

Seperti domain keamanan lain, Keamanan Operasi juga memperhatikan tiga hal utama yaitu:
1. Ancaman (Threat)
   Ancaman dalam domain Keamanan Operasi dapat didefinisikan sebagai adanya kejadian potensial yang dapat menyebabkan kerusakan dengan cara melanggar keamanan.
2. Kerawanan (Vulnerability)
   Kerawanan dalam domain ini dapat didefinisikan sebagai titik lemah dalam sebuah sistem yang dapat mengakibatkan terjadinya pelanggaran keamanan.
3. Aset (Asset)
   Aset adalah apa saja yang diyakini sebagai sumberdaya komputasi atau kemampuan, seperti perangkat keras, perangkat lunak, data, dan juga sumberdaya manusia (personel).

1.2.2 C.I.A.

Beberapa hal ini adalah beberapa dampak dari kontrol operasi pada C.I.A.:
1. Konfidensialitas (Confidentiality)
   Kontrol Operasi memberi dampak pada sensitivitas dan kerahasiaan dari informasi.

2. Integritas (Integrity)
   Bagaimana kontrol operasi diterapkan akan secara langsung berdampak pada akurasi data dan keotentikan.
3. Ketersediaan (Availability)
   Kontrol ini memberi dampak pada tingkat penanggulangan kesalahan (fault tolerance) organisasi dan kemampuannya untuk kembali dari kegagalan tersebut.

2. Kontrol dan Proteksi (Controls and Protections)

Domain Keamanan Operasi memperhatikan kontrol-kontrol yang akan digunakan untuk melindungi perangkat keras, perangkat lunak, dan sumberdaya media lainnya dari hal-hal sebagai berikut:
- Ancaman di sebuah lingkungan operasi
- Pihak pelanggar internal ataupun eksternal
- Operator yang tidak secara benar mengakses sumberdaya

Selain itu juga akan dibahas mengenai aspek kritikal dari kontrol operasi yaitu:
1. Pengamanan sumberdaya, meliputi kontrol perangkat keras
2. Kontrol entitas-kewenangan (privileged-entity)

2.1 Kontrol berdasarkan Kategori (Categories of Controls)

Berikut ini beberapa kategori kontrol yang utama:
1. Kontrol Pencegahan (Preventative Controls)
   Kontrol Pencegahan adalah kontrol yang dirancang untuk mencapai dua hal yakni untuk merendahkan jumlah dan akibat dari kesalahan yang tidak disengaja yang memasuki sistem dan untuk mencegah penerobos yang tidak berhak dari mengakses sistem melalui internal atau ekternal. Contoh dari tipe kontrol seperti ini antara lain adalah pemberian nomor urutan pada form-form baik form tersebut bersifat hardcopy ataupun softcopy atau validasi data dan prosedur pemeriksaan untuk mencegah duplikasi.

   Penerapannya di UKM:
   Seperti dijelaskan di atas bahwa untuk melakukan kontrol ini pada form-form yang digunakan untuk menyimpan data penting bagi organisasi sebaiknya diberikan urutan nomor agar memudahkan dalam mengelolanya, dan juga nantinya apabila dilakukan audit atau pemeriksaan dapat terdata dengan baik dan mudah.
2. Kontrol Penyidikan (Detective Controls)
   Kontrol Penyidikan digunakan untuk mendeteksi sebuah kesalahan tepat pada saat terjadi. Tidak seperti kontrol pencegahan, kontrol ini berjalan setelah kejadian dan dapat digunakan untuk melacak transaksi yang tidak berhak dan selanjutnya dituntut, atau dapat juga dijadikan sumber informasi untuk mengurangi akibat dari kesalahan pada sistem dengan mengidentifikasikannya secara cepat sebelum terjadinya kesalahan serupa. Contoh dari tipe kontrol seperti ini antara lain adalah jejak audit (audit trails).

   Penerapannya di UKM:
   Seperti dijelaskan di atas antara lain dengan melakukan jejak audit terhadap penggunaan sistem oleh user melalui pemeriksaan terhadap log/catatan sistem atau

aplikasi. Dalam hal ini log sistem terpasang langsung di dalam sistem yang diakses oleh user sehari-hari. Sedangkan log aplikasi terpasang pada masing-masing aplikasi yang ada pada sistem, pada umumnya belum tentu seluruh aplikasi memiliki kemampuan untuk mendata kegiatan apa saja yang dilakukan oleh user melalui aplikasi tersebut, oleh karena itu ada baiknya memilih aplikasi secara selektif atau apabila sudah terlambat memiliki aplikasi yang tidak memiliki fasilitas untuk log maka sebaiknya dibangun perangkat lunak tambahan yang dapat melakukan log berbarengan dengan penggunaan aplikasi tersebut, namun apabila hal tersebut tidak dimungkinkan maka sebaiknya diterapkan prosedur/mekanisme di tingkat organisasi untuk melakukan kontrol secara manual atas penggunaan aplikasi tersebut.

3. Kontrol Koreksi/Pengembalian Ulang (Corrective/Recovery Controls)
   Kontrol Koreksi diterapkan untuk membantu mitigasi dampak dari kejadian kehilangan melalui prosedur recovery. Kontrol ini dapat digunakan untuk mengatur langkah-langkah yang harus diambil agar suatu sistem dapat kembali ke kondisi seperti semula (recover) setelah kerusakan, contohnya antara lain yakni langkah-langkah untuk mengembalikan kembali data yang secara tidak disengaja terhapus dari floppy disk.

   Penerapannya di UKM:
   Untuk menerapkan kontrol ini maka dapat dilakukan dengan pelaksanaan back-up terhadap semua kegiatan yang berhubungan dengan data sensitif/berharga bagi organisasi, sehingga apabila terjadi kehilangan data maka dapat dengan mudah diatasi. Untuk UKM dapat diterapkan dengan membuat salinan (copy) pada dua floppy disk untuk setiap aksi penyalinan. Namun apabila sudah terlambat mengalami kehilangan maka dapat saja menggunakan beberapa perangkat lunak alat bantu recovery data yang cukup banyak ada. Sedangkan untuk tingkat sistem maka sebaiknya tiap-tiap komputer yang memiliki data berharga atau berfungsi penting bagi kelangsungan berjalannya kegiatan organisasi dilakukan mirror disisi data dan penyediaan perangkat keras cadangan (back-up) untuk berjaga-jaga terhadap timbulnya masalah pada perangkat utama.

Sedangkan beberapa hal berikut ini adalah kategori kontrol tambahan:

1. Kontrol Pembatas/Pengarah (Deterrent/Directive Controls)
   Kontrol Pembatas digunakan untuk mendorong suatu kepatuhan (compliance) dengan kontrol ekternal, seperti regulatory compliance. Kontrol ini ditujukan untuk melengkapi kontrol lain, seperti kontrol pencegahan dan penyidikan. Kontrol ini dikenal juga sebagai kontrol pengarah.

   Penerapannya di UKM:
   Pada umumnya untuk menerapkan kontrol ini UKM belum memiliki suatu langkah-langkah tertentu, karena biasanya hanya mengikuti apa yang ditetapkan oleh pemerintah antara lain undang-undang yang berlaku. Sebagai contoh seperti setiap usaha warnet yang ingin mendirikan usahanya diharuskan mengikuti aturan pemerintah tertentu tentang telekomunikasi dan teknologi informasi. Apabila tidak mengikuti peraturan tersebut maka dikemudian hari dikhawatirkan akan terjadi pelanggaran oleh UKM-UKM lain yang tentu saja tidak diingini oleh banyak pihak tidak hanya pemerintah saja. Contoh lainnya antara lain apakah suatu UKM ingin mengadakan usaha yang berhubungan dengan luar negeri, maka harus dapat

mengerti peraturan yang berlaku di negeri tersebut. Dimaksudkan agar tidak merugikan kedua belah pihak.

2. Kontrol Aplikasi (Application Controls)
   Kontrol Aplikasi adalah kontrol yang dirancang ke dalam aplikasi perangkat lunak untuk mengurangi dan mendeteksi ketidakbiasaan/keanehan operasi perangkat lunak. Sebagai tambahan, kontrol-kontrol selanjutnya adalah juga merupakan bagian dari beragam tipe kontrol aplikasi.

   Penerapannya di UKM:
   Untuk kontrol ini biasanya pada UKM karena perangkat lunak/aplikasi yang dipergunakan adalah membeli, jarang yang dikembangkan sendiri, maka sebaiknya pada saat seleksi aplikasi mana yang digunakan memperhatikan fitur yang dapat memberikan kontrol bagi sistem atas setiap aplikasi yang ada di dalam sistem tersebut. Antara lain sistem dapat memberikan peringatan (alert) pada pengguna akan anomali atau keanehan jalannya suatu aplikasi (pada umumnya sistem operasi telah memiliki fitur peringatan ini, misalnya peringatan apabila suatu aplikasi crash dan pencatatan kejadian tersebut ke dalam log sistem). Untuk selanjutnya dapat dilakukan langkah perbaikan ataupun pencegahan agar tidak terulang kembali. Atau apabila tidak memungkinkan maka kontrol aplikasi dilakukan secara manual melalui prosedur organisasi yang mengharuskan pencatatan penggunaan aplikasi dan keanehan yang timbul.
3. Kontrol Transaksi (Transaction Controls)
   Kontrol Transaksi digunakan untuk menyediakan kontrol pada berbagai tahapan peristiwa transaksi – dimulai dari inisiasi sampai output melalui kontrol pengujian dan perubahan.
   Ada beberapa tipe Kontrol Transaksi:
   a. Kontrol Input (Input Controls)
      Kontrol Input digunakan untuk memastikan bahwa transaksi-transaksi yang dilakukan, secara benar masuk ke dalam sistem satu kali saja. Unsur dari kontrol ini meliputi penghitungan data dan pemberian tanda waktu/tanggal data tersebut dimasukkan atau diubah.

      Penerapannya di UKM:
      Sebagaimana telah dijelaskan pada kontrol aplikasi dimana UKM pada umumnya membeli perangkat luak yang digunakannya maka kontrol yang dilakukan lebih berat pada saat seleksi perangkat lunak yang akan digunakan. Sebagai contoh suatu perangkat lunak akuntasi, apakah perangkat lunak tersebut memiliki fitur yang dapat mengakomodasi kontrol input, seperti di atas. Sedangkan di sisi manusianya sebaiknya juga dilakukan kontrol seperti pengecekan oleh minimal dua orang untuk setiap input yang kiranya kritis bagi organisasi. Selanjutnya, di sisi manusianya juga, yang tidak kalah penting adalah pelaksanaan pelatihan dan pengenalan akan setiap perangkat lunak yang akan digunakan oleh anggota organisasi. Seluruh hal tersebut dapat juga diartikan dengan kata lain organisasi memiliki prosedur kontrol yang tersusun dan tersampaikan dengan baik ke anggota organisasi.
   b. Kontrol Pemroresan (Processing Controls)
      Kontrol Pemroresan digunakan untuk menjamin bahwa transaksi-transaksi yang dilakukan adalah valid dan akurat serta masukan-masukan yang salah diproses ulang secara benar dan diketahui.

Penerapannya di UKM:
Seperti yang telah dijelaskan pada kontrol input, sebagian besar kontrol yang dilakukan adalah sama antara lain garis besarnya yaitu seleksi perangkat lunak yang memenuhi kriteria kontrol proses, pengecekan minimal dua kali atau oleh dua orang, dan pelatihan akan perangkat lunak tersebut. Apabila ada kesalahan maka memiliki prosedur propagasi perbaikan ke tingkat lebih tinggi atau minimal didokumentasikan agar dapat menjadi bahan pertimbangan di waktu akan datang.

c. Kontrol Output (Output Controls)
Kontrol Output digunakan untuk dua hal yakni untuk melindungi konfidensialitas dari output dan untuk memverifikasi integritas dari output dengan cara membandingkan transaksi input dan data output. Unsur dari kontrol output yang benar adalah dengan meliputi penjaminan bahwa output telah mencapai user yang semestinya, membatasi akses ke output cetak pada suatu area penyimpanan, heading dan trailing banners dari suatu cetakan, dan mencetak banner “tidak ada output” ketika laporan yang ingin dicetak memang kosong.

Penerapannya di UKM:
Seperti telah dijelaskan pada kontrol output di atas, untuk penerapannya di UKM kurang lebih sama, lebih kepada prosedur di organisasi tersebut bagaimana menangani kontrol output. Seperti pengecekan oleh minimal dua kali atau oleh dua orang untuk menghindari kesalahan analisa.

d. Kontrol Perubahan (Change Controls)
Kontrol Perubahan diimplementasikan untuk melindungi integritas data dalam sebuah sistem pada saat perubahan dilakukan terhadap konfigurasi. Prosedur dan standar akan diterapkan untuk mengelola perubahan tersebut dan modifikasi pada sistem dan konfigurasinya.

Penerapannya di UKM:
Untuk kontrol ini maka dapat dilakukan dengan membuat suatu skenario baik di sisi sistem ataupun prosedur yang mengakomodasi kondisi sebelum, saat perubahan, dan sesudah perubahan. Di sisi sistem dapat dilakukan minimal dengan adanya pemberian kode-kode versi dari sesuatu yang diubah tersebut. Selanjutnya dinformasikan kepada seluruh anggota organisasi yang berkepentingan.

e. Kontrol Uji (Test Controls)
Kontrol Uji dilaksanakan pada saat pengujuan sebuah sistem untuk menghindari pelanggaran konfidensialitas dan untuk menjamin integritas transaksi. Sebagai contoh dari tipe kontrol yang seperti ini adalah penggunaan secara tepat dari data uji yang telah disaring. Kontrol uji seringkali merupakan bagian dari proses kontrol perubahan.

Penerapannya di UKM:
Sebagaimana pada kontrol perubahan, namun pada kontrol ini dibedakan dengan penciptaan suatu lingkungan (environment) khusus yang diperuntukkan untuk dilaksanakannya pengujian, tidak terhubung atau mengganggu ke sistem yang sedang berjalan. Pada UKM karena perangkat lunak/aplikasi yang digunakan tidak begitu banyak maka kontrol pengujian ini biasanya berlangsung sederhana dan singkat.

2.2 Kontrol berdasarkan Orange Book (Orange Book Controls)

Trusted Computer Security Evaluation Criteria (TCSEC, Orange Book) mendefinisikan beberapa tingkat dari jaminan kebutuhan akan operasi komputer yang aman. Orange Book mendefinisikan dua tipe jaminan, yakni:

1. Operational Assurance:
   Menitikberatkan pada fitur-fitur dan arsitektur dasar dari sebuah sistem, meliputi:
   a. System Architecture
   b. System Integrity
   c. Covert Channel Analysis
   d. Trusted Facility Management
   e. Trusted Recovery
2. Life Cycle Assurance
   Menitikberatkan pada kontrol-kontrol dan standar-standar yang dibutuhkan pada saat membangun dan mengelola sistem, meliputi:
   a. Security Testing
   b. Design Specification and Testing
   c. Configuration Management
   d. Trusted Distribution

Pada domain Kontrol Operasi, Operational Assurance meliputi Covert Channel Analysis, Trusted Facility Management, dan Trusted Recovery. Sedangkan Life Cycle Assurance meliputi Configuration Management.

2.2.1 Covert Channel Analysis

Covert channel adalah jalur informasi yang tidak normal digunakan untuk berkomunikasi dengan sistem; sehingga, jalur tersebut tidak dilindungi oleh mekanisme keamanan normal sistem. Covert channel adalah cara rahasia untuk mengalihkan informasi ke orang atau program lain.

Ada dua tipe Covert channel:

1. Covert storage channels
   Covert storage channels mengalihkan informasi dengan cara mengubah data tersimpan sistem. Contohnya, sebuah program dapat mengalihkan informasi ke program yang kurang-aman dengan cara mengubah jumlah atau pola free space dari sebuah hard disk.

   Penerapannya di UKM:
   Untuk mengatasi covert storage channels maka diperlukan suatu sistem operasi yang dapat mengamankan atau tidak memungkinkan pengubahan pola free space dari sebuah hard disk secara tidak sah. Atau minimal memiliki mekanisme untuk melakukan pencatatan dan pelaporan apabila terjadi covert storage channels. Untuk itu kontrol yang dapat dilakukan pada UKM adalah menseleksi fitur-fitur dari sistem operasi yang dapat melakukan hal tersebut.
2. Covert timing channels
   Covert timing channels mengalihkan informasi dengan cara menghilangkan performa dari atau memodifikasi pewaktuan (timing) dari sumberdaya sistem dengan cara tertentu. Timing channels seringkali berhasil dengan mengambil

keuntungan dari suatu clock sistem atau alat timing pada sistem. Informasi dialihkan dengan menggunakan unsur seperti waktu terpakai (elapsed time) yang diperlukan untuk menjalankan suatu operasi, jumlah CPU time yang dihabiskan, atau waktu berjalannya antara dua kejadian.

Penerapannya di UKM:
Dalam hal ini serupa dengan apa yang dapat dilakukan untuk mengatasi covert storage channels. Diiringi, nantinya pada saat sistem beroperasi, dengan memperhatikan catatan log sistem yang dihasilkan secara otomatis oleh sistem operasi untuk melihat terjadinya pelanggaran. Dan juga bagaimana prosedur di sisi organisasi untuk menanganinya.

Penghasilan noise dan traffic adalah cara yang efektif untuk menangani penyerangan dengan tipe covert channel.

Penerapannya di UKM:
Pada umumnya sistem-sistem operasi saat ini telah memiliki fasilitas pengawasan sumberdaya sistemnya. Seperti pada sistem operasi Windows memiliki Task Manager, yang menampilkan status dan statistik pemakaian sumberdaya pada saat sistem berjalan. Pada sistem operasi berbasis UNIX bahkan dapat dengan mudah dipasang perangkat lunak yang dapat melakukan penampilan statistik pemakaian sumberdaya (utilisasi CPU, utilisasi RAM, utilisasi hard disk, utilisasi jaringan, dan sebagainya) secara grafik contohnya MRTG (Multi Router Traffic Grapher) yang dapat dimonitor secara jarak jauh melalui jaringan komputer. Selain dihasilkan penampilan pemakaian sumberdaya, selanjutnya dapat pula dibangun suatu program yang dapat menganalisa covert channel dan melakukan pengambilan langkah pencegahan secara otomatis agar penyerangan tidak terus-menerus berlangsung. Namun dalam hal ini untuk UKM minimal kontrol yang dapat dilakukan adalah dengan memperhatikan pemakaian sumberdaya secara seksama, untuk kemudian dianalisa dan disusun prosedur-prosedur pencegahan dari masalah-masalah yang mungkin timbul.

2.2.2 Trusted Facility Management

Trusted Facility Management didefinisikan sebagai penugasan individu spesifik untuk melakukan administrasi fungsi-fungsi yang berhubungan dengan keamanan pada sebuah sistem. Walaupun trusted facility management adalah hanya merupakan kebutuhan jaminan untuk sistem yang sangat aman (B2, B3, dan A1), banyak sistem yang melakukan evaluasi di tingkat keamanan yang lebih rendah sesuai struktur yang diperlukan oelh kebutuhan ini.
Trusted Facility Management erat hubungannya dengan konsep kewenangan terbatas (least privilege), dan juga dengan konsep administrasi pemisahan tugas (separation of duties) dan apa yang perlu diketahui (need to know).
Adapun penjelasannya sebagai berikut:

1. Pemisahan Tugas (Separation of Duties)
   Pemisahan Tugas dilaksanakan dengan cara menugaskan bagian-bagian dari suatu pekerjaan ke beberapa personel. Sehingga jika tidak ada satu orang yang memiliki kontrol total akan mekanisme keamanan suatu sistem, maka secara teori tidak akan ada satu orang yang juga dapat menggagalkan sistem. Konsep ini berhubungan dengan prinsip dari sedikit kewenangan (least privilege). Pada

konteks ini, sedikit kewenangan bermakna bahwa pengguna sistem sebaiknya memiliki tingkat hak dan kewenangan yang terendah dibutuhan untuk melakukan pekerjaan mereka dan juga hanya membolehkannya untuk jangka waktu yang singkat.
Pada sistem yang umum ditemui, seorang administrator sistem biasanya memiliki kuasa total dari administrasi sistem dan fungsi-fungsi keamanan. Konsolidasi dari kekuatan seperti ini tidak diperbolehkan pada sistem yang aman karena tugas dan fungsi keamanan sebaiknya tidak secara otomatis diberikan ke peran administrator sistem. Pada sistem yang sangat aman, diperlukan tiga peran administratif yang berbeda, antara lain seorang administrator sistem, seorang administrator keamanan yang biasanya adalah seorang Information System Security Office (ISSO), dan seorang operator dengan fungsi lebih.
Administrator keamanan, administrator sistem, dan operator dapat juga bukan merupakan orang yang berbeda, pada umumnya sering seperti itu. Namun, ketika administrator sistem memegang peran sebagai administrator keamanan, peran tersebut harus dikontrol dan diaudit. Karena tugas administrator keamanan adalah untuk melakukan fungsi-fungsi keamanan, performa dari kegiatan-kegiatan yang tidak berhubungan dengan keamanan harus dibatas dengan ketat. Pemisahan tugas seperti ini dapat mengurangi kemungkinan kehilangan yang dihasilkan dari penyalahgunaan otoritas pengguna-pengguna dengan cara mengambil tindakan di luar dari yang diberikan menurut tanggungjawab fungsional mereka. Walaupun hal ini sepertinya menyulitkan bagi seseorang untuk berpindah-pindah dari satu peran ke peran lain, peran-peran tersebut adalah berbeda secara fungsional dan harus dilakukan seperti itu.
Pada konsep kontrol dua orang, dua operator memeriksa dan mensahkan pekerjaan satu sama lain. Fungsi dari kontrol dua orang adalah untuk menghasilkan akuntabilitas dan untuk meminimalisasi fraud pada transaksi yang sangat sensitif dan beresiko tinggi. Konsep dari kontrol dua orang bermakna bahwa kedua orang diperlukan untuk menyelesaikan suatu kegiatan sensitif.

Berikut ini fungsi umum dari administrator dan operator dengan fungsi lebih, meliputi:
- Melakukan instalasi perangkat lunak
- Menyalakan (start/boot) dan mematikan (shutdown) sistem
- Menambahkan dan mengurangi user
- Melakukan back-up dan recovery
- Menangani printer dan mengelola antrian pencetakan

Berikut ini fungsi umum dari administrator keamanan, meliputi:
- Menetapkan user clearances, password awal, dan karakteristik keamanan lain untuk user baru
- Mengubah profil keamanan untuk user yang sudah ada
- Menetapkan atau mengubah label dari file yang sensitif
- Menetapkan karakteristik keamanan dari peralatan dan jalur komunikasi
- Melakukan pemeriksaan audit data

Sedangkan operator dapat melakukan beberapa peran dari administrator sistem, seperti back-up. Hal ini dapat terjadi pada fasilitas organisasi dimana sumberdaya manusia/personel terbatas.

Adalah bukan hanya di organisasi kecil saja yang membutuhkan administrator sistem untuk berperan sebagai administrator keamanan. Peran administrator Jaringan Lokal (LAN)/Jaringan Internet menimbulkan resiko keamanan dikarenakan kurangnya pemisahan dari tugas-tugas personel. Dengan alasan untuk mengurangi ekonomi internet, seorang administrator jaringan harus menggunakan banyak topi – dan melaksanakan pekerjaan yang berhubungan dengan keamanan adalah pasti salah satunya (disertai dengan berbagai fungsi operator lainnya). Hal yang kadangkala menyusahkan namun merupakan konsep yang sangat penting yakni pemisahan tugas adalah vital untuk kontrol operasi.

Penerapannya di UKM:
Pada UKM penerapan pemisahan tugas antara lain adalah seperti yang dijelaskan sebelumnya yakni dilakukan pemisahan peran-peran administrator dan operator yang ada di dalam sistem, walaupun terdapat perangkapan peran pada orang yang sama karena sumberdaya manusia yang terbatas di UKM. Hal yang dijelaskan tersebut adalah pengelolaan secara organisasi, sedangkan untuk mengakomodasinya ke dalam sistem maka diperlukan suatu sistem yang dapat melakukan hal-hal seperti pengelompokkan user, penetapan hak dan wewenangnya, pencatatan pemakaian akun tersebut. Sebagai contohnya pada sistem operasi Windows khususnya versi server terdapat fasilitas Active Directory (http://www.microsoft.com/WindowsServer2003/techinfo/overview/adsmallbiz.mspx) yang secara garis besar memungkinkan pengaturan group policy, mengurangi down time, enkripsi, dan kerjasama dengan aplikasi lain. Sedangkan untuk sistem operasi berbasis UNIX telah cukup dikenal Lightweight Directory Access Protocol (LDAP) dipelopori oleh OpenLDAP (http://www.openldap.org/doc/admin23/) yang bila digabungkan dengan Samba (http://us2.samba.org/samba/docs/using_samba/toc.html), OpenAFS (http://www.openafs.org/doc/index.htm), dan Kerberos (http://web.mit.edu/kerberos/www/krb5-1.4/#documentation) akan menghasilkan sistem yang serupa dengan Active Directory pada Windows dengan keuntungan bukan perangkat lunak propietary.

2. Perotasian Tugas (Rotation of Duties)
   Variasi lain dari pemisahan tugas adalah disebut dengan perotasian tugas. Didefinisikan sebagai proses pembatasan jumlah waktu yang diberikan pada seorang operator dalam melaksanakan suatu tugas berhubungan dengan kemananan sebelum selanjutnya dipindahkan ke tugas lain dengan klasifikasi keamanan yang berbeda pula. Kontrol ini mengurangi kesempatan berbuat kolusi diantara operator-operator pada fungsi-fungsi yang memungkinkan.

   Penerapannya di UKM:
   Perotasian tugas dapat dilakukan pada anggota organisasi yang berada ditingkat operator atau dapat juga administrator sistem secara berkala atau saat pergantian jabatan. Dalam hal ini hanya diperlukan penyusunan prosedur di sisi organisasi. Sedangkan di sisi sistem hanya mengatasi masalah penetapan hak dan wewenang anggota organisasi tersebut di dalam sistem.

2.2.3 Trusted Recovery

Trusted Recovery menjamin bahwa keamanan tidak diterobos ketika sistem mengalami kerusakan (crash) atau kegagalan sistem lain (seringkali disebut dengan

"discontinuity"). Menjamin bahwa sistem di start/boot ulang tanpa meninggalkan prosedur pengamanan yang diperlukan dan dapat recover dan roll back tanpa terpengaruh adanya kegagalan. Contohnya, jika sistem crash saat data sensitif sedang dituliskan ke disk (di mana normalnya terlindungi oleh suatu kontrol), data mungkin tertinggal tidak terlindungi di memori dan mungkin dapat diakses oleh personel yang tidak berhak.

Trusted Recovery memiliki dua kegiatan utama:

1. Persiapan Kegagalan (Failure Preparation)
   Persiapan Kegagalan yang dilakukan menghadapi suatu kegagalan sistem meliputi melakukan back-up semua file yang kritikal secara teratur. Persiapan ini harus mencakup data recovery dalam cara yang terlindungi disamping juga menjamin keberlangsungan keamanan pada sistem. Prosedur-prosedur ini juga diperlukan apabila terjadi masalah dalam sistem seperti hilangnya sumberdaya, basisdata yang tidak konsisten, atau pelanggaran apa pun, yang terdeteksi, atau jika sistem memerlukan untuk dimatikan atau start/boot ulang.

   Penerapannya di UKM:
   Secara umum dapat diterapkan dengan melakukan back-up file yang kritis menggunakan jadwal otomatis, pada sistem berbasis Windows dapat digunakan Scheduled Tasks, pada sistem berbasis UNIX dapat digunakan cron, ke tempat yang kiranya aman dari kegagalan Untuk basisdata biasanya sudah disediakan fasilitas back-up di dalam sistem basisdata tersebut. Selain itu juga dalam aplikasi perangkat lunak yang mengakses ke basisdata dibuat suatu mekanisme kontrol transaksi meliputi pembukaan dan penutupan transaksi, sehingga data selalu konsisten. Kemudian untuk menjamin keberlangsungan sistem maka dapat dilakukan mirroring pada hard disk yang sensitif dan berharga bagi organisasi.
2. Pengembalian Sistem (System Recovery)
   Jika prosedur-prosedur yang spesifik dari Trust Recovery bergantung secara langsung pada kebutuhan sistem, maka secara umum, prosedur Pengembalian Sistem meliputi hal-hal berikut:
   a. Boot ulang sistem ke mode single user (satu user) – sistem operasi dijalankan tanpa aktivasi sisi pengamanan muka – sehingga tidak ada user lain yang dapat mengakses sistem pada saat itu.
   b. Recover semua sistem file yang aktif pada saat terjadinya kegagalan sisten
   c. Restore semua file dan basisdata yang hilang atau rusak dari simpanan back-up yang terbaru.
   d. Recover semua karakteristik keamanan yang diperlukan, seperti label-label keamanan file.
   e. Memeriksa semua file yang kritikal akan keamanan, seperti file password.

   Setelah semua langkah tersebut dilakukan dan data sistem tidak dapat disalahgunakan, operator dapat kembali mengakses sistem.

   Penerapannya di UKM:
   Untuk langkah-langkah pengembalian sistem secara umum untuk UKM sama dengan apa yang dijelaskan di atas. Namun juga disertai dengan penyusunan prosedur-prosedur yang kemudian diinformasikan ke anggota-anggota organisasi yang berkepentingan.

Sebagai tambahan, Common Criteria juga mendeskripsikan tiga tipe recovery hirarkis yaitu:

1. Manual Recovery
   Campur tangan administrator sistem diperlukan untuk mengembalikan sistem ke kondisi keamanan setelah sistem crash.
2. Automated Recovery
   Recovery ke kondisi keamanan secara otomatis (tanpa campur tangan administrator sistem) ketika menangani satu kegagalan; namun, penanganan secara manual diperlukan untuk menangani beberapa kegagalan lainnya.
3. Automated Recovery without Undue Loss
   Memiliki kemiripan dengan Automated Recovery, tipe recovery ini dikenal sebagai recovery tingkat tinggi karena mendefinisikan pencegahan terhadap undue loss dari obyek-obyek yang dilindungi.

Penerapannya di UKM:
Pada UKM umumnya minimal dilakukan tipe pertama Manual Recovery, namun juga memungkinkan untuk dilakukan tipe selanjutnya. Sebagai contoh, pada sistem berbasis Windows dapat dibuat suatu batch (.bat) file, pada sistem berbasis UNIX dapat digunakan shell skrip (.sh), yang dapat secara otomatis melakukan recovery semua data back-up setelah terjadi suatu kegagalan.Selain itu juga harus ditentukan pihak-pihak yang bertanggungjawab menangani sistem pada saat recovery.

2.2.4 Configuration/Change Management Control

Manajemen konfigurasi adalah proses pelacakan dan penyetujuan perubahan pada sebuah sistem. Meliputi pengidentifikasian, pengontrolan, dan pengauditan semua perubahan yang dilakukan terhadap sistem tersebut. Hal-hal yang terjadi dapat mencakup perubahan perangkat keras dan perangkat lunak, perubahan jaringan, atau perubahan lain yang memberi dampak pada keamanan. Manajemen konfigurasi juga dapat digunakan untuk melindungin sistem terpercaya pada saat dalam perancangan dan pengembangan.

Berikut ini adalah fungsi-fungsi utama kontrol konfigurasi atau perubahan:

- Untuk menjamin bahwa perubahan diterapkan dengan urutan cara yang benar dan telah melalui tahap pengujian formal
- Untuk menjamin bahwa pengguna dasar diinformasikan akan perubahan yang tertunda
- Untuk menganalisa akan dampak dari perubahan pada sistem setelah dilakukan implementasi
- Untuk mengurangi dampak negatif yang mungkin ditemukan pada suatu perubahan terutama pada layanan dan sumberdaya komputasi.

Lima prosedur umum yang ada dan dapat diterima untuk menerapkan dan mendukung proses kontrol perubahan:

1. Melakukan pengenalan perubahan
2. Mengkatalogkan perubahan yang ingin dilakukan
3. Menjadwalkan perubahan
4. Menerapkan perubahan
5. Melaporkan perubahan tersebut ke pihak yang berkepentingan

Penerapannya di UKM:
Kelima prosedur tersebut dapat langsung diterapkan pada suatuh UKM sebagai langkah-langkah mengontrol perubahan. Hanya saja mungkin dalam implementasinya ada yang dilakukan secara menyeluruh.

2.3 Kontrol di tingkat Administratif (Administrative Controls)

Kontrol di tingkat Administratif ini dapat didefinisikan sebagai kontrol yang dicanangkan dan dipelihara oleh pihak manajemen administratif untuk mengurangi ancaman atau dampak dari pelanggaran keamanan komputer. Kontrol ini terpisahkan dari kontrol operasi karena memiliki hubungan lebih banyak dengan administrasi personel sumberdaya manusia dan kebijakan (policy) dibandingkan dengan kontrol perangkat keras atau perangkat lunak.

Beberapa hal berikut adalah contoh dari kontrol administratif:

1. Keamanan Personel (Personnel Security)
   Kontrol ini adalah kontrol sumberdaya manusia administratif yang digunakan untuk mendukung jaminan dari tingkat kualitas dari personel yang melakukan operasi-operasi komputer. Unsur-unsur dari kontrol ini meliputi:
   a. Penyeleksian penerimaan pegawai atau pemeriksaan latar belakang
      Penyeleksian pra-penerimaan untuk posisi-posisi yang sensitif layaknya dilakukan. Sedangkan untuk posisi yang kurang sensitif, pemeriksaan latar belakang pasca-penerimaan kiranya lebih layak dilakukan.
   b. Libur yang wajib diambil dalam periode waktu satu minggu
      Praktek ini adalah umum digunakan di institusi keuangan atau organisasi lain dimana operator memiliki akses ke transaksi finansial yang sensitif. Selama operator tersebut mengambil libur, dilakukan audit pada akun, proses, dan prosedur operator untuk mengungkapkan apabila ada bukti pelanggaran.
   c. Peringatan kerja atau pemberhentian
      Langkah ini diambil apabila pegawai melanggar standar kebiasaan komputer yang telah ditetapkan.

   Penerapannya di UKM:
   Hal-hal tersebut dapat langsung diterapkan untuk suatu UKM, namun pada umumnya yang pasti dilakukan adalah unsur pertama dan ketiga. Mengingat keterbatasan sumberdaya manusia yang UKM miliki.
2. Pemisahan Tugas dan Tanggungjawab (Separation of Duties and Responsibilities)
   Pemisahan Tugas dan Tanggungjawab adalah konsep dengan cara menugaskan bagian-bagian dari pekerjaan yang sensitif akan keamanan ke beberapa individu. Sebagaimana telah dibahas pada poin 2.2.2.
3. Kewenangan Terbatas (Least Privilege)
   Kewenangan Terbatas memerlukan bahwa setiap subjek diberi set kewenangan terbatas yang diperlukan untuk melakukan tugas mereka. Apabila memungkinkan diperlukan adanya pemisahan tingkat akses berdasarkan fungsi pekerjaan operator. Pendekatan yang efektif adalah pemberian kewenangan yang terbatas. Sebuah contoh penerapan kewenangan terbatas antara lain yakni konsep dari operator komputer yang tidak diperbolehkan mengakses sumberdaya komputer lain di tingkat yang melampaui apa yang dibutuhkan oleh tugas spesifik mereka. Pada contoh ini operator diorganisasikan ke dalam kelompok-kelompok tingkat-

kewenangan (privilege-level). Setiap kelompok kemudian diberikan tingkat kewenangan paling terbatas yang mungkin diaplikasikan.

Tiga tingkat dasar dari kewenangan didefinisikan sebagai berikut:

a. Read Only
   Adalah tingkat paling bawah dari kewenangan dan juga merupakan satu kewenangan yang akan diberikan ke hampir semua operator. Operator diperbolehkan untuk melihat data tapi tidak diperbolehkan untuk menambahkan, menghapus, atau melakukan perubahan pada salinan asli dari data tersebut.
b. Read/Write
   Adalah tingkat yang memungkinkan operator untuk membaca, menambahkan, atau menulis pada data apa saja yang memiliki otoritas bagi mereka. Operator biasanya hanya memiliki akses read/write akan data yang disalin dari tempat asalnya, mereka tidak dapat mengakses data asal/original.
c. Access Change
   Adalah tingkat tertinggi yang memberikan operator hak untuk dapat memodifikasi data secara langsung ke tempat asal data tersebut, sebagai tambahan dari data yang disalin dari lokasi asalnya. Operator sebaiknya memiliki kewenangan untuk mengubah file dan hak akses operator di sistem (hak supervisor).

Penerapannya di UKM:
Tingkatan dasar kewenangan tersebut di atas umumnya adalah merupakan fitur-fitur yang terdapat pada atribut-atribut file system sistem operasi. Pada prakteknya biasanya dilakukan pengelompokan-pengelompokan pengguna sistem kemudian dari kelompok-kelompok tersebut ditetapkan kewenangannya. Sistem juga harus mendukung administrasi kewenangan tersebut untuk environment jaringan komputer, contohnya sebagaimana telah dijelaskan pada poin 2.2.2, pada sistem berbasis Windows dapat digunakan Active Directory, dan pada sistem berbasis UNIX dapat digunakan OpenLDAP bersama Samba, OpenAFS, dan Kerberos.

4. Yang Perlu Diketahui (Need to Know)
   Yang Perlu Diketahui memiliki makna sebagai suatu akses ke, pengetahuan akan, atau kepemilikan dari informasi spesifik yang diperlukan untuk melakuan fungsi tugas tertentu. Akan memerlukan bahwa subjek tertentu diberikan informasi yang diperlukan saja untuk dapat melakukan suatu pekerjaan.

   Penerapannya di UKM:
   Prakteknya pada UKM adalah dengan memberikan petunjuk teknis dan prosedur kepada masing-masing anggota organisasi sesuai dengan apa saja yang ia perlukan untuk melakukan pekerjaannya. Dokumen tersebut harus disimpan secara baik agar tidak terjadi kebocoran informasi yang dapat berakibat fatal seperti penyalahgunaan informasi oleh pegawai yang mengetahui petunjuk pengelolaan suatu aplikasi yang bukan wewenangnya.
5. Kontrol Manajemen Perubahan/Konfigurasi (Change/Configuration Management Controls)
   Fungsi dari kontrol ini adalah untuk melindungi sistem dari masalah dan kesalahan yang dapat menyebabkan dijalankan secara tidak baik, atau untuk mengujicoba suatu perubahan di dalam sebuah sistem.

Penerapannya di UKM:
Untuk menerapkan kontrol tersebut maka umumnya disusun suatu petunjuk dan prosedur untuk melakikan perubahan sebagaimana dijelaskan pada poin 2.2.4. Selanjutnya di sisi sistem sebaiknya disediakan suatu mekanisme pencatatan perubahan dan konfigurasi agar di lain waktu dapat diperiksa dan diaudit apakah sudah sesuai dengan yang direncanakan atau belum.

6. Pemeliharaan Rekaman dan Dokumentasi (Record Retention and Documentation)
   Administrasi dari kontrol keamanan pada dokumentasi dan prosedur-prosedur yanf diterapkan untuk record retention memiliki dampak pada keamanan operasional.
   a. Data Remanence
      Memiliki makna suatu data yang tertinggal di media setelah media tersebut dihapus. Setelah penghapusan, dapat saja ada beberapa jejak fisik tertinggal, yang dapat menyebabkan data dapat disusun ulang bersama informasi yang sensitif.

      Penerapannya di UKM:
      Terdapat dua hal yang harus diperhatikan yakni data remanence yang bersifat hardcopy dan softcopy. Untuk data yang hardcopy seperti kertas-kertas berisi informasi berharga maka apabila sudah tidak dirasakan penting lagi harus dihancurkan dengan menggunakan penghancur kertas atau dibakar, untuk menutup kemungkinan data tersebut disusun ulang dan jatuh ke pihak yang dapat menyalahgunakannya. Sedangkan pada data yang softcopy maka dapat dilakukan proses penghapusan dengan menggunakan bantuan perangkat lunak yang memenuhi standar keamanan dari pemerintah, misalnya program McAfee Shredder dapat menghapus sesuai dengan standar keamanan U.S. Government yakni tujuh kali proses penghapusan.
   b. Due Care and Due Diligence
      Konsep dari due care dan due diligence membutuhkan sebuah organisasi untuk menjalankan praktek bisnis yang baik relatif ke industri organisasi. Contoh dari Due Care adalah pelaksanaan pelatihan pegawai dalam hal kesadaran akan keamanan, bukan melainkan menyusun kebijakan tanpa adanya implementasi rencana dan follow-up. Contoh dari Due Diligence adalah kebutuhan akan banyak hukum di industri organisasi atau melalui compliance dengan standar regulasi pemerintah.

      Penerapannya di UKM:
      Untuk due care penerapannya lebih ke sisi internal organisasi yaitu bagaimana meningkatkan kualitas anggota organisasinya terhadap keadaan yang ada di lingkungan industri organisasi tersebut. Sedangkan untuk due diligence penerapannya lebih ke kepatuhan terhadap hukum yang berlaku di industri organisasi tersebut. Dimana suatu UKM dalam melakukan kegiatannya apakah sudah sesuai dengan ketetapan dan peraturan yang ditetapkan pemerintah. Apabila telah memenuhi akan kegiatan akan berjalan, jika sebaliknya maka dapat dikenakan sanksi dan kegiatan terhenti.
   c. Documentation
      Sistem keamanan memerlukan kontrol dokumen. Dokumen dapat mencakup beberapa hal seperti rencana keamanan, rencana kontijensi, analisa resiko, dan kebijakan dan prosedur. Sebagian besar dari dokumentasi ini harus

dilindungi dari pengaksesan tidak berhak, dan juga harus tersedia pada saat kejadian suatu bencana.

Penerapannya di UKM:
Kontrol dokumen dapat dilakukan untuk dokumen yang sifatnya hardcopy maupun softcopy. Untuk data yang sifatnya hardcopy maka sebaiknya disimpan ke tempat penyimpanan yang tahan segala macam cuaca (panas, dingin, lembab) dan bencana (banjir, kebakaran, badai), misalnya brankas besi baja yang dilengkapi kunci. Sedangkan untuk dokumen yang sifatnya softcopy maka sebaiknya dibuat dokumen salinan dan disimpan di tempat berbeda dari dokumen utamanya, misalnya dokumen pada tape back-up yang ditempatkan di lokasi berbeda, namun dokumen tersebut tetap terjaga kerahasiaannya dengan dienkripsi. Agar dapat tersedia dengan cepat pada saat terjadinya bencana maka harus diperhatikan juga akses transportasi untuk memindahkan tape back-up tersebut dengan cepat.

2.4 Kontrol di tingkat Operasi (Operations Controls)

Kontrol di tingkat Operasi mencakup prosedur yang digunakan dari hari ke hari untuk melindungi operasi-operasi yang berhubungan dengan komputer. Konsep yang dibahas meliputi pengamanan sumberdaya, kontrol perangkat keras dan perangkat lunak, dan entitas kewenangan (privileged entity).

Beberapa hal berikut merupakan aspek-aspek penting dalam kontrol operasi:
1. Pengamanan sumberdaya (Resource protection)
2. Kontrol perangkat keras (Hardware controls)
3. Kontrol perangkat lunak (Software controls)
4. Kontrol entitas-kewenangan (Privileged-entity controls)
5. Kontrol media (Media controls)
6. Kontrol terhadap akses fisik (Physical access controls)

2.4.1 Pengamanan Sumberdaya (Resource Protection)

Pengamanan sumberdaya adalah merupakan arti sesungguhnya – konsep melindungi sumberdaya dan aset komputasi organisasi dari kehilangan dan penyalahgunaan. Sumberdaya komputasi didefinisikan sebagai seluruh perangkat keras, perangkat lunak, atau data yang dimiliki dan digunakan oleh organisasi. Pengamanan sumberdaya dirancang untuk membantu mengurangi kemungkinan kerusakan yang dihasilkan dari penggunaan tidak sah dan/atau penghapusan data dengan cara membatasi kesempatan untuk penyalahgunaan ini.

Beberapa contoh sumberdaya yang memerlukan pengamanan:
1. Sumberdaya perangkat keras, meliputi:
   - Komunikasi: router, firewall, gateway, switch, modem, access server
   - Media penyimpanan: floppy, removable drive, hard drive eksternal, tape, cartridge
   - Sistem pemrosesan: file server, mail server, internet server, back-up server, tape drive
   - Perangkat standalone: workstation, modem, disk, tape
   - Printer dan mesin faks

Penerapannya di UKM:
Pada umumnya UKM tidak memiliki semua sumberdaya tersebut, sebagian besar menyewa ke suatu Internet Service Provider (ISP). Dan juga apabila ada, biasanya sumberdaya tersebut merupakan gabungan dari beberapa fungsi sumberdaya, misalnya satu server untuk beragam fungsi seperti web, mail, database server. Sehingga untuk mengamankannya tidak dibutuhkan biaya dan tenaga yang besar. Sebagai saran tambahan untuk melindungi jaringan, melihat perkembangan teknologi jaringan nirkabel saat ini yang begitu maju disertai pula dengan biaya yang cukup masuk akal, ada baiknya mempertimbangkan untuk menggunakan seluruh jaringan lokal menjadi jaringan nirkabel. Dikarenakan kemudahan dalam membangunnya dan apabila terjadi bencana juga dimungkinkan untuk lebih cepat memindahkannya ke tempat lain daripada jaringan dengan kabel biasa, untuk merendahkan down time akibat bencana.

2. Sumberdaya perangkat lunak, meliputi:
   - Program library dan source code
   - Vendor perangkat lunak atau paket-paket propietary
   - Perangkat lunak sistem operasi dan utiliti sistem

   Penerapannya di UKM:
   Sebagaimana menangani kontrol dokumen softcopy maka untuk mengamankan sumberdaya perangkat lunak juga seperti tersebut, dilakukan back-up periodik untuk perangkat lunak sensitif bagi organisasi. Khusus untuk progam library dan source code diberikan pengamanan yang lebih dari yang lain karena merupakan aset yang sangat berharga bagi organisasi. Seperti otorisasi menggunakan kontrol dua orang untuk dapat mengaksesnya dan juga pengamanan media penyimpanan fisiknya lebih diperhatikan.
3. Sumberdaya data, meliputi:
   - Data back-up
   - File-file data pengguna
   - File-file password
   - Direktori-direktori data operasi
   - Log sistem dan jejak audit

   Penerapannya di UKM:
   Seperti pada pengamanan sumberdaya perangkat lunak disertai dengan memperhatikan tingkat keberhargaan data tersebut. Dalam hal ini file-file data pengguna dan file-file password masuk prioritas utama.

2.4.2 Kontrol Perangkat Keras (Hardware Controls)

Kontrol perangkat keras yang dilakukan meliputi:

1. Pemeliharaan perangkat keras
   Pemeliharaan sistem memerlukan akses secara fisik atau logik ke dalam sistem melalui staf pendukung dan operasi, vendor-vendor, atau penyedia layanan. Pemeliharaan mungkin dapat dilakukan di tempat itu langsung, atau dapat juga ditransportasi ke tempat khusus perbaikan. Bahkan dapat juga dilakukan melalui jarak jauh. Lebih jauh lagi, penyidikan terhadap personel layanan juga layak dilakukan. Penyuluhan dan penyaluran terhadap personel pemelihara saat mereka berada di tempat perbaikan juga layak dilakukan.

Penerapannya di UKM:
Untuk kontrol terhadap pemeliharaan perangkat keras dalam UKM secara umum tidak begitu banyak dan rumit dikarenakan umumnya UKM memiliki kantor yang ada di suatu rumah toko (ruko) sehingga apabila ada pihak yang ingin mengadakan pemeliharaan, misalnya setting server, akan langsung terlihat oleh orang-orang disekitarnya. Dalam hal ini kontrol yang dilakukan hanya bersifat penyampaian/pengumuman informasi ke seluruh anggota organisasi akan adanya pihak yang ingin melakukan pemeliharaan, agar tidak terjadi kesalahpahaman. Atau dengan menugaskan salah seorang untuk menemani pihak pemelihara tersebut hingga urusannya selesai.

2. Akun pemeliharaan
   Banyak sistem komputer menyediakan akun pemeriharaan. Akun di tingkat teratas ini diset dari pabrik dan menggunakan password yang diketahui oleh umum. Sangat penting untuk mengganti password tersebut atau sekurangnya mematikan akun tersebut sampai saatnya diperlukan. Apabila akun ini digunakan melalui jarak jauh, otentikasi dari penyedia pemelihara dapat dilakukan dengan cara callback atau enkripsi.

   Penerapannya di UKM:
   Untuk kontrol ini dilakukan di sisi administrasi sistem, dimana administrator keamanan bertugas untuk membuat akun user, menetapkan passwordnya, dan ekspirasi akun tersebut. Untuk perangkat yang memiliki password dari pabrik, misalnya router, sebaiknya diubah langsung saat mulai digunakan.
3. Kontrol port diagnosa
   Banyak sistem memiliki port untuk melakukan diagnosa terhadap sistem yang dapat dilalui oleh pengkoreksi masalah untuk mengakses secara langsung ke perangkat keras. Port ini seharusnya hanya dapat digunakan oleh personel yang sah dan juga tidak membolehkan akses tidak sah baik secara internal maupun eksternal. Penyerangan port diagnosa adalah istilah yang menjelaskan tipe penyalahgunaan tersebut.

   Penerapannya di UKM:
   Untuk kontrol ini dilakukan di sisi administrasi sistem, dimana administrator sistem bertugas untuk menetapkan port diagnosa mana yang dibuka, dan administrator keamanan bertugas untuk menetapkan akun user dan passwordnya yang berhak mengakses port diagnosa tersebut.
4. Kontrol perangkat keras fisik
   Banyak area pemrosesan daya yang memiliki perangkat keras membutuhkan kunci dan alarm. Beberapa contohnya sebagai berikut:
   - Terminal dan keyboard operator yang sensitif
   - Kabinet atau ruangan media penyimpanan
   - Data center server atau perlengkapan komunikasi
   - Ruangan kumpulan modem atau sirkuit telekomunikasi

   Penerapannya di UKM:
   Untuk kontrol terhadap pemeliharaan perangkat keras dalam UKM secara umum tidak begitu banyak dan rumit dikarenakan umumnya UKM memiliki kantor yang ada di suatu rumah toko (ruko) yang hanya memiliki beberapa ruangan, untuk itu kontrol lebih mudah dilakukan. Minimal dengan memberi kunci dan dijaga oleh petugas keamanan, atau dapat juga ditempatkan di dekat ruangannya. Ada baiknya

petugas juga harus mengetahui anggota organisasi mana saja yang memiliki hak akses ke ruang tersebut. Jangan sampai orang yang tidak berhak diperbolehkan masuk, walaupun sudah minta izin ke petugas.

2.4.3 Kontrol Perangkat Lunak (Software Controls)

Unsur penting dari kontrol operasi adalah dukungan perangkat lunak – mengontrol perangkat lunak apa saja yang digunakan di dalam sistem. Unsur dari kontrol perangkat lunak, antara lain:

1. Manajemen anti-virus
   Jika personel dapat menjalankan perangkat lunak apa saja yang ada di dalam sistem, maka sistem akan rawan terhadap virus, interaksi perangkat lunak yang tidak semestinya, dan juga pengubahan paksa kontrol keamanan.

   Penerapannya di UKM:
   Manajemen anti-virus pada UKM dapat dilakukan terutama pada saat seleksi perangkat lunak anti-virus itu sendiri. Pada seleksi ada baiknya memperhatikan fitur-fitur yang diberikan oleh anti-virus tersebut dan juga banyak mencari informasi tentang bagaimana kualitas anti-virus tersebut diasosiasikan dengan sistem operasi yang digunakan UKM. Beberapa informasi penting dapat diperoleh di ICSA Labs (https://www.icsalabs.com/icsa/icsahome.php) tentang perangkat lunak yang memenuhi sertifikasi sebagai anti-virus, firewall, dan sebagainya untuk berbagai sistem operasi. Selain itu dapat pula mengunjungi situs vendor pembuat sistem operasi untuk mengetahui kerawanan terhadap virus apa saja yang sedang dihadapi, misalnya pada sistem operasi berbasis Windows dapat ke http://www.microsoft.com/athome/security/viruses/default.mspx, dan sistem berbasis UNIX pada umumnya sudah anti terhadap virus namun dapat juga melihat beberapa referensi di http://cvs.sourceforge.net/viewcvs.py/openantivirus/mini-faq/av-unix_e.txt?rev=HEAD. Selanjutnya apabila anti-virus sudah terpasang pada komputer-komputer maka jangan lupa untuk melakukan update secara periodik. Untuk UKM sebagai saran carilah anti-virus yang ringan sumberdaya komputasi namun ampuh membasmi virus, disertai dengan fasilitas update otomatis yang tidak membebani jaringan, lebih bagus lagi bila ada fasilitas administrasi update secara lokal (file update didownload oleh server untuk disalin ke client-client).
2. Uji perangkat lunak
   Proses pengujian perangkat lunak yang kaku dan formal diperlukan untuk menentukan kompabilitas dengan aplikasi khusus atau untuk mengidentifikasikan interaksi lain yang tidak dikira sebelumnya. Prosedur ini sebaiknya diterapkan pada saat upgrade perangkat lunak.

   Penerapannya di UKM:
   Untuk UKM cukup dilakukan dengan penyusunan prosedur pelaksanaan uji perangkat lunak, dengan catatan pihak yang menguji tidak boleh sama dengan pihak pembuat (developer). Hal ini dilakukan untuk menghindari pihak developer menutup-nutup kerawanan yang ada pada perangkat lunak diuji.
3. Utiliti perangkat lunak
   Utiliti sistem yang sangat berkuasa dapat menyalahgunakan integritas dari sistem pengoperasian dan kontrol akses logik. Sebaiknya dikontrol oleh kebijakan keamanan.

Penerapannya di UKM:
Tidak diperlukan kontrol secara khusus untuk UKM. Umumnya sudah termasuk di dalam sistem pengaturan kewenangan di tingkat sistem operasi, yang kuasanya dipegang oleh administrator sistem dan administrator keamanan.

4. Penyimpanan perangkat lunak secara aman
   Kombinasi dari kontrol logik dan fisik sebaiknya diterapkan untuk menjamin bahwa perangkat lunak dan salinan dari back-up tidak dimodifikasi secara tidak sah.

   Penerapannya di UKM:
   Serupa dengan penanganan sumberdaya data. Biasanya perangkat lunak back-up dipisahkan dan dienkripsi serta menggunakan password yang diketahui administrator sistem dan administrator keamanan.
5. Kontrol back-up
   Tidak hanya personel pendukung dan operasi melakukan back-up perangkat lunak dan data, di lingkungan yang terdistribusi pengguna dapat juga melakukan back-up terhadap data mereka sendiri. Adalah penting untuk secara rutin melakukan pengujian akurasi pengembalian (restore) dari suatu sistem back-up. Suatu back-up harus dapat disimpan secara aman untuk melindungi dari pencurian, pengrusakan, ataupun masalah lingkungan.

   Penerapannya di UKM:
   Mengingat keterbatasan sumberdaya pada UKM maka untuk hal ini sebaiknya dilakukan pada saat libur kerja dan apabila tidak memungkinkan minimal dilakukan sebagian data saja yang dianggap sangat berharga saja, bukan data seluruhnya. Atau dapat juga simulasi dengan menggunakan data palsu.

2.4.4 Kontrol Entitas-Kewenangan (Privileged-Entity Controls)

Kontrol entitas kewenangan didefinisikan sebagai akses lebih atau khusus ke suatu sumberdaya komputasi yang diberikan kepada operator dan administrator sistem. Banyak tugas kerja dan fungsi memerlukan akses tertentu.

Akses entitas kewenangan umumnya dipisahkan ke dalam kelas-kelas. Operator sebaiknya ditugaskan ke dalam kelas dengan berdasarkan job title mereka. Berikut ini adalah contoh dari fungsi operator dengan entitas kewenangannya:
- Akses khusus ke system command
- Akses ke parameter khusus
- Akses ke program kontrol sistem

2.4.5 Kontrol Media (Media Controls)

Pengamanan sumberdaya media dapat diklasifikasikan ke dalam dua area yaitu kontrol pengamanan media dan kontrol penanganan media. Kontrol pengamanan media diterapkan untuk mencegah ancaman pada C.I.A. dari pengungkapan data sensitif secara sengaja atau tidak disengaja. Kontrol ketersediaan media diterapkan untuk melindungi keadaan kerja yang benar dari media, khususnya untuk memfasilitasi pengembalian data (restore) secara akurat dan tepat waktu pada saat terjadi kegagalan sistem.

Berikut penjelasan klasifikasi kontrol media:

1. Kontrol Pengamanan Media (Media Security Controls)
   Kontrol Pengamanan Media sebaiknya dirancang untuk mencegah hilangnya informasi sensitif ketika media dikirim keluar sistem.

   Beberapa elemen kontrol pengamanan media:

   a. Pencatatan (Logging)
      Pencatatan dengan menggunakan media data menghasilkan akuntabilitas. Pencatatan juga membantu di kontrol penyimpanan fisik dengan cara mencegah tape berpindah tempat dan juga memfasilitasi proses recovery yang diperlukan.

      Penerapannya di UKM:
      Sebagian besar sistem operasi dapat melakukan pencatatan secara otomatis terhadap media data.

   b. Kontrol akses (Access Control)
      Akses kontrol fisik ke media digunakan untuk mencegah akses ke media oleh personel yang tidak sah. Prosedur ini juga merupakan kontrol penyimpanan fisik.

      Penerapannya di UKM:
      Kontrol ini lebih menekankan bagaimana prosedur pengamanan media di sisi organisasi yakni pengalokasian sumberdaya manusianya.

   c. Pembuangan yang Benar (Proper Disposal)
      Pembuangan media yang tepat dan benar diperlukan untuk menghindari adanya data yang tertinggal. Proses untuk menghilangkan informasi dari data media yang sudah terpakai disebut dengan sanitasi. Tiga teknik yang umum digunakan untuk sanitasi yaitu penulisan ulang, pen-degauss-an, dan penghancuran.

      Penerapannya di UKM:
      Sebagaimana telah dijelaskan pada poin 2.3 bagian 6 mengenai Pemeliharaan Rekaman dan Dokumentasi (Record Retention and Documentation) khususnya mengenai Data Remanence. Untuk UKM minimal dapat melakukan teknik penulisan ulang terhadap isi media sebelum dibuang. Sedangkan secara fisik dapat dilakukan penghancuran dengan cara dibakar.

2. Kontrol Ketersediaan Media (Media Viability Controls)
   Banyak kontrol fisik yang seharusnya digunakan untuk melindungi ketersediaan dari media penyimpanan data. Tujuannya adalah untuk mengamankan media dari kerusakan pada saat penanganan dan pemindahtempatan atau dalam jangka waktu pendek ataupun panjang. Penandaan yang benar dan pelabelan media diperlukan pada saat proses recovery sistem.

   Beberapa elemen kontrol ketersediaan media:

   a. Penandaan (Marking)
      Semua media penyimpanan data sebaiknya diberi tanda dan label dengan akurat. Label dapat digunakan untuk mengidentifikasikan media dengan instruksi penanganan media tersebut atau untuk mencatat serial number atau bar code untuk penanganan pada saat recovery sistem.

Penerapannya di UKM:
Setiap media diberi tanda berisi nomor/kode, jangan menyatakan makna isi sesungguhnya dari media pada label tersebut, untuk menghindari keingintahuan pihak yang bermaksud tidak baik.

b. Penanganan (Handling)
Penanganan media dengan benar adalah penting. Beberapa hal yang berhubungan dengan penanganan media antara lain termasuk kebersihan media dan pengamanan dari pengrusakan secara fisik ke media pada saat pemindahan ke tempat pengumpulan media.

Penerapannya di UKM:
Setiap media disimpan ke dalam suatu perangkat penyimpanan yang cukup kuat serta tahan goncangan.

c. Penyimpanan (Storage): Penyimpanan dari media adalah sangat penting untuk alasan keamanan dan lingkungan. Lingkungan yang memiliki panas tepat dan bebas kelembaban harus disediakan untuk media. Media data sensitif terhadap temperatur, cairan, medan magnet, asap, dan debu.

Penerapannya di UKM:
Setiap media disimpan ke dalam suatu perangkat penyimpanan yang dapat menjaga kondisi media dari lingkungan sekitarnya serta anti listrik statis.

2.4.6 Kontrol Terhadap Akses Fisik (Physical Access Controls)

Kontrol pada akses fisik suatu sumberdaya adalah merupakan salah satu pembahasan utama di domain Keamanan Fisik (Physical Security). Secara tidak langsung domain Keamanan Operasi (Operations Security) juga memerlukan kontrol akses fisik.

Berikut ini mengandung beberapa contoh unsur dari sumberdaya operasi yang memerlukan kontrol akses fisik:

1. Perangkat keras, meliputi:
   - Kontrol komunikasi dan perlengkapan komputasi
   - Kontrol media penyimpanan
   - Kontrol log dan report yang tercetak
2. Perangkat lunak, meliputi:
   - Kontrol file back-up
   - Kontrol log sistem
   - Kontrol aplikasi produksi
   - Kontrol data sensitif/kritikal

Secara tidak langsung, semua personel memerlukan suatu kontrol dan akuntabilitas ketika mengakses sumberdaya fisik, dan juga semua personel memerlukan akses fisik khusus untuk dapat melakukan fungsi pekerjaan mereka. Berikut ini contoh tipe dari personel-personel tersebut:

- Personel departemen Teknologi Informasi
- Staf kebersihan
- Personel pemelihara Heating Ventilation and Air Conditioning (HVAC)
- Personel pihak ketiga
- Konsultan, kontraktor, dan staf temporer

Perjanjian khusus untuk mengawasi sistem harus dibuat ketika ada personel pendukung luar yang memasuki data center.

Penerapannya di UKM:
Untuk kontrol terhadap akses fisik dalam UKM secara umum tidak begitu banyak dan rumit dikarenakan umumnya UKM memiliki kantor yang ada di suatu rumah toko (ruko) yang hanya memiliki beberapa ruangan, untuk itu kontrol lebih mudah dilakukan. Minimal dengan memberi kunci dan dijaga oleh petugas keamanan, atau dapat juga ditempatkan di dekat ruangannya. Ada baiknya petugas juga harus mengetahui anggota organisasi mana saja yang memiliki hak akses ke ruang tersebut. Jangan sampai orang yang tidak berhak diperbolehkan masuk, walaupun sudah minta izin ke petugas.

3. Pengawasan dan Pengauditan (Monitoring and Auditing)

Pengawasan disini diimplementasikan pada fasilitas operasional dimana untuk mengidentifikasikan penggunaan computer yang tidak semestinya. Mendeteksi kerusakan dan responnya, termasuk mekanisme pelaporan adalah bagian penting dari pengawasan.

3.1 Pengawasan (Monitoring)

Pengawasan terdiri mekanisme, peralatan dan teknik yang mengijinkan identifikasi dari kejadian keamanan yang dapat mempengaruhi operasi dari komputer. Konsep pengawasan termasuk pengawasan untuk instalasi perangkat lunak ilegal, memonitor perangkat keras untuk kesalahan, dan memonitor kegiatan operasional untuk anomali/keanehan.

Teknik-teknik dalam Pengawasan, antara lain sebagai berikut:

1. Intrusion Detection
   Intrusion Detection adalah sarana sangat bermanfaat untuk dapat membimbing proses analisa dari gangguan yang terjadi, tidak hanya dapat digunakan untuk mengidentifikasikan gangguan tapi juga untuk membuat contoh pola lalu lintas. Dengan menganalisa aktivitas yang terjadi di atas tingkat normal.

   Penerapannya di UKM:
   Mengingat keterbatasan sumberdaya pada UKM untuk dapat menerapkan Intrusion Detection pada UKM maka dapat menggunakan komputer yang difungsikan sebagai router, firewall, dan IDS. Alternatif yang cukup handal dan murah biaya adalah menggunakan sistem operasi berbasis UNIX yang menjalankan perangkat lunak firewall iptables (built-in) dan IDS Snort (http://www.snort.org/docs/) untuk melindungi komputer-komputer di dalam jaringan lokal. Snort akan melakukan analisa terhadap paket-paket jaringan dan melakukan pelaporan apabila ditemua pola lalu lintas yang serupa dengan pola tindak pelanggaran baik itu disebabkan manusia atau perangkat lunak lain seperti virus dan worm.
2. Penetration Testing
   Penetration Testing adalah proses uji ketahanan jaringan dengan mencoba menerobos sistem dari luar dengan menggunakan teknik sama seperti yang

digunakan oleh penerobos eksternal (contoh: cracker). Pengujian ini memberikan para profesional akan gambaran keadaan keamanan organisasi.

Dari berbagai macam teknik yang digunakan pada Penetration Testing terdapat beberapa teknik yang umum, antara lain:

- Scanning dan Probing
  Berbagai macam scanner seperti port scanner, dapat memberikan informasi tentang infrastruktur jaringan komputer dan memungkinkan penerobos untuk mengakses port jaringan yang tidak diamankan.
- Demon Dialing
  Demon (atau perang) dialer akan secara otomatis mengakses setiap sambungan telepon yang ada untuk mencoba menempatkan modem yang terhubung dengan jaringan. Informasi tentang modem ini kemudian dapat digunakan untuk akses dari luar secara tidak sah.
- Sniffing
  Sebuah penganalisa protokol (protocol analyzer) dapat digunakan untuk menangkap (capture) paket data yang kemudian dapat dikodekan untuk mengumpulkan informasi seperti password atau konfigurasi infrastruktur.

Teknik lain yang tidak berbasiskan teknologi namun dapat digunakan untuk melengkapi Penetration Testing, antara lain :

- Dumpster Diving
  Pencarian kertas-kertas berisi informasi berharga yang dibuang untuk mencari laporan-laporan penting yang tidak terpotong.
- Social Engineering
  Teknik yang paling umum dan mudah digunakan untuk mendapatkan informasi seperti password yaitu dengan bertanya langsung kepada mereka yang memiliki password tersebut.

Penerapannya di UKM:
Untuk UKM yang pada umumnya tidak memiliki pengetahuan cukup tentang bagaimana keamanan yang maka dapat saja melakukan uji penerobosan secara online di internet, namun sebaiknya dipasang terlebih dahulu semua perangkat lunak pengamanannya. Salah satu contohnya Hackerwatch.org.

3. Violation Analysis
   Salah satu teknik yang paling banyak digunakan untuk melacak perubahan aktivitas pengguna adalah pelacakan pelanggaran, pemrosesan, dan analisa. Agar pengunaan pelacakan pelanggaran efektif, clipping level harus ditetapkan terlebih dahulu. Clipping level adalah suatu dasar untuk aktivitas pengguna yang dipercayai sebagai kesalahan pengguna tingkat rutin. Clipping level digunakan agar sistem dapat mengabaikan kesalahan normal pengguna, namun ketika clipping level terlampaui maka catatan pelanggaran akan terbentuk. Clipping level juga digunakan untuk berbagai macam detektor.

   Penggunaan clipping level dan deteksi anomali berdasarkan profil di bawah ini adalah tipe dari pelanggaran yang harus dilacak, diproses dan dianalisa:
   - Kesalahan berulang-ulang yang melewati batas angka clipping level
   - Individu yang melampaui otorisasinya
   - Terlalu banyak orang yang memiliki akses tidak terbatas
   - Pola-pola yang mengindikasikan percobaan penerobosan

Penerapannya di UKM:
Pada UKM umumnya untuk mengendalikan hal tersebut diatur di sistem operasi, seperti penanganan kesalahan pemasukkan password yang diperbolehkan sampai berapa kali, untuk kemudian sistem akan mengunci terminal/workstation tersebut dan secara otomatis melaporkan ke administrator sistem dari terminal mana, user siapa, dan kapan kesalahan tersebut terjadi. Sedangan untuk clipping level di jaringan maka akan ditangani oleh IDS, misalnya IDS mendeteksi dan otomatis melaporkan terjadinya percobaan penerobosan ke administrator sistem.

3.2 Pengauditan (Auditing)

Implementasi dari audit sistem yang teratur adalah merupakan fondasi bagi pengawasan kontrol keamanan operasional. Sebagai tambahan dari dilakukannya pengecekan compliance baik internal maupun eksternal, pelaksanaan audit pada jejak audit (transaksi) dan log dapat membantu fungsi pengawasan dengan cara mengenali pola-pola yang abnormal dari kebiasaan pengguna.

3.2.1 Audit Keamanan (Security Auditing)

Auditor Teknologi Informasi (TI) sering dibagi menjadi dua tipe yaitu internal dan eksternal. Auditor internal biasanya bekerja untuk organisasi sedangkan eksternal tidak. Auditor eksternal sering bersertifikat Public Accountants atau Audit Professional yang lain yang diberi imbalan untuk malakukan audit independen pada organisasi finansial. Sedangkan auditor internal biasanya mempunyai cakupan pekerjaan yang lebih luas mengecek apakah standar yang ditetapkan telah terpenuhi, mengaudit efisiensi biaya operasi dan merekomendasikan kontrol yang tepat.

Auditor TI biasanya mengaudit hal-hal sebagai berikut:
- Kontrol back-up
- Kontrol sistem dan transaksi
- Prosedur perpustakaan data
- Standar pengembangan sistem
- Keamanan data center
- Rencana keberlangsungan (contingency plan)

Auditor TI dapat juga merekomendasikan perbaikan kontrol dan mereka sering berpartisipasi dalam proses pengembangan sistem untuk membantu organisasi mengindari rekayasa ulang berbiaya besar setelah sistem diimplementasi.

Penerapannya di UKM:
Untuk UKM yang masih berkembang audit keamanan umumnya tidak dilakukan karena untuk dapat menyewa auditor keamanan independen pasti akan memakan biaya yang cukup mahal. Sebagai gantinya pihak penanggungjawab keamanan di dalam organisasilah yang melakukan langkah-langkah seperti yang dilakukan auditor keamanan umumnya dengan mengikuti berbagai informasi mengenai audit keamanan.

3.2.2 Jejak Audit (Audit Trails)

Jejak audit memungkinkan praktisi keamanan untuk melacak sebuah sejarah transaksi. Jejak audit menyediakan informasi tentang penambahan, penghapusan dan modifikasi

data dalam sistem yang seluruhnya disusun ulang menjadi suatu rangkaian kejadian menurut waktu. Jejak audit digunakan untuk membimbing mengidentifikasi problem dimana dapat membantu memecahkan problem tersebut.

Log audit sebaiknya mencatat hal-hal sebagai berikut:
- Tanggal dan waktu transaksi
- Siapa yang memproses transaksi tersebut
- Terminal mana transaksi tersebut di proses
- Berbagai macam kejadian keamanan yang berhubungan dengan transaksi

Auditor sebaiknya juga memeriksa log audit untuk hal-hal berikut:
- Amandemen ke pekerjaan produksi
- Pengerjaan ulang pekerjaan produksi
- Praktek operator komputer

Hal-hal lain yang juga penting untuk diperhatikan sehubungan dengan penggunaan media dan laporan audit adalah sebagai berikut:
- Retensi dan pengamanan dari media dan laporan audit ketika dikeluarkan dari tempat asalnya
- Pengamanan terhadap penghilangan audit atau log transaksi
- Pengamanan terhadap ketidaksediaan dari media audit pada suatu kejadian

Penerapannya di UKM:
Untuk dapat melakukan jejak audit pada sistem keamanan di UKM maka yang mungkin dilakukan adalah melihat berkas-berkas catatan pelaksanaan prosedur-prosedur kegiatan dan juga melihat log sistem.

3.2.3 Konsep Manajemen Masalah (Problem Management Concept)

Audit yang efektif mencakup konsep dari manajemen masalah. Manajemen masalah adalah cara untuk mengontrol proses isolasi maslaah dan penyelesaian masalah. Auditor dapat juga menggunakan manajemen masalah untuk memecahkan isu yang berkembang seputar audit keamanan TI.

Ada tiga tujuan dari manajemen masalah:
1. Mengurangi kesalahan sampai ke tingkat yang dapat dikelola
2. Mencegah ulangan atau pengulangan dari masalah
3. Menangani dampak negatif dari masalah pada layanan komputasi dan sumberdaya

Langkah pertama dalam penerapan manajemen masalah adalah mendefinisikan area masalah yang potensial dan kejadian abnormal yang harus diselidiki. Beberapa contoh area masalah yang potensial, antara lain:
- Kemampuan dan ketersediaan dari sumberdaya komputasi dan layanan
- Infrasuktur sistem dan jaringan
- Prosedur dan transaksi
- Keselamatan dan keamanan personel

Beberapa contoh kejadian abnormal yang mungkin dapat ditemui pada saat audit, antara lain:
- Degradasi kemampuan perangkat keras atau lunak

- Deviasi dari prosedur standar transaksi
- Kejadian yang tidak dapat dijelaskan pada rantai proses

4. Ancaman dan Kerawanan (Threats and Vulnerabilities)

Ancaman adalah semua hal yang apabila terjadi dapat menyebabkan kerusakan pada sistem dan kehilangan kerahasiaan, kemampuan, dan integritas. Ancaman dapat berbahaya seperti mengubah data-data yang sensitif atau dapat terjadi secara tidak sengaja seperti kesalahan pada kalkulasi transaksi atau penghapusan file yang tidak disengaja. Kerawanan adalah kelemahan yang terdapat pada sistem yang dapat dimanfaatkan oleh ancaman. Mengurangi aspek kerawanan pada sistem dapat mengurangi resiko dan efek dari ancaman pada sistem. Contohnya pada progam password generation yang dapat membantu user memilih password robust (tidak mudah ditebak), yang dapat mengurangi kemungkinan user menggunakan password yang buruk (kerawanan) dan membuat password semakin susah untuk ditembus (ancaman). Salah satu contoh pada sistem berbasis UNIX memiliki fasilitas untuk memberitahu kalau password mudah ditebak.

4.1 Ancaman (Threats)

Ancaman dapat dikelompokkan menjadi beberapa macam, antara lain:

1. Kehilangan tidak disengaja (Accidental Loss)
   Kehilangan tidak disengaja adalah kehilangan yang terjadi tidak secara terus-menerus dapat juga karena tidak adanya perlatihan terhadap operator atau kesalahan pada proses prosedur penggunaan perangkat lunak/aplikasi.

   Beberapa contoh kehilangan tidak disengaja, antara lain:
   - Kesalahan menginput pada operator atau kelalaian, hal ini dapat berupa kesalahan pada input transaksi, entri data ataupun penghapusan data dan kesalahan pada modifikasi data.
   - Kesalahan pada proses transaksi, kesalahan dapat terjadi pada data karena kesalahan pada program aplikasi atau prosedur proses.

   Penanggulangannya di UKM:
   Dilakukan penyusunan prosedur yang dikomunikasikan dengan anggota organisasi terkait agar pihak penyusun prosedur dan pelaksana satu pemikiran serta tidak ada yang merasa dipaksa.
2. Aktivitas tidak layak (Inappropriate Activities)
   Kebiasaan menggunakan computer untuk aktivitas yang tidak layak selama itu bukan merupakan tindakan kriminal namun dapat dikenakan sanksi dari perusahaan pada pegawai yang melakukannya.

   Beberapa contoh aktivitas yang tidak layak:
   - Konten tidak layak
     Menggunakan sistem perusahaan untuk menyimpan pornografi, hiburan, politik maupun muatan kekerasan

     Penanggulangannya di UKM:
     Di sisi akses ke luar terhadap konten tidak layak maka server yang berfungsi sebagai proxy internet akan membatasi akses ke konten tersebut, sedangkan di

sisi internal sistem operasi tiap-tiap terminal dilengkapi perangkat lunak untuk memfilter konten yang diakses user.

- Sampah dari sumber perusahaan
  Seseorang menggunakan perangkat keras maupun perangkat lunak, seperti mengadakan suatu bisnis pribadi dengan mempergunakan sistem komputer perusahaan

  Penanggulangannya di UKM:
  Melalui policy yang ditetapkan oleh administrator sistem, baik itu pada sistem yang menggunakan Active Directory maupun LDAP, membatasi user untuk tidak dapat instal perangkat lunak sendiri (harus izin administrator). Secara periodik melakukan pengecekan terhadap perangkat keras maupun perangkat lunak yang potensial.
- Kejahatan seksual ataupun rasial
  Menggunakan e-mail atau sumberdaya komputer lainnya untuk mendistribusikan material yang tidak layak atau melanggar norma-norma.

  Penanggulangannya di UKM:
  Di sisi sistem yaitu dengan memasang perangkat lunak untuk memfilter e-mail yang dianggap tidak layak. Dapat dilakukan di sisi server e-mail dan juga e-mail client yang digunakan user. Di sisi user yaitu dengan mengadakan penyuluhan tentang bahayanya penyalahgunaan e-mail atau sumberdaya komputer lainnya.
- Penyalagunaan kewenangan atau hak
  Menggunakan tingkat akses secara tidak sah untuk melanggar kerahasiaan informasi perusahaan

  Penanggulangannya di UKM:
  Sistem dirancang untuk dapat mencatat aktivitas yang dapat dikategorikan rahasia bagi organisasi. Misalnya akses ke data tertentu di jaringan. Disusun peraturan agar secara periodik untuk mengganti password ke terminal, dibantu dengan password generator.

3. Operasi Komputer Ilegal dan Penyerangan yang Disengaja (Illegal Computer Operations and Intentional Attacks)
   Dibawah ini adalah kelompok area kegiatan yang dipertimbangkan sebagai kegiatan komputer ilegal yang disengaja untuk keuntungan finansial pribadi penerobos dan juga untuk pengrusakan:
   - Kegiatan memata-matai
     Mengais-ngais data, lalu lintas data maupun analisa perkembangan, social engineering, ekonomi ataupun mata-mata politik, sniffing maupun pengamatan keystroke ataupun melakukan pemecahan terhadap segala jenis kegiatan mata-mata untuk mendapatkan informasi atau untuk menciptakan suatu pijakan untuk penyerangan berikutnya. Kegiatan memata-matai merupakan penyebab utama dari kegagalan kerahasiaan.

     Penanggulangannya di UKM:
     Gabungan dari beragam penangkalan meliputi pembatasan wewenang untuk instalasi perangkat lunak, pembatasan wewenang pada aplikasi, pendeteksian paket-paket mencurigakan di jaringan, pengubahan password secara periodik, dan penyuluhan terhadap anggota organisasi.

- Penipuan
  Contoh dari jenis penipuan adalah kolusi, transaksi fiktif, manipulasi data dan pengubahan data lainnya secara integritas untuk suatu keuntungan.

  Penanggulangannya di UKM:
  Merancang kontrol transaksi pada aplikasi yang melakukan transaksi sensitif bagi organisasi. Misalnya pencatatan user dan waktu transaksi.
- Pencurian
  Contoh dari jenis pencurian adalah pencurian informasi atau rahasia perdagangan untuk keuntungan atau penyingkapan data secara tidak sah serta pencurian secara fisik perangkat keras maupun perangkat lunak.

  Penanggulangannya di UKM:
  Pengamanan secara fisik perangkat keras meliputi pemberian kunci pada ruangan berharga dan dijaga oleh petugas keamanan. Pengamanan perangkat lunak seperti enkripsi data berharga.
- Sabotase
  Sabotase termasuk didalamnya Denial of Service (DoS), penundaan produksi dan sabotase data terintegritas.

  Penanggulangannya di UKM:
  Dengan memasang firewall dengan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) pada router.
- Serangan Eksternal
  Contoh dari serangan eksternal adalah cracking yang berbahaya, scanning dan probing yang berusaha untuk merusak infrasuktur informasi, demon dialing untuk mencari sambungan modem yang tidak terlindungi, dan menyebarkan kode program atau virus yang berbahaya.

  Penanggulangannya di UKM:
  Gabungan dari beberapa pengamanan antara lain dengan memasang firewall dengan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) pada router, memasang anti-virus dan anti-spyware di tiap terminal, didukung oleh update (anti-virus dan sistem operasi) secara periodik, dan sistem deteksi hardware baru dinon-aktifkan untuk mencegah user menambahkan hardware, seperti modem, secara langsung ke terminal.

4.2 Kerawanan (Vulnerabilities)

1. Analisa Tren/Lalu lintas (Traffic/Trend Analysis)
   Traffic analysis kadang kala disebut juga sebagai trend analysis, yaitu sebuah teknik yang digunakan oleh penerobos untuk menganalisa karakteristik data (panjang pesan, frekuensi pesan, dan sebagainya) dan pola pengiriman, untuk menjaring informasi yang berguna untuk penerobos.

   Untuk menangkal analisa lalulintas, digunakan cara yang mirip dengan untuk menangkal serangan terhadap kriptografi, antara lain:
   - Padding message
     Membuat semua message menjadi seragam bentuk datanya dengan menempatkan tempat kosong pada data.

- Sending noise
  Memasukkan data yang tidak mengandung informasi apapun digabungkan ke dalam informasi yang sesungguhnya untuk mengacaukan pesan yang sesungguhnya.
- Covert channel analysis
  Telah dijelaskan pada poin 2.2.1.

2. Akun Pemeliharaan (Maintenance Account)
   Salah satu cara untuk menerobos ke dalam sistem komputer adalah dengan menggunakan akun pemeliharaan yang masih memiliki password awal yang ditetapkan oleh pabrik pembuatnya atau password tersebut mudah ditebak. Akses fisik ke perangkat keras yang diserahkan pengelolaannya pada perorangan juga dapat menyebabkan pelanggaran keamanan.

   Penanggulangannya di UKM:
   Dilakukan di sisi administrasi sistem, dimana administrator keamanan bertugas untuk membuat akun user, menetapkan passwordnya, dan ekspirasi akun tersebut. Untuk perangkat yang memiliki password dari pabrik, misalnya router, sebaiknya diubah langsung saat mulai digunakan.
3. Penyerangan Pengaisan Data (Data-Scavenging Attacks)
   Pengaisan data adalah salah satu teknik penyerangan dengan cara menyatukan kembali potongan-potongan data informasi yang telah terpisah-pisah menjadi satu kesatuan data yang memiliki informasi berharga bagi organisasi/perusahaan. Terdapat dua tipe penyerangan pengaisan data yang umum digunakan:
   - Penyerangan melalui Keyboard
     Data dikais melalui sumberdaya yang tersedia ke user, pada kondisi sistem yang normal, yang duduk di depan keyboard menggunakan peralatan normal untuk mengumpulkan informasi.

     Penanggulangannya di UKM:
     Dilakukan pemasangan anti-virus dan anti-spyware yang dapat mendeteksi adanya program key logger.
   - Penyerangan melalui Laboratorium
     Data dikais dengan menggunakan peralatan elektronik yang canggih dan dengan perencanaan yang tepat.

     Penanggulangannya di UKM:
     Di sisi sistem ditangani oleh IDS dan IPS, sedangkan di sisi terminal dilakukan pemasangan anti-virus dan anti-spyware yang dapat mendeteksi adanya program virus atau trojan yang dapat melakukan penyerangan terdistribusi Distributed Denial of Service (DDoS).
4. Kerawanan IPL (IPL Vulnerabilities)
   Dimulai dari sistem itu sendiri, Initial Program Load (IPL), adalah spesifik sistem kerawanan yang spesifik suatu sistem dimana tipe sistem komputer atau mainframe tersentralisasi atau tipe LAN yang terdistribusi. Selama IPL, operator membawa fasilitas sistem. Operator ini mempunyai kemampuan membawa sistem ke dalam mode single user (satu user), tanpa adanya pengamanan secara penuh, yang dalam keadaan mode single user ini terdapat kewenangan tidak terbatas. Pada keadaan ini operator dapat membawa banyak program atau data tanpa otorisasi, mengganti kunci (password), mengganti nama banyak sumberdaya, atau mengganti waktu dan tanggal sistem. Operator dapat juga menentukan saluran

(port) data atau jalur komunikasi yang digunakan untuk mengirimkan informasi pada sekutunya di luar data center sistem komputer. Pada sebuah local area network (LAN), administrator sistem dapat melihat bagian dari tape, CD-ROM atau floppy disk, melewati keamanan sistem operasi pada hard drive.

Penanggulangannya di UKM:
Membatasi sistem operasi untuk tidak dapat berjalan di mode single user.

5. Pembajakan Alamat Jaringan (Network Address Hijacking)
   Penerobos dapat melihat kembali data lalu lintas dari server atau perangkat jaringan ke komputer seseorang, demikian juga dengan memodifikasi alamat perangkat atau pembajakan alamat jaringan. Hal ini memungkinkan penerobos memantau lalu lintas dari dan keluar perangkat tersebut untuk analisa data atau modifikasi atau mencuri file password dari server dan memperoleh akses ke akun pengguna. Dengan menyelusuri output data, penerobos dapat mengabaikan pengawasan dari terminal dan mengelabui log sistem.

   Penanggulangannya di UKM:
   Di sisi sistem ditangani oleh IDS yang akan mendeteksi IP spoofing atau perubahan MAC address dari suatu IP yang sama secara tiba-tiba. Di sisi client dapat diinstal perangkat lunak untuk mendeteksi IP spoofing. Contohnya untuk browser internet dapat diinstal plugin yang mendeteksi IP spoofing dari situs-situs yang dikunjungi.

5. Penutup

Keamanan adalah suatu proses, bukan produk. Jika Anda memasang firewall, IDS, honeypots (sarang madu) yang berfungsi sebagai jebakan, dan sebagainya, mungkin dapat menyediakan lapisan-lapisan untuk bertahan, akan tetapi peralatan paling canggih di dunia tidak akan menolong suatu sistem keamanan organisasi sampai organisasi tersebut mempunyai proses untuk upgrade sistem, instal patch, atau memeriksa keamanan pada sistem sendiri dengan metode lain.
Telah banyak organisasi dan perusahaan yang memakai IDS tetapi tidak memonitor file log, mereka instal anti-virus, anti-spyware, anti-spam, dan firewall, tetapi tidak melakukan upgrade dan update. Sehingga aman atau tidaknya suatu sistem komputer di suatu organisasi/perusahaan adalah juga terikat erat dengan peran manusianya.

Daftar Pustaka

ICSA Labs. 2005. *Standards for commercial security products are set by ICSA Labs*. Diakses 27 Oktober 2005, dari https://www.icsalabs.com/icsa/icsahome.php

Krutz, Ronald L., Russell Dean Vines. 2003. *The CISSP® Prep Guide: Gold Edition*. Indiana: Wiley Publishing, Inc.

Link, Rainer. 2004. *Mini-FAQ: "antivirus software for Linux/Unix"*. Diakses 11 Desember 2005, dari http://cvs.sourceforge.net/viewcvs.py/openantivirus/mini-faq/av-unix_e.txt?rev=HEAD

Microsoft Corporation. 2005. *e-mail*. Diakses 11 Desember 2005, dari http://www.microsoft.com/athome/security/email/default.mspx

Microsoft Corporation. 2005. *Microsoft Small Business Center*. Diakses 27 Oktober 2005, dari http://www.microsoft.com/smallbusiness/hub.mspx

Microsoft Corporation. 2005. *online activities*. Diakses 11 Desember 2005, dari http://www.microsoft.com/athome/security/online/default.mspx

Microsoft Corporation. 2005. *Security Bulletin Search*. Diakses 27 Oktober 2005, dari http://www.microsoft.com/technet/security/current.aspx

Microsoft Corporation. 2005. *spyware*. Diakses 11 Desember 2005, dari http://www.microsoft.com/athome/security/spyware/default.mspx

Microsoft Corporation. 2005. *viruses & worms*. Diakses 11 Desember 2005, dari http://www.microsoft.com/athome/security/viruses/default.mspx

Microsoft Corporation. 2005. *Windows Server 2003 Active Directory*. Diakses 11 Desember 2005, dari http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx

MIT Kerberos. 2005. *Kerberos: The Network Authentication Protocol*. Diakses 11 Desember 2005, dari http://web.mit.edu/kerberos/www/

Muhammad, Reza. 2003. *15 Jenis Serangan Cracker*. Indonesia: IlmuKomputer.Com. Diakses 27 Oktober 2005, dari http://ilmukomputer.com/populer/reza-cracker.php

Purbo, Onno W. 2003. *Ensiklopedia Serangan Denial of Service*. Indonesia: IlmuKomputer.Com. Diakses 27 Oktober 2005, dari http://ilmukomputer.com/populer/onno-dos.php

Purbosudibyo, Gani. 2003. *Mengenal Social Engineering*. Indonesia: IlmuKomputer.Com. Diakses 27 Oktober 2005, dari http://ilmukomputer.com/populer/gani-socialeng.php

Sourcefire, Inc. 2005. *Snort Documents*. Diakses 27 Oktober 2005, dari http://www.snort.org/docs/

Terpstra, John H. 2005. *Practical Exercises in Successful Samba Deployment*. Samba Team. Diakses 27 Oktober 2005, dari http://us2.samba.org/samba/docs/man/Samba-Guide/

The OpenLDAP Project. 2005. *OpenLDAP Software 2.3 Administrator's Guide*. Diakses 27 Oktober 2005, dari http://www.openldap.org/doc/admin23/

Ts, Jay, Robert Eckstein, David Collier-Brown. 2003. *Using Samba, 2nd Edition*. O'Reilly & Associates. Diakses 27 Oktober 2005, dari http://us2.samba.org/samba/docs/using_samba/toc.html