BAB 2

LANDASAN TEORI

2.1 Pengertian Sistem

Sistem adalah suatu rangkaian yang saling mebutuhkan untuk dapat menghasilkan suatu tujuan tertentu dan dapat diterima oleh semua pengambil keputusan dalam suatu perusahaan (*McLeod, Raymond and schel, 200l7*)

2.1.1 Pengertian Informasi

Informasi adalah suatu kabar yang dapat dianggap penting apabila informasi tersebut berguna untuk kepentingan suatu organisasi atau perusahaan yang membutuhkannya. Sebaliknya, informasi dianggap tidak penting apabila perusahaan tersebut tidak memperlukan informasi tesebut (McLeod 2007).

2.1.2 Pengertian Sistem Informasi

Sistem Informasi adalah suatu laporan yang dibutuhkan oleh perusahaan untuk meningkatkan kegiatan opersasional dan strategi dalam suatu perusahaan dan didokumentasikan apabila suatu saat dibutukan kembali untuk kepentingan suatu perusahaan yang bersangkutan (*Laudon, Kenneth C., & Jane, P. Laudon* 2010).

2.1.3 Pengertian Manajemen

Menurut *Robbins, Stephen P.Coulter,Mary*.(2010) manajemen adalah tekni yang dimiliki oleh orang untuk memberikan pengarahan, mempengaruhi,

mengawasi dan mengorganisasikan komponen – komponen yang ada dan saling menunjukan untuk dapat mencapai tujuan yang dimaksud yang telah ditentukan sebelumnya.

2.1.4 Pengertian Manajemen Risiko

Menurut Djohanputro (2008;43) risiko adalah proses dalam mengidentifikasi, mengukur , memantau dan melakukan pengembangan cara lain dalam penanganan risiko , memonitoring dan melakukan pengendalian dalam penanganan risiko.

2.2 Ancamana Terhadap Sistem Informasi

Ancaman adalah kejadian dimana hal ini terjadi dikarenakan kesalahan, ketidaktelitian, bencana alam, *software* yang tidak mendukung dan juga virus. Ancaman juga dapat merugikan perusahaan. Kerugian tersebut bisa berupa uang, tenaga dan bisnis. Kemungkinan dari bisnis itu sendiri pun akan membuat reputasi yang tidak dipercaya oleh masyarakat dikarenakan sistem yang tidak aman dan membuat perusahaan tersebut mengalami kegagalan (*failed*).

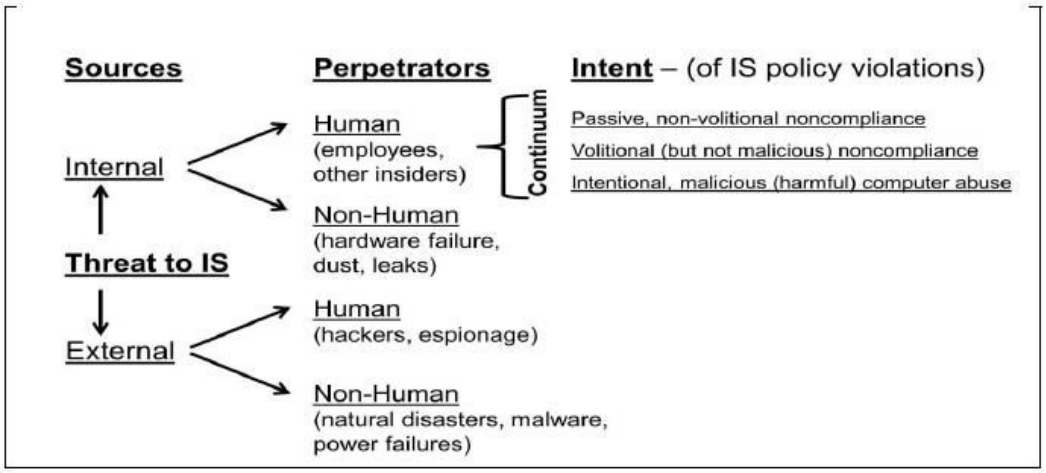
Menurut *W.Stallings* inilah beberapa kemungkinan dari ancaman yang dapat ditemukan:

1. *Interruption* (Interupsi) adalah dimana data rusak diakibatkan serangan ditujukan dari ketersediaan sistem (*danial of service attact*).
2. *Interception* (Pengalihan) adalah dimana pihak yang tidak berkepentingan atau yang tidak berwewenang berhasil mengakses aset atau informasi. (Penyadapan (*wiretapping*)).

3. *Modification* (Pengubahan) adalah orang yang tidak berkepentingan melakukan perubahan untuk memberikan informasi yang tidak dapat dipercaya kebenarannya.
4. *Fabrication* (Pemalsuan) adalah dimana pihak yang tidak berwewenang menyisipkan objek palsu kedalam website atau database untuk dan memberikan pesan - pesan yang tidak sesuai dengan konten dari website tersebut. (Memasukan pesan palsu melalui jaringan komputer).

Sedangkan menurut *Debra box* dan *Dalenca Pottas* dalam jurnal yang berjudul *a model for information security compliant behaviour in the healthcare context* (2014) mengatakan bahwa ancaman kesehatan keamanan sistem informasi adalah:

1. Kurangnya rasa keamanan adalah dikarenakan kurangnya penerapan *SOP* dari perusahaan yang dibangun.
2. Pengguna sistem informasi mengambil risiko yang ada dikarenakan ketidaktahuan terhadap risiko yang ada.
3. Tindakan yang dilakukan dengan sengaja, kelalaian atau tidak mengetahui mengenai kegiantan yang ternyata risikonya berdampak pada sistem informasi yang saling berhubungan.



Gambar 2.1 Information Security Threat Vector Taxonomy Abridged – Sourced

2.3 Tata Kelola Keamanan Sistem Informasi

Keamanan sistem informasi dibangun untuk memberikan keamanan dalam sebuah sistem informasi yang dibangun dalam suatu perusahaan agar informasi yang disampaikan dapat dipercaya dan dipertanggung jawabkan kebenarannya. Oleh sebab itu, maka diperlukannya keamanan sistem informasi yang bertujuan menjaga aset yang ada dan informasi yang ada dalam perusahaan yang dibangun dan membuatkan setiap akses kontrol untuk setiap pengguna agar dapat terstruktur dengan baik , rapih dan sesuai dengan *SOP* yang berlaku.

Masalah terbesar dalam keamanan sistem informasi adalah berdampak pada tujuh hal sistem informasi yaitu sebagai berikut:

1. Efektifitas adalah dimana tingkat kinerja diukur untuk melihat seberapa jauh tingkat kinerja yang dilakukan dengan tingkat kinerja yang ditargetkan.
2. Efisiensi adalah dimana tingkat pengukuran dapat tercapai sesuai dengan sasaran dan tujuan dari sebuah organisasi yang telah ditetapkan

sebelumnya (Drs. Soewarno Handayaningrat, Pengantar Studi Ilmu Administrasi dan Manajemen, 1990, hal 15).

3. Kerahasiaan adalah penjagaan sebuah dokumen , ucapan , rekaman video dan segala hal yang diceritakan oleh orang lain untuk dapat dijaga dan juga tidak disebarkan oleh orang lain yang tidak memiliki kepentinga.
4. Integritas adalah suatu kesatuan yang tidak bisa dipisahkan agar sistem informasi dapat berjalan sesuai dengan integrasi yang ada dalam sebuah organisasi dan dapat meningkatkan efektifitas dan efesiensi dalam pekerjaan.
5. Keberadaan (*availability*) adalah dimana informasi yang tepat dapat ditahan dengan benar dan dapat diakses oleh siapa pun yang memiliki legitimasi untuk mengakses informasi tersebut.
6. Kepatuhan (*Complaince*) adalah dimana semua aturan yang ada dalam sebuah organisasi atau perusahaan dapat dijalankan sesuai dengan peraturan yang berlaku dalam perusahaan tersebut(Tim Penyusun Kamus Pusat Bahasa. 2002)
7. Keadaan (*Reliability*) adalah dilihat dari bagaiaman keadaan sebuah perusahaan untuk kesiapan dalam keamanan sistem informasi yang sudah berjalan apakah sudah sesuai dengan *SOP* yang ada.

Menurut Prof. Richardus Eko Indrajit Kebijakan keamanan sistem informasi adalah infrastruk yang harus dijaga dan dilindungin dalam sebuah perusahaan agar tata kelola keamanan sistem informasi dapat dengan baik digunakan untuk pengelolahan data dan informasi. Apabila dalam pengelolahan data yang kurang baik akan menimbulkan permasalahan yang akan menjadi

kelemahan *(vulnerabilities)* sehingga akan majadi ancaman *(theats)* seperti kejadian pencurian, kehilangan data, perusakan dan penyadapan data penting dalam suatu perusahaan atau organisasi.

2.4 Sistem Manajemen Keamanan Informasi (SMKI)

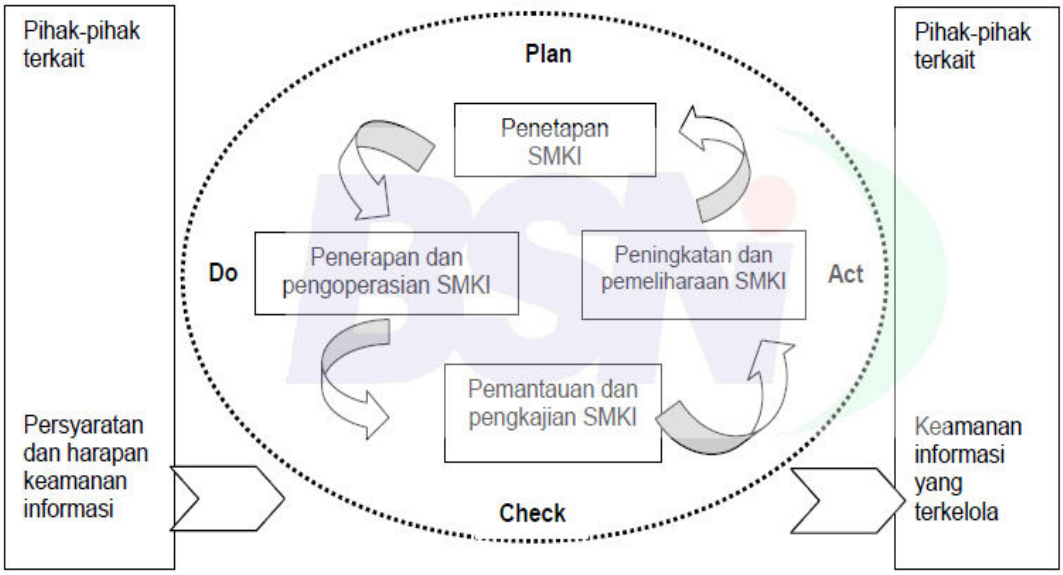
Keamanan informasi dilakukan untuk menjaga aset dan seluruh sistem informasi dari ancaman dan juga upaya manupulasi data yang dilakukan oleh orang yang tidak berkepentingan. Keamanan sistem informasi dilakukan untuk memastikan kelangsungan bisnis dan meminimalisasi risiko (Sarno, R. dan Iffano, I. 2009)

Sistem Manajemen keamanan informasi (SMKI) adalah standard yang digunakan untuk mengukur proses yang ada dalam panduan SNI *ISO/IEC* 27001:2009 dengan mengadopsi *Plan* (Perencanaan dan mengimplementasikan) - *Do* (Memonitoring dan melakukan pengecekan) - *Check* (melihat, meninjau dan melakukan peningkatan dan mengembangkan) - *Ack* (memelihara SKMI) (PDCA) yang diterapkan untuk membentuk seluruh proses SMKI. Aspek dari SMKI juga ditinjau untuk meningkatkan dan menjaga kerahasiaan, keutuhan dan ketersediaan dari informasi yang ada.

Definisi proses Sistem Manajemen Keamanan Informasi diantaranya adalah:

- *Plan* (Penetapan SMKI): Menetapkan kebijakan, sasaran, proses dan prosedur SKMI yang sesuai untuk mengelola risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.

- *Do* (Penerapan dan pengoprasian SKMI): Menerapkan dan mengoprasikan kebijakan, pengendalian, proses dan prosedur SKMI.
- *Check* (Pemantauan dan pengkajian SKMI): Mengases dan , apabila berlaku , mengukur kinerja proses terhadap kebijakan , sasaran SKMI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
- *Act* (Peningkatan dan pemeliharaan SKMI): Mengambil tindakan korektif dan pencegahan bedasarkan hasil internal audit SKMI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SKMI (16137_SNI ISO IEC 27001_2009_3.PDF)



Gambar 2.2 PDCA ISO/IEC 27001:2009

2.5 Penilaian dan Evaluasi Resiko

Penilaian dan evaluasi risiko adalah suatu kegiatan yang dilakukan atau dijalankan disebuah organisasi atau perusahaan untuk mengetahui seberapa besar hasil dari penilaian tersebut untuk dapat meninjau kembali (*rewiev*) manajemen risiko yang terjadi dalam sebuah perusahaan.Apabila terjadi kesalahan yang harus melakukan mitigasi, maka hal tersebut harus segera mungkin dilakukan agar data yang masih atau dapat dipakai bisa dipindahkan ketempat yang lebih aman untuk sementara waktu. Apabila data yang sudah dimitigasi sudah benar - benar pulih keseluruhan, maka akan digabungkan kembali data yang tadi sudah dipisahkan agar menjadi data satu kesatuan yang kembali utuh.

Pengertian manajemen risiko menurut Djohanputro (2008;43) Manajemen risiko adalah pengendalian yang terstruktur dan secara sistematis dalam hal identifikasi , mengukur , memetakan , melakukan pengembangan pananganan risiko , memantau dan melakukan penanganan risiko untuk memperkecil terjadinya kejadian yang tidak diharapkan oleh perusahaan.

2.6 Tahapan Manajemen Risiko

Untuk mengetahui apakah risiko tersebut dalam rentang level yang berbahaya atau tidak, maka harus dilakukan beberapa tahapan manajemen risiko dalam suatu organisasi atau perusahaan. Ini adalah beberapa tahapan - tahapan manajemen risiko:

1. Investigasi adalah melakukan peninjauan kembali atas sistem informasi yang sudah digunakan apakah terdapat masalah dan nantinya akan menjadi kendala dalam kemajuan menjalankan bisnis.

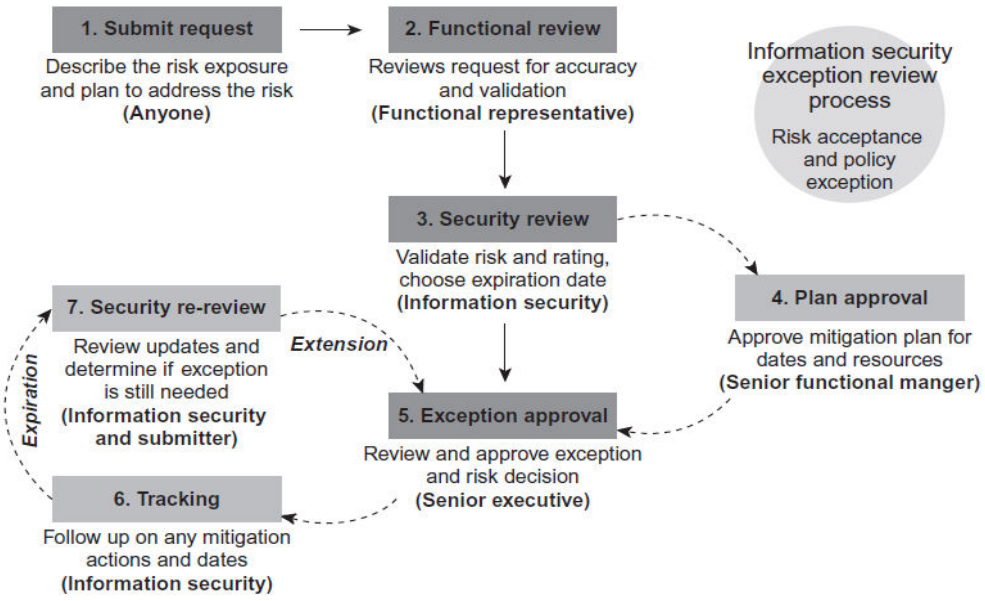
2. Pengembangan adalah tahapan setelah melakukan investigasi dalam sebuah perusahaan yang menggunakan sistem informasi sebagai penunjang kemajuan bisnis. Tahapan ini akan dilihat apakah sistem informasi yang digunakan perlu dilakukan pengembang atau tidak.
3. Implementasi adalah langkah yang dilakukan seletah pengembangan telah ditinjau kembali. Apabila pada tahap pengembangan ada perbaikan sistem informasi, maka akan dilakukan implementasi terkait pengembangan sistem informasi yang telah dilakukan sebelumnya.
4. Pengoprasian dan perawatan adalah dimana tahap implementasi telah dilakukan dan pada tahap ini dilakukan semua perawatan terkait pengimplementasian sistem informasi yang baru saja ditambahkan atau diperbaiki pada tahap implementasi.
5. Penyelesaian ini adalah tahap terakhir setelah tahapan perawatan sistem informasi yang baru telah diimplementasikan dengan benar dan sesuai dengan *SOP* dalam suatu perusahaan.

2.7 *Risk Evaluation and Mitigation Strategies*

Evaluasi risiko dan strategi mitigasi adalah penanganan yang dilakukan dalam sebuah organisasi atau perusahaan untuk menindaklanjuti risiko – risiko yang ada dalam sistem informasi yang digunakan untuk memajukan bisnis yang dijalankan oleh perusahaan tersebut. Oleh karena itu, sangat dibutuhkan evaluasi risiko yang ada dalam sistem informasi dan juga perusahaan tersebut. Risiko tidak hanya ada di eksternal namun ada juga di internal.

Menurut *Evan Wheeler* ,2001 dalam buku yang diterbitkan berjudul *security risk management* dikatakan bahwa Alur kerja harus melakukan

pengujian tinjauan yang akan dilakukan oleh team keamanan informasi sebelum diberikan laporan ke pihak manajemen untuk mendapatkan pesetujuan. Tim keamanan juga dapat merubah hasil evaluasi risiko bedasarkan dampak yang ada dan setelah di diskusikan oleh tim manajemen perusahaan dan disetujui oleh pihak terkait.

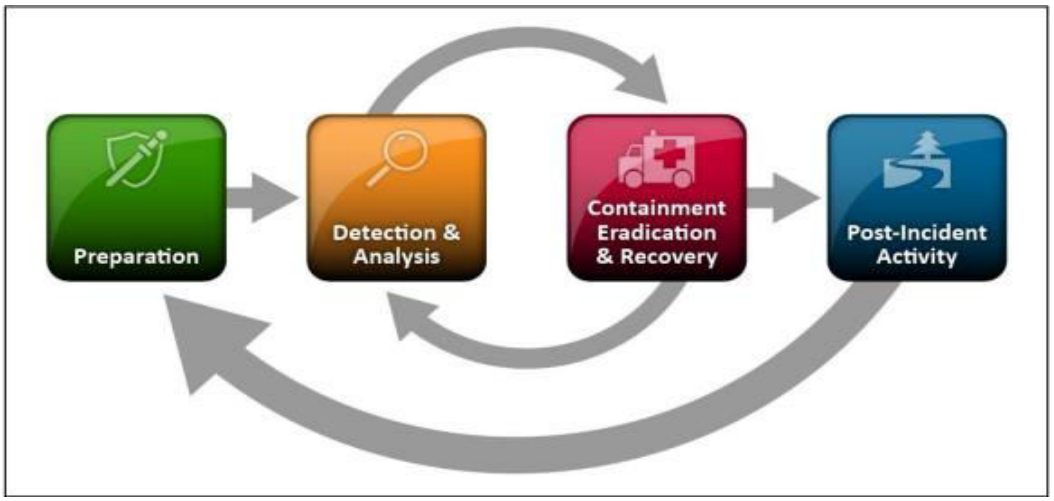


Gambar 2.3 Risk exception approval workflow (Evan Wheeler, 2001)

2.8 *Incident Response life cycle*

Pada tahap ini akan dipersiapkan untuk melatih dan membangun tim manajemen risiko untuk dapat menditeksi risiko yang ada dalam sebuah organisasi atau perusahaan. Pada tahap ini perusahaan juga membatasi jumlah kejadian - kejadian yang ada untuk pemilihan penerapan dalam satu set kontrol keamanan bedasarkan hasil penilaian risiko. namun setelah masa implementasi sudah dijalankan dalam sebuah perusahaan, akan ada permasalah yang akan timbul dalam proses tersebut. Contohnya adalah pada saat proses penambahan

host apakah tidak terditeksi oleh *malware* sementara proses pembersihan *malware* sendang dalam proses.



Gambar 2.4 Incident Response life cycle (Paul Cichonski Agust 2012)

2.8.1 *Prepation*

Respon metodologi kejadian biasanya menekankan pada persiapan dan membangun kemampuan untuk merespon kejadian yang terjadi dalam perusahaan untuk siap dalam menindaki kejadian yang terjadi dan juga memastikan pencegahan kejadian yang belum terjadi.Tim yang dibentuk juga diharapkan dapat memberikan saran mendasar terkait untuk menangani kejadian dan mencegah kejadian yang belum terjadi.

2.8.2 *Preparing to Handle Incident*

Daftar di bawah ini memberikan beberapa contoh alat dan sumber daya yang tersedia untuk menangani kejadian yang ada dalam perusahaan. Daftar - daftar ini menjadi titik awal untuk dapat di diskusikan di dalam perusahaan untuk meminimalisasikan risiko yang akan terjadi.

Menangani kejadian komunikasi dan fasilitas:

A. *Information contact*: Kontak yang digunakan untuk anggota tim dan keperluan lain - lain di dalam dan di luar organisasi (kontak utama dan cadangan), untuk penanganan hukum dan tim kejadian lainnya. Informasi mungkin termasuk nomor telepon, email, enkripsi publik dan untuk keperluan verifikasi identitas kontak.
B. *On - call information:* Panggilan untuk tim lain dalam organisasi, termasuk informasi eksalasi.
C. *Incident reporting mechanisms*: Kejadian pelaporan seperti nomer telepon, *email* , formulir *online* dan penanganan sistem pesan instan yang didapat oleh pengguna untuk digunakan dalam pelaporan kejadian yang dicurigankan. Setidaknya satu mekanisme harus dapat melaporkan kejadian anonim.
D. *Issue tracking system:* Untuk melacak kejadian informasi, status dan sebagainya.
E. *Smartphone:* Agar dapat digunakan anggota tim setiap waktu untuk support di dalam komunikasi.
F. *Encryption software:* Digunakan untuk komunikasi antara anggota tim dalam organisasi dan dengan pihak eksternal dan juga untuk lembaga federal. Untuk software harus menggunakan algoritma enkripsi FIPS - divalidasi
G. *War room:* Ruangan yang digunakan untuk komunikasi dan kordinasi. Tim diharuskan membuat prosedur untuk pengadaan ruangan sementara bila diperlukan.

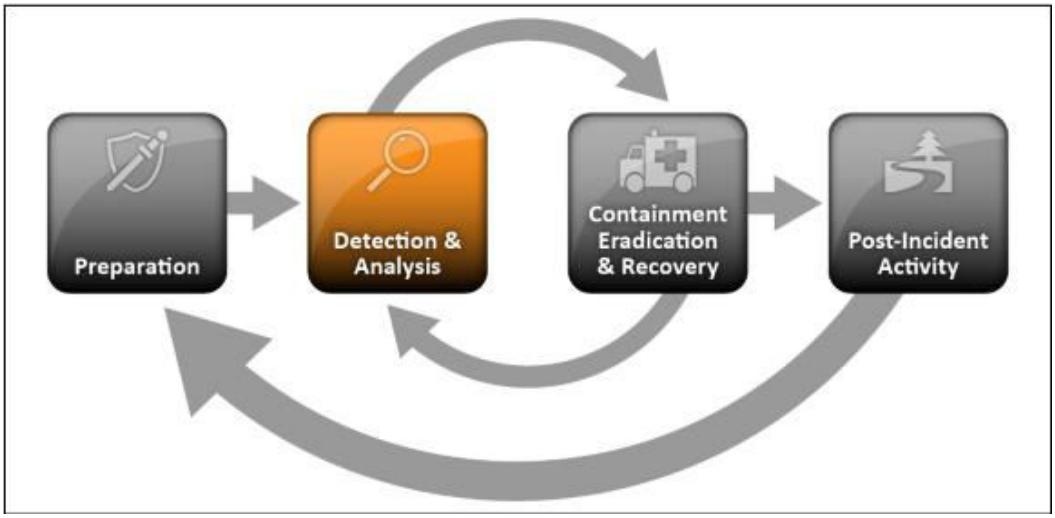
H. *Security storage facility:* Bukti pengamanan dan fasilitas - fasilitas material yang bersifat sensitif.

2.8.3 *Ditection and Analysis*

Melakukan diteksi ancaman yang ada dan menganalisis ancaman tersebut agar tidak menjadi gangguan atau ancaman bagi perusahaan dalam mengembangkan bisnis yang sedang berjalan. Kejadian - kejadian dapat terjadi dengan beberapa cara yaitu:

A. *External / removeable* media: Kode yang berbahaya menyebar dari *flasdisk* yang sudah terinfeksi virus.
B. *Attrition:* Serangan yang menggunakan *brute force* untuk menurunkan performa sistem atau menghancurkan jarigan sistem (DDos misalnya untuk menolak ke dalam akses layanan atau aplikasi, serangan *brute force* terhadap otentikasi, *password* dan tanda tangan digital).
C. Web : Serangan dari pihak luar dari situs *web - based* seperti *scripting*untuk men - *redirect web* agar tidak berfungsi dengan benar dan menginstal *malware*
D. Email: Menyerang melalui pesan *email* atau lampiran email. sebagai contoh : memasukan kode ke dalam dokumen yang sudah di *attached*atau link ke *webmaliciouse*kedalam *body email message.*
E. Loss or thief of Equipment: Kehilangan atau pencurian perangkat komputer atau media yang digunakan perusahaan seperti laptop, *smartphone* atau token autentikasi.

F. *Other*: Serangan yang terjadi diluar kategori yang sudah dijelaskan di atas.



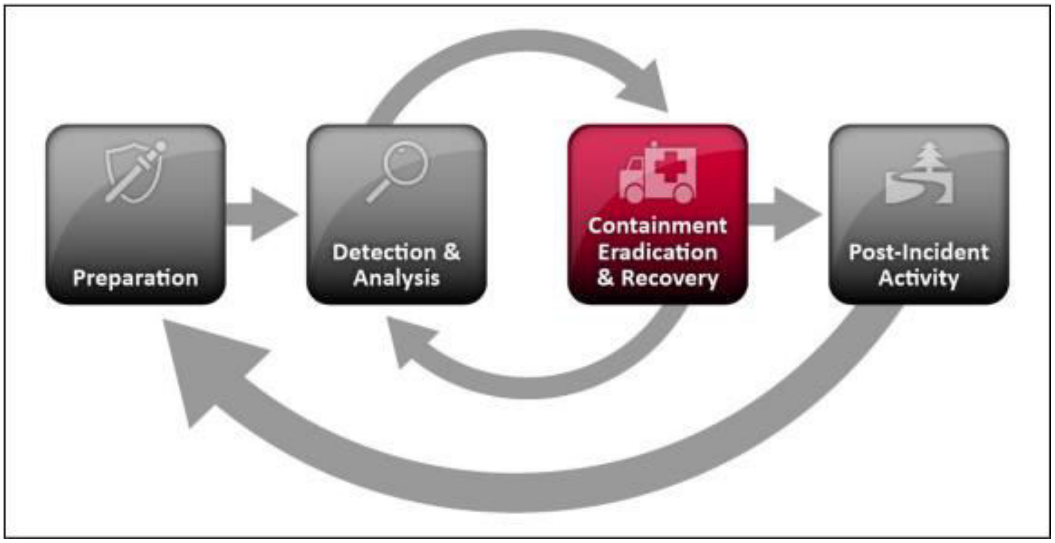
Gambar 2.5 Incident Response Life Cycle (Paul Cichonski Agust 2012)

2.8.4 *Containment, Eradication, and Recovery*

Pada tahap ini adalah dimana tahap untuk penahanan, pemberantasan dan juga pemulihan data yang akan dipertahankan untuk di pulihkan kembali. Strategi yang dilakukan oleh setiap perusahaan pasti akan berbeda - beda dalam penanganan masalah yang terjadi. Perusahaan harus membuat kriteria yang tepat di dokumentasikan dengan jelas untuk mefasilitasi pengambilan keputusan. Keputusan strategi yang tepat meliputi beberapa kriteria seperti:

1. Potensi kurusakan dan pencurian sumber daya.
2. Perlunya bukti - bukti yang mendukung.
3. Ketersedian layanan yang memadai (konektivitas jaringan, layanan yang diberikan oleh pihak eksternal).
4. Waktu dan sumber daya yang dibutuhkan untuk penerapan strategi.
5. Efektivitas strategi (sebagian penahanan atau penahanan penuh).

6. Durasi dan solusi (solusi untuk dihapus dalam waktu empat jam , solusi sementara untuk dihapus dalam waktu dua minggu dan solusi permanen).

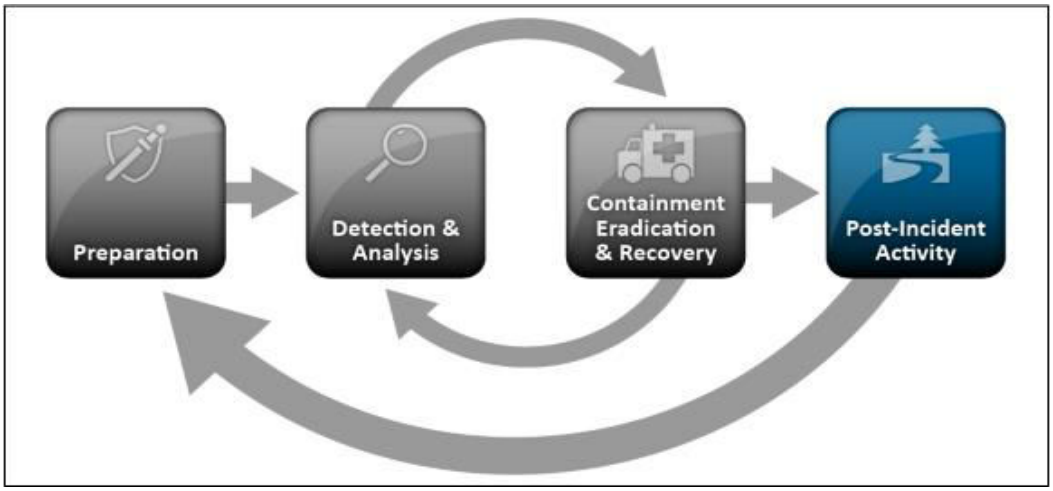


Gambar 2.6 Containment, Eradication, and Recovery (Paul Cichonski Agust 2012)

2.8.5 *Post Incident Activity*

Proses ini berfokus pada perbaikan yang akan dilakukan setelah sistem informasi telah diimplementasikan dengan baik dan benar. Dari penanganan ini , diharapkan tim keamanan informasi dapat berkembang untuk mengetahui penanganan masalah yang sudah terjadi atau penanganan masalah yang belum terjadi agar dapat memberikan kontrol - kontrol sesuai dengan keamanan *framework* yang digunakan dalam perusahaan.

Apabila masalah yang ada di dalam perusahaan terjadi terulang , maka *life cycle* tersebut akan kembali ke fase awal sampai fase *post incident acitivity* untuk dapat memperbaiki dan mempertahankan keamanan sistem informasi yang ada dalam perusahaan tersebut dengan baik dan benar sesuai dengan *SOP* dan *framework* yang ada pada perusahaan yang bersangkutan.



Gambar 2.7 *Post incident activity* (Paul Cichonski Agust 2012)

2.9 Studi Literatur Terdahulu

Ini adalah beberapa studi literature terdahulu yang sudah melakukan penelitian mengenai *ISO / IEC* 27001 diantaranya adalah:

1. Pada tahun : 2016

   Nama Penulis: Fikri akbar et al.

   Permasalahan:

   - Bagaimana penerapan standar *ISO* 27001 pada perusahaan SVM Europe?
   - Apa manfaat dari penerapan standar *ISO* 27001 di perusahaan SVM Europe?

   Pembahasan *ISO / IEC*27001:

   - Mahasiswa dapat memahami dengan baik manfaat dari sertifikasi standar *ISO* 27001
   - Mahasiswa mampu menerapkan standar *ISO* 27001 dengan baik

Kesimpulan:

- Semua departemen di SVM Europe kini menjadi lebih selaras dan dikelola dengan lebih baik.
- Sejak memperoleh sertifikasi, SVM Europe mendapatkan cakupan Public Relations yang lebih besar dan meningkatkan reputasi bisnis yang dijalankan.

Sumber:

- fikriakbarhedianto

2. Pada tahun : 2015

Nama Penulis: Alvin aldo

Permasalahan:

- Apa yang dimaksud dan bagaimana menerapkan pengelolaan layanan TI menggunakan standar internasional *ISO/IEC*27001?
- Apa yang dimaksud dan bagaimana menerapkan pengelolaah layanan TI menggunakan standar internasional *ISO/IEC*20000?

Pembahasan ISO 27001:

- Menambah pengetahuan tentang pengelolaan layanan TI di dunia nyata dan perannya dalam pertumbuhan organisasi.
- Mengetahui penerapan ITSM dan ISMS melalui standar *ISO/IEC* 20000 dan *ISO/IEC* 27001.

Kesimpulan:

- Antar organisasi tentunya akan saling bersaing untuk meningkatkan layanannya. Bagi penyedia layanan ini bersaing untuk memberikan layanan yang terbaik agar diminati oleh pelanggan adalah hal penting dalam bisnisnya.

- Saat ini, manajemen seperti ini sudah dapat dipaparkan dalam bentuk yang lebih tersetruktur dengan menggunakan manajemen teknologi informasi (ITSM) dan juga manajemen keamanan informasi (ISMS).

Sumber

- Alvin Aldo

3. Tahun : 2010

Nama Penulis: Rajia Rafigue

Masalah:

- risiko operasional yang terkait dengan Keamanan Informasi di keuangan

  organisasi?
- Risiko operasional dapat mempengaruhi bisnis dalam organisasi keuangan?
- Berapa banyak manajemen puncak menyadari, terlibat dan berkomitmen risiko informasi pengelolaan.
- Bagaimana masalah dapat diselesaikan untuk meningkatkan keamanan informasi?

Pembahasan *ISO* 27001:

- Tampaknya banyak orang yang tahu tentang risiko yang terlibat dalam keamanan informasi, namun sebenarnya beberapa dari mereka memiliki ide nyata tentang risiko ini. Hal ini karena keamanan informasi dapat dipertimbangkan dari berbagai aspek seperti aspek yang berbeda dari proses bisnis, teknologi, organisasi dan perilaku individu.

- Dalam studi ini, kita dimaksudkan untuk menggambarkan dan menganalisis risiko operasional terkait dengan keamanan informasi sehubungan dengan organisasi keuangan. Setelah penyelidikan signifikan risiko operasional diidentifikasi dianalisis dalarangka memberikan solusi untuk meningkatkan keamanan informasi.

Kesimpulan:

- Risiko operasional dari perspektif bisnis ini paling sering didefinisikan sebagai risiko yang datang melalui produksi barang dan jasa yang diberikan kepada klien dari organisasi keuangan. Tapi setelah menganalisis kami menyimpulkan bahwa risiko operasional terkait dengan keamanan informasi dalam organisasi keuangan adalah serangan virus, kegagalan backup (kehilangan data), prosedur operasional yang tidak pantas, penggunaan yang tidak sah, dan ketergantungan pada tenaga eksternal seperti vendor, kesalahan pengguna, kerusakan jaringan, dan hacks destruktif seperti Distributed Denial of Service serangan.

Sumber:

- Rajia Rafigue

4. Tahun : 2015

   Nama Penulis: Melwin Syafrizal, S.Kom

   Masalah:

   - Struktur organisasi
   - Kebijakan keamanan
   - Prosedur dan prosesTanggung jawab atau responsibility

- Sumber Daya Manusia

Pembahasan *ISO* 27001:

- Audit ISMS memberi pemahaman yang lebih baik mengenai aset informasi dan proses manajemen keamanan informasi yang diperlukan.
- Membantu memberikan pemahaman pentingnya keamanan informasi pada karyawan, stakeholder dan masyarakat umum,
- Membantu mengarahkan implementasi sistem manajemen keamanan informasi berdasarkan kepada pertimbangan manajemen risiko.
- Mendukung organisasi dengan memberi kerangka kerja (panduan) proses untuk mengimplementasikan dan melakukan manajemen serta kontrol terhadap keamanan informasi agar dapat menjamin bahwa objek-objek keamanan tertentu telah dicapai

Kesimpulan:

- Struktur organisasi, biasarnya berupa keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi. Misalnya; Chief Security Offi cer dan beberapa lainnya.
- Kebijakan keamanan, atau dalam bahasa Inggris disebut sebagai *Security Policy*. Contoh kebijakan keamanan ini misalnya adalah sebagai berikut: Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan

harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk logon pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terkoneksi ke jaringan.

- Prosedur dan proses, yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur permohonan ijin akses aplikasi, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.
- Tanggung jawab, yang dimaksud dengan tanggung jawab atau responsibility di sini adalah tercerminnya konsep dan aspek-aspek keamanan informasi perusahaan di dalam job description setiap jabatan dalam perusahaan. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamaan informasi perusahaan untuk staf dan karyawannya.

Sumber:

- Melwin Syafrizal, S.Kom

5. Tahun : 2015

   Nama Penulis: Santosa Iwan

   Masalah:

   - Menganalisa perubahan kebutuhan dan prioritas organisasi yang baru sesuai dengan pertumbuhannya.

- Mempelajari ancaman-ancaman atau kelamahan-kelemahan baru apa yang terjadi akibat perubahan yang ada tersebut.
- Memastikan bahwa kendali-kendali yang dimiliki tetap efektif dalam menghadapi ancaman-ancaman kejadian terkait.

Pembahasan *ISO* 27001:

- Seluruh pihak yang terlibat dalam proses keamanan informasi memiliki kesamaan pengertian, istilah, dan metodologi dalam melakukan upaya-upaya yang berkaitan dengan keamanan data.
- Tidak terdapat aspek-aspek keamanan informasi yang terlupakan karena standar yang baik telah mencakup keseluruhan spektrum keamanan informasi yang disusun melalui pendekatan komprehensif dan holistik (utuh dan menyeluruh).
- Upaya yang dilakukan untuk membangun keamanansistem in formasi.

Kesimpulan:

- Faktor utama yang menyebabkanterjadinya insiden adalah tidaksegeranya melaporkan setiap insidenyang terjadi berdasarkan hasil surveyyaitu 73,3% .
- Minimal formulir pelaporan terdapatinformasi pelapor, waktu terjadiinsiden, jenis serangan (insiden),deskripsi insiden, perangkat yangdiserang dan log file.
- *SOP* yang telah dibuat 95,5 %memenuhi standarisasi *ISO/IEC* 27001dan 27002 dari sudut pandangkelengkapan proses pelaporan insidenyang terjadi.

Sumber:

- Pengembangan prosedur pelaporan insiden keamanan informasi Menggunakan stadarisasi *ISO/IEC* 27001 dan 27002.

6. Tahun : 2013

   Nama: Reza Zulfkar Ruslam

   Masalah:

   - Apa kepatuhan perusahaan terhadap visi dan misi *best service*terhadap pelanggan sudah memenuhi aspek keamanan informasi?
   - Kebijakan dan prosedur yang ada sudah dapat dikaitkan *best service*terhadap aspek keamanan informasi?

   Pembahasan *ISO* 27001:

   - Mengetahui apakah kepatuhan perusahaan terhadap visi dan misi *best services* terhadap pelanggan sudah memenuhi aspek keamanan informasi?
   - Mengetahui apakah Kebijakan dan prosedur yang ada sudah dapat dikaitkan *best service*terhadap aspek keamanan informasi?

   Kesimpulan:

   - Dari analis gap yang ada, dapat disimpulkan bahwa kepatuhan perusahaan terhadap visi dan misi *best service*terhadap pelanggan belum memenuhi aspek keamanan sistem inforamsi.
   - 11 kebijakan dan prosedur yang ada belum dapat dikatakan *best services* terhadap keamanan sistem informasi.

Sumber:

- Reza Zulfkar Ruslam

7. Tahun : 2014

Nama: Riawan Arbi Kusuma

Masalah:

- Bagaimana merencanakan audit sistem informasi akademik Sunan kalijaga dengan menggunakan stadarisasi *ISO* 27001?
- Bagaimana memformulasikan hasil audit keamanan sistem informasi akadek Sunan Kalijaga terhadap faktor keamanan CIA (*Confidentiality, Integrity, and Availability*)

Pembahasan ISO 27001:

- Membuat perencanaan audit keamanan sistem informasi akademik di Sunan Kalijaga.
- Melakukan audit keamanan sistem informasi akademik dengan melakukan evaluasi terhadap kendali dan bukti yang ada , mendokumentasikan temuan audit dan menyusun laporan audit.

Kesimpulan:

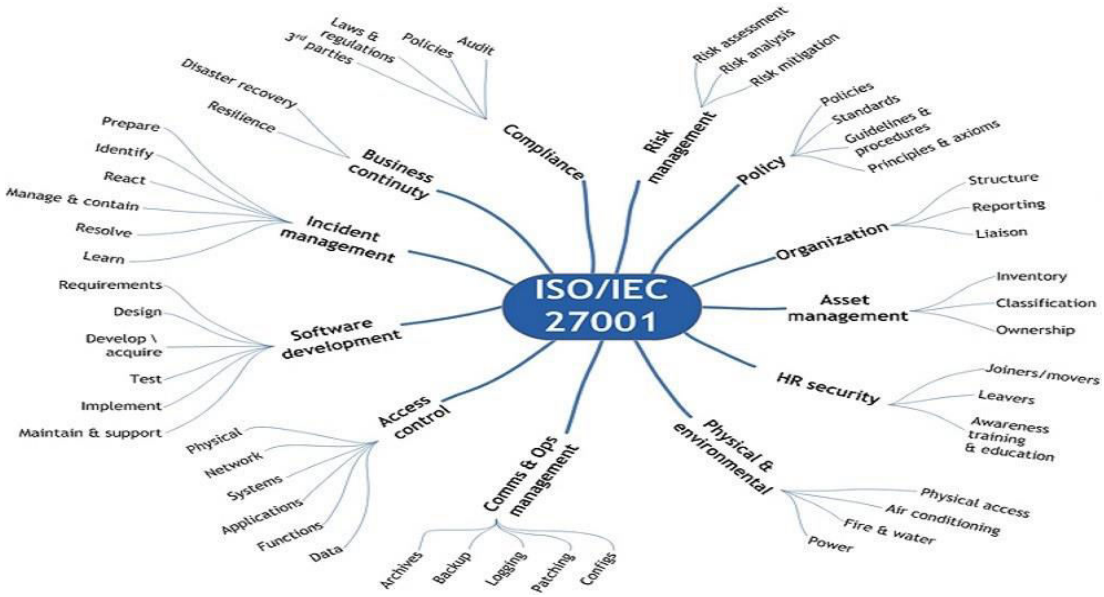
- Hasil audit yang telah dihitung maturity levelnya, maka terdapat pada level 2 untuk keamanan sistem informasi di Sunan Kalijaga.
- *Maturity level* pada *domain ISO* yang bersifat mandatory terdapat pada level 1 yaitu keamanan sistem informasi hanya mengikuti pola yang teratur dan tidak adanya pelatihan bagi karyawan.

Sumber:

- Riawan Arbi Kusuma

2.10 *ISO 27001 Controls and Objectives*

Standarisasi SNI *ISO IEC* 27001_2009 adalah standar yang digunakan untuk audit keamanan sistem informasi dalam sebuah perusahaan atau organisasi. Ini adalah beberapa control objektif beserta penjelasannya yang ada didalam standarisasi SNI *ISO IEC* 27001_2009 untuk memudahkan dalam memilih ruang lingkup dalam menjalan audit keamanan sistem informasi.



Gambar 2.8 ISO/IEC 27001

isoindonesiacenter.com/mengapa-perlu-menerapkan-iso-270012013/

Ini adalah beberapa kontrol yang ada pada *ISO* 27001 yang dibagi menjadi beberapa bagian seperti:

1. Annex 5 Kebijakan keamanan informasi.
2. Annex 6 Organisais keamanan informasi.
3. Annex 7 Pengelolahan aset.
4. Annex 8 Keamanan sumber daya manusia.
5. Annex 9 Keamanan fisik dan lingkungan.
6. Annex 10 Manajemen komunikasi dan operasi.

7. Annex 11 Pengendalian akses.
8. Annex 12 Akuisis, pengembangan dan pemeliharaan sistem informasi.
9. Annex 13 Manajemen insiden keamanan sistem informasi.
10. Annex 14 Manajemen keberlangsungan bisnis.
11. Annex 15 Kesesuaian.

2.11 Indeks Keamanan Informasi (KAMI)

Indeks keamanan informasi adalah sebuah module yang digunakan untuk menghitung tingkat kematangan (maturity level) dari standarisasi *ISO* 27001:2009 untuk mempermudah mencari hal - hal yang harus dipertahankan, diperbaiki dan juga yang harus dimitigasi karena proses data yang tidak sesuai dengan *SOP* yang berlaku dalam sebuah perusahaan.

Tahapan evaluasi dilakukan melalui sejumlah pertanyaan yang masing - masing area dibawah ini:

1. Peran TIK didalam instansi.
2. Tata kelola keamanan informasi.
3. Pengelolahan risiko keamanan informasi.
4. Pengelolahan aset informasi dan.
5. Teknologi dan keamanan informasi.

Dari module yang sudah disediakan, maka akan diberikan beberapa pertanyaan yang akan dijawab oleh pihak terkait. Untuk mendapat jawaban yang sesungguhnya, maka diharapkan untuk menjawab pertanyaan yang sudah disediakan dengan kejujuran dan keterbukaan. Hal ini untuk mewakili apa - apa saja yang harus dipertahankan, diperbaiki dan dilakukan mitigasi dari suatu perusahaan yang masih belum menerapkan SKMI dalam perusahaan.

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Gambar 2.9 Status Pengamanan

(JURNAL TEKNIK ITS Vol. 6, No. 1, (2017) ISSN: 2337-3539)

Diatas adalah contoh *table* untuk status pengamanan yang nantinya akan dilakukan oleh perusahaan yang akan mengisi kuisioner untuk melihat tingkat kesiapan / *maturity level*. Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai:

1. Tingkat I - Kondisi Awal
2. Tingkat II - Penerapan Kerangka Kerja Dasar
3. Tingkat III - Terdefinisi dan Konsisten
4. Tingkat IV - Terkelola dan Teruku
5. Tingkat V - Optimal

Untuk membantu memberikan uraian yang lebih detil, tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar *ISO/IEC* 2700:2005, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

Dari gambar ini dijelaskan bahwa ada tingkatan dalam menentukan manajemen risiko yang ada dalam sebuah organisasi tentunya berbeda - beda atau

tidak akan sama tingkat risiko yang ada untuk semua divisi dari perusahaan itu tersebut.

dari gambar ini akan dijelaskan bahwa apabila suatu perusahaan ada pada sekala :

A. Rendah : 0 - 12
B. Sedang : 13 - 24
C. Tinggi : 25 - 36
D. Kritis : 37 - 48

		Severity		
		High	**Moderate**	**Low**
Likelihood	**High**	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

Gambar 2.10 Risk Mapping Table for Exceptions

*(*JURNAL TEKNIK ITS Vol. 6, No. 1, (2017) ISSN: 2337-3539*)*

2.12 *Maturity Level CMMI*

Maturiy level adalah alat untuk mengukur seberapa matangnya tingkat yang sudah dicapai oleh sebuah perusahaan dalam penerapan audit sistem informasi. Untuk itu, maka ini adalah beberapa tingkatan yang dapat dilihat dari setiap level yang ada pada *framework CMMI* untuk keperluan menghitung tingkat kematangan dalam sebuah perusahaan atau organisasi:

Menurut *CMMI*, ini adalah beberapa model level tingkat kematangan dari model *CMMI*:

Level 1 – *Initial*

Hampir setiap organisasi memulai dari level yang seringkali disebut anarki atau kekacauan (*chaos*) ini. Pengembangan system tidak menggunakan proses yang terstruktur dan tiap developer menggunakan alat dan metodenya masing-masing. Pada tahap ini umumnya proses tidak dapat diprediksi, tidak berulang, sering mengalami krisis, over-budget, dan gagal mencapai target waktu. Ciri-ciri dari fungsi initial adalah tidak ada manajemen proyek, tidak adanya quality assurance, tidak adanya mekanisme manajemen perubahan (*change management*), tidak ada dokumentasi, adanya seorang ahli yang tau segalanya tentang perangkat lunak yang dikembangkan, dan sangat bergantung pada kemampuan individual.

Level 2 – *Repeatable*

Proses dan praktek manajemen proyek pengembangan system telah dirancang untuk melacak biaya proyek, jadwal, dan kegunaan dari sistem. Pada tahap ini, fokus ditekankan pada manajemen proyeknya, bukan pada pengembangan sistem (pengembangan sistem bervariasi untuk tiap proyek). Kesuksesan dan kegagalan masih bergantung pada kemampuan dan pengalaman dari tim yang mengerjakan proyek. Walaupun begitu, telah terdapat usaha untuk mengulang keberhasilan proyek sebelumnya, dan manajemen proyek yang efektif pun akhirnya menjadi pondasi bagi standardisasi proses level berikutnya.

Ciri-ciri dari fungsi repeatable adalah kualitas perangkat lunak mulai bergantung pada proses bukan pada orang, ada manajemen proyek sederhana, ada quality assurance sederhana, ada dokumen sederhana, ada software configuration management sederhana, tidak adanya knowledge management, tidak adanya

komitmen untuk selalu mengikuti *SDLC* dalam kondisi apapun, tidak adanya stastikal control untuk estimasi proyek dan rentan perubahan struktur organisasi.

Level 3 – *Defined*

Proses pengembangan sistem standar (umumnya disebut metodologi) telah dimiliki atau dikembangkan dan telah digunakan secara terintegrasi melalui unit sistem atau pelayanan informasi organisasi. Sebagai hasilnya, hasil dari setiap proyek menjadi lebih konsisten, dokumentasi serta penyampaian yang berkualitas tinggi, dan proses menjadi lebih stabil, mampu diprediksi (*predictable*), dan berulang *(repeatable*).

Ciri-ciri dari level Defined adalah *SDLC* sudah ditentukan, ada komitmen untuk mengikuti SDLC dalam keadaan apapun, kualitas proses dan produk masih bersifat kualitatif atau hanya perkiraan saja, tidak menerapkan Activity Based Costing, dan tidak adanya mekanisme umpan balik yang baku.

Level 4 – *Managed*

Telah memiliki tujuan yang terukur untuk kualitas dan produktivitas. Ukuran mendetail mengenai proses pengembangan proses standar dan kualitas produk telah dikumpulkan secara rutin dan disimpan dalam database. Pada tahap ini manajemen lebih proaktif dalam melihat masalah pengembangan sistem. Jadi walaupun proyek menemui masalah atau isu yang tidak diperkirakan, proses masih akan dapat disesuaikan berdasarkan efek dari kondisi yang mampu diprediksi dan terukur.

Ciri-cirinya adalah sebagai berikut, sudah ada Activity Based Costing dan digunakan untuk estimasi proyek berikutnya, proses penilaian kualitas perangkat lunak dan proyek bersifat kuantitatif, terjadi pemborosan biaya untuk

pengumpulan data karena proses pengumpulan data masih dilakukan secara manual, cenderung belum jelas disebabkan karena manusia ketika diperhatikan perilakuknya cenderung berubah, tidak ada mekanisme pencegahan defect dan adanya mekanisme umpan balik.

Level 5 – *Optimized*

Proses pengembangan sistem terstandarisasi secara kontinu dimonitor dan ditingkatkan berdasarkan ukuran dan analisa data di level 4. Setiap pembelajaran yang ada disebarluaskan pada seluruh bagian organisasi dengan penekanan pada penurunan ketidakefisienandalam proses pengembangan sistem ketika menjaga kestabilan kualitas. Sebagai kesimpulan, organisasi telah menjadikan peningkatan proses pengembangan sistem yang kontinu bagian dari dirinya.

Cirri-cirinya adalah sebagai berikut, Pengumpulan data secara automatis, adanya mekanisme pencegahan defect, adanya mekanisme umpan balik yang sangat baik, dan adanya peningkatan kualitas dari SDM dan juga peningkatan kualitas proses.

Gambar 2.11 Tahapan Kematangan *CMMI (2015)*

(ocw.upj.ac.id/files/Slide-TIF407-Capability-Maturity-Model-Integration-CMMI.pptx)

Perusahaan international yang sudah menerapkan *CMMI* sampai level 5 adalah Huawei (*CMMI Level 5*).

Litbang di Huawei menjadi bagian terpenting dari industri teknologi baik software maupun hardware. Inilah yang membuat Huawei terbukti responsif terhadap kebutuhan masa depan dan masa kini pelanggan. Investasi di area ini penting untuk terus-menerus mengembangkan teknologi, solusi dan layanan yang tujuan akhirnya adalah memaksimalkan keuntungan dan memberikan nilai tambah bagi pelanggan.

Pada akhir September 2008, sekitar 44% dari total 96.800 karyawan Huawei terlibat dalam R&D. Sebagai bagian terintegrasi dari keseluruhan proses, Huawei menanamkan kembali 10% pendapatan dari hasil penjualannya untuk

riset dan pengembangan di mana 10% tersebut diarahkan untuk mendanai pengembangan berbagai teknologi mutakhir dan teknologi dasar setiap tahunnya.

Perusahaan Internasional lainnya yang meraih level maturity 5 adalah Toshiba, NASA dan ATSI (*The Association of Thai Software Industry*).

Sumber: (ocw.upj.ac.id/files/Slide-TIF407-Capability-Maturity-Model-Integration-CMMI.pptx))