Asosiasi
Asuransi Jiwa
Indonesia

MARI
Berasuransi

PANDUAN TATA KELOLA TEKNOLOGI INFORMASI (TI) ASURANSI JIWA

Daftar Isi

Daftar Isi i

Pengantar ii

Apakah Tata Kelola Teknologi Informasi? 1

Struktur Organisasi Teknologi Informasi 2

A. Strategi Teknologi Informasi 5
Manajemen Risiko Teknologi Informasi 6

B. Sistem yang Minimal Harus Dimiliki oleh Perusahaan Asuransi Jiwa 8

C. *System Development Life Cycle* 10

D. IT *Infrastructure* 18

E. Konsep-konsep Tata Kelola TI 23

F. IT *Security* 28
Information Security 32

G. Pemantauan dan Pemeliharaan Sistem Teknologi Informasi 35

H. Manajemen Perubahan (*Change Management*) 37
Proses Manajemen Perubahan 37

I. Manajemen Insiden 40

J. Manajemen Aset TI 45

K. Pemulihan Bencana 46

L. Perencanaan Utama Teknologi Informasi 50

Pengantar

Di zaman modern ini, ketergantungan terhadap teknologi sudah sangatlah tinggi. Terutama di dunia asuransi jiwa, dimana produk yang dibeli merupakan produk yang tidak dapat disentuh alias jasa sehingga pemberian layanan terbaik kepada seluruh nasabah asuransi sangatlah penting sebagai suatu hal yang dapat dirasakan langsung oleh para nasabah. Adapun terkait dengan pelayanan, pelayanan dapat diberikan dengan baik akan sangat terbantu bila menggunakan teknologi. Hal-hal seperti pengiriman polis *via email* dan aplikasi *mobile*, pengecekan saldo nasabah *via aplikasi mobile*, layanan interaksi *artificial intelligence* (AI) seperti *chatbot messenger* dan lain sebagainya merupakan layanan yang merefleksikan layanan yang modern dan tentunya layanan-layanan ini merupakan layanan yang dapat mempermudah nasabah. Hal ini termasuk pengelolaan data nasabah sudah harus didukung dengan teknologi dikarenakan jumlah nasabah yang sudah jutaan dan juga tentunya terdapat informasi-informasi keuangan nasabah yang harus dikelola dengan cepat serta akurat.

Oleh karena itu, pedoman dalam mengelola teknologi pada perusahaan asuransi jiwa merupakan hal yang sangat penting dimana perawatan sistem serta pembaharuan sistem merupakan hal yang menjadi kunci utama dalam mengembangkan industri asuransi jiwa.

Pada dokumen ini kami menghadirkan panduan yang kami percayai dapat digunakan dengan baik oleh perusahaan asuransi jiwa mulai dari yang berskala kecil maupun yang berskala besar. Semoga dokumen ini dapat berguna dalam mengembangkan industri asuransi jiwa yang tentunya diharapkan dapat dinikmati oleh masyarakat Indonesia dalam hal perlindungan terhadap perencanaan keluarga.

Jakarta, Agustus 2022

Working Group Digital Initiatives
Asosiasi Asuransi Jiwa Indonesia

Apakah Tata Kelola Teknologi Informasi?

Tata Kelola Teknologi Informasi (TI) atau *Information Technology* (IT) *Governance* adalah suatu bentuk komitmen, kesadaran, dan proses pengendalian manajemen organisasi terhadap sumber daya TI mencakup mulai dari sumber daya komputer (*software, brainware, database* dan sebagainya) hingga ke Teknologi Informasi dan Jaringan LAN/Internet.

Menurut COBIT yang menjadi standar umum Tata Kelola TI dari lembaga ISACA (https://www.isaca.org). Tata Kelola TI didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengendalikan perusahaan untuk mencapai tujuan perusahaan berdasarkan nilai sekaligus menyeimbangkan risiko dengan pengembalian atas TI dan prosesnya. Sedangkan Oltsik (2003) mendefinisikan TI sebagai kumpulan kebijakan, proses/aktivitas dan prosedur untuk mendukung pengoperasian TI agar hasilnya sejalan dengan strategi bisnis (strategi organisasi).

Perusahaan masa kini tentunya mempunyai ketergantungan yang besar terhadap teknologi informasi atau yang biasa juga disebut sebagai sistem informasi. Ketergantungan perusahaan terhadap TI yaitu berupa:

- Kecepatan dalam melakukan proses
- Keakuratan dalam proses
- Menjaga kerahasiaan nasabah
- Meningkatkan penjualan
- Membantu dalam melayani nasabah
- *Back up* dan *recovery* data serta sistem aplikasi

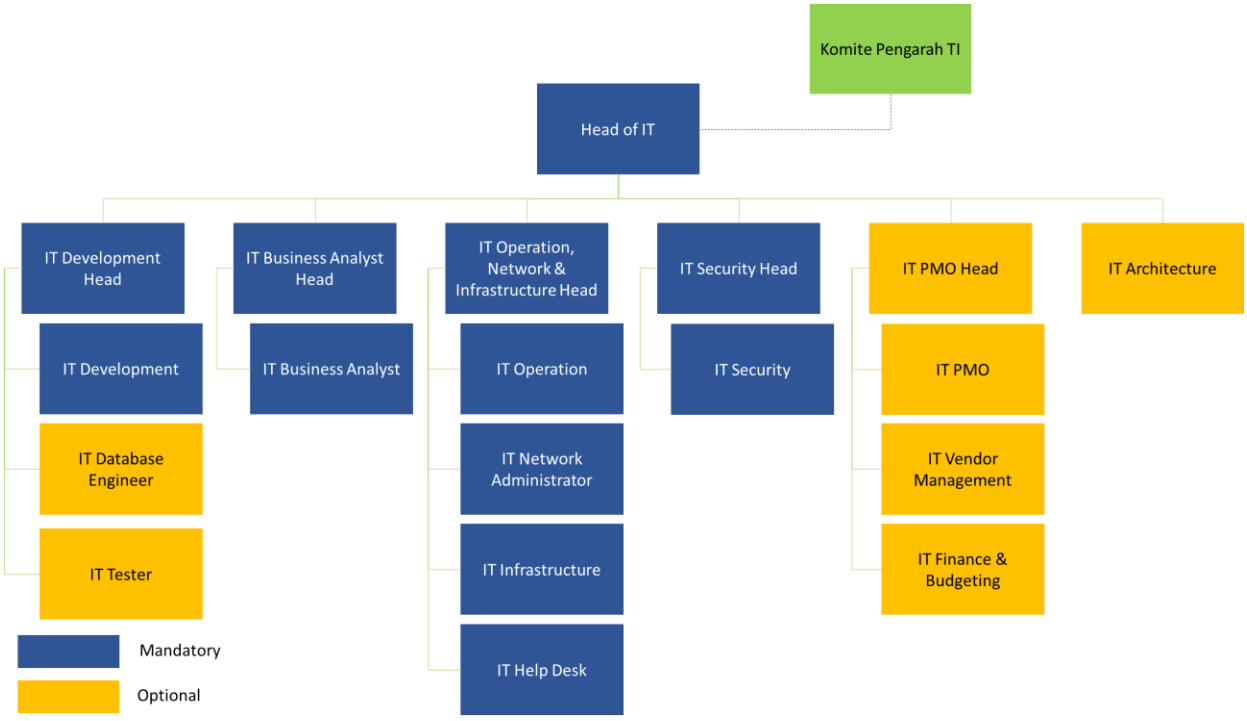
Kerahasian informasi tenaga pemasar dimana intinya peran TI sangat dibutuhkan dalam menjaga daya saing perusahaan. Apabila sebuah perusahaan asuransi masih belum mempunyai sistem dengan pembuatan polis masih menggunakan mesin tik dan penyimpanan data masih berupa pengarsipan dokumen fisik, maka perusahaan asuransi akan sulit untuk bersaing dalam kemajuan teknologi saat ini.

Struktur Organisasi Teknologi Informasi

Dalam menjalankan fungsi TI secara baik untuk dapat mendukung tujuan perusahaan, hal dasar yang harus diperhatikan adalah dari susunan struktur organisasi TI. Dalam menyusun struktur organisasi TI harus melihat beberapa aspek yang dapat dijadikan pertimbangan yaitu:

- Bagaimana dukungan terhadap bisnis agar dapat membantu meningkatkan penjualan, membuat proses operasional yang efisien & efektif, dan meningkatkan layanan
- Kestabilan serta performa dari sistem yang digunakan oleh perusahaan
- Keamanan sistem perusahaan mencakup keamanan data perusahaan dan juga data nasabah
- Skala keuangan perusahaan
- Membantu dan mendukung perusahaan dalam meraih visi dan misi perusahaan

Di bawah ini merupakan diagram yang menggambarkan sebuah struktur organisasi TI yang ideal bagi perusahaan asuransi:



Struktur organisasi di atas dapat dipertimbangkan dan disesuaikan kembali oleh masing-masing perusahaan. Adapun tugas dan tanggung jawab pada struktur organisasi di atas akan membantu perusahaan dalam hal berikut:

- Komite Pengarah TI – adalah komite yang di atur berdasarkan POJK-4-POJK—5-2021 (khusus aset di atas IDR 1 Trilyun) yang bertugas merekomendasikan rencana pengembangan TI, kebijakan & prosedur TI, proyek pengembangan TI dan kesesuaian TI dengan informasi manajemen. Adapun Anggota Komite Pengarah TI sesuai dengan ketentuan OJK harus beranggotakan:

- ✓ Direktur yang membawahi satuan kerja TI
- ✓ Direktur yang membawahi fungsi Manajemen Risiko
- ✓ Pejabat tertinggi yang membawahi TI (Head of IT)
- ✓ Pejabat tertinggi sebagai pengguna jasa TI

- Head of IT – merancang keberlangsungan TI pada perusahaan berikut bertanggung jawab atas operasional harian TI termasuk proyek-proyek TI dan kestabilan layanan TI.
- IT Development Head – bertanggung jawab dalam memimpin sistem pengembangan baik sistem baru maupun yang sifatnya perubahan untuk menghasilkan *development* yang dapat memenuhi kebutuhan bisnis dengan kualitas yang baik.
- IT Development – melakukan sistem pengembangan baik sistem baru maupun yang sifatnya perubahan untuk menghasilkan pengembangan yang dapat memenuhi kebutuhan bisnis dengan kualitas yang baik.
- IT Database Engineer – mendesain serta melakukan *tuning* terhadap *database* untuk menjaga kinerja *database* agar tetap optimal. Namun fungsi ini sifatnya opsional, maka untuk beberapa organisasi dengan skala tertentu yang menganggap bahwa fungsi ini belum *mandatory*, maka fungsi ini dapat dirangkap oleh tim IT Development.
- IT Tester – memiliki fungsi untuk melakukan pengujian sistem setelah melalui proses *development*. Hal ini berguna agar saat pengujian dilakukan oleh *user*, aplikasi yang akan di uji sudah jauh lebih siap uji
- IT Business Analyst Head – bertanggung jawab dalam menjembatani bisnis dengan TI Development terhadap kualitas hasil dari sebuah sistem pengembangan untuk dapat memberikan hasil yang baik dengan kualitas yang baik.
- IT Business Analyst – menjembatani bisnis dan IT Development tim untuk memberikan hasil dan kualitas yang baik dari sebuah sistem pengembangan.
- IT Operation, Network & Infrastructure Head – bertanggung jawab terhadap kestabilan infranstruktur TI berikut dengan performanya beserta layanan kepada bisnis bila terjadi insiden.
- IT Operation – menjamin kestabilan infrastruktur TI beserta sistemnya dalam operasional harian termasuk menjaga keutuhan data perusahaan serta layanan kepada bisnis saat terjadi insiden.
- IT Network Administrator – menjaga kestabilan jaringan beserta memonitor performa jaringan.
- IT Infrastructure – menjaga kestabilan perangkat-perangkat yang digunakan dalam mendukung TI operasional secara harian termasuk pemeliharaan perangkat-perangkat tersebut.
- IT Help Desk – membantu menyelesaikan permasalahan bisnis terkait dengan sistem TI perusahaan.
- IT Security Head – bertanggung jawab dalam menjaga kerahasiaan sistem perusahaan dalam hal ini termasuk menjaga keamanan data perusahaan termasuk data nasabah.
- IT Security – menjaga kerahasiaan sistem perusahaan dalam hal ini termasuk menjaga keamanan data perusahaan termasuk data nasabah.
- IT Project Management Office (PMO) Head – bertanggung jawab dalam memonitor kualitas proyek dan meminimalkan *redundancy* proyek untuk dapat mencapai target waktu serta anggaran keuangan yang telah ditentukan tentunya juga meyakinkan bahwa proyek yang diselesaikan sesuai dengan

kebutuhan perusahaan. Sehubungan dengan opsionalnya fungsi ini, maka fungsi ini dapat dirangkap oleh Head of IT.

- IT PMO – memonitor kualitas proyek dan meminimalkan *redundancy* proyek untuk dapat mencapai target waktu serta anggaran keuangan yang telah ditentukan tentunya juga meyakinkan bahwa proyek yang diselesaikan sesuai dengan kebutuhan perusahaan. Sehubungan dengan opsionalnya fungsi ini, maka fungsi ini dapat dirangkap oleh Head of IT.
- IT Vendor Management – meyakinkan bahwa pembelian perangkat TI mendapatkan kualitas barang dan jasa yang bagus dengan harga terbaik serta mendapat layanan purna jual yang baik termasuk melakukan tinjauan berkala atas kinerja masing-masing vendor atas layanan purna jual yang diberikan
- IT Finance & Budgeting – membuat laporan keuangan terkait dengan pengeluaran pada TI serta membantu menentukan *budgeting* TI sebagai bagian dari *budget planning* perusahaan termasuk mengawasi agar biaya pada TI sesuai dengan yang direncakan. Sehubungan dengan opsionalnya fungsi ini, maka fungsi ini dapat dirangkap oleh Head of IT.
- IT Architecture – melakukan rancangan terhadap infrastruktur TI secara keseluruhan termasuk perangkat lunak untuk menjaga efisiensi dan optimalnya kinerja sistem termasuk kemudahan dalam melakukan pemeliharaan karena fungsi ini bersifat opsional (bergantung skala perusahaan) dan dapat dirangkap oleh Head of IT.

Adapun minimum struktur yang terbaik adalah sesuai dengan struktur di atas yang ditandai dengan warna biru. Namun demikian untuk atas jumlah dari *reporting line* pada setiap masing-masing bagian dapat digabung sesuai dengan ukuran perusahaan masing-masing. Seperti contoh bila fungsi IT Network Administrator dengan IT Infrastructure dipegang oleh orang yang sama.

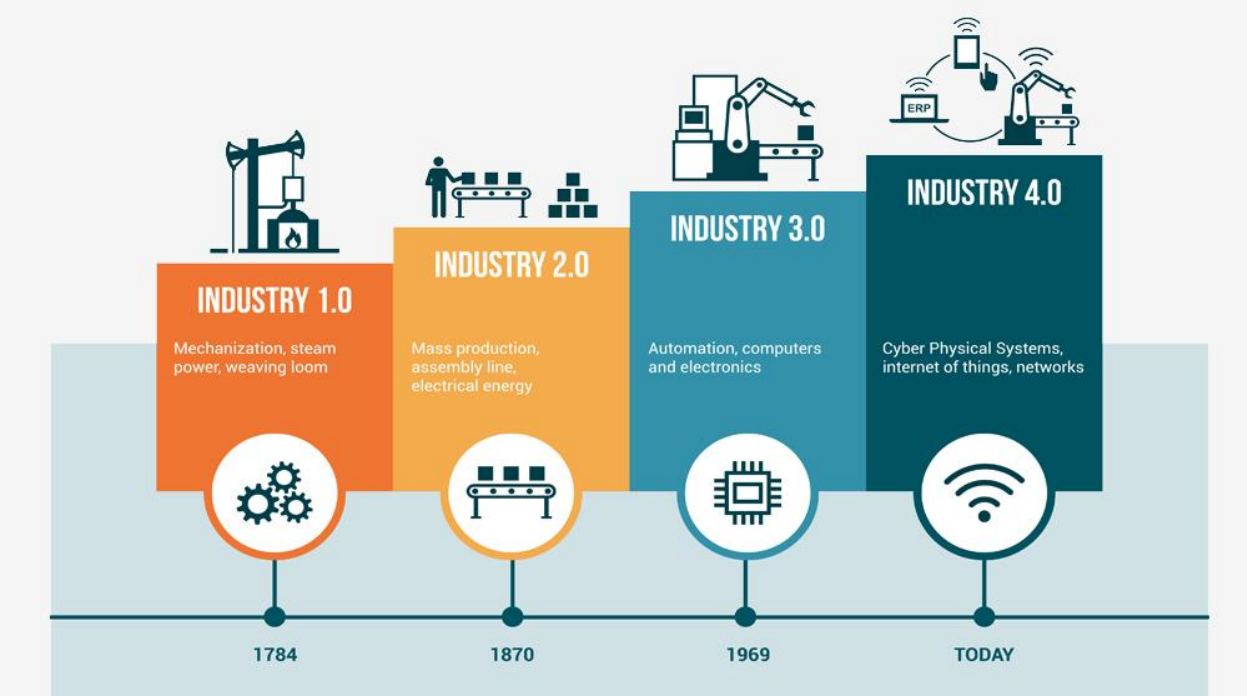
Sesuai dengan POJK No. 4/POJK.05/2021 terkait Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Non-Bank, pada setiap perusahaan diharuskan untuk memiliki Komite Pengarah Teknologi Informasi dan kiranya struktur IT ini bertanggung jawab kepada Komite Pengarah Teknologi.

A. Strategi Teknologi Informasi

Penanggung Jawab Utama	Head of IT

Dalam tata kelola IT yang baik, diperlukan strategi dalam melakukan pengelolaan dimana strategi itu harus berdasarkan:

1. Sistem yang stabil – sebelum mencapai level lainnya dari sebuah strategi, memiliki sebuah lingkungan sistem yang stabil merupakan dasar paling utama. Sebagus apapun sistem kita, bila sering terjadi *downtime* maka semuanya akan sia-sia. Hal ini termasuk bagaimana meminimalisir *downtime system* saat terjadi hal-hal yang tidak diinginkan seperti bencana alam
2. Sistem yang menghasilkan data yang akurat – data yang dihasilkan oleh sistem haruslah akurat. Banyak hal yang dapat berdampak bila data yang dihasilkan oleh sistem tidaklah akurat. Misal angka penjualan yang tidak akurat maka akan dapat menyebabkan keputusan bisnis yang salah. Laporan komisi agen pemasar yang tidak akurat tentunya akan dapat menghasilkan suatu permasalahan tersendiri antara perusahaan dan agen pemasar
3. Sistem yang dapat memotong proses atau meningkatkan efisiensi kerja – salah satu tujuan perusahaan adalah tentunya dengan meningkatkan efisiensi dalam bekerja. Tentunya perusahaan akan menghindari kenaikan produksi seiring dengan kenaikan biaya. Diharapkan dengan terjadinya efisiensi yang baik di sebuah perusahaan, maka pertumbuhan biaya tidak linear dengan pertumbuhan produksi, sehingga dapat memberikan hasil dividen yang optimal kepada pemangku kepentingan yaitu termasuk pemegang saham dan juga karyawan sebagai penerima bonus tahunan
4. Sistem yang dapat menjamin keamanan data-data yang dimaksud di sini adalah data-data para pemangku kepentingan yaitu pemegang saham, nasabah, agen pemasar, dll.
5. Sistem yang dapat mendukung dinamika perubahan pada bisnis dunia berubah dengan cepat. Bila melihat dari revolusi industri sendiri sekarang kita sudah memasuki industri 4.0. Bahkan dalam masa industri 4.0 sendiri perkembangan serta perubahan-perubahan dalam dunia bisnis sendiri baik yang terkait teknologi maupun tidak terkait teknologi sangat sering terjadi. Contoh yang berhubungan dengan teknologi, pada tahun 2020 pertemuan dengan aplikasi online sangat marak dimana setahun sebelumnya penggunaan pertemuan dengan aplikasi online masih kecil. Hal-hal seperti ini yang tentunya mempengaruhi dinamika bisnis. Sebuah sistem yang bagus tentunya harus dapat mendukung dinamika bisnis dengan baik. Contoh bila perusahaan ingin meluncurkan sebuah produk baru, maka sistem dalam perusahaan tersebut harus dinamis sehingga tidak diperlukan persiapan yang panjang pada sistem sehingga tidak tertinggal dengan pesaing-pesaing bisnis.
6. Sehubungan dengan perkembangan zaman pada masa kini, kebutuhan dalam bekerja tidak hanya dari kantor saja namun dapat dilakukan di mana saja saat sedang berpergian ataupun bila sedang di rumah. Untuk itu dalam merancang suatu sistem, ada baiknya untuk sistem tersebut dapat di akses darimana saja dengan performa yang stabil dan juga keamanan sistem yang baik.



Oleh karena itu minimum strategi yang harus dibuat oleh suatu divisi TI dalam rangka mendukung suksesnya sebuah perusahaan minimum harus mengandung 5 hal di atas.

Manajemen Risiko Teknologi Informasi

Penanggung Jawab Utama	• Head of IT • IT Development • IT Business Analyst • IT Operation, Network & Infrastructure • IT Security
Penanggung Jawab Tambahan (bila ada)	• IT Architecture

Manajemen risiko TI telah menjadi topik ketika organisasi menjadi semakin tergantung pada aset teknologi informasi dan modal intelektual, area utama dari risiko TI (operasional) biasanya dilihat sebagai berikut:

1. Infrastruktur TI dan keamanan yaitu *firewall*, jaringan, aplikasi, transaksi, data, dan informasi. Kekhawatiran atas risiko yang mungkin muncul diantaranya peretas, teroris, penjahat dunia maya

baik dari dalam maupun dari luar, virus, *malware*, dan *phishing* yang dapat diklasifikasikan di bawah judul 'risiko informasi'.

2. Integritas data, kerahasiaan, privasi, dan kepatuhan yang timbul dari peraturan dan tekanan pasar untuk melindungi data pribadi (misalnya, undang-undang perlindungan data) dan data perusahaan (misalnya, peraturan pengungkapan yang adil), serta keuangan dan operasional data dapat disebut sebagai 'risiko kepatuhan'.
3. Kesinambungan bisnis dan pemulihan bencana yang timbul dari kekhawatiran tentang kemampuan organisasi untuk melanjutkan bisnis setelah bencana alam atau akibat ulah manusia dapat disebut sebagai 'risiko kontinuitas'.
4. Masalah manajemen TI yang timbul dari kekhawatiran tentang kegagalan proyek, kinerja operasional TI yang buruk, infrastruktur TI yang tidak memadai, dan lain-lain disebut sebagai 'risiko manajemen'.

Manajemen risiko dalam menjalankan bisnis penting dilakukan untuk melindungi organisasi dari risiko yang menghambat pencapaian tujuan dan berbagai hal yang berpotensi menimbulkan kerugian bagi perusahaan.

Efek dari risiko ini tidak terbatas pada departemen TI, dampaknya dirasakan di seluruh organisasi dan karena itu harus dikelola dalam kerangka kerja manajemen risiko perusahaan. Risiko TI harus membentuk kategorinya sendiri dalam daftar risiko perusahaan, risiko utama TI harus diidentifikasi dan dimiliki dalam kerangka tata kelola TI yang terintegrasi penuh ke dalam organisasi dan yang memungkinkan pimpinan untuk mengatur TI dalam konteks model bisnis, strategi, dan kerangka kerja manajemen risiko secara keseluruhan.

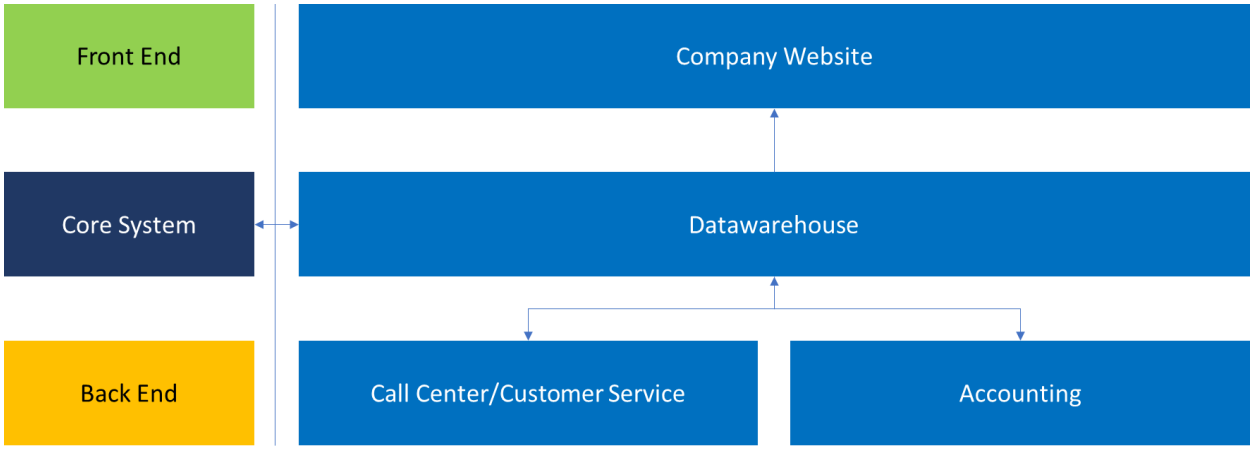
Manajemen risiko TI diatur pada peraturan Otoritas Jasa Keuangan (OJK) Repulik Indonesia (POJK No. 4/POJK.05/2021 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Non-Bank) sehingga hal ini menjadi kewajiban bagi perusahaan asuransi agar melaksanakan aturan tersebut di antaranya bagaimana manajemen perusahaan mendukung pelaksanaan manajemen risiko TI, menerapkan risiko dalam penggunaan I, membuat kebijakan dan prosedur TI, membuat arsitektur aplikasi, ketentuan tentang jaringan komunikasi dan pusat data serta pusat pemulihan data serta pengamanan teknologi informasi serta rencana pemulihan bencana.[*]

**Alan Calder Book – IT Governance*

B. Sistem yang Minimal Harus Dimiliki oleh Perusahaan Asuransi Jiwa

Penanggung Jawab Utama	• Head of IT • IT Development • IT Business Analyst • IT Operation, Network & Infrastructure • IT Security

Untuk dapat mendukung sebuah perusahaan asuransi jiwa agar dapat bersaing dengan para pesaing maka ada sistem-sistem yang wajib dimiliki. Sistem-sistem tersebut juga harus saling berintegrasi dan berkomunikasi satu sama lain agar terjadi efisiensi serta akurasi proses kerja. Di bawah ini merupakan sistem diagram atas minimal yang harus dimiliki beserta interkoneksinya:



Dari diagram di atas dapat dikategorikan menjadi 3 bagian sistem yaitu:

1. *Front End* – merupakan sistem yang berinteraksi langsung dengan pihak yang berhubungan dengan agen pemasar atau nasabah. Pada contoh di atas minimal sistem yang harus ada pada *front end* adalah situs web dimana setiap perusahaan harus menampilkan informasi-informasi wajib seperti laporan keuangan, struktur organisasi dan lainnya seperti informasi produk, sejarah pendirian perusahaan, aktivitas perusahaan, dll. Pada diagram di atas digambarkan adanya garis interkoneksi antara *data warehouse* dan situs web dimana hal ini bisa saja terjadi pengiriman informasi dari *data warehouse* seperti nilai unit bagi perusahaan asuransi jiwa yang berjualan produk *unit link* atau nilai tukar mata uang bagi perusahaan yang masih mempunyai produk aktif dengan mata uang asing. Situs web perusahaan disini juga termasuk sarana untuk nasabah dan agen pemasar untuk mendapatkan pembaharuan tentang polis-polis yang mereka miliki. Khusus untuk agen pemasar, dalam sistem *front end* juga, mereka akan bisa mendapatkan pelatihan tentang produk baru maupun pelatihan khusus sebagai agen pemasar.

2. *Core System* – ini sendiri sebetulnya bukan suatu kategori, namun *core system* sendiri merupakan sistem utama yang wajib untuk dimiliki oleh perusahaan asuransi jiwa karena sistem ini merupakan sistem yang melakukan pemrosesan polis baik mulai dari *setup produk*, *input* polis, *layanan* polis, *klaim*, dan *mengeluarkan tagihan* yang bergantung pada sistem perusahaannya. Ada beberapa perusahaan yang mempunyai beberapa sistem utama sesuai dengan saluran bisnisnya. Misal pada perusahaan yang mempunyai saluran bisnis *Corporate Group Health* & *Individual* maka memiliki dua sistem utama atau dua *core system*.

   Pada diagram di atas, ditunjukkan bahwa *core system* mempunyai interkoneksi dengan *data warehouse*. Hal ini merupakan suatu hal yang lazimnya dimiliki. Mengingat *core system* mempunyai beban kerja yang berat karena diakses oleh hampir seluruh fungsi-fungsi *back office* perusahaan, maka sebaiknya disediakan sebuah *data warehouse* yang bisa di akses oleh sistem-sistem yang sifatnya bukan sistem utama. Seperti pada contoh di atas ada situs web, *call center/customer service* maupun *accounting*. Bila sistem-sistem yang sifatnya bukan utama ikut mengakses langsung *core system* maka beban kerja *core system* bisa menjadi lambat terutama bila diakses oleh laporan-laporan.

   Untuk sinkronisasi *data warehouse* bergantung dari kemampuan masing-masing perusahan dengan minimal sinkronisasi data antara *core system* dengan *data warehouse* adalah H-1. Yang terbaik adalah *real time* namun memerlukan investasi *hardware* yang besar untuk dapat melakukan sinkronisasi *real time* sehingga kembali lagi kepada masing-masing perusahaan

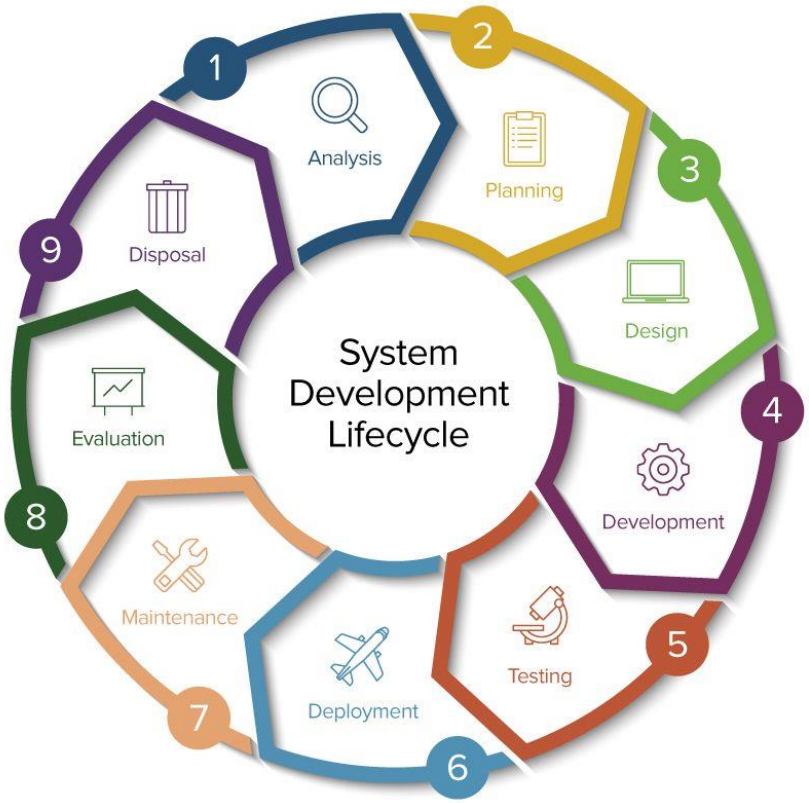
   Data warehouse ini jugalah yang akan berfungsi sebagai sentralisasi penarikan laporan-laporan yang dibutuhkan oleh semua departemen di dalam perusahaan. Dengan tujuan pelaporan yang dibutuhkan oleh perusahaan akan tersentralisasi dan berasal dari satu sumber data sehingga akurasi serta konsistensi data akan terjaga.

3. *Back End* – yaitu sistem yang sifatnya hanya berinteraksi dengan fungsi-fungsi *back office* perusahaan. Seperti contoh pada diagram di atas adalah sistem *call center/customer service* dan *accounting.*

   Sistem *call center/customer service* adalah sistem *ticketing* yang digunakan untuk melayani nasabah dan atau agen pemasar bila perusahaan memiliki saluran individu atau *agency*. Sedangkan *accounting system* adalah sistem yang membantu *accounting* untuk menjurnal transaksi-transaksi teknis dan nonteknis perusahaan.

C. *System Development Life Cycle*

Penanggung Jawab Utama	• Head of IT • IT Development • IT Business Analyst • IT PMO • IT Security



Adapun di dalam mengikuti ketentuan sebuah IT *Governance* yang sesuai secara proses sistem pengembangan, proses pengembangan sebuah sistem dianjurkan untuk mengikuti ilmu yang ada saat ini yang dikenal dengan *System Development Life Cycle* atau yang biasa di singkat dengan SDLC. Berikut merupakan deskripsi dari masing-masing proses yang ada pada konsep SDLC:

1. ***Analysis*** – untuk terciptanya hasil sistem pengembangan yang baik yang dapat membantu kebutuhan bisnis maka diperlukan suatu analisis yang tepat tentang kebutuhan dari bisnis tersebut. Analisis dapat dimulai dari apa yang menjadi kebutuhan dan yang menjadi kekurangan dari yang ada saat ini untuk dapat diperbaiki dari hasil sistem pengembangan. Selain analisis tersebut, hal-hal lain yang juga harus dianalisis adalah apakah usaha yang dikeluarkan sesuai dengan hasil yang diharapkan, apakah hal ini bisa diprioritaskan mengingat banyaknya prioritas

dari sisi bisnis, bagaimana hasil perubahan proses setelah sistem pengembangan dilakukan, apakah ada perubahan tugas dari personel yang biasa menangani proses ini, berapa biaya yang dibutuhkan, siapa saja yang akan terlibat dalam proyek ini, dan berapa lama yang dibutuhkan untuk menyelesaikan proyek ini termasuk apakah diperlukan pembelian atau peningkatan perangkat lunak *(software)* dan perangkat keras *(hardware)*

2. ***Planning*** – setelah analisis selesai dilakukan dan diputuskan bahwa sistem pengembangan perlu dilakukan, maka tahap selanjutnya adalah merupakan tahap perencanaan dimana hal ini termasuk memutuskan apakah dapat meningkatkan dari sistem yang ada, mengembangkan sistem baru, atau bahkan mengadopsi sistem dari luar. Pada tahap ini membutuhkan personel dari sisi bisnis untuk dapat membuat kebutuhan bisnis secara detail agar pihak TI dapat menyampaikan kebutuhan tersebut dalam suatu model sistem sesuai dengan hasil yang diinginkan. Pembuatan kebutuhan bisnis ini tentunya harus dilakukan dengan mendapatkan asistensi dari IT Business Analyst agar kebutuhan bisnis yang dibuat oleh personel bisnis dapat dipahami oleh pihak IT Developer.
3. ***Design*** – pada tahap ini, IT Business Analyst kiranya diharapkan dapat membuat dokumen teknis yang sifatnya adalah penerjemahan dari kebutuhan bisnis yang dibuat oleh bisnis sehingga dapat dibaca dan dipahami dengan mudah oleh pihak IT Development. Adapun dokumen yang dibuat oleh IT Business Analyst ini biasa disebut dengan dokumen *functional specification*. *Functional specification* ini dapat berupa desain *user interface* (UI) dari sistem yang akan dikembangkan beserta formula, validasi, serta bisnis proses dari UI tersebut. *Functional specification* ini dapat juga dijelaskan kepada bisnis untuk dapat persetujuan sebelum akhirnya diformulasikan ke dalam sistem pengembangan.
4. ***Development*** – tahap ini adalah tahap di mana IT Development melakukan sistem pengembangan berdasarkan *functional specification* yang di buat oleh IT Business Analyst. Pada tahap ini idealnya dapat dilakukan pengujian internal yang dilakukan bersama antara IT Business Analyst dengan IT Development. Adapun pengujian yang dilakukan pada tahap *development* biasa disebut dengan *System Integration Test* (SIT)
5. ***Testing*** – hasil dari sistem pengembangan yang sudah selesai dan tentunya sudah diuji oleh IT Development bersama dengan IT Business Analyst, maka harus disebarkan ke *user acceptance testing* (UAT) *environment* agar bisnis dapat melakukan pengujian apakah sistem pengembangan sudah sesuai keingingan, apakah ada *error*, apakah betul dapat memenuhi kebutuhan bisnis, apakah betul performa sistem yang dikembangkan sudah memenuhi persyaratan bisnis dan lain sebagainya. Pada tahap ini bisa terjadi pengerja antara bisnis dengan IT Development bila ada hal-hal yang masih belum sesuai. Pada tahap ini bisnis dituntut untuk membuat berbagai skenario pengujian yang mungkin terjadi pada saat sistem sudah dapat dijalankan.
6. ***Deployment*** – sistem yang sudah lulus hasil pengujian maka dapat segera disebarkan ke bagian produksi untuk selanjutnya dapat langsung digunakan untuk kebutuhan bisnis. Diperlukan adanya mekanisme kontrol ketika melakukan penyebaran dari lingkungan UAT ke lingkungan produksi production untuk memastikan tidak ada masalah yang timbul di lingkungan produksi.

7. ***Maintenance*** – tahap ini merupakan tahap pengawasan dari hasil sistem yang sudah digunakan secara langsung. Pada tahap ini biasanya lazim terjadi suatu *bugs* yang timbul dan tidak dimasukkan pada skenario tahap pengujian. Diperlukan adanya sebuah pencatatan untuk isu-isu yang muncul pada lingkungan produksi beserta resolusi dan waktu penyelesaian sebagai bahan dokumentasi dan pelajaran kedepan jika menemui masalah yang sama.
8. ***Evaluation*** – setelah semua berjalan dengan baik, maka evaluasi harus dilakukan untuk melihat apakah hasil sudah sesuai atau belum dan bahkan dapat dijadikan sebagai acuan untuk perbaikan yang lebih baik lagi kedepannya bila hasilnya sudah sesuai dengan kebutuhan. Namun demikian bisa saja terjadi dimana hasil dari proyek tidak sesuai dengan harapan, maka berbagai keputusan dapat dilakukan dari mulai meningkatkan hasil sistem pengembangan yang sudah digunakan, penggantian baru dan sebagai sesuai dengan keputusan terbaik pada kondisi tersebut
9. ***Disposal*** – saat semua tahapan pada SDLC ini sudah selesai, maka proses pembuangan sangat diperlukan. Terutama untuk hal-hal yang sifatnya dapat berdampak terhadap kemanan data perusahan. Contoh yang terbaik adalah data-data yang digunakan saat pengujian harus dibuang secepatnya agar data-data tersebut tidak disalahgunakan

Proses SDLC ini memberikan keuntungan yang banyak bagi bisnis yaitu:

- Mempunyai pandangan yang lebih jelas terhadap proyek yang dijalankan. Berapa sumber daya yang digunakan, persyaratan kemampuan terhadap sumber daya yang terlibat pada proyek, berapa lama waktu yang dibutuhkan, keuntungan apa yang bisa diberikan kepada bisnis dan lebih tepatnya tujuan dari proyek ini
- Lebih jelas atas biaya yang dibutuhkan dan berapa keuntungan dari proyek yang dijalankan
- Tersedianya dokumentasi yang jelas dan lengkap sehingga dapat memberikan gambaran yang jelas untuk pemeliharaan atau pengembangan kedepannya walaupun personel yang terlibat adalah personel baru
- Lebih akuratnya hasil sistem pengembangan sesuai dengan kebutuhan bisnis mengingat IT Development dapat mengembangkan sesuai dengan arahan yang tepat dan jelas
- Kualitas dari sebuh proyek IT Development akan jauh lebih baik

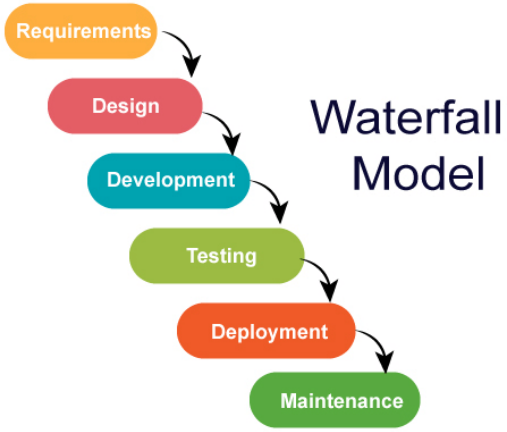
Namun demikian konsep ini selain dapat memberikan keuntungan yang banyak bagi bisnis, konsep ini mempunyai beberapa kelemahan yaitu:

- Tidak fleksibel terutama untuk proyek-proyek berskala kecil
- Membutuhkan biaya yang lebih besar
- Membutuhkan usaha yang besar dalam dokumentasi
- Kecepatan dalam menyelesaikan suatu proyek akan menjadi lebih lambat*

Dari kelemahan-kelemahan atas konsep ini, sebetulnya dapat disikapi dimana pada proyek TI dikenal juga dengan konsep yang disebut sebagai *Waterfall Methodology* yang tentunya lebih sederhana untuk proyek-proyek berskala kecil.

**https://www.smartsheet.com/system-development-life-cycle-guide*

Adapun di bawah ini merupakan sedikit penjelasan untuk *Waterfall Methodology*:



1. *Requirements* – sama dengan SDLC dimana *user requirement* juga perlu dilakukan mengingat hal ini merupakan dasar dari pengembangan sebuah sistem. Ibarat dalam sebuah restoran, maka untuk tukang masak dapat membuat suatu menu yang disediakan kepada para pelanggan, *user requirement* ini merupakan resep makanan. Sehingga para tukang masak dapat memasak makanannya sesuai petunjuk yang ada pada resep yang membuat proses ini tidak dapat dilewati sama sekali
2. *Design* – merupakan tahap yang sama dengan tahap pada SDLC dimana IT Business Analyst dapat memberikan desain *user interface* (UI)/*layer* beserta validasi, proses pada *layer* tersebut dan lainnya yang terkait pada hasil yang dihasilkan pada UI tersebut
3. *Development* – merupakan tahap pengembangan sistem berdasarkan arah dari *user requirement* dan juga *design* UI dan tentunya pada tahap ini dilakukan pengujian bersama antara IT Development dan IT Business Analyst sebelum di uji oleh bisnis
4. *Testing* – merupakan pengujian yang dilakukan oleh bisnis berdasarkan hasil sistem pengembangan.
5. *Deployment* – bila sistem pengembangan telah lulus hasil uji dari bisnis, maka sistem dapat dikirimkan ke produksi untuk selanjutnya dapat digunakan untuk kebutuhan bisnis
6. *Maintenance* – tahap dimana sistem akan dimonitor dan biasanya dilakukan *bugs fixing* bila masih ditemukan adanya *bugs* setelah sistem *live.*

Tentunya *Waterfall Model* ini mempunyai kelebihan dan kekurangannya masing-masing namun demikian untuk proyek berskala besar model ini tidak direkomendasikan melainkan rekomendasi yang tepat adalah menggunakan konsep SDLC.* Yang terbaru saat ini beberapa perusahaan modern sudah menggunakan konsep *agile* dalam melakukan *development* sebuah sistem. *Agile* adalah konsep yang terdiri dari kumpulan-kumpulan metode agar tim bisa menghasilkan potensi kualitas yang baik dalam pengembangan suatu produk, entah itu sebuah *software* atau projek lainnya.

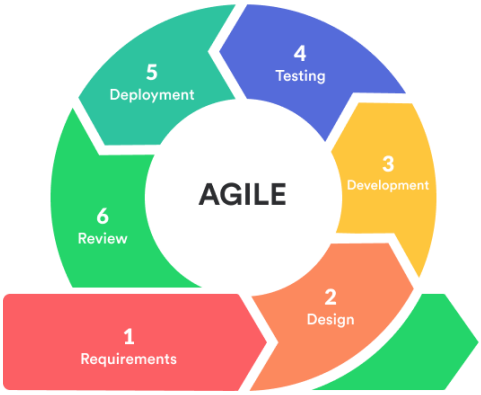
**https://www.javatpoint.com/jira-waterfall-model*

Adapun 4 nilai utama dari konsep *agile* adalah:

1. Individu lebih penting dari proses dan peralatan. Proses *development* lebih diutamakan berdasarkan arahan orang dari pada peralatan. Hal ini disebabkan karena konsep ini lebih fokus untuk menghasilkan perangkat lunak yang mendekati kebutuhan pengguna
2. Lebih fokus kepada bekerja dengan perangkat lunak daripada pembuatan dokumentasi. Pada konsep SDLC, banyak pekerjaan terkait dokumentasi yang harus dilakukan sehingga banyak memakan waktu dalam melakukan pengembangan sebuah sistem
3. Kolaborasi yang kuat antara Project Manager dan pengguna. Hal ini dimaksudkan agar hasil akhir dari sebuah sistem sangat mendekati dari keinginan pengguna
4. Penggunaan konsep *agile* ini memungkinkan untuk dapat merubah sebuah sistem dengan cara yang jauh lebih mudah dan biaya yang jauh lebih rendah sehingga dapat mengikuti perubahan-perubahan yang dibutuhkan oleh bisnis

Konsep *agile* ini terbagi menjadi 6 tahap yaitu:

1. Pembuatan konsep yang melibatkan identifikasi yang berguna bagi bisnis dan juga perkiraan waktu serta biaya yang dibutuhkan. Hal ini dapat digunakan dalam melakukan prioritas proyek pada suatu organisasi – ***Requirements***
2. Tahap kelahiran, yaitu tahap dimana dilakukannya pengidentifikasian anggota tim, pendanaan yang diperlukan serta permintaan sesuai dengan kebutuhan bisnis. Lama waktu pekerjaan yang melibatkan masing-masing anggota tim juga harus diidentifikasikan – ***Design***
3. Iterasi atau konstruksi dimana tim mulai melakukan pengembangan sistem berdasarkan permintaan bisnis. *Flow* iterasi/pengulangan yang terjadi pada tahap ini adalah – ***Development***:
    a. Menentukan persyaratan berdasarkan permintaan bisnis
    b. Melakukan pengembangan sistem berdasarkan permintaan bisnis
    c. Melakukan uji coba untuk meyakinkan hasil dari pengembangan termasuk memberikan pelatihan atas penggunaan sistem
    d. Mengintegrasikan sistem yang sedang dikembangkan dengan sistem dan proses yang sedang berjalan
    e. Meminta pendapat dari bisnis atas hasil pengembangan dan bisa berulang ke poin a sampai ditentukan hasil pengembangan sudah sesuai harapan
4. Menyiapkan hasil pengembangan sistem untuk dapat digunakan dalam proses bisnis dengan melibatkan pengecekan terhadap kualitas dan identifikasi terhadap kekurangan-kekurangan yang masih ada sampai akhirnya dilepas pada *production* – ***Testing***
5. Setelah dilepas di *production*, maka masuk kedalam tahap *support* dimana para tim siap sedia untuk melakukan *support* bila terjadi permasalahan di *production* – ***Deployment***
6. Tahap selesainya proyek, dimana dianggap sistem sudah stabil dan tidak membutuhkan ekstra perhatian untuk menjaga-jaga bila ada permasalahan dimana selanjutnya dapat dilakukan tinjauan atas sistem yang sudah dikembangkan – ***Review***



Beberapa metodologi dari *agile* ini yang sering digunakan adalah:

- *Scrum*
- *Lean Software Development*
- *Extreme Programming*
- *Crystal*
- *Kanban*
- *Dynamic Systems Development Method*
- *Feature-Driven Development*

Untuk refernsi atas metodologi di atas dapat di cari refrensi-referensi nya pada internet kecuali *scrum* karena akan di bahas pada bagian setelah ini.

Scrum saat ini banyak digunakan dalam pengembangan sistem walaupun secara konsep *scrum* bisa digunakan juga untuk proyek-proyek yang tidak berkaitan dengan sistem. Tapi pada dasarnya metode tersebut bisa diterapkan ke dalam segala upaya produk atau pengembangan sistem.

Metode *scrum* adalah teknik yang dibentuk dari beberapa tahapan proses mulai dari *Product Backlog* (lihat keterangan di bawah) hingga *Sprint Retrospective* (lihat keterangan di bawah). Berikut ini penjelasan lengkap tentang tahapan metode *scrum*:

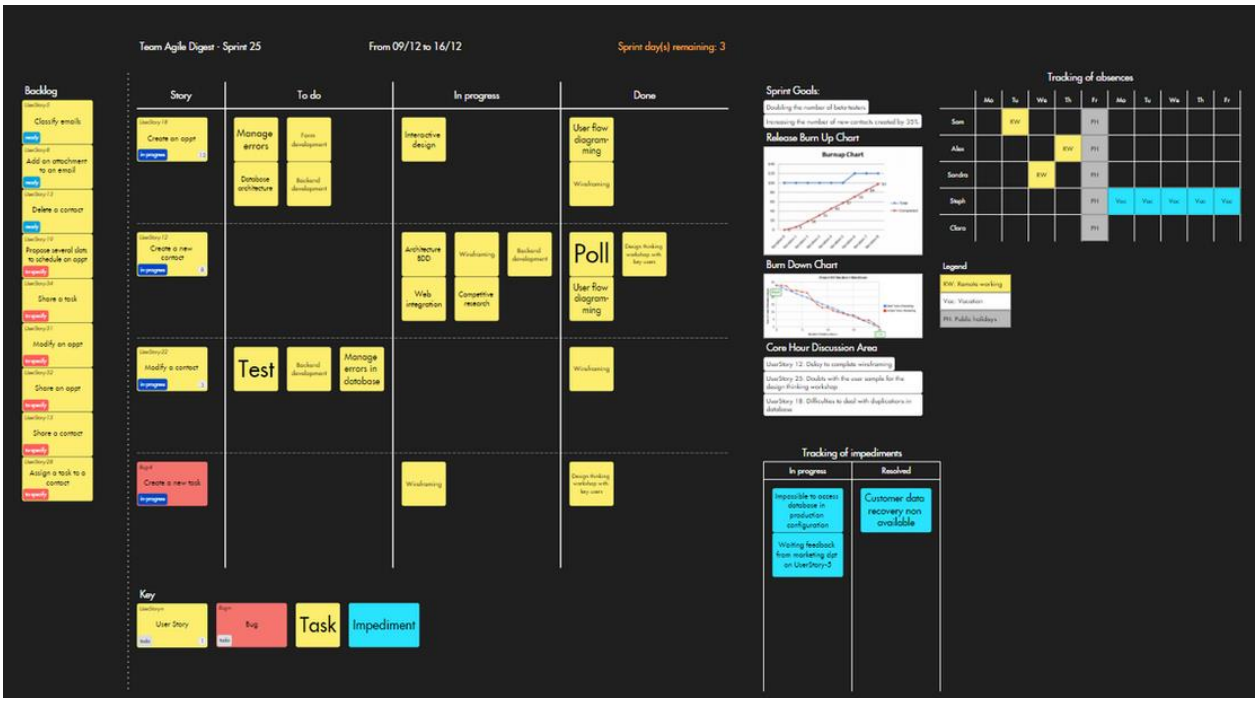
1. *Product Backlog* – pada tahapan awal ini menjadi tanggung jawab Project Manager dan manajemen. Secara sederhana pada tahapan ini berisi daftar apa saja yang harus dilakukan oleh tim sesuai dengan skala prioritas perusahaan.
2. *Sprint Planning* – Produk atau proyek teratas sesuai dengan hasil prioritas pada tahapan *Product Backlog* disusun kembali menjadi *Sprint Backlog* dimana ditentukan bagaimana akan menyelesaikan apa yang ada dalam tahapan ini
3. *Sprint* – Setelah cara dan batas waktu ditentukan pada point 2 di atas ini, lalu dilakukanlah proses dimana tim berkumpul setiap hari untuk memastikan dan bekerja atas pengembangan sistem yang diinginkan. Umumnya tim yang terlibat dalam proses ini adalah sekelompok orang dimana

di antara orang-orang tersebut ada yang ditunjuk sebagai *Scrum Master* (yang membantu agar tim tetap fokus)

4. *Sprint Review* – Dalam proses ini sistem yang dikembangkan harus sudah selesai dan siap digunakan. Kemudian sistem ini akan ditinjau kembali.
5. *Retrospective Process* – *Scrum* adalah metode yang sifatnya berulang. Proses yang dilakukan dari poin 1 sampai dengan poin 4 diingat dan dilakukan kembali pada proses *scrum* selanjutnya

Scrum bermanfaat untuk membantu perusahaan dalam mendapatkan keuntungan yang lebih besar dari sebuah proyek dalam hal ini proyek pengembangan sistem. Dengan *scrum* waktu dan biaya yang dikeluarkan setiap tim yang terlibat akan lebih hemat. Di samping itu konsep ini memudahkan dalam implementasi proyek dan juga dalam melakukan pantauan proyek sehingga baik perusahaan maupun sistem itu sendiri akan dapat selalu dikembangkan di masa depan dan bisnis juga akan selalu puas dengan hasil yang didapatkan.

Berikut ini adalah contoh *scrum* dengan menggunakan *scrum board*:



Contoh ini menggambarkan bahwa setiap pekerjaan harus dipetakan dengan jelas dengan waktu penyelesaian dan orang-orang yang melakukan. Di samping itu kita juga bisa mengklasifikasikan kegiatan-kegiatan yang dilakukan ke dalam tiga kategori pada contoh tabel di atas yaitu:

- ***To Do***, kategori atau bagian atas pekerjaan yang harus dilakukan
- ***In Progress***, berisi pekerjaan-pekerjaan yang sedang dalam tahap pengerjaan
- ***Done***, berisi pekerjaan-pekerjaan yang sudah selesai dilakukan

Selain itu dapat juga ditambahkan bentuk seperti panah dan lingkaran sebagai penanda prioritas dan petugas yang bertanggung jawab atas pekerjaan yang dilakukan. Dengan begitu *scrum board* dapat lebih mudah dibaca.

Secara kesimpulan, konsep *agile* ini memungkinkan pengembangan sebuah sistem menjadi lebih cepat, memakan biaya yang lebih sedikit, dapat beradaptasi dengan cepat sesuai perubahan bisnis serta fokus kepada sistem yang lebih mendekati kepada kebutuhan bisnis. Sedangkan konsep SDLC mempunyai tujuan yang sama namun ada beberapa kelemahan dimana waktu lebih lama, biaya lebih tinggi, kurang fleksibel dalam menghadapi perubahan bisnis namun mempunyai kelebihan dimana dokumentasi lebih lengkap sehingga lebih mudah diindentifikasi di masa depan bila ada pengembangan lebih lanjut atas sistem yang dikembangkan.

D. IT *Infrastructure*

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure • IT Security

Saat ini dalam membuat *data center* yang baik mempunyai 2 standarisasi ilmu yaitu berdasarkan:

1. American National Standard Institute (ANSI) – ANSI/TIA-942. Persyaratan ini lebih banyak membahas kepada *uptime service* suatu *data center* untuk dapat mendukung bisnis.
2. SysAdmin, Audit, Network, and Security (SANS) Institute yaitu organisasi internasional yang fokus pada kelayakan lokasi serta tempat yang akan dijadikan *data center* karena tempat juga mempunyai peran yang sangat kritis.

Bila berdasarkan ANSI maka berikut yang akan menjadi standarnya:

Parameter	TIER I	TIER II	TIER III	TIER IV
Availability	99.671%	99.741%	99.982%	99.995%
Vulnerability to Disaster	Vulnerable	Rather Vulnerable	Vulnerable to unplanned but invulnerable to planned	Invulnerable
Power & Cooling Distribution	Single path no redundant	Single path with redundant component	Multiple power and cooling distribution path but 1 active path only incl. redundant component	Multiple active power and cooling distribution path incl. redundant component
Raised Floor, UPS, Generator Availability	Can be available or not	All are available	All are available	All are available
Annual Downtime	28.8 hours	22 hours	1.6 hours	0.4 hours

Preventive Maintenance Method	Shutdown all	Partial equipment shutdown	No shutdown required	No shutdown required

Dari 4 standarisasi yang disebutkan pada tabel di atas, yang paling ideal minimal harus dipenuhi oleh sebuah perusahaan asuransi adalah *tier* 2. Hal ini berdasarkan beberapa alasan yaitu:

- Sudah menggunakan *raised floor* yang dapat meminimalisir kerusakan yang disebabkan oleh air (baik air dari luar *data center* maupun dari dalam seperti air AC yang rusak).
- Sudah ada UPS sehingga saat terjadinya pemadaman listrik dan daya dialihkan ke generator ada daya yang tersedia sampai listrik benar-benar pindah ke generator.
- Saat sesuatu hal terjadi tidak perlu mematikan semua perlatan sehingga meminimalisir usaha dan perlu diingat untuk peralatan seperti *server* bila mati mendadak kalau belum sempat dimatikan maka akan terkena risiko kerusakan *hard disk.*
- Yang terpenting dari sisi biaya tidak akan sebesar *tier* III dan *tier* IV karena pada dasarnya semakin tinggi tingkatannya maka akan semakin besar biaya yang dibutuhkan

Sedangkan untuk standarisasi berdasarkan SANS Institute bisa menggunakan diagram di bawah ini:

Requirement	Remark
Site Selection	Must be away from flood, explosives area, etc
Utilities	Recommendable to have access to multiple power sources
Building Design	Must not be easily accessible by outsiders
Mechanical Electrical System	Must have electrical backup
Facility/Security Monitoring	Must have monitoring tools such as Environment Monitoring System
Construction Building	The building construction must be strong
Electromagnetic Pulses	Away from High Voltage Transmission Towers

General Issues	Building condition must be good (e.g. no leakage)

Dari *item-item* di atas ada hal-hal yang harus diperhatikan dalam memilih lokasi *data center* termasuk apakah daerah yang dipilih rentan banjir, dan rentan terbakar karena area di sekelilingnya dipenuhi dengan tempat-tempat berisiko tinggi seperti pom bensin. Ada juga hal-hal lainnya yang tidak kalah penting, *data center* harus aman dari *electromagnetic* seperti bila berada di bawah saluran udara tegangan ekstra tinggi (sutet) karena pada dasarnya tegangan *electromagnetic* dapat mengakibatkan kerusakan pada peralatan elektronik termasuk *server*.

Hal yang termasuk harus diperhatikan untuk menjaga *availability* adalah redudansinya perangkat-perangkat kritikal. Hal ini termasuk:

- *Server* (minimum yang harus ada adalah *server production* dan *server testing*)
- Koneksi jaringan (internet) beserta backup koneksi
- Perangkat *security*
- Perangkat jaringan
- Dll

Dan tentunya sebuah *Monitoring System* juga merupakan suatu hal yang penting untuk me monitor *uptime* dari data center perusahaan seperti *Environment Monitoring System, Network Monitoring System, Humidity Censor, Temperature Censor*, dll. Dengan idealnya perangkat-perangkat *monitoring* ini akan memberikan *alert* kepada petugas yang bertanggung jawab baik dari sisi TI maupun dari sisi petugas gedung untuk dapat memberikan reaksi cepat bila terjadi sesuatu di luar jam bekerja.

Untuk perusahaan-perusahaan yang mempunyai keputusan untuk menggunakan jasa *cloud computing* juga sudah menggunakan jasa layanan tersebut yang juga sudah diatur oleh OJK (nomor 69 /POJK.05/2016 dengan *addendum* spesifik berbicara mengenai jasa cloud server yang berhubungan dengan Asuransi yaitu nomor 38/POJK.05/2020) yang menyebutkan bahwa:

- Penyelenggaraan pusat data baik yang berbentuk cloud, harus berdomisili di Indonesia kecuali bila telah mendapatkan persetujuan dari OJK dengan berbagai kondisi termasuk menyampaikan hasil analisa *country risk*, tidak mengurangi efektivitas pengawasan OJK dengan surat pernyataan dari Direksi Perusahaan, adanya perjanjian tertulis dengan penyedia jasa *cloud*
- Tidak digunakan untuk tujuan di luar yang diatur pada aturan terkait
- OJK berhak sewaktu-waktu untuk minta dikembalikan di domisili Indonesia bila ada ketidaksesuain dengan aturan yang ditemukan

NIST (National Institute of Standards and Technology) yaitu sebuah insitusi dari Amerika yang bertanggung jawab untuk mengembangkan standar dan pedoman termasuk persyaratan minimum atas keamanan informasi yang memadai untuk semua operasi, memberikan definisi dari *cloud computing* adalah suatu model komputasi yang memberikan kemudahan, kenyamanan, dan sesuai dengan permintaan (*on-*

demand access) untuk mengakses dan mengkonfigurasi sumber daya komputasi (*network, servers, storage, applications, and service*) yang bisa dengan cepat dirilis tanpa adanya banyak interaksi dengan penyedia layanan. *Cloud computing* adalah model, bukan sebuah teknologi spesifik, menggambarkan operasional dan ekonomi model untuk penyediaan dan penggunaan infrastruktur IT dan layanan terkait. Menurut dari beberapa definisi *cloud* memiliki persamaan karakteristik umum yang harus dimiliki sebuah sistem *cloud* yaitu *pay-per-use* (sewa atau bayar sesuai dengan yang digunakan), kapasitas yang elastis dan sumber daya yang tidak terbatas, *self-service interface* (antar muka berbasis layanan mandiri), dan sumber daya yang diabstraksi atau virtualisasi.

Keunggulan *cloud computing* menurut NIST adalah dapat menyediakan infrastruktur yang fleksibel sesuai dengan kebutuhan dan lebih murah, perusahaan dapat memfokuskan bisnisnya tanpa memikirkan TI. Perusahaan bisa berimprovisasi dengan kreasi dan layanan untuk solusi IT dengan memberikan layanan akses yang lebih fleksibel dan harga yang efektif.

Model layanan *cloud* menurut NIST dibagi menjadi Software as A Service (SAAS), Platform as A Service (PAAS), dan Infrastructure as A Service (IAAS). Adapun model layanan yang paling direkomendasikan yaitu model layanan IAAS di mana sistem *cloud server* ini menyediakan layanan berupa sewa *server* secara virtualisasi kepada pengguna. IAAS lebih dikenal dengan layanan komputasi dimana layanan yang diberikan berupa komputasi dasar berupa mesin yang dapat dijadikan berbagai jenis server sesuai dengan kebutuhan pengguna. Pengguna diberikan kemudahan dalam pemesan dan akses khusus untuk dapat mengonfigurasi komputasi paling mendasar yaitu komputer. Selain itu target dari IAAS adalah pengguna dengan tingkat penguasaan di bidang komputer yang lebih mendalam, dimana pengguna harus memiliki keahlian dalam mengakses *server* seperti dalam sistem ini yang dapat diakses dengan *remote server* seperti penggunaan *Putty* dengan protokol SSH ataupun telnet. Dalam sistem terlihat juga jika pengguna dapat melihat mesin yang dapat digunakan dan beberapa keterangan mengenai detail *server* yang disewa.

Hal yang perlu menjadi perhatian dalam menunjuk penyedia layanan *cloud computing* adalah:

- Keamanan data – apakah data anda aman berada di tangan penyedia layanan? Pastikan penyedia layanan anda memiliki mekanisme untuk mengamankan data atau informasi anda yang berharga baik itu di lapisan fisik, virtua, maupun personil yang mengoperasikannya
- Performa layanan – pastikan aplikasi atau layanan dapat berfungsi dengan baik di atas teknologi baru ini, biasanya penyedia layanan akan memberikan masa *trial* atau *test drive* platform mereka kepada pelanggan potensial. Manfaatkan masa ini untuk melakukan *performance benchmark* terhadap kemampuan komputasi, jaringan, dan media penyimpanan yang dimiliki. Kita dapat melakukannya secara manual maupun menggunakan beberapa *tools* yang ada di luar sana
- Skalabilitas dan elastisitas – *cloud computing* erat kaitannya dengan skalabilitas dan elastisitas, yakinkan bahwa penyedia layanan memiliki kemampuan untuk *scale up/scale down* tanpa mengganggu layanan yang sedang berjalan. Artinya sumber daya yang disewa dapat ditambahkan dan dikurangi sesuai dengan kebutuhan dan dapat dilakukan dengan dampak yang sangat

minimum atau bahkan tidak berdampak sama sekali terhadap aplikasi/layanan yang sedang berjalan

- Biaya layanan – sudut pandang yang harus dijaga adalah objektivitas penilaian atau pengambilan variabel pengukuran, ketika mencoba membandingkan satu layanan dengan layanan lainnya, pastikan menghitung parameter yang memiliki jumlah dan kemampuan yang setara. Contohnya jika membandingkan dari sisi media penyimpanan suatu penyedia layanan *cloud computing*, yang membutuhkan kapasitas sebesar 100GB, maka masing-masing penyedia layanan mungkin saja memberikan harga yang jauh berbeda. Mengapa hal itu bisa terjadi? Karena 100GB di atas *platform* yang memiliki performa (IOPS) dan tingkat efisiensi (deduplikasi dan kompresi) yang lebih tinggi tentu saja harga nya akan lebih mahal. Jadi sesuaikan biaya layanan dengan performa aplikasi dan tingkat kritikalitas yang ingin dicapai
- Dukungan layanan – beberapa hal yang dapat menjadi pertimbangan adalah bagaimana mekanisme penanganan insiden beserta responnya, bagaimana eskalasi dilakukan jika suatu permasalahan terjadi, melalui media apa saja bentuk dukungan yang akan di dapat nantinya (email, telepon, *remote session*, *on-site*, dll.). Yang jelas penyedia layanan lokal sepertinya dapat merespon dan berinteraksi lebih baik dalam hal *on-site support* dan komunikasi bahasa yang digunakan
- Yuridikasi dan lokasi data – hal ini dapat merujuk kepada peraturan OJK yang sudah disebutkan sebelumnya dan tentunya juga beberapa hal lain yang dapat dipertimbangkan adalah apakah lokasi nya berada pada lokasi bebas bencana dan lainnya
- Portabilitas dan interoperabilitas – data harus dapat dipindahkan dari satu penyedia layanan ke penyedia layanan lainnya ataupun kembali ke *data center* milik sendiri dan sebaliknya. Biasanya penyedia layanan akan menyediakan satu format standar tertentu yang bisa digunakan untuk memindahkan data atau beban kerja antar teknologi/*platform* yang berbeda, salah satu contohnya *Open Virtualization Format* (OVF)
- Backup dan Pemulihan Bencana – hal yang harus ditanyakan apakah mereka memiliki opsi layanan *backup* atau pemulihan bencana di lokasi yang berbeda dimana data-data perusahaan direplikasi dalam periode waktu tertentu, sehingga dampak bencana dapat diminimalisir. Jika tidak maka harus mereplikasi layanan ke penyedia layanan *cloud computing* yang berbeda
- SLA (*Service Level Agreement*) – ketepatan waktu dalam pelayanan jasa *cloud computing* sangatlah penting karena hal ini erat keterkaitannya dengan layanan perusahaan kita. Oleh karena itu beberapa hal yang harus dipastikan adalah apakah arsitektur *platform*, *facility data center*, dan jaringan didesain untuk bisa mencapai angka tersebut layanan yang dijanjikan dan pastikan bahwa semuanya *redundant* (meimiliki *backup*) setidaknya n+1 sehingga tidak ada *single point of failure*

E. Konsep-konsep Tata Kelola TI

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure • IT Security

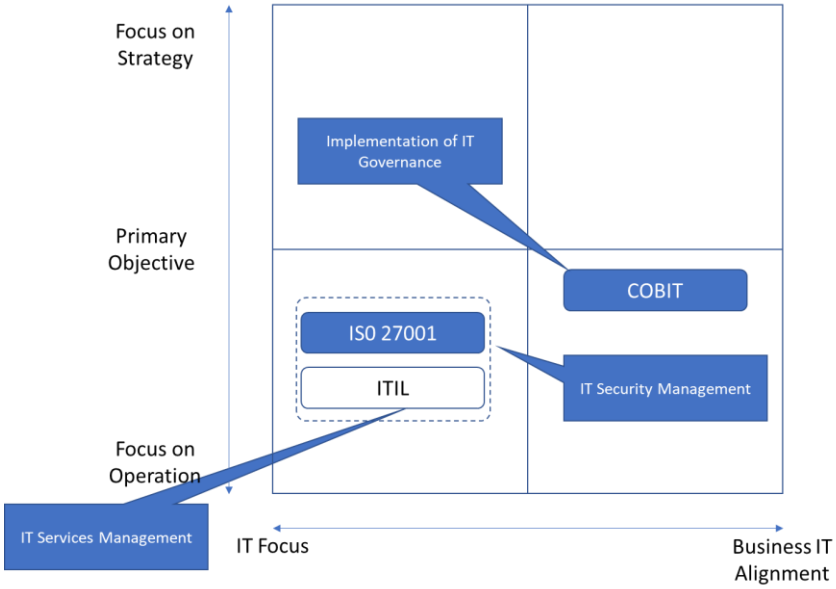
Good Corporate Governance (GCG) secara harfiah dapat diartikan sebagai tata kelola perusahaan. GCG merupakan suatu struktur yang mengatur pola hubungan harmonis tentang peran dewan komisaris, direksi, pemegang saham dan para *stakeholder* lainnya, dengan bentuk sistem pengecekan dan perimbangan kewenangan atas pengendalian perusahaan yang dapat membatasi munculnya dua peluang: pengelolaan yang salah dan penyalahgunaan aset perusahaan serta suatu proses yang transparan atas penentuan tujuan perusahaan, pencapaian, dan berikut pengukuran kinerjanya.

Secara prinsip GCG merupakan kaidah, norma, ataupun pedoman yang harus digunakan oleh pimpinan perusahaan dan para karyawan agar seluruh tindakan dan keputusan strategis yang dilakukan semata-mata dalam rangka untuk mendukung kepentingan perusahaan. Seluruh manajemen perusahaan diwajibkan untuk mematuhi dan melaksanakan pedoman yang telah disusun dalam rangka pelaksanaan GCG.

Untuk menerapkan prinsip-prinsip GCG dalam pengelolaan teknologi informasi (TI), maka perlu disusun tata kelola TI (IT *Governance*/tata kelola) yang menjadi bagian integral dari *Enterprise Governance* agar dapat menjamin pemanfaatan dari implementasi TI. IT *Governance* merupakan salah satu pilar utama dari GCG. Maka dalam pelaksanaan IT *Governance* atau tata kelola TI yang baik sangat diperlukan standar tata kelola TI dengan mengacu kepada standar tata kelola TI internasional yang telah diterima secara luas dan teruji implementasinya.

Dengan menyusun IT *Governance*, maka segala aktivitas perusahaan yang berbasis pada teknologi informasi akan lebih terkontrol, mencapai efisiensi, dan efektif. Teknologi informasi pada dasarnya berbentuk suatu sistem yang saling terintegrasi, jika ada kerusakan di salah satu titik, akan berdampak domino kepada titik yang lain. Maka dari itu untuk mencapai GCG diperlukan adanya penyusunan IT *Governance* yang baik.

Dalam implementasi IT *Governance*, terdapat beberapa *framework* atau kerangka kerja. Dijelaskan dalam lampiran PER-02/MBU/2013 bahwa IT *Governance* sebagai salah satu pilar utama GCG dalam pelaksanaannya membutuhkan *framework* yang mengacu kepada referensi tata kelola TI internasional yang telah diterima secara luas dan teruji implementasinya seperti COBIT, ITIL, ISO 27001, ISO 38500, TOGAF, dan PMBOK, yang dapat diimplementasi sesuai dengan kondisi perusahaan yang berbeda-beda.



Framework	Cakupan Proses	Kerjasama Panduan	Penggunaan Secara Umum
Control Objectives for Information and related Technology (COBIT)	Mencakup semua proses tata kelola TI yang meliputi: • Perencanaan dan pengorganisasian (PO), • Akuisisi dan implementasi (AI), • Penyampaian dan dukungan (DS), dan • Pengawasan (M)	Penjelasan cukup sampai kepada kontrol-kontrol yang harus ada dan tidak sampai kepada petunjuk rinci penerapannya	Sebagai referensi audit TI dan atau penilaian tata kelola TI
Information Technology Infrastructure Library (ITIL)	Proses Manajemen layanan TI yang meliputi 5 tahapan siklus layanan (service lifecycle): • Service Strategy • Service Design • Service Transition • Service Operation	Penjelasan meliputi ke 5 tahapan service life cycle dan proses proses pengelolaan layanan (ITSM) pada setiap tahapan service life cyle.	Sebagai penjelasan terhadap disiplin dan tanggung jawab dalam penentuan dan manajemen Layanan TI yang efektif.

	• Continual Service Improvement		
International Organization for Standardization (ISO) 27001	Dokumen standar sistem manajemen keamanan informasi atau Information Security Management System (ISMS) yang memberikan cakupan proses untuk melakukan evaluasi, implementasi dan memelihara keamanan informasi berdasarkan "best practice" dalam pengamanan informasi.	Petunjuk untuk penerapan keamanan informasi sebagai penjagaan informasi dalam rangka memastikan: kelangsungan bisnis minimasi risiko bisnis dan mengoptimalkan peluang bisnis dan investasi	Implementasi terhadap Information Security Management System (ISMS)
ISO 38500	Terdapat 6 prinsip sebagai framework IT Governance yang diterapkan untuk tata kelola TI, yaitu responsibility, strategy, acquisition, performance, conformance, dan human behaviour	Panduan terhadap prinsip-prinsip untuk manajemen organisasi dalam rangka pemanfaatan TI yang tepat guna, efektif dan efisien.	Pengelolaan TI dengan standar tata kelola secara high level yang diterapkan berdasarkan prinsip yang tercantum dalam ISO 38500
The Open Group Architecture Framework (TOGAF)	Berisi panduan framework dan metode pengembangan enterprise architecture yang meliputi tahapan: • Business Architecture • Information Architecture • Application Architecture • Technology Architecture • Transition Architecture	Panduan terhadap area-area yang harus ada dalam pengembangan enterprise architecture	Digunakan untuk mengembangkan enterprise architecture, dimana terdapat tools yang detail
Project Management Body of Knowledge (PMBOK)	Berisi panduan kerangka kerja pengelolaan proyek TI dan pengawasan kinerja proyek TI. Framework	Panduan terhadap area-area kerja yang detail dalam pengelolaan proyek	Sebagai panduan penyusunan kerangka kerja pengelolaan dan dan

	PMBOK memberikan referensi lebih detil untuk melengkapi framework COBIT terkait pengelolaan proyek TI.		pengawasan proyek TI sehingga proyek TI tersebut dapat berjalan sesuai dengan yang diharapkan*

Untuk melengkapi panduan tata kelola yang akan dipilih oleh sebuah perusahaan Asuransi, maka sebuah perusahaan asuransi juga harus mempertimbangkan POJK-4-POJK-05-2021 dalam pengelolaan TI. Apalagi Asuransi merupakan sebuah institusi yang wajib untuk mengikuti regulasi atau peraturan yang dikeluarkan oleh badan pengawas Asuransi yang sah dari pemerintah. Berdasarkan regulasi ini, beberapa hal yang harus menjadi catatan bagi perusahaan Asuransi yaitu Direksi harus terlibat dalam menetapkan:

- Perencanaan TI
- SOP yang jelas dan transaparan terkait dengan TI
- Program pengembangan sumber daya manusia sehingga sumber daya TI mempunyai kemampuan yang selalu terkini yang dapat membawa kebaikan bagi perusahaan serta masyarakat, nasabah, agen, dan lain-lain
- Pengembangan TI beserta proyek-proyek yang pendukungnya

Penerapan manajemen risiko juga menjadi suatu hal yang wajib dengan cara:

- Pengawasan aktif Direksi dan Dewan Komisaris
- Kebijakan dan prosedur penggunaan TI
- Proses identifikasi, pengukuran, pengendalian dan pemantauan resiko penggunaan TI
- Sistem pengendalian internal atas penggunaan TI

Bagi perusahaan Asuransi dengan *aset* lebih besar dari IDR 1 Trilyun, maka harus diadakan Komite Pengarah TI yang memberikan rekomendasi atas:

- Rencana pengembangan TI
- Kebijakan dan prosedur TI
- Proyek pengembangan TI
- Kesesuaian TI dengan sistem informasi manajemen

Beberapa hal lain yang juga harus diperhatikan yang terdapat dalam regulasi tersebt adalah:

- Asuransi dengan aset antara IDR 500 Milyar sampai dengan IDR 1 Trilyun harus mempunyai pusat data sendiri. Asuransi dengan aset di atas IDR 1 Trilyun harus mempunyai pusat data dan pemulihan bencana sendiri
- Wajib mempunyai rencana pemulihan bencana

http://itjambi.com/it-governance-salah-satu-pilar-utama-good-corporate-governance/

- Jadwal audit internal dan external secara berkala
- Pengelolaan TI dengan menggunakan jasa external harus mengikuti ketentuan POJK
- Kebijakan TI harus ada limit resiko, mempertimbangkan faktor keamanan informasi, dikaji secara berkala dan mempunyai jangka waktu

F. IT *Security*

Tentang IT *Security*

Penanggung Jawab Utama	• Head of IT • IT Security

Pada jaman digitalisasi seperti sekarang ini maka data menjadi salah satu aset perusahaan yang berharga. Penyalahgunaan data akan dapat merugikan banyak pihak termasuk perusahaan itu sendiri. Maka setiap perusahaan wajib memberikan perlindungan sebaik mungkin terhadap data perusahaan.

Tujuan IT *Security*:

1. Melindungi pengguna (*user*), perangkat komputer (*server* dan aset komputer perusahaan), sistem aplikasi, jaringan komunikasi, dan informasi
2. Membuat aturan sebagai arahan untuk pengguna (*user*), sistem administrator, manajemen, dan petugas keamanan sistem informasi
3. Menetapkan petugas keamanan untuk pengawasan, penyelidikan, atau pemeriksaan
4. Membantu mengurangi risiko yang mungkin akan muncul
5. Membantu arahan kepatuhan pada peraturan dan undang-undang.
6. Menetapkan peraturan resmi perusahaan mengenai keamanan

Ada 3 aspek (CIA (Confidentiality, Integrity dan Availability) Triad) mengenai data *security* yang harus dipenuhi, sebagai berikut:

1. ***Confidentiality*****,** melindungi informasi dari orang luar yang tidak berhak atau penghapusan informasi.
2. ***Integrity*****,** melindungi informasi dari modifikasi yang tidak berhak dan memastikan informasi tersebut akurat dan lengkap.

3. ***Availability*,** memastikan informasi tersedia ketika dibutuhkan.*

IT *Security* harus mencakup:

1. *Password Policy*
   - Perusahaan memberikan data *password* kepada karyawan yang berhak mengakses sistem informasi perusahaan berupa sistem operasi, *application network*, *email* untuk mendukung kegiatan usaha perusahaan;
   - Setiap karyawan yang memperoleh *password* wajib menjaga kerahasiaan dan keamanan kata sandi;
   - Setiap pengajuan *username* untuk sistem informasi harus mendapat persetujuan dari manajer karyawan yang bersangkutan. Bagian TI akan memberikan *default password* yang harus segera diganti oleh karyawan yang menerimanya saat pertama kali menggunakan *default password* dengan mengikuti ketentuan yang dijelaskan dalam "Pedoman Password";
   - Departemen TI akan segera menghapus/*menonaktifkan* semua *password* dari karyawan dengan status mengundurkan diri (tidak tercatat sebagai karyawan) atas permintaan dan pemberitahuan dari departemen SDM (Sumber Daya Manusia);
   - *Password* harus menggunakan kombinasi unik
   - *Password* harus diperbarui secara berkala

2. *Access Request & Recertification*
   Pemberian akses kedalam sistem harus melalui prosedur formal yang mencakup *approval* dari *Head of Business* Unit terkait dan IT *Team* terkait (*maker-checker mechanism*). *Recertification* secara berkala juga perlu dilakukan untuk memastikan validasi dari *active user* ID, baik secara *activity* maupun cakupan *granting* yang diberikan.

   Terkait dengan validasi akses, sebaiknya perusahaan dapat membuat integrasi ID *login* & *password* ke *active directory*. Jadi *users* tidak perlu mengingat banyak ID & *password* untuk masuk ke aplikasi yang terdapat *Single Sign on Concept*. Ini akan memudahkan juga saat ingin melakukan *in-activate account*.

3. *Software Version & Patch Management*
   Perkembangan *software* akan membutuhkan pembaharuan secara berkala untuk memastikan *security, support* & *compatibility aspect*. Jadwal *patch* secara berkala dan *review* tahunan untuk *End of Life Softwares* akan meningkatkan IT *Environmen*t perusahaan. Kalaupun ada pengecualian karena berbagai alasan/keterbatasan, risiko tersebut sebaiknya diketahui/disetujui oleh bagian yang berkepentingan (TI, *risk, compliance*, dan direktur terkait). Pengaplikasian patch harus dikoordinasikan dengan bagian IT Operation, Network & Infrastructure.

**https://www.logique.co.id/blog/2021/02/18/keamanan-informasi/*

4. *Install IT Security Software*

   Penjagaan keamanan sistem perlu dilakukan dengan melakukan instalasi *software* yang dapat mengamankan sistem perusahan. Adapun contoh dari *software* tersebut adalah seperti *antivirus*, *encryption software, firewall*, dll. Hal ini dapat dilakukan sesuai dengan kebutuhan dari perusahaan.

5. *Segregation of Duty*

   Untuk meminimalkan risiko, pemisahan tanggung jawab dan kontrol terhadap akses perlu dilakukan. Paling sedikit bisa dilakukan 2 hal:

   - *Maker – Checker*

     Semua kegiatan/traksaksi yang dipandang kritis dapat *menerapkan requestor & approver concept*. Untuk memastikan ada pihak lain yang melakukan cek keabsahan/keakuratan permintaan tersebut.
   - *Limitation of Environment Access*

     Super User / Admin akses sebaiknya hanya dimiliki orang-orang tertentu dengan akses kontrol yang jelas. Untuk kegiatan sehari-sehari, pembatasan tersebut dapat berupa:

     a. Developer tidak memiliki akses ke *production environment*
     b. IT Business Analyst tidak memiliki akses di *production environment*
     c. *Database Adminitstration* (DBA) *activity* dimonitor secara berkala oleh Head of IT yang bersangkutan
     d. Dan lain-lain sesuai dengan tingkat keamanan yang dibutuhkan perusahaan

     Jika ada pengecualian karena berbagai alasan/keterbatasan, risiko tersebut sebaiknya diketahui/disetujui oleh bagian yang berkepentingan (TI, *risk, compliance*, dan direktur terkait).

6. *End Point Protection*

   Untuk mengamankan data perusahaan, perlu diterapkan beberapa aturan dasar yang harus dipatuhi karyawan:

   - Menutup *port* pada perangkat TI (PC/laptop) agar data tidak dapat disalin keluar dari *environment* perusahaan.
   - Enkripsi *hard disk mobile device* (laptop)
   - Jika diperlukan pengiriman data keluar *environment* perusahaan, *file* harus diberi *password*/dienkripsi
   - *End User* sebaikya tidak memiliki *admin access* untuk perangkat yang dimiliki.

7. *Awareness*

   - Selalu memperbaharui material terkait IT *Security Awareness*
   - Melakukan training & sosialisasi terkait IT *Security* secara berkala
   - Memasukkan IT *Security Awareness* sebagai salah satu item orientasi karyawan baru

8. Lainnya
   - *Secured System Development* – contoh konsep yang biasa digunakan adalah Security Development Lifecycle (SDL) dengan konsep pondasi dalam membangun *software* yang lebih baik, termasuk mendesain keamanan, model ancaman, keamanan *coding*, *security test*, dan praktek seputar privasi
   - *Malware Protection* – sebagai perangkat lunak yang dapat memasuki dan merusak sistem komputer atau *server* tanpa diketahui termasuk bertujuan mencuri data, maka harus diberikan sebuah proteksi yang dapat memberikan keamanan terhadap sistem komputer perusahaan. Proteksi yang dapat digunakan saat ini sudah banyak tersedia di pasaran namun yang terpenting adalah perusahaan sudah harus mempunyai proteksi ini mengingat resiko pencurian data harus dihindari dimana umumnya perusahaan Asuransi mengelola data-data rahasia termasuk data nasabah dalam Jumlah besar dan harus dilindungi dengan baik
   - *Data Protection* – bila *malware* melakukan pencurian data melalui internet, maka khusus untuk *Data Protection* ini adalah proteksi dari pencurian yang terjadi dengan cara tidak melalui internet. Hal ini bisa terjadi melalui karyawan perusahaan sendiri misal dengan menggunakan USB. Oleh karena itu sangatlah penting untuk memperhatikan aspek ini. Banyak perangkat lunak di pasaran yang dapat melakukan proteksi terhadap hal ini yang umum bekerja dengan mengaplikasikan data enkripsi, keamanan komputer dan manajemen keamanan komputer secara terpusat
   - *Incident Response* – biasanya dilakukan dengan melakukan *Incident Response Planning* (IRP) yang terdiri dari satu set proses dan prosedur detail yang mengantisipasi, mendeteksi, dan mengurangi akibat dari insiden yang tidak diinginkan yang membahayakan sumber daya informasi dan aset organisasi, ketika insiden ini terdeteksi benar-benar terjadi dan mempengaruhi atau merusak aset informasi. Insiden merupakan ancaman yang telah terjadi dan menyerang aset informasi, dan mengancam *confidentiality*, *integrity* atau *availbility* sumber daya informasi. *Insident Response Planning* meliputi *incident detection, incident response*, dan *incident recovery.*
   - *Business Continuity Management* – adalah suatu rancangan yang diterapkan oleh perusahaan untuk menyakinkan usaha-usaha yang dilakukan perusahaan agar bisnis tetap beroperasi kembali pada kondisi yang dapat diterima setelah terjadinya insiden disrupsi
   - *Hardening server* – kegunaan dari penguatan atau pengerasan *server* adalah untuk mengurangi permukaan serangan *server* (*surface attacks*). Permukaan serangan adalah semua titik berbeda di mana penyerang dapat mencoba mengakses atau merusak sesuatu, baik itu *server*, database, aplikasi, jaringan atau pun OS (*Operating System*). Dalam komputasi, perlindungan dalam melakukan penguatan keamanan tersebut diberikan dalam berbagai lapisan (*layer*) dan sering disebut sebagai defense in depth (pertahanan mendalam). Melindungi dalam lapisan berarti melindungi pada level *host*, level aplikasi, level sistem operasi, level pengguna, level fisik, dan semua sublevel di antaranya
   - *Penetration Testing* – secara berkala untuk menguji keamaan sistem informasi dengan cara mensimulasikan serangan yang bisa dan mungkin dilakukan agar dapat menemukan titik lemah

dari suatu sistem. Cara ini umumnya dilakukan dengan menggunakan perangkat lunak yang tersedia di pasaran

- *Data disposal* – computer dan server pada perusahaan mempunyai masa pakai. Bila telah tiba pada masa pakai nyam aka perlu diperhatikan prosedur dalam membuang computer dan server karena data-data yang sudah dihapus pada perangkat tersebut masih mungkin dikembalikan lagi dengan berbagai teknik di dunia TI sehingga hal ini akan berpotensi sebagai sumber kebocoran data bila perangkat tersebut dibuang dengan prosedur yang tidak tepat. Cara yang mudah adalah dengan menghancurkan *hard disk* (perangkat penyimpanan data) dengan benda keras seperti palu. Namun bila masih ingin mempertahankan *hard disk* tersebut maka harus menggunakan perangkat lunak pihak ketiga yang berfungsi untuk menghapus data tersebut secara permanen tanpa bisa dikembalikan lagi

Sebagai tambahan informasi dalam rangka mengacu kepada peraturan yang berlaku yaitu Peraturan yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN) nomor 8 tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik dimana Asuransi merupakan perusahaan yang masuk ke dalam kategori sebagai Penyelenggara Elektronik. Untuk itu sebagai badan usaha Penyelenggara Elektronik diharuskan melakukan penerapan Sistem Manajemen Pengaman Informasi (SMPI) dengan mengadopsi SNI ISO/IEC 27001 (standar internasional dalam mengelola risiko keamanan informasi) atau standar keamanan lain yang ditentukan oleh BSSN.

Adapun terkait dengan SMPI, diharuskan menggunakan tenaga lokal ataupun konsultan lokal. Bilamana terpaksa menggunakan tenaga asing atau konsultan asing maka harus mendapat persetujuan dari BSSN sesuai yang tertera pada aturan ini.

Dalam hal penerapan SMPI akan dilakukan sertifikasi (audit) dalam kurun waktu 2 kali dalam setahun dengan lembaga yang disetujui oleh BSSN. Bilamana saat dilakukan sertfikasi ditemukan hal-hal yang tidak memenuhi standar, maka perusahaan akan diberikan waktu selambat-lambatnya 90 hari untuk melakukan penyesuaian dalam rangka memenuhi standar tersebut. Melebihi waktu yang ditentukan untuk memenuhi standar, maka akan menerima konsekuensi dimana sertifikasi akan dicabut oleh BSSN dengan sanksi administratif.

Information Security

Penanggung Jawab Utama	• Head of IT • IT Security

Information Security (IS) adalah model operasional khusus dari Sistem Manajemen Keamanan Informasi atau *Information Security Management System* (ISMS). Terdiri dari aturan dan pedoman, kerangka prosedural serta pengaturan organisasi pendukung untuk IS. Dengan demikian fungsi dan tugas terkait IS,

termasuk aturan, peran, tanggung jawab terhadap masing-masing di perusahaan yang diperlukan untuk melindungi informasi perusahaan secara memadai dengan cara yang sistematis.

ISMS didasarkan pada standar ISO / IEC 27000-*series*. Sasaran utama ISMS adalah perlindungan yang memadai atas informasi perusahaan dengan fokus khusus pada operasional.

Persyaratan IS ditentukan oleh fungsi keamanan informasi secara umum mencakup pelaksanaan:

1. Manajemen Akses Pengguna
   User Access Management (UAM), juga dikenal sebagai *Indentity and Access Management* (IAM), adalah administrasi yang memberikan pengguna individu dalam sistem akses ke alat yang mereka butuhkan pada waktu yang tepat. Untuk bisnis, ini biasanya mencakup akses ke aplikasi eksternal, izin, dan persyaratan keamanan.

2. Enkripsi
   Enkripsi adalah proses data dikodekan sehingga tetap tersembunyi atau tidak dapat diakses oleh pengguna yang tidak sah. Ini membantu melindungi informasi pribadi, data sensitif, dan dapat meningkatkan keamanan komunikasi antara aplikasi klien dan *server*.

3. Personel Keamanan
   Penanganan dan penggunaan yang benar dari proses dan tindakan terkait keamanan seperti;
   - Materi pelatihan untuk memberikan pemahaman yang baik kepada karyawan tentang alasan, dan keefektifan, perlindungan serta potensi kelemahan kontrol keamanan untuk menghindari pelanggaran keamanan
   - Menjelaskan tanggapan dan tindakan jika terjadi insiden terkait keamanan, sehingga karyawan dapat bereaksi dengan tepat.

4. Keamanan Jaringan
   Keamanan jaringan atau yang biasa disebut sebagai *network security* biasanya dilakukan untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, modifikasi, dan lain-lain. Dimana tindakan pencegahan untuk melindungi jaringan tersebut merupakan tugas dari seorang administrator jaringan.

5. Keamanan Pembuatan Aplikasi
   Memastikan bahwa aplikasi (termasuk yang sedang dikembangkan) memenuhi persyaratan keamanan bisnis dan informasi. Aplikasi termasuk semua komponen sistem yang diperlukan untuk memenuhi tujuan bisnis.

6. Keamanan Operasional I
   Memastikan keamanaan saat beroperasi untuk seluruh kegiatan sistem TI dan aplikasi.

7. Hubungan Layanan dengan Pihak Ketiga Termasuk *Outsourcing*

Memastikan perlindungan aset berharga perusahaan yang dapat diakses atau dipengaruhi oleh pemasok.

G. Pemantauan dan Pemeliharaan Sistem Teknologi Informasi

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure • IT Development • IT Security

Dalam menjaga keberlangsungan sistem informasi dan infrastruktur diperlukan kerjasama erat dari IT Operation yang paham akan kompleksitas, IT Insfrastructure, IT Development yang paham dengan struktur aplikasi, dan IT Security yang paham akan perkembangan terbaru dari keamanan informasi dan jenis serangan *cyber* yang berkembang cukup pesat.
Penting bagi perusahaan untuk dapat mempertahankan dan meningkatkan performa dari sistem TI nya agar dapat terus berjalan dengan baik dan bisa mendukung proses bisnis. Maka perlu dilakukan adanya proses pemantauan berikut pemeliharaannya sehingga dapat memperkecil *down time* dan kebocoran data.

Ada beberapa hal yang perlu dilakukan:

1. **Audit Sistem**
   Yaitu melakukan penggunaan dan penelitian formal untuk menentukan seberapa baik sistem baru dapat memenuhi kriteria kinerja. Hal semacam ini disebut penelaahan setelah penerapan dan dapat dilakukan oleh seorang auditor internal.

2. **Penjagaan Sistem**
   Yaitu melakukan pemantauan untuk pemeriksaan rutin sehingga sistem tetap beroperasi dengan baik. Selain itu juga untuk menjaga kemutakhiran sistem jika sewaktu-waktu terjadi perubahan lingkungan sistem atau modifikasi rancangan *software*.

3. **Perbaikan Sistem**
   Yaitu melakukan perbaikan jika dalam operasi terjadi kesalahan (*bugs*) dalam program atau kelemahan rancangan yang tidak terdeteksi saat tahap pengujian sistem. Mengganti sistem dan perangkat yang sudah tidak dapat digunakan.

4. **Peningkatan Sistem**
   Yaitu melakukan modifikasi terhadap sistem ketika terdapat potensi peningkatan sistem setelah sistem berjalan beberapa waktu, biasanya adanya potensi peningkatan sistem tersebut terlihat oleh manajer kemudian diteruskan kepada spesialis informasi untuk dilakukan modifikasi sesuai keinginan manajer.[*]

**https://ceritahosting.com/2021/01/13/pemeliharaan-sistem-perangkat-di-perusahaan/*

5. Pemeliharaan Sistem

Yaitu pemeliharaan perangkat lunak atau *software* aplikasi oleh manajer pada *security*, *backup (hal ini termasuk pengetesan recovery/restorasi data)*, dan *monitoring* terhadap keseluruhan aplikasi serta melakukan *update* perangkat lunak antivirus agar tidak terjadi kerusakan sistem atau perangkat lunak yang berisiko pada data-data yang ada di sistem tersebut.

6. Dokumentasi Pemantauan dan Pemeliharaan Sistem TI

Yaitu adanya dokumentasi aktivitas poin 1 s.d 5 agar dapat digunakan sebagai dokumen tetap, bahan pembelajaran, dan evaluasi terkait aktivitas tersebut.

H. Manajemen Perubahan *(Change Management)*

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure • IT Development • IT Security

Manajemen perubahan adalah disiplin TI. Tujuan dari manajemen perubahan dalam konteks ini adalah untuk memastikan bahwa metode dan prosedur standar digunakan untuk penanganan yang efisien dan cepat dari semua perubahan untuk mengendalikan infrastruktur TI dan juga sistem/aplikasi pada perusahaan.

Untuk meminimalkan jumlah dan dampak insiden terkait pada layanan. Perubahan dalam infrastruktur TI dapat muncul secara reaktif sebagai respon terhadap masalah atau persyaratan yang dipaksakan secara eksternal, misalnya perubahan legislatif, atau secara proaktif dari upaya peningkatan efisiensi dan efektivitas atau untuk mengaktifkan atau mencerminkan inisiatif bisnis, atau dari program, proyek, atau inisiatif peningkatan layanan. Manajemen perubahan dapat memastikan metode, proses, dan prosedur standar yang digunakan untuk semua perubahan, memfasilitasi penanganan semua perubahan yang efisien dan cepat, dan menjaga keseimbangan yang tepat antara kebutuhan akan perubahan dan potensi dampak perubahan yang merugikan.

Proses Manajemen Perubahan

1. Permintaan Perubahan Dibuat

   Perubahan dan masalah ditangkap melalui pertemuan tim proyek, kelompok kerja pemangku kepentingan eksternal termasuk lembaga pemerintah lainnya, pertemuan dewan proyek, hasil dari tahap persetujuan sudah melalui pemantauan oleh tim proyek dan sponsor proyek.*

   Forum ini memungkinkan perubahan dapat dipantau di semua tingkatan dari perubahan lingkup kecil yang dibuat untuk memperbaiki kesalahan, hingga masalah besar yang timbul dari perubahan kebijakan pemerintah. Sebagian besar perubahan ruang lingkup dilakukan pada tahap persetujuan, tetapi perubahan besar pada konten dipantau melalui pengetahuan tentang perkembangan kebijakan yang keluar dari kelompok kerja dan dari jaringan yang dilakukan oleh sponsor proyek dan dewan proyek.

2. Daftar dan Nilai Perubahannya

   Permintaan perubahan dilihat pada sentral yang memungkinkan manajer monitor perubahan. Ketika terdapat perubahan, perubahan tersebut dinilai oleh manajer proyek menggunakan saran spesialis dari tim proyek. Tim proyek memastikan:

   - Apakah berhubungan dengan proyek?

- Apakah benar-benar risiko atau masalah yang dapat diterima atau ditangani tanpa perubahan?
- Apakah benar-benar proyek baru?
- Apakah diperlukan untuk memenuhi tujuan proyek & KPI?
- Apa yang akan terjadi jika perubahan tidak diterapkan?*

3. Analisa dan Pengiriman *Request for Change Form* (RFC) ke Komite Pengarah Teknologi Informasi

   Jika perubahan tersebut *valid*, manajer proyek menilai dampak perubahan tersebut dengan tim proyek dan menyerahkan perubahan tersebut melalui formulir permintaan perubahan kepada manajer perubahan. Kemudian diserahkan kepada Komite Pengarah Teknologi Informasi yang menilai perubahan dan menyetujui atau menolaknya.

   Proses ini berinteraksi dengan proses manajemen konfigurasi untuk proyek dan program. Manajer perubahan bertanggung jawab untuk mengelola perubahan di seluruh program. Mereka melihat tren, isu strategis yang lebih luas, melakukan audit dan pemeriksaan kualitas, dan bekerja untuk meningkatkan proses.

4. *Request for Change Form* (RFC)

   Merupakan *form* yang di desain oleh masing-masing perusahaan untuk dapat lebih memperjelas keinginan perubahan dari tim bisnis kepada tim TI. Isi form tersebut biasanya mencakup:
   - Tanggal permintaan
   - Nama yang meminta
   - Atasan dari yang meminta beserta tanda tangan persetujuan
   - Tujuan dari perubahan
   - Perubahan yang di minta
   - Dampak serta keuntungan dari perubahan

5. *Change Board* (Tim Dewan Perubahan) Menerima atau Menolak Perubahan

   Dewan Perubahan mencakup klien dan manajer senior yang memiliki tinjauan strategis. Mereka menilai apakah perubahan tersebut dalam toleransi program dan dapat menyetujui sebagian besar perubahan. Mereka mungkin melihat:

   - Pengaruh perubahan pada kasus bisnis,
   - Perubahan dalam kaitannya dengan program secara keseluruhan,
   - Melihat efek dari perubahan,
   - Setiap risiko tambahan yang terkait dengan perubahan,
   - Pelajaran apa saja yang dapat dipetik dari perubahan tersebut,
   - Tren apa pun yang diungkapkan oleh perubahan.

**https://www.stakeholdermap.com/change/change-management-process.html*

Jika perubahan di luar toleransi program, itu berarti manajer proyek akan mengeskalasi perubahan tersebut ke dewan program dan manajer kontrak. Jika ini terjadi, perubahan akan ditangani secara terpisah pada proyek, tetapi dapat menyebabkan penutupan proyek jika hal itu secara mendasar akan mempengaruhi kasus bisnis proyek.

6. Perbarui Rencana & Terapkan Perubahan

   Setelah perubahan disetujui, *log* perubahan diperbarui dan pemangku kepentingan diinformasikan. Manajer proyek kemudian bekerja dengan tim proyek untuk merencanakan pelaksanaan perubahan; mengubah proyek dan rencana tahapan, mencari peralatan atau personel tambahan, memperbarui item konfigurasi dan menyelesaikan pekerjaan.*

**https://www.stakeholdermap.com/change/change-management-process.html*

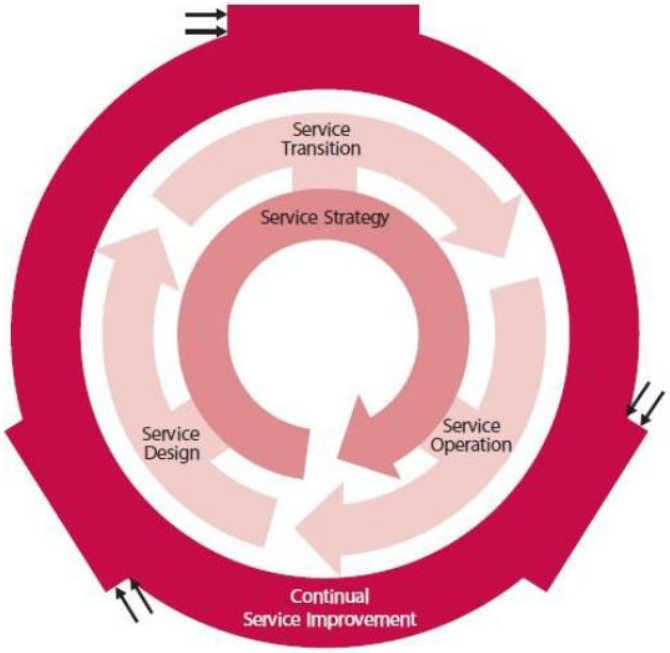
I. Manajemen Insiden

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure

Manajemen Insiden adalah proses dari IT *Service Management* atau biasa disingkat menjadi ITSM. Proses ini lebih berfokus untuk memperbaiki kinerja layanan TI sebuah organisasi atau perusahaan dalam waktu secepat mungkin agar bisa kembali normal. Dalam artian lain, proses ini mengelola gangguan layanan yang terjadi dalam TI serta memperbaiki gangguannya. Hal ini diberlakukan supaya tidak mengganggu jalannya bisnis. Pasalnya, gangguan TI tidak bisa kita hindari saat berlangsungnya kegiatan bekerja di kantor. Baik itu saluran telepon, data komputer, atau gangguan-gangguan TI lainnya bisa menyebabkan pekerjaan menjadi tertunda. Manajemen insiden juga terkadang disebut sebagai *ticket management, call management,* atau *request management*. Dalam prosesnya, biasanya manajemen insiden akan dikelola oleh tim TI di suatu perusahaan.

Lingkup tanggung jawab proses penanganan insiden tentu akan mencakup 6 kategori lingkup manajemen risiko pada perusahaan (infranstruktur, jaringan, aplikasi, data/informasi dan *security*) yang menjadi bagian masing-masing dari 3 unit kerja TI (Operation, Development dan Security). Oleh karena itu penanggung jawab utama manajemen indisen tentunya disesuaikan dengan lingkup masing-masing unit kerja TI.

Framework ITIL (Information Technology Infrastructure Library) adalah sebuah *framework* tata kelola TI yang berisi best practice secara khusus dalam manajemen servis TI [ITL07]. Pada saat ini *framework* ITIL sudah dikembangkan hingga versi 3. Pada versi ini, seperti yang tertuang dalam gambar di bawah ini., *Framework* ITIL dijelaskan tahap-tahap pengelolaan manajemen layanan TI yaitu sebagai *service lifecycle*.



Framework* ITIL v3 *Service Lifecycle

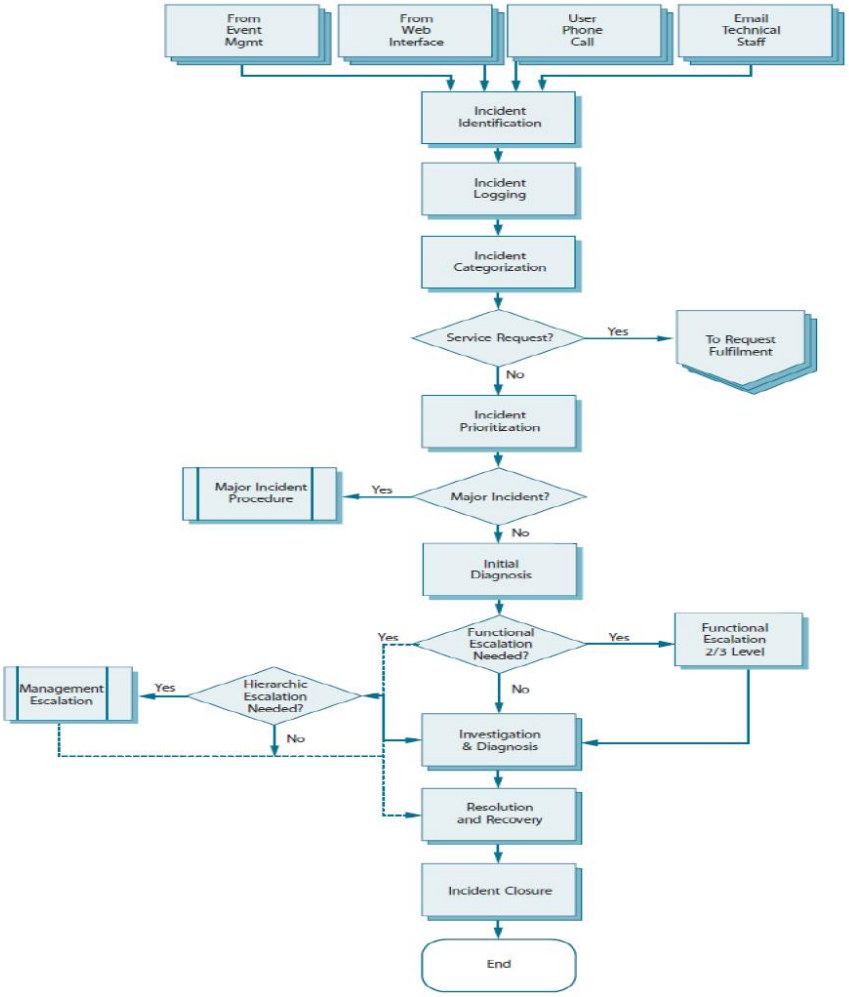
Ada 5 proses *service lifecycle* dalam ITIL [ITL07] seperti yang ditampilkan gambar di atas, yaitu:

1. *Service Strategy*: Pada tahap ini dilakukan pengembangan strategi untuk mengubah manajemen service TI menjadi sebuah aset strategis dari organisasi.
2. *Service Design*: Pada tahap ini dilakukan pembangunan panduan manajemen layanan TI berdasarkan strategi yang sudah dikembangkan sebelumnya pada tahap *Service Strategy*. Selain itu panduan dibangun berdasarkan kebijakan yang berlaku dalam organisasi dan untuk pemenuhan kepuasan pelanggan.
3. *Service Transition*: Pada tahap ini dilakukan proses transisi dari tata kelola yang lama kepada tata kelola yang baru yang sudah dikembangkan dalam tahap *Service Design*.
4. *Service Operation*: Pada bagian ini berisi langkah-langkah *best practice* untuk melakukan manajemen servis TI.
5. *Continual Service Improvement*: Pada bagian ini dilakukan pengelolaan masukan dari pelanggan yang kemudian dikolaborasikan kedalam empat tahap diatas. Hal ini bertujuan untuk meningkatkan hasil keluaran dari kegiatan *Service Strategy, Service Design, Service Transition*, dan *Service Operation*.

Menurut *framework* ITIL, pengertian insiden adalah sebuah interupsi atau pengurangan kualitas dari layanan TI. Selain itu sebuah kesalahan konfigurasi pada sistem dapat dikatakan sebagai insiden walaupun belum menimbulkan masalah yang berarti pada sistem tersebut. Manajemen insiden (*incident management*) adalah proses yang dilakukan untuk menyelesaikan suatu insiden. Proses manajemen insiden dilakukan berdasarkan *input* dari *user* melalui *service desk*, laporan teknisi, dan juga deteksi

otomatis dari sebuah *tool event management*. Manajemen insiden *(incident management)* pada *framework* ITIL v3 berada pada siklus *service operation*.

Manajemen Insiden ITIL



Aktivitas-aktivitas dalam manajemen insiden menurut *framework* ITIL seperti yang juga ditampilkan pada gambar diantaranya:*

1. Identifikasi Insiden *(Incident Identification)*

   Proses manajemen insiden dimulai dengan identifikasi. Identifikasi yang paling umum dilakukan adalah melalui layanan *service desk* dan laporan dari staf teknisi. Aktivitas-aktivitas dalam manajemen insiden menurut *framework* ITIL seperti yang juga ditampilkan pada gambar diantaranya

** http://digilib.its.ac.id/public/ITS-Master-12477-Paper.pdf*

2. Identifikasi Insiden *(Incident Identification)*
   Proses manajemen insiden dimulai dengan identifikasi. Identifikasi yang paling umum dilakukan adalah melalui layanan *service desk* dan laporan dari staf teknisi. Selain itu identifikasi insiden dapat dilakukan secara otomatis oleh *tool event management* yang dipasang pada perangkat-perangkat utama. Kondisi ideal dari langkah identifikasi adalah insiden dapat teridentifikasi sebelum terjadi implikasi terhadap *user*.

3. Pencatatan Insiden *(Incident Logging)*
   Langkah ini wajib dilakukan untuk setiap jenis insiden baik yang berskala besar maupun kecil. Beberapa informasi yang harus dicatat terkait suatu insiden adalah ID, kategori insiden, waktu terjadi, deskripsi insiden, nama orang/grup yang bertanggungjawab atas penanganan, implikasi insiden, dan waktu penutupan kasus.

4. Pengkategorisasian Insiden *(Incident Categorization)*
   Dalam membuat kategori insiden dibutuhkan sebuah proses khusus antara pengelola TI dan pihak manajemen organisasi. Hal ini bertujuan untuk menghasilkan kategori insiden dan prioritas penanganannya sejalan dengan proses bisnis organisasi. Kategori insiden dapat dibuat berdasarkan perkiraan lamanya penanganan, implikasi terhadap proses bisnis organisasi, dan jumlah staf teknis terkait.

5. Prioritas Insiden *(Incident Priorization)*
   Langkah prioritas insiden dilakukan berdasarkan kategorisasi yang telah dibuat sebelumnya. Prioritas penanganan insiden dapat dilakukan berdasarkan besarnya implikasi insiden terhadap kegiatan bisnis utama organisasi, ataupun berdasarkan lamanya penanganan insiden.

6. Diagnosa Awal *(Initial Diagnosis)*
   Diagnosa awal terhadap insiden wajib dilakukan oleh setiap pihak yang pertama kali berhubungan dengan insiden baik itu *service desk*, staf teknis, maupun perangkat otomatis seperti *event management*. Jika insiden ditemukan oleh *service desk* melalui telepon dari *user*, maka diusahakan *service desk* tersebut yang menyelesaikan insiden selama *user* masih berhubungan telepon.

7. Eskalasi Insiden *(Incident Escalation)*
   Eskalasi insiden adalah tindakan menaikkan level penanganan insiden. Hal ini berkaitan erat dengan hasil diagnosa awal terhadap insiden. Jika dari diagnosa ditemukan insiden yang tidak dapat ditangani, maka wajib dilakukan eskalasi insiden. Eskalasi insiden ada 2 macam, yaitu eskalasi fungsi dan eskalasi hierarki. Eskalasi fungsi adalah tindakan menaikkan level penanganan kepada satu level diatasnya. Sedangkan eskalasi hierarki adalah tindakan menaikkan level penanganan melintasi hierarki organisasi misalnya kepada manajer TI atau manajer bisnis yang terkait.

8. Investigasi *(Investigation and Diagnosis)*
   Tindakan investigasi dilakukan untuk menemukan sumber masalah dari insiden. Dalam melakukan investigasi, setiap tindakan wajib dilaporkan juga ke dalam formulir insiden. Hal ini berguna sebagai data historis tindakan penanganan suatu insiden.

9. Resolusi *(Resolution and Recovery)*
   Langkah ini merupakan tindakan yang diambil untuk menyelesaikan suatu insiden. Langkah resolusi dapat dilakukan oleh *service desk* sebagai pihak yang pertama menemukan insiden dari *user*, staf teknisi yang sedang mengerjakan kegiatan konfigurasi, maupun oleh *supplier* terhadap perangkat yang masih dalam garansi.

10. Penutupan *(Incident Closure)*
    Langkah penutupan adalah langkah yang dilakukan oleh *service desk* maupun staf teknisi terkait untuk memastikan apakah insiden telah benar selesai ditangani. Yang harus diperhatikan dalam langkah penutupan ini adalah dokumentasi proses penanganan insiden, perkiraan terhadap perulangan insiden, dan survei kepuasan *user* atas penanganan insiden.

J. Manajemen Aset TI

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure

Manajemen Aset TI merupakan hal yang sangat penting. Hal ini bertujuan:

- Berguna untuk memastikan status kepemilikan suatu aset di perusahaan
- Memudahkan untuk inventarisasi kekayaan dan masa pakai aset yang dimiliki
- Fungsi kontrol untuk menjaga agar nilai aset tetap tinggi dan memiliki usia hidup yang panjang.
- Meminimalisasi biaya selama umur suatu aset masih berlaku
- Sarana untuk memastikan suatu aset dapat menghasilkan keuntungan yang maksimum.
- Memandu agar penggunaan dan pemanfaatan aset bisa secara optimal
- Untuk keperluan pengamanan aset
- Sebagai acuan untuk menyusun neraca dalam akuntansi bagi tim inventarisasi

Beberapa hal terkait manajemen aset yang dapat diperhatikan adalah:

- Aturan dalam penggunaan aset TI perusahaan
- Berapa lama kelaikan suatu aset untuk dapat terus digunakan dengan nilai ekonomis yang baik untuk perusahaan
- Kecocokan antara data aset manajemen dengan jumlah yang ada secara fisik

Namun demikian secara fungsi, fungsi ini dapat secara langsung di bawah divisi TI atau di luar TI yang biasanya adalah divisi General Affair. Namun demikian walaupun pada perusahaan divisi ini di luar TI, TI tetap harus bekerja sama dalam hal penginventarisir terhadap aset-aset TI perusahaan.

K. Pemulihan Bencana

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure • IT Development • IT Security

Perencanaan Pemulihan Bencana atau yang dikenal dengan *Business Continuity Planning* (BCP) dalam bahasa Inggris, merupakan sebuah awal dari inisiatif perusahaan atas pemulihan bencana bila terjadi suatu bencana yang tidak diinginkan pada perusahaan. Bencana ini terutama merujuk lumpuhnya kegiatan bisnis bagian secara keseluruhan atau sebagian.

Business Continuity Plan (BCP) sendiri adalah strategi atau proses penyusunan sistem preventif dan kuratif dalam rangka mengurangi atau mencegah dampak terjadinya krisis terhadap aktivitas bisnis yang normal. Rencana strategis BCP menekankan pada fungsi sumber daya manusia atau sumber daya aset agar tetap berjalan di tengah-tengah krisis. Adapun krisis yang dimaksud adalah bencana alam, bencana kemanusiaan seperti peperangan, krisis moneter, krisis politik, krisis keamanan siber, dan krisis kesehatan seperti pandemi global.

Pada dasarnya kegiatan BCP adalah mengidentifikasikan masalah dan membuat kebijakan cepat dalam menghadapi masalah tersebut.

Tujuan dan fungsi *Business Continuity Plan* (BCP) adalah untuk memperkecil efek peristiwa mengganggu tersebut pada operasional perusahaan dan mengurangi risiko kerugian keuangan dan meningkatkan kemampuan organisasi dalam proses pemulihan sesegera mungkin dari suatu peristiwa yang mengganggu. Hal ini bisa ada keterkaitan dengan sistem namun bisa juga tidak ada keterkaitan dengan sistem.

Fungsi BCP juga adalah membantu memperkecil biaya yang berhubungan dengan peristiwa yang mengganggu tersebut dan mengurangi risiko yang berhubungan dengan itu. Sebelum menyusun BCP, Anda perlu memperhatikan ruang lingkup yang kemungkinan terdampak oleh krisis. Adapun ruang lingkup tersebut adalah:

1. **Sumber Daya Manusia**

   Dalam hal ini adalah karyawan. Contohnya dalam kasus COVID-19, bagaimana melindungi keselamatan dan kesehatan karyawan dan bagaimana tata kelola dan distribusi kerja karyawan. Bisa juga bagaimana agar bisnis tetap berjalan walaupun ada karyawan yang terpapar COVID-19.

2. Proses

Dalam hal ini adalah proses bisnis. Saat mengalami krisis, sudah pasti proses bisnis pada perusahaan terdampak akan berubah. Misalnya dalam kasus COVID-19 dimana anjuran *physical distancing* harus diberlakukan sehingga bekerja di rumah menjadi keharusan dimana dibutuhkan perencanaan perusahaan untuk dapat mengubah pola kerja ini.

3. Lokasi

Lokasi meliputi tempat proses bisnis seperti tempat kerja semasa krisis, apakah perlu bekerja dari luar gedung kantor, lokasi suplai, lokasi penyimpanan data dan juga lokasi sasaran pasar.

4. Teknologi

Teknologi meliputi proses dan tools yang digunakan dalam menunjang kinerja dan keamanan bisnis. Misalnya sistem *customer service*, sistem administrasi polis, dll**.** Ruang lingkup di atas bertujuan agar manajemen mengetahui bagian apa yang harus dikendalikan, dianalisis, dan juga dipulihkan dengan cepat agar bisnis dapat terus dijalankan.

Adapun contoh atau langkah-langkah yang harus dilakukan dalam *business continuity plan* adalah sebagai berikut:

1. Analisa Resiko

Tahap ini perusahaan harus menganalisis risiko terdampak menggunakan ruang lingkup risiko. Perusahaan juga perlu mengamati lingkungan eksternal yang dapat mempengaruhi kinerja bisnis. Selain itu asesmen risiko pada tubuh organisasi perusahaan juga perlu dilakukan.

2. Analisa Terhadap Dampak Bisnis

Business Impact Analysis (BIA) adalah suatu proses menentukan dan mendokumentasikan dampak bisnis dari gangguan terhadap kegiatan yang mendukung produk dan layanan utama. Dampak bisnisnya dapat berupa *revenue* dan *non-revenue* (*stakeholder*/pelanggan, regulasi dan reputasi). BIA akan menghasilkan daftar krisis aplikasi pada IT, krisis pada fasilitas, krisis proses bisnis pada customer service dan *business support*. Metode dalam membangun *Business Impact Analysis* adalah membuat daftar seluruh sistem atau fasilitas atau aktivitas, lalu menentukan tingkat dampak (*high, low, medium*) dan jangka dampak (*long* dan *short*), dan terakhir menentukan sistem aplikasi atau aktivitas kritis.

3. Perencanaan

Rencana meliputi rencana alternatif yang dapat diimplementasikan saat krisis. Rencana juga meliputi proses kebijakan yang dibentuk oleh perusahaan dan juga mengacu dengan kebijakan pemerintah. Perencanaan harus dilakukan secara komprehensif dan mencakup semua bisnis mulai dari proses hingga keuangan. Perencanaan ini bersifat parsial, artinya hanya unit tertentu yang terdampak misalnya marketing, keuangan, atau *people management*.

4. Pengembangan rencana

Dalam pengembangan rencana, perusahaan harus memikirkan langkah strategis perusahaan pasca-krisis atau saat *recovery*. Pada tahap ini perlu peran dari seluruh elemen organisasi bisnis terlibat mulai dari manajemen tingkat atas hingga karyawan pada tingkat bawah.

5. *Testing* dan *Audit*

Setelah BCP disusun, BCP juga harus diuji coba dengan mengimplementasikan langsung pada situasi krisis. Setelah diimplementasi, perusahaan juga perlu melakukan audit. Hal ini dilakukan untuk mengetahui seberapa efektif strategi yang dijalankan.

Itulah pengetahuan singkat dan contoh mengenai *business continuity plan* (BCP) sebagai strategi hadapi krisis bisnis. Seperti yang dikatakan sebelumnya, sistem merupakan salah satu ruang lingkup krisis yang perlu menjadi perhatian apalagi jika sistem itu menyangkut tentang keuangan. Adapun terkait dengan BCP, pada umumnya perusahaan Asuransi terutama dengan adanya POJK-4-POJK-05-2021 maka petunjuk dalam memilih lokasi Pusat Pemulihan Bencana menjadi suatu hal yang penting:

1. Lokasi harus berjarak udara antara 40 – 60 km dari pusat operasi. Hal ini mengingat bila pusat pemulihan bencana berdekatan dengan pusat operasi, maka krisis atau bencana yang sama akan berpotensi terjadi pada dua lokasi tersebut
2. Syarat-syarat teknis yang bisa mendukung peran dan kapasitas sebagai data center recovery ini selayaknya mengacu pada kepatuhan yang ditetapkan oleh PCI DSS dan ISO 27001, karena transaksi keuangan rentan terhadap intensitas serangan siber. GTN *Data Center* sendiri menyandang sertifikasi PCI DSS 3.2.
3. Sebagai DRC yang handal, jaminan ketersediaan layanan 99,999% juga merupakan tolok ukur. Untuk itu, minimal mempunyai sertifikasi Tier 3 dari Uptime Institute, atau Rated 3 dari TIA-942.org, dengan SLA 99,982% sementara untuk Tier 4, SLA 99,995%

Secara rutin, pengujian dari pusat pemulihan bencana ini juga diwajibkan sebagai bagian dari BCP dimana pengujian akan melibatkan tim bisnis dalam melakukan pengujian aktifitas ke dalam sistem yang ada pada lokasi pemulihan bencana. Hal ini juga termasuk dilakukan pengujian

restorasi sistem untuk mengetahui kecepatan dalam memulihkan bisnis dalam keadaan krisis sistem dan tentunya untuk melakukan pengujian apakah data *backup* yang di simpan pada pusat pemulihan bencana berjalan dengan baik.

L. Perencanaan Utama Teknologi Informasi

Penanggung Jawab Utama	• Head of IT • IT Operation, Network & Infrastructure • IT Development • IT Security

Perencanaan utama teknologi informasi atau yang biasa disebut juga dengan sebutan IT Master Plan, merupakan suatu perencanaan jangka panjang dalam pengembangan sistem informasi guna mendukung visi dan misi perusahaan. IT Master Plan berisi strategi-strategi organisasi atau perusahaan dalam memanfaatkan teknologi informasi sebagai enabler dan menambah keunggulan yang kompetitif. IT Master Plan membahas mulai dari visi dan misi organisasi atau perusahaan sampai pada perencanaan manajemen proyek IT.

Saat ini, penggunaan TI di perusahaan semakin meningkat. Tidak hanya untuk proses operasional sehari-hari, tetapi juga dalam proses pengambilan keputusan. Bahkan, di beberapa sektor industri seperti asuransi mempunyai ketergantungan kepada IT dengan sangat besar. Namun demikian, perusahaan tidak bisa secara gegabah mengeluarkan investasi untuk implementasi TI. Mereka perlu memperhitungkan *cost* dan *benefit* yang dihasilkannya. Itulah sebabnya, perusahaan membutuhkan *blue print* — yang sering disebut IT Master Plan — sebagai dasar perusahaan dalam mengimplementasi IT.

IT Master Plan intinya berisi rencana strategis perusahaan dalam mengimplementasi dan membangun sistem informasi. Di dalamnya memuat pedoman kebutuhan sistem informasi seperti apa yang diperlukan perusahaan. Yang penting dicatat, IT Master Plan merupakan turunan dari *business plan* perusahaan. Alasannya, TI diimplementasikan sebagai tool untuk membantu perusahaan mencapai visi dan misinya. Maka, tanpa ada visi dan misi yang jelas dari perusahaan. Dalam trainingIT Master Plan juga tidak bisa dibangun.

Banyak sekali manfaat IT Master Plan untuk perusahaan. Pertama, IT master plan menjadi dasar bagi perencanaan perusahaan dalam investasi dan implementasi TI. Dengan demikian, perusahaan tidak lagi sekadar beli ataupun instal, tetapi mempunyai perencanaan yang baik.

Kedua, perusahaan bisa mengurangi berbagai risiko yang mungkin timbul dalam implementasi IT. Banyak sekali risiko yang mungkin timbul dalam implementasi IT, di antaranya:

- Ketidaksesuaian antara kebutuhan bisnis dengan sistem informasi yang dibangun
- Banyak aplikasi yang tambal sulam, sehingga tidak bisa saling berkomunikasi antara satu dengan yang lain
- Investasi yang dikeluarkan tidak memberikan manfaat seperti yang diharapkan

- Standar kualitas sistem informasi tidak sesuai dengan standar industri yang semestinya. Dengan adanya perencanaan yang jelas, perusahaan bisa mengelola risiko tersebut dengan baik sejak awal.

Manfaat ketiga, IT master plan bisa menjadi alat kontrol dan parameter yang efektif untuk mengkaji performa dan keberhasilan implementasi TI di suatu perusahaan. Dalam satu tahun misalnya, perusahaan bisa melihat sistem apa saja yang sudah atau belum diimplementasi.

Salah satu pertanyaan yang sering diajukan orang adalah bagaimana memulai membangun IT Master Plan untuk perusahaan?Ini memang pertanyaan yang wajar mengingat pembangunan IT Master Plan bukanlah pekerjaan yang mudah.

IT Master Plan harus mengacu pada *business plan* perusahaan, maka langkah pertama yang harus dilakukan adalah memahami visi-misi perusahaan, serta target dan tujuan yang akan dicapai perusahaan dalam kurun waktu tertentu. Dari situ kita bisa melakukan *breakdown* secara lebih detail untuk mengetahui informasi bisnis seperti apa yang dibutuhkan.

Kebutuhan informasi itu misalnya bisa berupa informasi *real time* tentang kondisi keuangan, profil pelanggan, efektivitas *marketing channel*, produktivitas setiap pekerja, produktivitas mesin, tingkat inventori, profitabilitas setiap produk, dan berbagai informasi spesifik lain yang disesuaikan dengan kebutuhan masing-masing perusahaan.

Dari berbagai kebutuhan informasi bisnis inilah yang kemudian diterjemahkan menjadi kebutuhan sistem dan teknologi seperti apa yang harus diimplementasi perusahaan untuk memenuhi kebutuhan tersebut. Biasanya, kebutuhan sistem dan TI ini pada saat implementasi diterjemahkan secara teknis menjadi kebutuhan aplikasi perangkat lunak dan perangkat keras. Dalam proses ini juga dijabarkan bagaimana perusahaan akan mengelola berbagai sumber daya yang ada mulai dari aspek organisasi, sumber daya manusia ataupun perangkat lunak dan perangkat keras yang akan diimplementasi.

Bagian akhir dari IT Master Plan adalah manajemen proyek. Pada bagian ini dipetakan proyek TI apa yang menjadi skala prioritas perusahaan dibandingkan dengan proyek yang lain. Manajemen proyek juga mengatur kalender implementasi setiap proyek hingga kurun waktu tertentu, misalnya 3-5 tahun ke depan. Hal ini akan sangat berguna bagi perusahaan dalam mengatur sumber daya mulai dari keuangan, sumber daya manusia, dan berbagai sumber daya lain yang terkait.

Di beberapa kasus, IT Master Plan biasanya mengalami revisi sesuai dengan dinamika bisnis dan kebutuhan perusahaan. Tentu saja, biaya implementasi TI yang sering sangat mahal itu, akan lebih mudah dikelola dan dikontrol risikonya jika perusahaan mempunyai IT Master Plan yang baik.

Manfaat dari IT Master Plan:

- Perusahaan bisa mengurangi berbagai risiko yang mungkin timbul dalam implementasi TI.
- IT master plan bisa menjadi alat kontrol dan parameter yang efektif untuk mengkaji performa dan keberhasilan implementasi TI di suatu perusahaan.
- IT Master Plan akan menjadi dasar bagi perencanaan perusahaan dalam investasi dan implementasi teknologi informasi. Dengan demikian, perusahaan tidak lagi sekedar beli ataupun install, tetapi mempunyai perencanaan yang baik
- Perusahaan bisa mengurangi berbagai risiko yang mungkin timbul dalam implementasi TI.

Banyak sekali resiko-resiko yang mungkin timbul dalam implementasi TI, di antaranya:

- Ketidaksesuaian antara kebutuhan bisnis dengan sistem informasi yang dibangun.
- Banyaknya aplikasi yang tambal sulam sehingga tidak bisa saling berkomunikasi antara satu dengan yang lain.
- Investasi yang dikeluarkan tidak memberikan manfaat seperti yang diharapkan.
- Standar kualitas sistem informasi tidak sesuai dengan standar industri yang semestinya.
- Kesulitan menentukan prioritas investasi TI tahunan.
- Kesulitan dalam menentukan pilihan teknologi.
- Kesulitan dalam perencanaan kapasitas teknologi informasi.
- Ketidakseragaman tools yang dipakai dalam teknologi informasi.

Dengan adanya perencanaan yang jelas, perusahaan bisa mengelola resiko tersebut dengan baik sejak awal.

Dalam pembuatan IT Master Plan harus mengacu pada perencanaan bisnis perusahaan, maka langkah pertama yang harus dilakukan adalah memahami visi-misi perusahaan, target dan tujuan yang akan dicapai perusahaan dalam kurun waktu tertentu. Dari situ kita bisa melakukan pemecahan secara lebih detil kebutuhan informasi bisnis seperti apa yang dibutuhkan. Dari berbagai kebutuhan informasi bisnis inilah yang kemudian diterjemahkan menjadi kebutuhan sistem dan teknologi seperti apa yang harus diimplementasikan perusahaan untuk memenuhi kebutuhan tersebut. Kebutuhan sistem dan teknologi informasi ini pada saat implementasi diterjemahkan secara teknis menjadi kebutuhan aplikasi perangkat lunak dan perangkat keras.

Dalam proses ini juga menjabarkan bagaimana perusahaan mengelola berbagai sumber daya yang ada mulai dari aspek organisasi, personel, maupun perangkat lunak dan perangkat keras yang akan diimplementasikan.

IT Master Plan yang baik berisi:

1. Halaman pendahuluan yang menceritakan kondisi sekarang.
2. Halaman penjabaran yang menjabarkan tujuan dari master plan.
3. Halaman tentang kebijakan yang harus dibuat untuk mendukung *master plan*.
4. Halaman yang memuat strategi implemntasi dengan memperhitungkan analisis SWOT.
5. Halaman *action* yang harus diambil.
6. Halaman paparan hasil yang akan dicapai dari *action* tersebut.
7. Rekomendasi yang diberikan dalam implementasi IT.

Adapun cakupan dari IT master plan adalah:

- Konteks Bisnis
- Arsitektur Bisnis
- IT Visioning – menentukan visi TI
- Arsitektur Informasi
- Arsitektur Aplikasi
- Arsitektur Teknologi
- Rencana Program TI
- Roadmap Transisi Pengembangan & Implementasi TI
- IT Governance – tata Kelola TI pada perusahaan
- Rencana Sumber Daya TI
- IT Valuation – manfaat terhadap penerapan TI pada perusahaan