MODUL PERTEMUAN ONLINE 14
REVIEW MATERI

1. VAL IT

Val IT, adalah salah satu metoda yang dapat digunakan untuk memberikan gambaran yang jelas akan manfaat investasi TI pada organisasi. Val IT merupakan konsep baru yang diluncurkan oleh Information Technology Governance Institute (ITGI) sebagai sebuah kerangka kerja standar untuk melengkapi kerangka kerja tata kelola TI yang sudah lama dirilis dan dipergunakan secara luas yaitu COBIT. Karena Val IT merupakan pelengkap COBIT, maka dalam beberapa hal, asumsi yang digunakan serta cara pendeskripsian kerangka kerjanya sangat mirip dan sangat erat kaitannya dengan COBIT. Val IT terdiri atas sekumpulan prinsip dasar dan 3 proses utama untuk mengukur nilai TI. Masing-masing proses kemudian dirinci lagi menjadi beberapa item manajemen praktis seperti halnya pada COBIT.

IT Governance Institute (ITGI), lembaga yang mengeluarkan kerangka kerja tatakelola TI, sekitar bulan April 2006 mengeluarkan kerangka kerja pelengkap yang dapat digunakan untuk mengukur nilai TI yang disebut dengan Val IT. Saat ini, Val IT berfokus pada investasi TI baru dan selanjutnya akan dikembangkan hingga meliputi semua layanan dan asset TI. Tujuan inisiatif Val IT meliputi riset, publikasi dan dukungan layanan untuk membantu manajemen memahami nilai investasi TI dan menjamin bahwa organisasi dapat memperoleh nilai optimal atas investasi TI dalam konteks biaya dan resiko yang dapat diterima.

Val IT terdiri atas pedoman, proses dan beberapa saran praktis untuk membantu pihak manajemen dan eksekutif untuk memahami dan menjalankan perannya dalam investasi TI. Beberapa manfaat yang dapat diperoleh dari implementasi Val IT adalah sebagai berikut:

a. Meningkatkan pemahaman dan transparansi atas biaya, resiko, dan manfaat yang dihasilkan dari keputusan manajamen yang dilandasi oleh informasi yang memadai.
b. Meningkatkan kemampuan memilih investasi yang memiliki potensial pengembalian manfaat terbesar.
c. Meningkatkan kecenderungan keberhasilan dalam menjalankan investasi yang dipilih sehingga investasi tersebut dapat menghasilkan manfaat sesuai yang diharapkan.

d. Mengurangi biaya dengan hanya mengerjakan apa yang seharusnya dikerjakan dan segera mengambil tindakan korektif atau menghentikan investasi yang tidak menghasilkan potensi manfaat yang diharapkan.
e. Mengurangi resiko kegagalan, khususnya kegagalan yang beresiko tinggi.
f. Mengurangi 'kejutan' yang berhubungan dengan biaya dan delivery TI, sehingga dapat meningkatkan nilai bisnis, mengurangi biaya yang tidak perlu dan meningkatkan kepercayaan terhadap IT secara keseluruhan.

Val IT terdiri atas sekumpulan prinsip dasar dan sejumlah proses yang didasari oleh prinsip-prinsip tersebut, yang selanjutnya diturunkan menjadi sekumpulan manajemen praktis utama. Hubungan antar prinsip dasar dan proses serta kaitannya dengan COBIT dapat dilihat pada Gambar 2.

Gambar 1. Keterkaitan Konsep Val IT dengan COBIT

Beberapa prinsip dasar yang menjadi landasan Val IT adalah sebagai berikut:

a. Investasi TI yang mendukung bisnis akan dikelola sebagai portofolio investasi.
b. Investasi TI yang mendukung bisnis akan meliputi seluruh aktivitas yang diperlukan untuk mencapai nilai bisnis.
c. Investasi TI yang mendukung bisnis akan dikelola melalui seluruh siklus hidup ekonomis investasi tersebut.
d. Praktisi *value delivery* akan mengenali bahwa ada berberapa katagori yang berbeda atas investasi yang harus dievaluasi dan dikelola dengan cara yang berbeda pula.

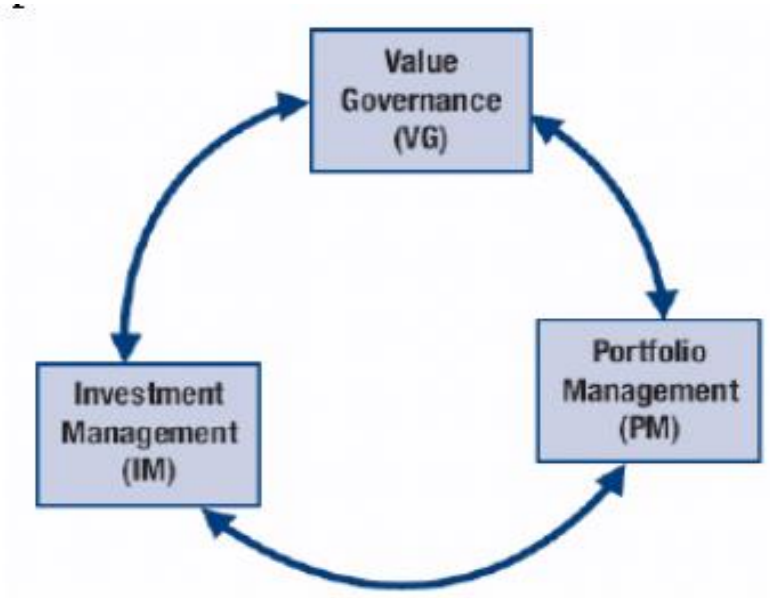
e. Praktisi *value delivery* akan mendefinisikan dan memonitor parameter pengukuran utama yang akan memberikan respon yang cepat terhadap perubahan atau deviasi yang terjadi.
f. Praktisi *value delivery* akan mengajak semua pihak yang berkepentingan dan menetapkan akuntabilitas yang sesuai terhadap kapabilitas yang harus dihaislkan dan realisasi manfaat bisnis.
g. Praktisi *value delivery* akan secara kontinyu dimonitor, dievaluasi dan ditingkatkan

Yang dimaksud dengan praktisi *Value Delivery* adalah orang atau fungsi yang bertanggung jawab untuk merealisasikan manfaat atas investasi TI pada perusahaan.

Untuk memperoleh hasil sebuah investasi, prinsip Val IT harus diterapkan oleh pihak yang berkepentingan, melalui tiga proses berikut:

- *Value governance(VG)*
- *Portfolio management (PM)*
- *Investment management (IM)*

Keterkaitan antara tiga proses tersebut dapat dilihat pada Gambar 3.



Gambar 2. Keterkaitan antara 3 proses pada Val IT

Value Governance (VG):

Tujuan VG adalah untuk mengoptimasi nilai yang diperlah atas investasi IT dengan cara:

- Menetapkan tata kelola, mengontrol dan memonitor kerangka kerjanya.

- Menyediakan arahan strategis bagi investasi
- Mendefinisikan karakteristik portofolio investasi.

Rincian pedoman praktis pada Value Governance adalah sebagai berikut:

VG1 Ensure informed and committed leadership
VG2 Define and implement processes.
VG3 Define roles and responsibilities.
VG4 Ensure appropriate and accepted accountability.
VG5 Define information requirements.
VG6 Establish reporting requirements.
VG7 Establish organisational structures.
VG8 Establish strategic direction.
VG9 Define investment categories.
VG10 Determine a target portfolio mix.
VG11 Define evaluation criteria by category.

Portfolio Management (PM)

Tujuan PM adalah untuk menjamin bahwa semua portofolio investasi IT selaras dan memberikan kontribusi optimal terhadap sasaran strategis organisasi dengan cara:

- Menetapkan dan mengelola profil sumber daya
- Mendefinisikan batasan investasi.
- Mengevaluasi, prioritasi dan memilih, menunda atau menolak investasi baru.
- Mengelola portofolio secara keseluruhan.
- Memonitor dan mengevaluasi kinerja portofolio

Portfolio Management dilengkapi dengan 14 pedoman praktis sebagai berikut:

PM1 Maintain a human resource inventory.
PM2 Identify resource requirements.
PM3 Perform a gap analysis.
PM4 Develop a resourcing plan.
PM5 Monitor resource requirements and utilisation.
PM6 Establish an investment threshold.
PM7 Evaluate the initial programme concept business case.
PM8 Evaluate and assign a relative score to the programme business case.
PM9 Create an overall portfolio view.
PM10 Make and communicate the investment decision.
PM11 Stage-gate (and fund) selected programmes.

PM12 Optimise portfolio performance.
PM13 Re-prioritise the portfolio.
PM14 Monitor and report on portfolio performance.

Investment Management (IM)

Tujuan investment management adalah untuk menjamin bahwa program investasi TI di organisasi dapat memberikan hasil yang optimal dengan biaya yang masuk akal dan dalam batas resiko yang masih dapat diterima, dengan cara:

- Identifikasi kebutuhan bisnis
- Membangun pemahaman yang jelas atas kandidat program investasi
- Menganilisi alternative
- Mendefinisikan program dan mendokumentasikan sebuah business case secara rinci termasuk menguraikan secara jelas dan terinci manfaat program tersebut bagi perusahaan.
- Menetapkan kejelasan akuntabilitas dan kepemilikan program.
- Memonitor dan melaporkan kinerja program

Rincian pedoman praktis pada Investment Management adalah sebagai berikut:

IM1 Develop a high-level definition of investment opportunity.
IM2 Develop an initial programme concept business case.
IM3 Develop a clear understanding of candidate programmes.
IM4 Perform alternatives analysis.
IM5 Develop a programme plan.
IM6 Develop a benefits realisation plan.
IM7 Identify full life cycle costs and benefits.
IM8 Develop a detailed programme business case.
IM9 Assign clear accountability and ownership.
IM10 Initiate, plan and launch the programme.
IM11 Manage the programme.
IM12 Manage/track benefits.
IM13 Update the business case.
IM14 Monitor and report on programme performance.
IM15 Retire the programme.

Beberapa pertimbangan penggunaan kerangka Val IT adalah:

a. Val IT relatif baru, saat ini hanya tersedia satu contoh kasus yaitu ING sehingga pengalaman praktisnya belum banyak. Meskipun kerangka kerjanya sudah lengkap dan sudah dipublikasikan secara luas, secara keseluruhan metodologinya masih dalam tahap penelitian.

- Val IT sangat erat terkait dengan COBIT, tetapi Val IT tidak memerlukan COBIT, tetapi akar pemikirannya adalah COBIT. Organisasi yang sudah memahami dan sepakat untuk menggunakan COBIT akan lebih mudah mengadopsi dan mengadaptasi Val IT. Karena Val IT relatif baru, maka hanya sedikit contoh studi kasus yang dapat dijadikan sumber pengalaman praktis.

2. STRATEGI TATA KELOLA

Tata kelola Teknologi Informasi adalah sebuah kerangka kebijakan, prosedur dan kumpulan proses-proses yang bertujuan untuk mengarahkan dan mengendalikan perusahaan untuk pencapaian tujuan perusahaan dengan memberikan tambahan nilai bisnis, melalui penyeimbangan keuntungan dan resiko TI beserta proses-proses yang ada di dalamnya. Mereka bertanggung jawab terhadap arah strategi organisasi, memastikan tujuan organisasi dapat tercapai dan sumber daya organisasi telah dimanfaatkan dengan tepat. Tata kelola TI juga membutuhkan pengaturan yang tepat untuk menggabungkan strategi TI dan pemanfaatan sumber daya TI untuk memberikan keuntungan yang kompetitif bagi organisasi. Secara tidak langsung, tata kelola TI menggunakan prinsip-prinsip tata kelola organisasi terhadap unit TI.

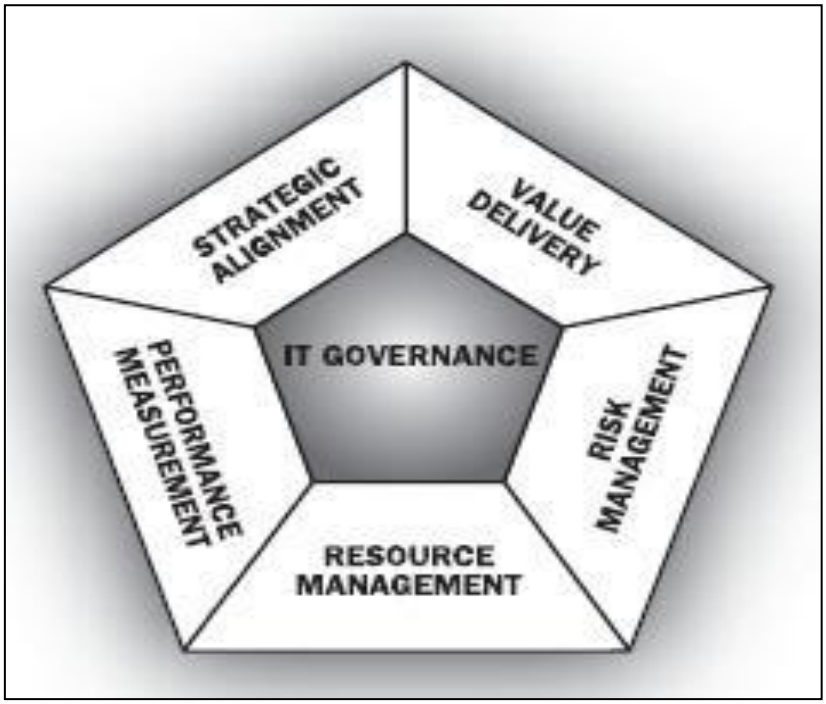
Jadi definisi dari Tata Kelola TI adalah suatu tanggung jawab yang akan di laksanakan oleh direksi yang semuanya melibatkan pimpinan, struktur organisasi, dan proses untuk memastikan bahwa TI menjadi pendukung dalam realisasi strategi suatu perusahaan. Selain itu dalam tatakelola bidang IT terdapat lima bidang utama dalam Tata Kelola TI, yaitu:

Tata kelola TI mencakup area sebagaimana ditunjukan pada gambar 3 dari kelima fokus area tata kelola TI dua diantaranya: value delivery and risk management merupakan outcome, sedang tiga lainnya merupakan driver (pendorong) : strategic alignment, resource management dan performace measurement: kelima hal ini semuanya digerakkan oleh stakeholder value.

a. Penyesuaian strategis (Strategic Allignment), penerapan TI harus mendukung pencapaian misi perusahaan. Strategi TI harus benar-benar mendukung strategi bisnis perusahaan.
b. Penambahan nilai (Value Delivery), penerapan TI harus memberikan nilai tambah bagi pencapaian misi perusahaan.
c. Pengelolaan resiko (Risk Management), penerapan TI harus disertai dengan identifikasi terhadap resiko-resiko TI, sehingga dapat

mengatasi dampak yang ditimbulkan olehnya. Resiko penerapan TI dapat berupa virus, penyalahgunaan hak akses, kesalahan/kerusakan sistem, kerusakan sistem pendukung dan lain-lain.

d. Pengelolaan sumber daya (Resource Management), penerapan TI harus didukung sumber daya yang memadai dan penggunaan sumber daya yang optimal.
e. Pengukuran kinerja (Performance Measurement), penerapan TI harus diukur dan dievaluasi secara berkala, untuk memastikan bahwa investasi dan kinerja TI sesuai dengan kebutuhan bisnis perusahaan.



Gambar 3 Fokus Area tata kelola TI [ITGI, 2005]

3. AUDIT SI

Audit Sistem Informasi memiliki beberapa fokus tujuan, salah satunya adalah pada tata kelola TI atau *IT Governance*. Tata kelola TI adalah suatu cabang dari tata kelola perusahaan yang terfokus pada sistem teknologi informasi (TI) serta manajemen kinerja dan risikonya.

IT governance adalah istilah inklusif yang mencakup sistem informasi, teknologi, dan komunikasi, bisnis, masalah hukum dan lainnya, dan

semua *stakeholder* bersangkutan, direktur, manajemen senior, pemilik proses, TI pemasok, pengguna dan auditor.

Jenis-jenis audit Sistem Informasi dikelompokkan berdasarkan Luas Pemeriksaan, Bidang Pemeriksan dan Kelompok Pelaksana Audit (Auditor).

a. Jenis-jenis audit ditinjau dari luas pemeriksaan
    1) **Pemeriksaan Umum *(General Audit)***
       Merupakan suatu pemeriksaaan umum atas laporan keuangan yang dilakukan oleh Kantor Akuntan Publik (KAP) yang indipendent dengan tujuan dapat menilai sekaligus memberikan opini mengenai kewajaran laporan keuangan.
    2) **Pemeriksaan Khusus *(Special Audit)***
       Merupakan suatu pemeriksaan yang hanya terbatas hanya pada permintaan audit yang dilakukan oleh Kantor Akuntan Publik (KAP). Dengan memberikan opini
b. Jenis-jenis audit ditinjau dari bidang pemeriksaan
    1) **Audit Laporan Keuangan (*Financial Statement Audit)***
       Berkaitan dengan kegiatan mengumpulkan dan mengevaluasi bukti tentang laporan-laporan suatu entitas dengan tujuan memberikan pendapat (opini) tentang laporan tersebut apakah sesuai dengan kriteria yang ditetapkan sesuai prinsip-prinsip akuntansi yang berlaku umum.
    2) **Audit Operasional *(Management Audit)***
       Adalah jenis pemeriksaan terhadap kegiatan operasi suatu perusahaan. meliputi kebijakan akuntansi dan kebijakan operasional manajemen yang telah ditetapkan, dengan tujuan untuk mengetahui kegiatan operasi yang dilakukan berjalan secara efektif dan efisien.
    3) **Audit Ketaatan *(Compliance Audit)***
       Audit ketaatan berfungsi untuk menentukan sejauh mana perusahaan mentaati peraturan, kebijakan, peraturan pemerintah bahkan hukum yang harus dipatuhi oleh entitas yang di audit.
    4) **Audit Sistem Informasi**
       Yaitu pemeriksaan yang dilakukan Kantor Akuntan Publik (KAP) terhadap perusahaan yang melakukan proses data akuntansi, umumnya menggunakan system *Elektronik Data Processing*(EDP). Auditor harus memperhatikan hal-hal berikut :
        - Perlengkapan keamanan melindungi perlengkapan computer baik program, komunikasi, atau data dari akses yang tidak sah, modifikasi bahkan penghancuran.

- Pengembangan program yang dilakukan atas otorisasi khusus dan umum dari pihak manajemen perusahaan.
- Pemrosesan transaksi, file, laporan dan catatan computer dengan akurat dan lengkap.
- Data file laporan yang tersimpan di computer sangat dijaga kerahasiaanya.

5) **Audit Forensik**

Tujuan dilakukan audit forensic adalah sebagai upaya pencegahan terjadinya kecurangan (*fraud).* Hal yang dapat dilakukan audit forensik termasuk :

- Investigasi kriminal
- Indikasi kecurangan dalam bisnis atau karyawan
- Mengetahui kerugian suatu bisnis

6) **Audit Investigasi**Yang dimaksud audit investigasi adalah serangkaian kegiatan mengenali *(recorganized),*menidentifikasi *(Identify)* dan menguji *(examine)* fakta-fakta dan informasi yang ada guna mengungkap kejadian yang sebenarnya dalam rangka pembuktian demi mendukung proses hukum atas dugaan penyimpangan yang dapat merugikan keuangan suatu entitas (organisasi/perusahaan/negara/daerah).

7) **Audit Lingkungan**

Menurut (Kep. Men. LH 42/1994) audit lingkungan adalah proses manajemen yang meliputi evaluasi secara sistematik, tercatat (terdkumentasi), serta obyektif tentang bagaimana suatu kinerja manajemen organisasi yang bertujuan memfasilitasi kendali manajemen terhadap upaya pengendalian dampak lingkungan dan pemanfaatan kebijakan usaha terhadap perundang-undangan tentang pengelolaan lingkungan.

c. Jenis-jenis audit ditinjau dari kelompok pelaksana audit (auditor)

1) Auditor Internal

Mempunyai tugas membantu manajemen puncak *(top management)* dalam mengawasi asset *(saveguard of asset)* dan mengawasi kegiatan operasional perusahaan sehari-hari. bekerja untuk perusahaan yang mereka audit, oleh karena itu tugas auditor intern adalah mengaudit manajemen perusahaan termasuk *compliance* audit.

2) Auditor Ekstern

Bekerja untuk lembaga/kantor akuntan publik (pihak ke-3) yang statusnya diluar struktur perusahaan yang mereka audit dan

bekerja secara independent dan objektif. Umumnya auditor ekstern menghasilkan laporan *financial* audit.

3) **Auditor Pajak**
   Mempunyai tugas melakukan ketaatan wajib pajak yang diaudit menurut undang-undang perpajakan yang berlaku. Di Indonesia dilaksanakan oleh Direktorat Jendral Pajak (DJP) yang berada dibawah naungan Departemen Keuangan Republik Indonesia.
4) **Auditor Pemerintah**
   Adalah lembaga yang mempunyai tugas menilai kewajaran informasi laporan keuangan instansi pemerintah atas pelaksanaan program dan penggunaan asset milik pemerintah. Audit instansi pemerintah umumnya dilaksanakan oleh Badan Pemeriksa Keuangan (BPK) atau Badan Pemeriksa Keuangan dan Pembangunan (BPKP).

4. LIMA STANDAR REGULASI YANG BERPERAN DALAM PENGAMANAN PUSAT DATA PEMERINTAHAN

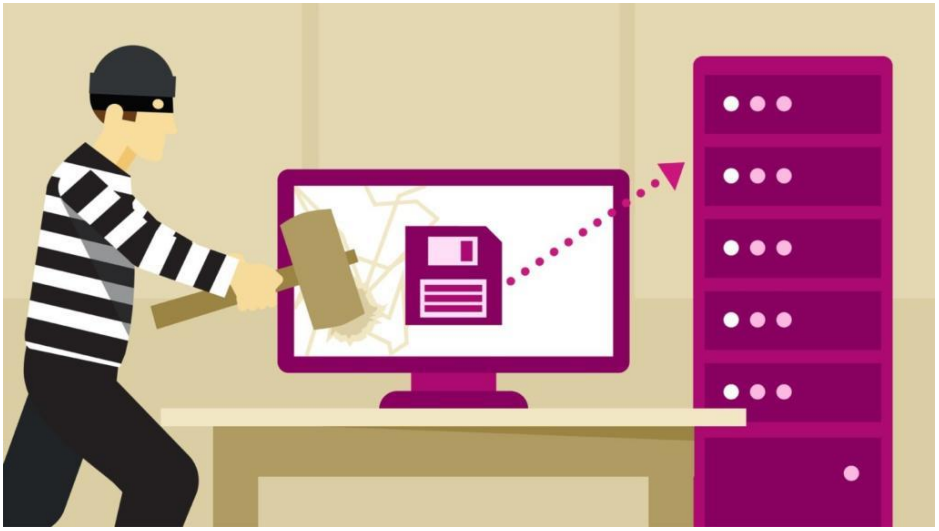
a. FIPS 140.2

Gambar 2. Fips 140.2

Federal Information Processing Standard yang lebih terkenal dengan istilah publikasi FIPS 140.2 adalah standar regulasi keamanan jaringan komputer pemerintahan yang dikembangkan oleh pemerintahan federal Amerika Serikat. Regulasi ini memfokuskan layanannya pada proses

penyelidikan kode-kode rahasia atau kriptografi yang meliputi pengolahan data dan dokumen, enkripsi algoritma, serta sejumlah standar regulasi lain dalam teknologi informasi yang digunakan dalam ruang lingkup pemerintahan.

b. PII



Gambar 3. *Personally Identifiable Information*

Istilah PII merupakan singkatan dari *Personally Identifiable Information*. Standar regulasi PII bergerak untuk mendeteksi, membedakan, serta mencari jejak identitas individu maupun kelompok yang terhubung dengan sistem dalam pusat data utama.

Saat digunakan dalam pusat data pemerintahan yang telah menerapkan *government cybersecurity*, PII membantu pemerintah dan pihak-pihak terkait untuk menemukan identitas penyusup maupun peretas yang masuk ke dalam pusat data. Dengan begitu, keamanan dari pusat data pemerintahan akan tetap terjaga dari pihak luar yang tidak memiliki izin untuk mengolah atau melakukan transmisi data milik pemerintah.

c. HIPAA

Salah satu elemen utama dari pemerintahan adalah fasilitas kesehatan. Dalam hal ini, HIPAA (*Health Insurance Portability and Accountability*) menjadi regulasi yang membawahi proses perekaman data serta aktivitas medis yang terjadi di fasilitas kesehatan suatu wilayah. Melalui HIPAA, seluruh informasi yang dibuat, diterima, dan disebarkan untuk kepentingan medis akan dijamin kerahasiaan serta perlindungannya.

Gambar 4. *Health Insurance Portability and Accountability*

Aturan Hukum dan Privasi HIPAA telah ada untuk melindungi data layanan kesehatan pribadi mulai tahun 1996. Seiring teknologi telah berubah dan informasi menjadi lebih mudah diakses, ada Juga telah direvisi karena perubahan lingkungan dan kemajuan teknologi selama bertahun-tahun. Semua peraturan ini telah disiapkan untuk membantu menjaga keamanan informasi pribadi.

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) dan Aturan Privasi HIPAA menetapkan standar untuk melindungi data pasien yang sensitif dengan menciptakan standar untuk pertukaran elektronik , Dan privasi dan keamanan informasi medis pasien oleh orang-orang di industri kesehatan. Sebagai bagian dari HIPAA, Aturan Penyederhanaan Administratif dirancang untuk melindungi kerahasiaan pasien, sambil membiarkan informasi medis diperlukan untuk dibagikan sambil menghormati hak pasien terhadap privasi. Sebagian besar penyedia layanan kesehatan, organisasi kesehatan, dan rencana kesehatan pemerintah Yang menggunakan, menyimpan, memelihara, atau mengirimkan informasi perawatan kesehatan pasien diminta untuk mematuhi peraturan privasi hukum HIPAA.

Tujuan utama HIPAA adalah untuk membantu individu mempertahankan cakupan asuransi kesehatan dengan: menyederhanakan prosedur administratif (Administrative Simplification Rules) dan mengendalikan biaya administrasi. Dengan begitu banyak informasi yang berpindah tangan antara penyedia layanan medis dan

perusahaan asuransi kesehatan dan begitu banyak pihak lain di dunia layanan kesehatan, Undang-undang HIPAA tampaknya mempermudah penanganan dokumentasi dan informasi pasien yang sensitif di industri perawatan kesehatan, sementara Melindungi kerahasiaan informasi kesehatan pasien.

HIPAA bukan Hukum yang Melindungi Kerahasiaan Pasien dan Rekaman Kesehatan. HIPAA adalah undang-undang federal, ada banyak undang-undang individu lainnya yang bekerja untuk melindungi privasi pribadi Anda dan penanganan data yang terdapat dalam Catatan medismu Hukum dan peraturan ini bervariasi dari satu negara bagian ke negara bagian lainnya.

HIPAA adalah standar dasar dan setiap negara dapat menambahkannya dan memiliki standar tambahan mereka sendiri. Hukum HIPAA difokuskan untuk menyederhanakan sistem perawatan kesehatan dan memastikan keamanan bagi pasien. Judul IV adalah perlindungan yang menjamin perlindungan privasi untuk informasi medis Anda. Seiring dengan federal memastikan privasi Anda, hukum HIPAA dimaksudkan untuk menyebabkan berkurangnya aktivitas penipuan dan peningkatan sistem data. Bila dipatuhi sepenuhnya oleh semua yang diminta untuk mematuhi.

4 Aturan HIPAA untuk Kepatuhan oleh Penyedia Layanan Kesehatan

- HIPAA Privacy Rule – Melindungi jenis data yang dikomunikasikan
- HIPAA Aturan Keamanan – Melindungi database dan data untuk keamanan
- Aturan Penegakan HIPAA – Menunjukkan prosedur untuk penegakan dan prosedur untuk dengar pendapat dan hukuman.
- Peraturan Pemberitahuan Pelanggaran HIPAA – Memerlukan penyedia layanan kesehatan untuk memberitahukan Individu ketika telah terjadi pelanggaran informasi kesehatan yang dilindungi

HIPAA diterapkan pada Aturan Privasi, dan juga semua peraturan Penyederhanaan Administratif, berlaku untuk rencana kesehatan*, clearing house* perawatan kesehatan, dan penyedia layanan kesehatan yang mentransmisikan kesehatan Informasi dalam bentuk elektronik sehubungan dengan transaksi dimana Sekretaris HHS telah mengadopsi standar di bawah HIPAA (“entitas yang tercakup”).
Contoh aturan HIPAA yang tidak diterapkan pada orang atau perusahaan:

- perusahaan pengujian genetik langsung ke konsumen (DTC)

- aplikasi seluler yang digunakan Untuk tujuan kesehatan dan kebugaran
- praktisi pengobatan alternatif
- lembaga negara, seperti layanan perlindungan anak
- lembaga penegak hukum
- perusahaan asuransi jiwa
- sekolah
- atasan

Tujuan Aturan Keamanan HIPAA yaitu untuk memenuhi persyaratan kepatuhan oleh penyedia layanan kesehatan. Agar penyedia layanan mematuhi HIPAA, mereka harus memenuhi persyaratan yang ditetapkan oleh HIPAA Security Rule. Ini termasuk persyaratan dan pedoman seputar pengamanan administratif, fisik, dan teknis yang sesuai untuk memastikan kerahasiaan, integritas, dan keamanan informasi kesehatan yang dilindungi (PHI).

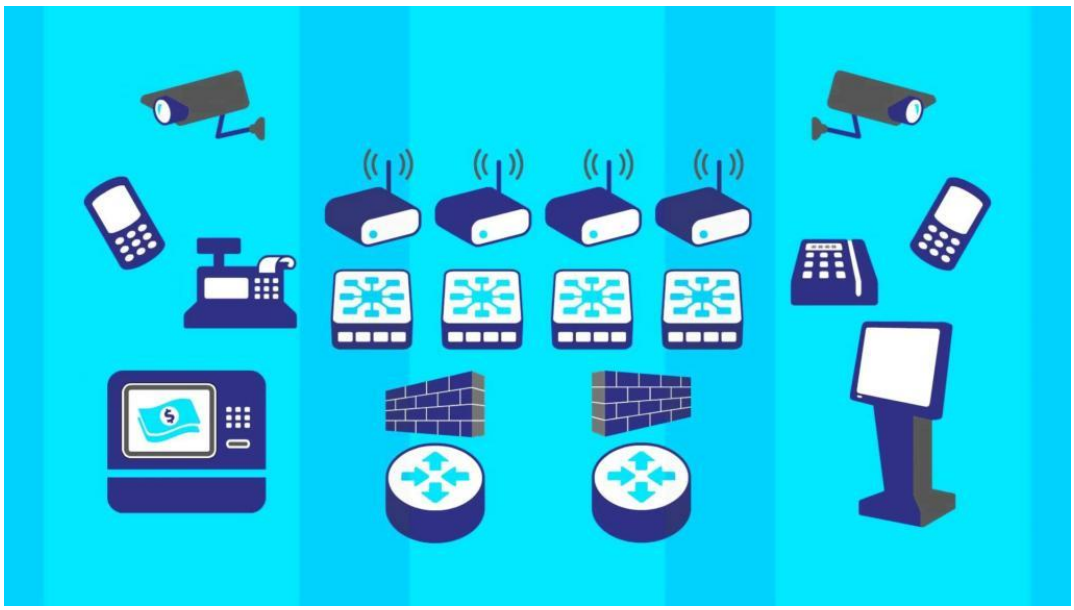
Beberapa penyedia layanan kesehatan telah mengambil langkah-langkah seperti mengendalikan akses ke kantor dengan file medis dengan sistem kartu kunci elektronik. Dan hanya mengizinkan karyawan membatasi akses terhadap jumlah minimum informasi yang dibutuhkan. Selain itu, penggunaan layanan khusus untuk membuat transaksi elektronik aman juga digunakan oleh banyak fasilitas medis dan penyedia asuransi. Jika Anda khawatir tentang apa yang dokter atau dokter anda lakukan untuk mematuhi undang-undang HIPAA, tanyakan kepada mereka langkah-langkah apa yang telah mereka lakukan untuk memastikan privasi Anda. Ingat bahwa jika mereka mematuhi HIPAA, mereka memiliki daftar panjang hal yang harus dilakukan untuk dianggap sesuai dengan HIPAA. Hukum privasi dan perlindungan data pasien yang sensitif diambil dengan sangat serius. Ada kemungkinan mereka mengikuti peraturan ini dengan sangat ketat karena undang-undang itu.

Jika asuransi kesehatan Anda berasal dari organisasi kesehatan kecil yang dikelola sendiri, mereka mungkin tidak harus mematuhi HIPAA Peraturan. Penting untuk diperiksa dengan mereka untuk melihat apakah mereka mematuhi, dan jika tidak, langkah apa yang mereka ambil sendiri untuk memastikan privasi Anda.

Pengecualian privasi HIPAA diberikan kepada penyedia layanan kesehatan dan orang lain yang diwajibkan untuk mengikuti HIPAA pengecualian di beberapa area di mana mereka tidak harus mengikuti peraturan yang digariskan oleh Tindakan dan peraturan Anda harus

memberi tahu diri Anda tentang tiga pengecualian privasi HIPAA yang paling umum sehingga Anda dapat mengetahui informasi atau data medis tentang Anda yang mungkin diungkapkan secara hukum dan tidak dilindungi oleh perlindungan HIPAA.

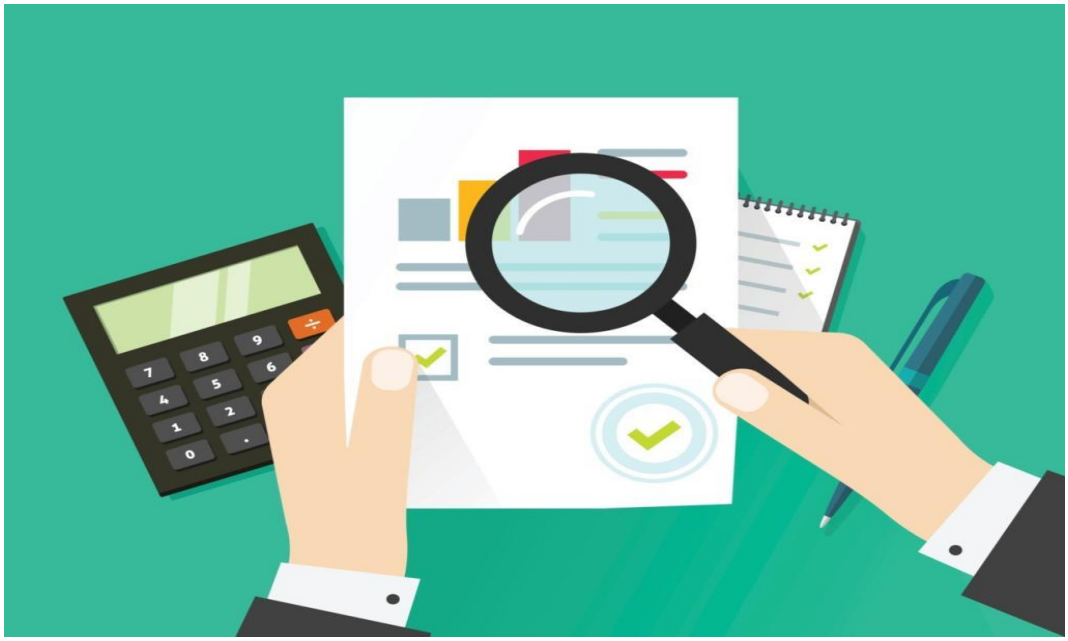
d. PCI DDS



Gambar5. *Payment Card Industry Data Security Standard*

Payment Card Industry Data Security Standard (PCI DDS) merupakan regulasi yang diberlakukan bagi institusi finansial atau perbankan, terutama institusi yang memiliki wewenang untuk menerbitkan kartu kredit. Praktik yang diterapkan PCI DDS difokuskan kepada pengembangan, pemeliharaan, serta pengawasan sistem pengamanan data pemegang kartu kredit. Hal ini bertujuan untuk mendeteksi dan mencegah kemungkinan insiden cyber threats yang terjadi.

e. FINRA



Gambar 6. *Financial Industry Regulatory Authority*

Tak jauh berbeda dari PCI DDS, FINRA atau *Financial Industry Regulatory Authority* juga bergerak dalam bidang organisasi finansial dari pemerintah. Program FINRA yang paling terkenal dinamakan '*sweep*', yakni program yang mengharuskan seluruh instansi finansial untuk memberikan respons terhadap surat pemeriksaan mengenai kesiapan instansi dalam menggalakkan upaya-upaya *cyber security*. Pemeriksaan ini dilakukan secara berkala untuk memastikan bahwa sistem pengamanan data instansi finansial tetap terjaga dan bekerja dengan seharusnya.

Itulah ulasan mengenai lima standar regulasi dari *government cybersecurity*. Memilih sistem pengamanan siber yang telah sesuai dan memenuhi seluruh regulasi tersebut, menjadi hal yang sangat krusial untuk keamanan data dan informasi sensitif dalam ruang lingkup instansi pemerintah.

DAFTAR PUSTAKA

1. Adikara, F. 2013. Implementasi Tata Kelola Teknologi Informasi Perguruan Tinggi Berdasarkan COBIT 5 Pada Laboratorium Rekayasa Perangkat Lunak Universitas Esa Unggul, Seminar Nasional Sistem Informasi Indonesia, SESINDO.
2. ITGI. 2000. IT Governance Institute: Board briefing on IT governance. www.itgi.org