KAJIAN ATAS TATAKELOLA TEKNOLOGI INFORMASI: PENGERTIAN, PANDUAN-PANDUAN, SERTA CONTOH PENERAPAN

Michael Iskandar
Fakultas Ekonomi Universitas Katolik Parahyangan

Abstract

Governance of the firm's information technology (IT Governance) has become more and more important to the successful management of corporations around the world. To achieve IT Governance, each corporation may develop its own unique approach, or otherwise it may utilize a number of guidelines that have been developed, such as the Sarbanes-Oxley Act (SOX), Committee of Sponsoring Organizations of the Treadway Commission Framework (COSO), and Control Objectives for Information Technology (COBIT). This paper discusses IT Governance as a concept, explains some of the guidelines mentioned above that can be used to achieve it, attempts a categorization of those guidelines, and ends with an example. In this example the framework used is COBIT and the IT governance aspect evaluated is the business continuity plan.

Keywords: *IT governance, IT governance guidelines, COBIT, business continuity plan*

1. Pendahuluan

Tatakelola teknologi informasi (*IT Governance*) merupakan hal yang semakin banyak diusahakan oleh perusahaan-perusahaan, terutama perusahaan yang sudah berskala besar, atau telah melakukan IPO (*initial public offering*) sehingga telah menjadi perusahaan *go public*, atau perusahaan lain-lain yang telah menganggap bahwa teknologi informasi merupakan hal yang sangat penting bagi kelangsungan hidup perusahaan mereka. Makalah ini membahas tatakelola teknologi informasi mulai dari pengertian dasarnya, kemudian dibahas pula sejumlah panduan-panduan (*guidelines*) yang telah banyak dipergunakan oleh perusahaan-perusahaan. Akhirnya juga diusahakan sebuah studi kasus menggunakan *business continuity plan* dari Massachusetts Institute of Technology (MIT) yang dibandingkan dengan COBIT.

2. Pengertian Dasar Tatakelola Teknologi Informasi

Untuk memahami apa yang dimaksud dengan "tatakelola teknologi informasi", maka perlu dibahas terlebih dahulu tentang apa yang dimaksud dengan istilah "tatakelola" itu sendiri. Merupakan terjemahan dari istilah Bahasa Inggris, *governance*, kata ini memiliki arti "pemerintahan" (*government, rule*) dan "pengendalian" (*control*). [Barnhart, 1989:921]. Jadi istilah "tatakelola" memiliki makna "pengaturan" dan "pengendalian" atas sesuatu hal. Secara tersirat di dalam istilah *IT Governance* juga adalah makna dari *good governance*, yaitu bentuk *governance* yang benar, baik, dan bertanggung jawab. Yang dimaksud dengan "benar, baik, dan bertanggung jawab" adalah bahwa hal ini harus dilihat secara internal (dari kacamata perusahaan) maupun eksternal (dari kaca mata pihak luar perusahaan).

Akhirnya dapat disimpulkan bahwa *IT Governance* adalah pengaturan dan pengendalian yang dilakukan dalam usaha terlaksananya praktek-praktek yang benar dan bertanggung jawab, yaitu yang akan menguntungkan atau setidak-tidaknya tidak merugikan perusahaan dan para *stakeholder*, atas teknologi informasi yang dimiliki suatu perusahaan.

3. Bentuk-bentuk Tatakelola Teknologi Informasi

Berangkat dari pengertian di atas, maka dapat disimpulkan bahwa hal utama yang harus diadakan jika perusahaan hendak memiliki tatakelola teknologi informasi adalah membuat peraturan dan menyiapkan pengendalian atas teknologi informasi yang dimilikinya. Bagaimana cara pengadaan *IT governance* tersebut, sebenarnya dapat dikembangkan oleh masing-masing perusahaan, disesuaikan dengan kondisi perusahaan itu sendiri maupun kondisi lingkungannya. Pengecualian dari kebebasan pengembangan metode *IT governance* itu hanyalah jika perusahaan memang terikat secara hukum untuk melaksanakan *IT governance* dengan metode tertentu, misalnya karena merupakan peraturan pemerintah, atau karena tercantum dalam akte pendirian perusahaan atau merupakan hasil rapat umum pemegang sahamnya.

Meskipun demikian, telah pula tersedia sejumlah standard, kerangka kerja, ataupun kumpulan *best practices* yang sering dipergunakan oleh perusahaan-perusahaan yang hendak mengusahakan *IT governance*. Panduan-panduan itu adalah misalnya: [Wikipedia, 2006]

1. Sarbanes-Oxley Act (SOX)
2. Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework
3. Control Objectives for Information and Related Technology (COBIT).

4. Information Technology Infrastructure Library (ITIL)
5. ISO 27001
6. Information Security Management Maturity Model (ISM3)
7. Australian Standard for Corporate Governance of Information and Communication Technology (AS8015)
8. Capability Maturity Model (CMM)
9. Balanced Scorecard (BSC)
10. Six Sigma

Berbagai panduan *IT governance* itu tidaklah dapat dianggap setara. Misalnya, SOX adalah sebuah hukum (law) yang disusun dan diberlakukan di Amerika Serikat untuk menanggulangi terjadinya penipuan-penipuan akuntansi setelah terungkapnya skandal Enron, Arthur Andersen, dan WorldCOM. Isi dari SOX juga tidak seluruhnya berkait dengan *IT governance*, meskipun ada beberapa bagian, terutama *section* 404 yang sangat berpengaruh terhadap keharusan pengelolaan IT secara baik dan benar. Justru satu hal utama dari SOX sebenarnya tidak memiliki kaitan langsung dengan *IT governance*, yaitu dibentuknya sebuah lembaga dengan nama *Public Company Accounting Oversight Board* (PCAOB) untuk memantau pelaporan perusahaan-perusahaan yang telah go public.

PCAOB justru merekomendasikan kerangka kerja COSO untuk meyakinkan *IT governance* yang baik. Kerangka kerja ini ditujukan untuk *internal control* dan memiliki lima buah komponen yaitu:

1. *Control environment* (integritas, kode etik, gaya manajemen, dan lain-lain)
2. *Risk assessment*
3. *Control activities* (termasuk *segregation of duties*)
4. *Information and Communication*
5. *Monitoring*

Di lain pihak COBIT menunjukkan berbagai tujuan yang harus dicapai dalam rangka *good IT governance*. Berbeda dengan COSO yang menunjukkan lima jenis komponen, maka COBIT mendefinisikan 34 *high-level objectives*, yang kemudian dapat dirinci menjadi 215 *control objectives*. Tujuan-tujuan ini dikategorikan ke dalam empat domain yaitu: *Plan and Organize* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS), dan *Monitor and Evaluate* (ME).

Jika SOX adalah perangkat hukum, COSO menyediakan kerangka kerja dan COBIT menekankan teknik-teknik pencapaian tujuan *IT governance*, maka ITIL merupakan kumpulan tulisan-tulisan yang berisi sejumlah *best practices* di bidang pengendalian IT. Tulisan-tulisan itu dibagi menjadi dua kelompok besar yaitu tulisan tentang *service support* dan tentang *service delivery*.

ISO 27001 juga merupakan kumpulan *best practices,* ISM3 dan CMM merupakan *maturity models*, ASM8015 merupakan seperangkat standard, dan BSC serta Six Sigma, sebenarnya merupakan perkakas generik yang dipergunakan untuk melakukan manajemen perusahaan, namun dapat dipergunakan pula untuk mengusahakan tatakelola IT yang baik.

4. Diagram Metode-metode Tatakelola Teknologi Informasi

Berdasarkan pembahasan dalam sub-bab 3 di atas, maka dapat disimpulkan bahwa panduan-panduan *IT governance* dapat diklasifikasikan sebagai berikut:

1. Hukum / peraturan resmi (SOX)
2. Kerangka kerja (COSO, COBIT)
3. *Best practices* (ITIL, ISO 27001)
4. *Maturity models* (CMM, ISM3)
5. Standard (ASM8015)
6. Model manajemen generik (BSC, Six Sigma)

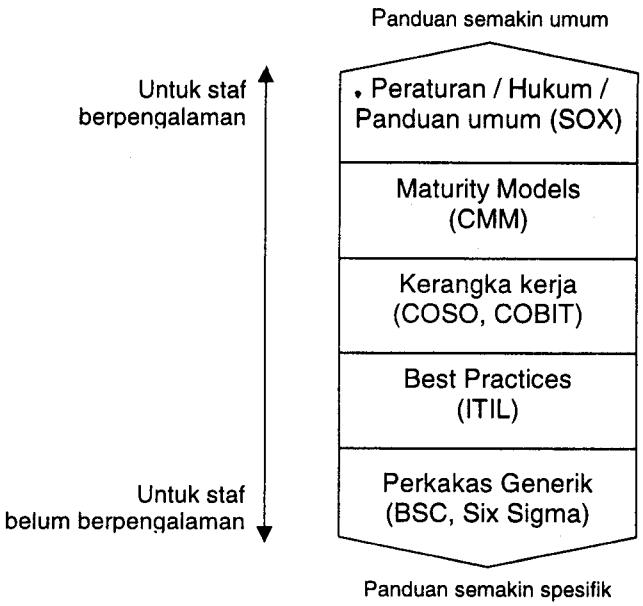
Klasifikasi di atas tidaklah bersifat *mutually exclusive* sepenuhnya, misalnya saja COBIT juga memiliki *maturity model* (yang dibuat berdasarkan *Computer Maturity Model* atau CMM), dan ITIL pun dapat dikategorikan sebagai kerangka kerja. Klasifikasi di atas lebih menekankan kepada gambaran umum yang diperoleh dari masing-masing panduan, dan bukan dari karakteristik detail panduan-panduan itu.

Metode atau panduan mana yang sebaiknya dipakai oleh perusahaan yang hendak melakukan *good IT governance*? Hal ini sangat tergantung dari karakteristik organisasi baik secara internal maupun secara eksternal (lingkungan organisasi). Misalkan saja, sebuah perusahaan yang telah melaksanakan Six Sigma di berbagai fungsi perusahaan itu, kemungkinan akan berhasil jika kemudian mencanangkan pencapaian *good IT governance* juga dengan menggunakan Six Sigma. Hal ini dikarenakan dua hal: (1) manajemen perusahaan ini telah menunjukkan komitmennya terhadap Six Sigma, dan (2) para pelaksana di perusahaan ini telah berpengalaman menggunakan Six Sigma. Justru jika perusahaan ini tiba-tiba membedakan metode untuk pencapaian *IT governance* dan memaksakan metode lain, misalnya COBIT, maka kemungkinan gagalnya usaha ini justru lebih tinggi.

Bagi perusahaan yang masih asing dengan semua metode atau panduan di atas, dapat mengevaluasi sejauh mana staf perusahaan lebih mampu dan lebih baik jika mengandalkan kreativitas dan pemecahan masalah sendiri, atau tidak. Bagi staf yang dapat diandalkan kemahirannya untuk mencapai *good IT governance* dengan caranya

sendiri, maka petunjuk-petunjuk umum adalah lebih baik, seperti misalnya SOX. Sebaliknya, jika staf kurang berpengalaman dalam hal *IT governance*, maka dapat menggunakan perkakas yang lebih spesifik seperti misalnya ITIL, BSC, atau COBIT.

Oleh karena itu, anjuran penggunaan metode, perkakas, atau panduan *IT governance* dapat dibandingkan dengan kemampuan manajemen dan staf perusahaan sebagai berikut:



Gambar 1. Klasifikasi Metode / Panduan IT Governance

Gambar di atas menunjukkan kesesuaian penggunaan panduan tertentu dengan tingkat kemahiran dan pengalaman staf yang harus menggunakannya. Asumsi pada gambar ini adalah bahwa (1) perusahaan tidak terikat oleh peraturan tertentu yang mewajibkan suatu bentuk panduan *IT governance*, dan (2) staf di perusahaan tersebut belum berpengalaman dengan panduan mana pun.

Alternatif lain dari penggunaan berbagai panduan *IT governance* yang disebutkan di atas adalah untuk mengkombinasikan antara beberapa pendekatan. Misalnya saja, untuk perencanaan strategik dipergunakan SOX, untuk perencanaan taktikal dipergunakan COBIT, dan untuk perencanaan operasional dipergunakan Six Sigma. Tentu harus diperhatikan agar memilih panduan-panduan yang saling mengisi dan tidak kontradiktif.

Sebuah contoh yang dapat disebutkan dari lembaga yang mengusahakan *good IT governance* tanpa perlu menggunakan panduan-panduan di atas adalah organisasi-organisasi di King County, Washington, Amerika Serikat. Khusus untuk *IT business continuity planning*, telah disusun sebuah dokumen *Guidelines for Implementing an Information Technology Business Continuity Program for King County Organizations.* Dokumen ini berisi panduan membuat rencana kontinuitas bisnis khusus bagian teknologi informasinya, dan sama sekali tidak menyinggung berbagai metode yang telah disebutkan di atas [King County Business Continuity Program, 2004].

5. Contoh Penerapan Tatakelola Teknologi Informasi di MIT

Dalam sub-bab ini dilakukan evaluasi kesesuaian *Business Continuity Plan* (BCP) yang diterapkan di Massachusetts Institute of Technology (MIT) pada tahun 1995, dengan COBIT 4.0 *high-level control objective* DS4, yaitu *ensure continuous service.* Perbandingan ini menarik dilakukan karena BCP yang disusun oleh MIT ini tidak mungkin dibuat berdasarkan COBIT, sebab COBIT 1.0 pun baru selesai disusun pada tahun 1996 [Wikipedia, 2006]. Sedangkan COBIT 4.0, sebagai versi yang paling mutakhir, baru dapat diperoleh pada tahun 2005 [The IT Governance Institute, 2005].

5.1. Penjelasan Singkat Business Continuity Plan MIT

Business Continuity Plan dari MIT dapat diperoleh dari situs web-nya, yang URLnya dapat dilihat di bagian Daftar Pustaka. *Business Continuity Plan* itu terdiri dari empat bagian yaitu: *Introduction, Design of the Plan, Team Descriptions,* dan *Recovery Procedures.* Secara garis besar, masing-masing bagian mengandung hal-hal sebagai berikut:

1. *Introduction*
   a. Memberikan penjelasan singkat dari keseluruhan dokumen ini.
2. *Design of the Plan*
   a. Menyebutkan pentingnya IT bagi kelangsungan operasional MIT.
   b. Menjelaskan hasil dari analisa risiko yang pernah dilakukan, serta rencana pelaksanaan *risk assessment* secara berkala.
   c. Tujuan BCP adalah menurunkan tingkat risiko.
   d. Rencana ini mengidentifikasi fungsi kritis dan memberikan panduan untuk mengantisipasi terjadinya bencana.
   e. BCP mendefinisikan tanggung jawab dari *Business Continuity Management Team.*
   f. Menyebutkan asumsi-asumsi yang dipergunakan dalam penyusunan BCP
   g. Pengembangan BCP, pengadaan *training*, serta pelaksanaan *review* atas BCP secara berkala.

h. Pengujian BCP, secara parsial maupun menyeluruh.
i. Deskripsi dari organisasi penanggulangan bencana, terdiri dari:
    i. *Administrative Computing Steering Committee*
    ii. *Business Continuity Management Team*
    iii. *Institute Support Team*
    iv. *Functional Area Recovery Management* (FARM)

    Juga dijelaskan pejabat-pejabat yang menjadi anggota masing-masing komite/team serta tanggung jawab / peran mereka.
j. Langkah-langkah yang harus ditempuh jika terjadi bencana, mulai dari *emergency plan* untuk menyelamatkan karyawan, hingga fase *backup* dan fase *recovery*. Juga menjelaskan secara cukup detail prosedur dan persyaratan yang harus dipenuhi untuk mengaktifkan *hot site* maupun *shell site*.
k. Menyebutkan empat kategori sistem yang dimiliki MIT, yaitu: category I (*critical*), category II (*essential*), category III (*necessary*), dan category IV (*desirable*).

3. *Team Descriptions*
    a. Menjelaskan secara lebih detail peran, tanggung jawab, dan *job description* dari masing-masing pejabat yang telah disebut dalam point 2.i di atas.
4. *Recovery Procedures*
    a. Menyebutkan nama dan nomor telepon dari semua pihak yang harus diberitahu jika terjadi bencana.
    b. Menyebutkan prosedur-prosedur secara rinci apa yang harus dilakukan setiap anggota team dalam menangani bencana.

Selain keempat bagian tersebut, juga disediakan beberapa *appendix* yang antara lain menyebutkan lokasi dari *emergency operations center*, *hot site*, serta *shell site*; jadwal hadir dari anggota *Business Continuity Management Team*, karena selalu harus ada anggota yang siap di lokasi untuk berjaga-jaga seandainya terjadi *emergency situation*; serta sebuah *Plan Distribution Matrix* yang mirip dengan *RACI Chart*.

5.2. *Maturity Level* dari BCP MIT

COBIT menerapkan model *maturity* sebagai berikut: *non-existent, initial, repeatable, defined, managed*, dan *optimized*. Dalam sub-bab ini BCP MIT dievaluasi untuk menemukan *maturity level*-nya. Pada tabel berikut ini dijelaskan pengertian masing-masing level tersebut menurut COBIT 4.0 untuk DS4.

TABEL 1
COBIT MATURITY LEVEL UNTUK DS4

0 Non-existent (tidak ada) jika Tidak ada pemahaman akan risiko, kelemahan-kelemahan dan ancaman terhadap operasi IT ataupun pengaruh dari hilangnya pelayanan IT atas bisnis. Kontinuitas pelayanan IT tidak dianggap cukup penting untuk menjadi perhatian manajemen.
1 Initial / Ad Hoc (awal / ad hoc) jika Tanggung jawab untuk mengadakan pelayanan IT secara kontinu ditetapkan secara informal dan otoritas untuk melaksanakan tanggung jawab itu terbatas. Manajemen mulai menyadari risiko-risiko yang terkait dengan, dan kebutuhan akan pelayanan IT secara kontinu. Fokus dari perhatian manajemen atas pelayanan IT secara kontinu adalah pada sumber daya infrastruktur, dan bukan pada jasa pelayanan IT. Pengguna berusaha mengatasi sendiri jika ada gangguan dalam pelayanan IT. Tanggapan dari bagian IT atas gangguan-gangguan besar bersifat reaktif dan tanpa persiapan. Penonaktifan layanan sudah dijadwalkan sesuai dengan kebutuhan bagian IT, namun tidak memperhatikan kebutuhan bisnis.
2 Repeatable but Intuitive (Dapat diulang tetapi secara intuitif) jika Sudah ada keputusan resmi tentang tanggung jawab untuk meyakinkan pelayanan IT secara kontinu. Pendekatan-pendekatan untuk meyakinkan pelayanan IT secara kontinu masih terfragmentasi. Pelaporan tentang ketersediaan sistem bersifat sporadis, mungkin saja tidak lengkap, dan tidak memperhatikan pengaruh terhadap bisnis. Tidak ada rencana kontinuitas IT yang terdokumentasi, meskipun ada komitmen untuk menyediakan pelayanan secara kontinu dan prinsip-prinsip utamanya telah diketahui. Telah dibuat daftar sistem-sistem dan komponen-komponen penting, tetapi daftar itu mungkin kurang dapat dipercaya. Praktek pelayanan IT secara kontinu telah muncul tetapi keberhasilannya lebih bergantung pada individu.
3 Defined Process (Proses Terdefinisi) jika Tidak ada ketidakjelasan bahwa manajemen memiliki ketanggunggugatan (accountability) atas pelayanan IT secara kontinu. Tanggung jawab untuk perencanaan jasa pelayanan IT secara kontinu terdefinisikan dan teralokasikan dengan jelas. Rencana kontinuitas IT sudah didokumentasi dan berdasarkan pada pentingnya sistem maupun pengaruh bisnis. Sudah ada pelaporan berkala tentang pengujian atas kontinuitas pelayanan. Individu memiliki inisiatif untuk mengikuti standard dan untuk memperoleh pelatihan dalam kaitan dengan penanganan insiden besar atau bencana. Manajemen memberikan komunikasi secara konsisten tentang kebutuhan akan perencanaan pelayanan IT secara kontinu. Komponen-komponen yang mudah diperoleh dan system redundancy telah diadakan. Daftar sistem-sistem dan komponen-komponen penting telah ada dan selalu diperbaharui.

4 Managed and Measurable (Dikelola dan Dapat Diukur) jika
Tanggung jawab dan standard untuk pelayanan IT secara kontinu telah diadakan dan diwajibkan. Tanggung jawab untuk merawat rencana pelayanan IT secara kontinu telah ditetapkan. Aktivitas-aktivitas perawatan didasarkan pada hasil pengujian pelayanan IT secara kontinu, praktek-praktek internal yang baik, dan perubahan lingkungan IT dan bisnis. Data terstruktur tentang pelayanan IT secara kontinu dikumpulkan, dianalisa, dilaporkan, dan menimbulkan reaksi. Pelatihan tentang proses-proses pelayanan IT secara kontinu diadakan secara formal dan bersifat wajib. Praktek-praktek yang baik untuk mengadakan ketersediaan sistem dilaksanakan secara konsisten. Praktek-praktek mengenai ketersediaan sistem dan perencanaan pelayanan IT secara kontinu saling mempengaruhi. Jika terjadi insiden yang menyebabkan terputusnya pelayanan IT akan diklasifikasikan dan kecenderungan dari masing-masing insiden telah diketahui oleh semua pihak yang terlibat. KGI dan KPI untuk pelayanan IT secara kontinu telah dikembangkan dan disetujui namun mungkin belum terukur secara konsisten.

5 Optimised (Teroptimasi) jika
Proses-proses pelayanan IT secara kontinu yang terintegrasi telah mempertimbangkan benchmarking dan praktek-praktek terbaik dari luar. Rencana kontinuitas IT telah terintegrasi dengan rencana kontinuitas bisnis dan dirawat secara rutin. Kebutuhan-kebutuhan akan pelayanan IT secara kontinu telah terpenuhi melalui vendor dan pemasok besar. Pengujian global telah dilakukan atas rencana kontinuitas IT dan hasil pengujian dipakai sebagai masukan untuk mengupdate rencana itu. Pengumpulan dan analisis atas data dipergunakan untuk terus menerus memperbaiki proses. Praktek-praktek mengenai ketersediaan sistem dan perencanaan pelayanan IT secara kontinu sepenuhnya selaras. Manajemen meyakinkan bahwa tidak akan terjadi bencana atau insiden besar akibat satu titik kegagalan saja. Praktek-praktek eskalasi telah diketahui dan sepenuhnya diterapkan. KGI dan KPI atas keberhasilan pengadaan pelayanan IT secara kontinu diukur secara sistematis. Manajemen menyesuaikan perencanaan atas pelayanan IT secara kontinu terhadap KGI dan KPI.

Apabila deskripsi BCP MIT dibandingkan dengan karakteristik-karakteristik masing-masing *level of maturity*, maka dapat kita simpulkan bahwa BCP MIT telah mencapai level 4, yakni *managed and measurable*. Hal ini terbukti antara lain dengan adanya tanggung jawab yang jelas (seluruh Bagian 3, *Team Descriptions* menjelaskan tentang hal ini), serta adanya perawatan (*maintenance*) secara berkala (seperti yang disebutkan di 2.g.).

5.3. Aturan Tatakelola BCP MIT Menurut COBIT 4.0 DS4

Dalam COBIT 4.0 DS4, yakni *ensure continuous service*, disebutkan bahwa terdapat sepuluh hal yang harus diatur, sebagai berikut:

1. Kerangka kerja kontinuitas IT
2. Rencana kontinuitas IT
3. Sumber daya IT yang bersifat penting (*critical*)
4. Perawatan (*maintenance*) rencana kontinuitas IT
5. Pengujian atas rencana kontinuitas IT
6. Pelatihan rencana kontinuitas IT
7. Penyebarluasan rencana kontinuitas IT
8. Rencana kegiatan-kegiatan untuk *recovery* dan pengaktifan kembali layanan IT
9. Penyimpanan backup tidak pada lokasi (*off site*)
10. *Review* setelah pengaktifan kembali

Ternyata, dari kesepuluh hal yang harus diatur menurut COBIT 4.0 untuk DS4: *ensure continuous service*, yang belum tercantum dalam BCP dari MIT adalah yang ke-9 dan ke-10. Jadi, berikut ini adalah contoh kebijakan (aturan) yang dapat dikembangkan oleh MIT untuk melengkapi BCP-nya. Format dari kebijakan ini mengikuti *template* kebijakan yang telah disusun oleh lembaga SANS [The SANS Institute, 2007].

TABEL 2.
CONTOH KEBIJAKAN *IT SECURITY* (A)

Kebijakan Backup Data

1.0. Tujuan
Kebijakan ini dibuat dengan tujuan agar keamanan data yang dimiliki institusi terjamin keselamatannya baik dari bencana yang berupa force majeure maupun yang tidak.

2.0. Ruang Lingkup
Data yang dimaksud di sini adalah semua data berkenaan dengan kegiatan akademik mahasiswa, data-data keuangan lembaga, data-data kepegawaian baik data dosen, staf administrasi, serta non-administrasi, data-data inventaris, dan data-data alumni.

3.0. Kebijakan
3.1. Frekuensi Backup
Seluruh data yang disebut dalam point 2.0 harus di-backup secara berkala yaitu sebulan sekali untuk data-data keuangan lembaga, serta satu kuartal sekali untuk data-data yang lain.

3.2. Lokasi Backup
Seluruh backup data yang disebut dalam point 3.1. harus disimpan di lokasi yang berjarak sekurang-kurangnya 15 kilometer dari lokasi penyimpanan data utamanya.

4.0. Hukuman
Setiap karyawan yang bertanggung jawab melakukan backup dan diketahui telah melanggar kebijakan ini dapat dikenakan hukuman, di mana hukuman yang terberat adalah pemutusan hubungan kerja (PHK).

5.0. Definisi

Istilah	Definisi
Data	Setiap item berupa teks, angka, gambar, suara, atau video, yang tersimpan dalam database.
Backup data	Data cadangan yang merupakan hasil copy dari data utama (asli).

6.0. Sejarah revisi

TABEL 3.
CONTOH KEBIJAKAN *IT SECURITY* (B)

Kebijakan Post-resumption Review

1.0. Tujuan
Setiap insiden yang menyebabkan kegagalan sistem-sistem yang termasuk kategori critical function, essential function, dan/atau necessary function akan menimbulkan respons sesuai dengan Business Continuity Plan (BCP) yang telah disusun. Kebijakan ini dibuat dengan tujuan agar BCP serta penerapannya mengalami evaluasi dan perbaikan secara kontinu.

2.0. Ruang Lingkup
Post-resumption review ini mencakup seluruh prosedur-prosedur yang dilaksanakan dalam usaha mengatasi insiden yang telah dialami, serta semua hal yang terkait dengan prosedur-prosedur tadi.

3.0. Kebijakan
Selambat-lambatnya 3 (tiga) bulan setelah insiden tersebut terjadi, sudah harus selesai dilaksanakan sebuah review atas efektivitas prosedur-prosedur yang telah dilaksanakan dalam menanggulangi insiden tersebut.

4.0. Pelaksana
Team yang melakukan review adalah FARM team di mana insiden tersebut terjadi, dipimpin oleh FARM Team Coordinator terkait.

5.0. Pelaporan
Hasil dari review ini harus dilaporkan kepada Information Security Officer. Jika Information Security Officer menganggap perlu, maka ia dapat meneruskan laporan ini kepada ketua Administrative Computing Steering Committee

6.0. Hukuman
Setiap karyawan yang bertanggung jawab melakukan post-resumption review dan diketahui telah melanggar kebijakan ini dapat dikenakan hukuman, di mana hukuman yang terberat adalah pemutusan hubungan kerja (PHK).

7.0. Definisi

Istilah	Definisi
Post-resumption review	Sebuah review yang dilakukan setelah pelaksanaan prosedur-prosedur dalam BCP dikarenakan terjadinya insiden yang mengganggu kontinuitas layanan IT.

8.0. Sejarah revisi

5.4. Ukuran-ukuran Penilaian

COBIT juga mensyaratkan adanya ukuran (*metrics*) yang dapat dipergunakan untuk melakukan penilaian. Dalam BCP dari MIT ini, semua *metrics* adalah berupa satuan waktu. Sebagai contoh, di awal bagian *Design of the Plan*, disebutkan bahwa:

> *"The Institute's Business Continuity Plan is designed to reduce the risk to an acceptable level by ensuring the restoration of Critical processing within __ hours, and all essential production (Category II processing) within _____ week(s) of the outage."*

Meskipun dalam dokumen yang boleh dibaca oleh khalayak ramai ini jumlah jam ataupun pekan yang merupakan batas *recovery* itu dirahasiakan oleh MIT, namun pada prinsipnya dapat dilihat bahwa untuk penilaian dari efektivitas BCP itu akan mengambil ukuran waktu.

6. Kesimpulan

Dari pembahasan ini dapat disimpulkan bahwa tatakelola teknologi informasi adalah merupakan hal yang tidak mudah dilaksanakan, dikarenakan banyaknya aspek yang harus diperhatikan. Manajemen perusahaan dapat memutuskan untuk mengembangkan pendekatannya sendiri untuk mencapai *good IT governance*, atau dapat pula menggunakan sejumlah panduan yang telah dikembangkan oleh berbagai lembaga yang memiliki perhatian tentang hal ini.

Daftar Pustaka

Barnhart, C.L., and Barnhart, R.K. (ed.), (1989) *The World Book Dictionary*, Volume One A-K, World Book Inc., Chicago.

Wikipedia (2006), *Information Technology Governance*, http://en.wikipedia.org/wiki/IT_governance, diakses tanggal 13 Oktober 2006 pukul 5:20.

King County Business Continuity Program (2004), *Guidelines for Implementing an Information Technology Business Continuity Program for King County Organizations*, http://www.metrokc.gov/oirm/services/standards/BC_Guidelines.pdf#search=%22information%20technology%20continuity%20plan%22, diakses tanggal 11 Oktober 2006 pukul 4:21.

The IT Governance Institute (2005), *COBIT 4.0*, USA.

Massachusetts Institute of Technology (1995), *MIT Business Continuity Plan*, http://web.mit.edu/security/www/pubplan.htm, diakses tanggal 11 Oktober 2006 pukul 4:13.

The SANS Institute (2007), *The SANS Security Policy Project*, http://www.sans.org, diakses tanggal 4 Februari 2007 pukul 11:10.