



STANDAR MANAJEMEN LAYANAN & KEAMANAN SI/TI ISO/IEC 20000 DAN ISO/IEC 27001

Studi Kasus : PT. Astra Graphia Information Technology & PT. Visionet Internasional

Alvin Aldo Kassidy | Billy Alfredo | Kharisma Dharma Pertiwi | Galih Putra Perdana

**Sistem Informasi | Fakultas Sains dan Teknologi |
Universitas Ma Chung Malang | 2015**

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan hidayah-Nya makalah dengan judul “Standar Manajemen Layanan & Keamanan SI/TI ISO/IEC 20000 dan ISO/IEC 27001, Studi Kasus: PT. Astra Graphia Information Technology & PT. Visionet Internasional ” yang sesuai dengan permintaan dosen pengampu mata kuliah Audit SI/TI dapat terealisasi dengan baik dan lancar.

Makalan ini bersisi tentang penjelasan mengenai ISO/IEC 20000 dan ISO/IEC 27001 *Information Security Management System* yang disertai dengan contoh studi kasus agar lebih mudah untuk dipahami oleh pembaca.

Penulis menyadari makalah ini jauh dari kata sempurna. Oleh karena itu penulis membutuhkan kritik dan saran untuk evaluasi dan perbaikan agar bermanfaat bagi pengulasan lebih lanjut sehingga kajian yang diberikan akan lebih informatif dan tepat sasaran kepada setiap pembaca.

Akhir kata, penulis ucapkan terima kasih kepada semua pihak yang terlibat dalam pembuatan makalah ini, dan semoga makalan ini dapat bermanfaat dan memberikan pengetahuan baru bagi pembaca dan bagi penulis khususnya.

Malang, 15 Oktober 2015

Penulis

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI.....	ii
DAFTAR GAMBAR	iii
DAFTAR TABEL.....	iii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Tujuan.....	3
1.4. Manfaat.....	3
1.5. Metode Studi Pustaka	3
BAB II TELAAH PUSTAKA	4
BAB III PEMBAHASAN.....	9
3.1 ISO/IEC 20000.....	9
3.1.1 Gambaran ISO/IEC 20000.....	9
3.1.2 Sertifikasi ISO/IEC 20000	12
3.1.3 Manfaat Sertifikasi ISO/IEC 20000.....	13
3.1.4 Langkah-Langkah Sertifikasi ISO/IEC 20000.....	14
3.1.5 Lama Implementasi Sertifikasi ISO/IEC 20000	16
3.1.6 Contoh Studi Kasus	17
3.2 ISO/IEC 27001	20
3.2.1 Gambaran ISO/IEC 27001	20
3.2.2 Fungsi ISO/IEC 27001.....	23
3.2.3 Sertifikasi ISO/IEC 27001	24
3.2.4 Langkah-Langkah Sertifikasi ISO/IEC 27001	25
3.2.5 Lama Implementasi Sertifikasi ISO/IEC 27001	28
3.2.6 Contoh Studi Kasus	29
3.3 Perbandingan ISO/IEC 20000 dan ISO/IEC 27001	30
BAB IV KESIMPULAN	33
DAFTAR PUSTAKA	34

DAFTAR GAMBAR

Gambar 1 Struktur dan Proses ISO/IEC 20000	6
Gambar 2 Proses Sertifikasi ISO-20000	7
Gambar 3 Model PDCA (cybersecurity, 2015)	8
Gambar 4 Tahapan Implementasi Program Perbaikan Layanan (John, DiMaria, 2006)	15
Gambar 5 Langkah-Langkah Mencapai Sertifikat ISO/IEC 20000	16
Gambar 6 Hasil Sertifikasi ISO/IEC AGIT	19
Gambar 7 AGIT Business Strategy 2013-2015	20
Gambar 8 Aspek Keamanan Informasi	22
Gambar 9 Ancaman Keamanan Informasi	23

DAFTAR TABEL

Tabel 1 Perbedaan ISO/IEC 20000 dan ISO/IEC 27001	31
---	----

BAB I

PENDAHULUAN

1.1. Latar Belakang

Menurut Muchtar A.F layanan adalah suatu sikap yang dapat mengakibatkan rasa puas atau tidak puas yang dialami oleh konsumen pada saat terjadinya proses tindakan. Sedangkan menurut Antonius Aditya & Onno Purbo, layanan adalah sebuah produk yang memberikan solusi kepada pelanggan (Carapedia, 2015). Dari dua definisi tersebut dapat disimpulkan bahwa layanan merupakan suatu produk yang diberikan kepada pelanggan bertujuan memberikan kepuasan terhadap solusi yang diberikan oleh perusahaan. Kepuasan tersebut akan membuat pelanggan mempertimbangkan perusahaan mana yang dapat memberikan *value* lebih atas layanannya, karena pelanggan saat ini sudah semakin cerdas yaitu telah menempatkan kualitas layanan pada urutan teratas mengalahkan kualitas produk/jasa dalam hal pertimbangan untuk menggunakan/membeli barang/jasa. Oleh karena itu, penyampaian layanan kepada pelanggan juga tidak kalah penting untuk menjadi perhatian perusahaan. Karena kepuasan pelanggan adalah bentuk tercapainya tujuan bisnis perusahaan.

Mengelolah atau manajemen layanan diperlukan ketekunan dan keahlian agar dapat menarik perhatian pelanggan, dengan cara meningkatkan kualitas layanan dan pelayanan salah satunya. Pelanggan akan cenderung memilih perusahaan yang memberikan pelayanan dengan *value* lebih dibandingkan perusahaan yang hanya menjual produk atau jasanya saja. Pelayanan yang dimaksud adalah mulai dari pemesanan, pengiriman yang tepat waktu dan tanpa cacat, hingga pemberian jaminan atas produk/jasa yang dibeli oleh pelanggan.

Persaingan bisnis saat ini sudah semakin maju. Masing-masing penyedia layanan bersaing untuk memberikan layanan yang terbaik agar diminati oleh pelanggan. Kemajuan tersebut didukung dengan adanya teknologi informasi (TI) yang turut berkembang di era teknologi saat ini. Perkembangan teknologi ini semakin hari semakin

kompleks yang memungkinkan segala sesuatu menjadi lebih cepat dan terjangkau hingga menyebabkan pelanggan juga memiliki hak atas permintaan yang lebih beragam. Keadaan ini membuat perusahaan memerlukan pendekatan yang lebih fleksibel untuk integrasi antara layanan TI dengan layanan konvensional perusahaan agar dapat bersaing dengan perusahaan lainnya yang serupa.

Integrasi yang melibatkan layanan TI dengan layanan konvensional serta semua sumber daya manusia tentunya akan membuat informasi yang dihasilkan juga semakin banyak dan kompleks. Informasi-informasi ini dapat digunakan oleh perusahaan sebagai sumber pengambilan keputusan atas pengembangan bisnis yang dijalankan. Namun, tidak menutup kemungkinan bahwa informasi yang sudah tersimpan rapi menggunakan teknologi informasi kerap kali hilang atau jatuh ke tangan yang tidak memiliki hak semestinya. Oleh karena itu, dibutuhkan pengawasan dan pengontrolan terhadap informasi-informasi yang tersimpan.

Berdasarkan paparan sebelumnya, perusahaan yang berfokus pada kepuasan pelanggan dengan menerapkan bantuan teknologi informasi dalam bisnisnya tentunya akan menghitung ulang biaya yang harus dikeluarkan. Karena penerapan TI juga akan mengeluarkan biaya yang cukup besar. Bagi perusahaan yang kurang atau bahkan tidak bisa mengelola biaya perusahaan akan mengalami kesulitan bahkan kebangkrutan. Untuk itu, dibutuhkan adanya kontrol atas manajemen layanan terutama manajemen TI atau *IT Service Management* (ITSM) dan juga pengamanan data untuk kontrol atas informasi yang ada pada manajemen informasi atau *Information Security Management System* (ISMS).

Makalah ini akan memaparkan tentang pengelolaan ITSM dan ISMS dalam sebuah organisasi. Dalam hal ini akan dibahas standar yang menggunakan ITSM yaitu ISO/IEC 20000 dan ISMS yaitu ISO/IEC 27001. Pemaparan akan diberikan contoh studi kasus agar lebih mudah dipahami jika diterapkan secara nyata dalam unit bisnis tertentu.

1.2. Rumusan Masalah

Berdasarkan latar belakang permasalahan yang dipaparkan sebelumnya, maka dapat dirumuskan rumusan masalahnya sebagai berikut.

- (1) Apa yang dimaksud dan bagaimana menerapkan pengelolaan layanan TI menggunakan standar internasional ISO/IEC 20000 ?
- (2) Apa yang dimaksud dan bagaimana menerapkan pengelolaan layanan TI menggunakan standar internasional ISO/IEC 27001 ?

1.3. Tujuan

Tujuan penulisan makalah ini adalah untuk memahami standar ISO/IEC 20000 dan ISO/IEC 27001 yang berperan dalam pengelolaan layanan TI dalam sebuah organisasi serta mengetahui prosedur dan contoh nyata pengelolaan layanan TI yang sudah tersertifikasi.

1.4. Manfaat

Manfaat dari penulisan Makalah ini diantaranya.

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

1.5. Metode Studi Pustaka

Metode studi pustaka yang dilakukan dalam penulisan makalah ini yaitu studi literatur. Studi literatur adalah metode pengumpulan informasi dengan berbagai sumber dari media cetak ataupun elektronik. Dalam hal ini digunakan media elektronik berupa *website* dan jurnal *online*.

BAB II

TELAAH PUSTAKA

Bagian ini akan memaparkan mengenai beberapa studi yang dilakukan sebelumnya terkait dengan bahasan makalah ini. Berikut penjelasan paparan hasil studi pustaka.

(1) Layanan Teknologi Informasi

Semakin maju dan berkembang sebuah organisasi, layanan TI yang ada dituntut selaras dengan tujuan organisasi. Dengan keselarasan ini layanan TI dapat digunakan sebagai pendorong tercapainya tujuan organisasi. Jika proses TI dan layanan TI didukung, disampaikan, dan diatur dengan cara yang tepat, bisnis akan lebih berhasil (Zhang, Ding, & Zong, 2009). Dengan demikian, memberikan layanan TI dengan kualitas tinggi yang selaras dengan bisnis merupakan suatu tantangan. Kualitas layanan TI merupakan salah satu pendorong tercapainya tujuan organisasi yang efektif dan efisien. Layanan TI harus dapat menyesuaikan perubahan bisnis yang berdampak pula pada perubahan kebutuhan layanan TI. Terjaganya kualitas layanan TI ditunjukkan dengan konsistensi dalam penyediaan layanan. Untuk menjaga terjaganya kualitas layanan TI yang konsisten dibutuhkan suatu proses yang menghubungkan kebutuhan unit bisnis dengan unit TI yang juga dapat digunakan sebagai jaminan untuk penyedia layanan TI yang berkualitas. Proses ini biasa disebut dengan manajemen tingkat layanan TI.

Kualitas layanan TI di sebuah organisasi dibuat atas kesepakatan antara penyedia layanan dengan pelanggan. Atribut kualitas layanan TI yang umum digunakan, diantaranya (Lepmets, Ras, & Renault, 2011).

- a. Ketersediaan, yaitu sistem informasi yang tersedia bagi pengguna pada tempat dan waktu yang disepakati.
- b. Kapasitas, yaitu semua kapasitas terkait sistem informasi dan TI secara umum.
- c. Kinerja, yaitu kecepatan pemrosesan informasi yang dilihat sudut pandang pengguna.

- d. Keamanan.
- e. Kerahasiaan, yaitu bagan dari keamanan dan berperan penting bergantung pada bisnis pengguna.
- f. Skalabilitas, yaitu penyedia layanan harus menjamin pertumbuhan pada kecepatan yang dibutuhkan tanpa mengganggu bisnis.
- g. Kecakapan, yaitu penyedia layanan harus memilih metode pengembangannya, arsitektur infrastruktur dan hal lain yang mendukung kecakapan sistem informasi.

Menjaga kualitas layanan secara konsisten merupakan hal yang paling penting, karena layanan yang diberikan dapat mempengaruhi kepuasan pelanggan (Lepmets, Ras, & Renault, 2011). Oleh karena itu, dibutuhkan jaminan atas kualitas layanan yang disediakan. Jaminan ini dapat diwujudkan dengan adanya kesepakatan antara unit bisnis dengan penyedia layanan. Kesepakatan berisi mengenai target tingkat layanan yang akan disediakan yang disesuaikan dengan kemampuan penyedia layanan. Semua itu diatur sedemikian rupa agar kualitas layanan tetap terjaga. *IT service management* (ITSM) merupakan serangkaian proses yang memungkinkan perencanaan, pengorganisasian, pengarahan, dan pengontrolan penyediaan layanan TI (Correia & Brito e Abreu, 2010). Manajemen tingkat layanan TI merupakan bagian dari ITSM. Proses pada ITSM tentunya juga melibatkan banyak data dan informasi yang penting dan harus dijaga. Kebutuhan untuk memanajemen informasi tersebut dapat diwujudkan dengan menggunakan manajemen keamanan sistem atau *information security management system* (ISMS).

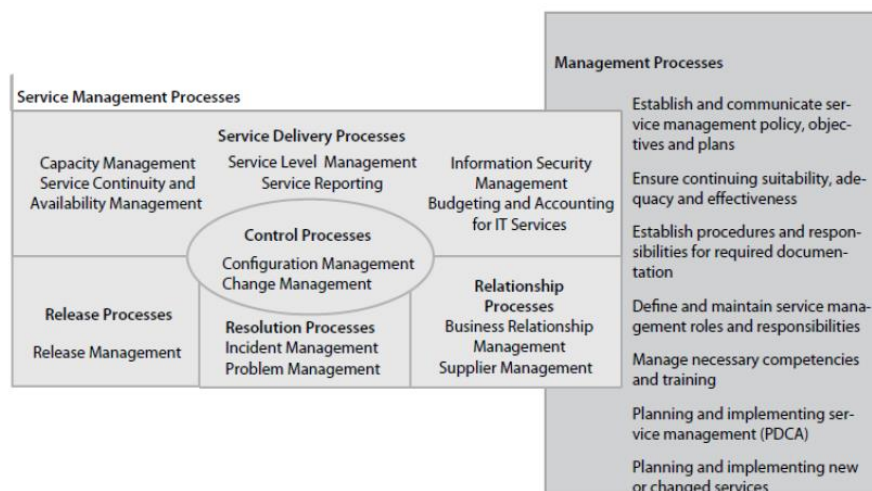
(2) *Information Technology Service Management* (ITSM)

Information technology service management (ITSM) merupakan konsep manajemen dalam memberi layanan TI secara baik dan berhasil kepada pelanggan. ITSM meliputi semua proses yang digunakan untuk meningkatkan kualitas sesuai dengan tingkat level yang telah disepakati bersama pelanggan, guna memberi suatu

layanan yang bernilai dan sesuai dengan kebutuhan-kebutuhan pelanggan (Andgaa, 2015).

Sistem, proses, dan strategi ITSM yang efektif dan efisien sangat penting bagi suksesnya penerapan TI. ITSM membahas inisiasi, desain, organisasi, kontrol, ketentuan, dukungan dan perbaikan layanan TI. Fokus dari ITSM menangani masalah operasional manajemen TI dalam organisasi bukan menangani proses pembuatan perangkat lunak tertentu serta membahas tentang keselarasan antara kebutuhan layanan TI dengan kebutuhan bisnis (Wikipedia, 2015). Proses untuk meningkatkan dan mengelola kualitas layanan TI dapat menggunakan manajemen ITSM untuk memastikan bahwa layanan didesain dan dikelola sejalan dengan spesifikasinya.

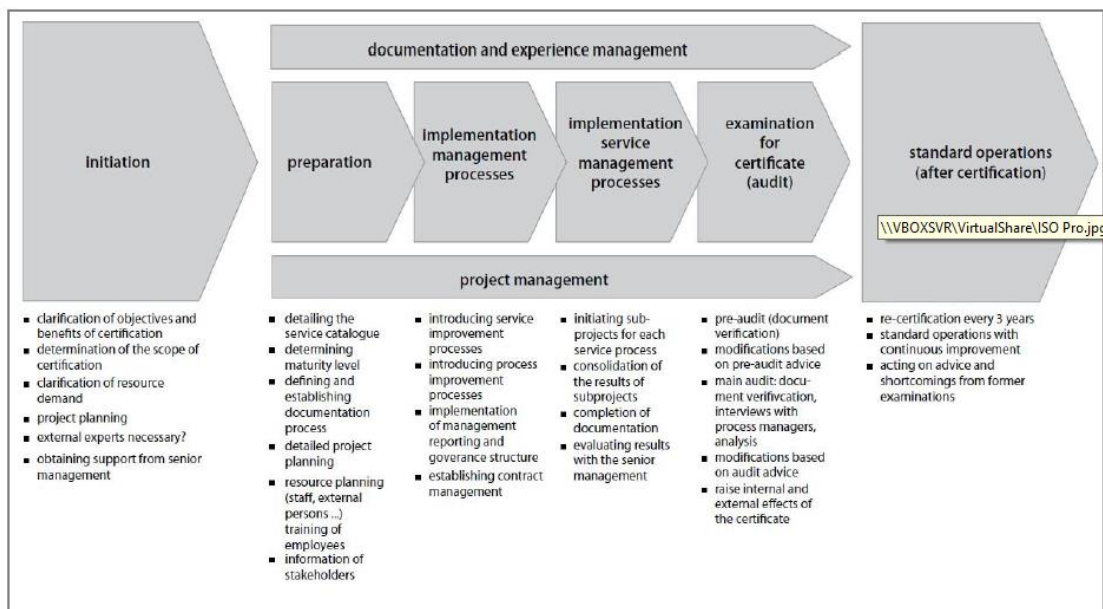
Dalam penerapan ITSM, dapat digunakan standar yang dapat membantu terarahnya pengukuran kinerja dan penilaian hasil kualitas layanan TI. ISO/IEC 20000 memberikan standar untuk manajemen layanan TI yang dapat menentukan persyaratan minimum yang harus disiapkan oleh organisasi dalam sebuah proses menyediakan dan mengelola layanan berkualitas tinggi. Proses yang ada pada ISO 20000 selaras dan saling melengkapi dengan proses ITIL. Gambar 1 menunjukkan pendefinisian kebutuhan pada proses tersebut (Kuller, Grabowski, PetrSames, & Vogt, 2010).



Gambar 1 Struktur dan Proses ISO/IEC 20000

Standar ISO 20000 disusun dalam tiga dokumen, yaitu ISO 20000-1 *Service Management : Specification*, ISO 20000-2 *Service Management : Code of Practice*, dan ISO 20000-3 *Service Management : Practical Guidance*.. Dokumen pertama berisi tentang deskripsi format standar dan menjelaskan persyaratan yang harus dipenuhi untuk mencapai sertifikasi. Dokumen kedua menjelaskan persyaratan kebutuhan dan memberikan *best practices* dalam implementasi yang baik. Dokumen ketiga berisi mengenai ruang lingkup dan penerapan pada bagian pertama.

Pada ISO 20000 menggunakan alur proses PDCA yang merupakan bagian utama dari standar. PDCA meliputi *Plan (planning)*, *Do (executions of the plans)*, *Check (monitor services)* dan *Act (procedures for mprovement)*. Sebuah perusahaan dapat melakukan sertifikasi ISO 20000 dengan melakukan langkan-langkah seperti pada gambar 2 (Kuller, Grabowski, PetrSames, & Vogt, 2010).



Gambar 2 Proses Sertifikasi ISO-20000

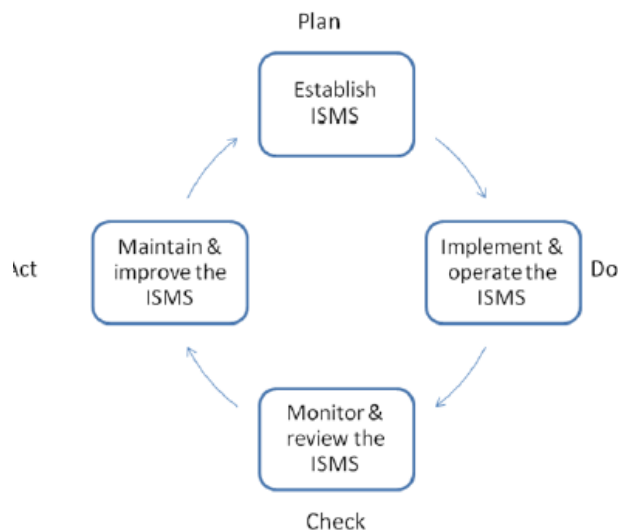
(3) *Information Security Management System (ISMS)*

Information security management system (ISMS) adalah pendekatan yang sistematis dan terstruktur untuk mengelola informasi sehingga tersimpan dengan

aman. ISMS ini meliputi pelaksanaan kebijakan, proses, prosedur, dan struktur organisasi, serta fungsi *software* dan *hardware* (cybersecurity, 2015).

Sebuah organisasi dan sistem informasi kerap kali banyak mendapat ancaman keamanan informasi, seperti penipuan kebakaran, banjir, dan sabotase dari pihak luar. Meningkatnya jumlah pelanggaran keamanan telah menyebabkan meningkatnya kekhawatiran keamanan informasi oleh organisasi di seluruh dunia. Mencapai keamanan dalam informasi adalah capaian yang cukup sulit bagi organisasi. Dengan demikian dibutuhkan cara atau proses untuk mengelola keamanan informasi dari perspektif holistik dan metodologi untuk manajemen keamanan informasi yang sistematis. Standar yang dapat digunakan oleh ISMS dalam implementasi manajemen ini salah satunya adalah ISO/IEC 27001:2005.

ISO/IEC 27001:2005 merupakan bagian dari ISMS yang memaparkan persyaratan kebutuhan mendirikan, melaksanakan, operasi, pemantauan, peninjauan, pemeliharaan, dan peningkatan ISMS dalam konteks risiko bisnis organisasi secara keseluruhan. Proses ini didasarkan pada model PDCA, yaitu *Plan, Do, Check, and Act*.



Gambar 3 Model PDCA (cybersecurity, 2015)

BAB III

PEMBAHASAN

The International Organization for Standardization merupakan sebuah organisasi internasional yang mengembangkan dan menerbitkan standar internasional. ISO ini beranggotakan badan-badan standarisasi nasional, diantaranya BSN (Indonesia), BSI (UK), ANSI (USA), dan DIN (Jerman) (kemkes, 2015). Standar manajemen sistem ISO menyediakan model untuk diikuti dalam pengaturan dan operasi sistem manajemen. Manfaat dari sistem manajemen yang efektif diantaranya (ISO, 2015).

- (1) Lebih efisien penggunaan sumber daya.
- (2) Meningkatkan manajemen risiko.
- (3) Meningkatkan kepuasan pelanggan atas layanan dan produk secara konsisten.

Audit adalah bagian penting dari pendekatan sistem manajemen karena keduanya memungkinkan perusahaan atau organisasi untuk memeriksa seberapa jauh prestasi mereka dalam mencapai tujuan dan menunjukkan kesesuaian dengan standar. Berikut akan dibahas dua standar internasional yang dapat digunakan untuk menilai kinerja organisasi dalam meningkatkan kualitas layanan TI.

3.1 ISO/IEC 20000

3.1.1 Gambaran ISO/IEC 20000

Saat hendak menggunakan jasa pihak ketiga dalam implementasi teknologi informasi (TI), tentu perlu dilakukan *beauty contest* terlebih dahulu. *Beauty contest* yang dimaksud adalah uji kualitas perusahaan yang dilihat dari berbagai aspek. Salah satu aspek yang dinilai adalah kinerja perusahaan. Perusahaan yang berkinerja baik adalah perusahaan yang memiliki layanan handal, efisien, dan fokus pada pelanggan. ISO/IEC 20000 berpedoman untuk mencapai tujuan tersebut. ISO/IEC 20000 adalah mekanisme bagi penyedia layanan untuk memvalidasi kemampuan dalam memberikan layanan TI. Tujuan

ISO/IEC 20000 adalah mengurangi gangguan layanan dan meningkatkan kepuasan pelanggan melalui penyediaan layanan TI yang lebih baik (Wardani, 2007).

ISO/IEC 20000 merupakan standar internasional yang memungkinkan sebuah organisasi untuk mendemonstrasikan keunggulan dan terbukti dapat menyajikan *IT service management* yang terbaik. Beberapa kegunaan ISO/IEC 20000, diantaranya (ISO, 2015).

- (1) Bisnis yang akan keluar dari tender untuk layanan mereka.
- (2) Pendekatan yang konsisten oleh semua penyedia layanan dalam rantai pasokan.
- (3) Sebagai patokan manajemen layanan TI.
- (4) Sebagai dasar penilaian independen.
- (5) Menunjukkan kemampuan kebutuhan pelanggan.
- (6) Meningkatkan pelayanan.

ISO/IEC 20000 menunjukkan bahwa organisasi berorientasi pada kualitas dengan memberikan layanan TI yang efisien dan efektif. ISO/IEC 20000 pertama kali diliris pada tahun 2005, dan sekarang telah beranjak ke edisi kedua. Hal ini sejajar dengan daftar pustaka infrastruktur IT yaitu *Information Technology Infrastructure Library* (ITIL), sebagai kerangka praktik terbaik (APMG International, 2015). Penerapan ISO/IEC 20000 telah berkembang pesat dalam dunia internasional untuk area *internal* dan *external IT Service provider*, dan telah menjadi standar kompetensi dalam penerapan bidang *IT Services*. ISO / IEC 20000 mendefinisikan persyaratan untuk penyedia layanan TI. ISO / IEC 20000 berdasarkan BS 15000 dulunya dikelola oleh *British Standards Institutions* (BSI) yang merupakan sebuah standar internasional, *testing* dan organisasi sertifikasi.

ISO/IEC 20000 terdiri dari tiga bagian, yaitu. ISO/IEC 20000-1:2011, ISO/IEC 20000-2:2012, ISO/IEC 20000-3:2012 (ISO, 2015).

(1) ISO/IEC 20000-1:2011 (Bagian pertama)

ISO/IEC 20000-1:2011 adalah spesifikasi *auditable* dengan mendefinisikan persyaratan untuk sertifikasi dan sistem pelayanan yang meliputi.

- a. Persyaratan umum untuk sistem manajemen pelayanan.
- b. Desain dan transisi dari layanan baru ataupun diubah.
- c. Proses pelayanan.
- d. Proses hubungan.
- e. Proses penyelesaian.
- f. Proses kontrol.

(2) ISO/IEC 20000-2: 2012 (Bagian kedua)

ISO/IEC 20000-2: 2012 memberikan bimbingan pada penerapan sistem manajemen pelayanan, perbaikan pelayanan dan dalam persiapan penilaian kesesuaian terhadap ISO/IEC 20000-1. Termasuk praktik-praktik terbaik untuk proses manajemen layanan dalam ruang lingkup ISO/ EC 20000-1.

(3) ISO/IEC 20000-3:2012 (Bagian ketiga)

ISO/IEC 20000-3:2012 berisi ruang lingkup dan penerapan pada bagian pertama, sangat berguna untuk penyedia layanan konsultan dan penilai manajemen pelayanan. Bagian ini termasuk *practical guidance* dalam satu ruang lingkup, penerapan dan demonstrasi kesesuaian dan persyaratan dalam ISO/IEC 20000-1.

Bimbingan pada berbagai jenis penilaian kesesuaian dan standar penilaian juga disertakan pada bagian ketiga. Hal ini akan membantu perencanaan perbaikan layanan dan dalam persiapan untuk penilaian kesesuaian terhadap ISO/IEC 20000-1. Melengkapi penerapan ISO/IEC 20000-1 yang telah diberikan dalam ISO/IEC 20000-2.

3.1.2 Sertifikasi ISO/IEC 20000

Berdasarkan ISO/IEC : 2011 sertifikasi untuk ISO/IEC pemeriksaan edisi 2011 didasarkan pada bagian pertama dan edisi 2012 dari bagian kedua, dan format penilaian sebelumnya semua mengarah pada struktur standar ISO/IEC 2000:2005. Sertifikasi ISO/IEC 20000 terbagi menjadi tiga yaitu (APMG International, 2015).

(1) *Foundation*

Sertifikasi *Foundation Level* adalah sertifikasi level pertama ISO/IEC 20000 dan sebagai salah satu syarat untuk lanjut ke level selanjutnya, hal ini bertujuan untuk memastikan kandidat mempunyai basis pengetahuan yang kuat mengenai konten dan *standard requirement* dari ISO/IEC 20000, memahami bagaimana pada umumnya ITSM beroperasi.

Kandidat yang memenuhi syarat ISO/IEC 20000 disebut sebagai *The Foundation*, dan mereka dapat melanjutkan ke level selanjutnya yaitu *Practitioner certification*.

(2) *Practitioner*

Kandidat harus memenuhi salah satu diantara tiga sertifikasi syarat untuk menjadi praktisionis atau praktisi level, yaitu:

- a. APMG ISO/IEC 20000 *Foundation*, atau
- b. BGC ISO/IEC 20000 *Foundation*, atau
- c. ITIL *Foundation*

Kandidat atau *The Foudation* sudah diharuskan mengerti untuk menerapkan konten standar dari ISO/IEC 20000.

(3) *Auditor*

Kandidat yang lulus ujian *Auditor* diharapkan bisa memahami prinsip ITSM dan persyaratan ISO/IEC 20000 -1:2011 (Bagian pertama). Ini tidak mencakup prinsip teknik audit sistem manajemen dan untuk alasan ini dilegasi atau kandidat

yang ingin menghadiri kursus *level auditor* wajib memiliki pengalaman tiga tahun di bidang *IT environment*. Para kandidat juga diwajibkan untuk menghadiri kursus Auditor APMG atau BGC yang terakreditasi untuk dapat mengambil ujian ini.

3.1.3 Manfaat Sertifikasi ISO/IEC 20000

Sertifikasi ISO/IEC 20000 sangat penting bagi perusahaan karena mampu memberikan beberapa manfaat diantaranya adalah sebagai berikut (**Kurnia, 2015**).

(1) Menunjukkan komitmen perusahaan dan meningkatkan daya saing.

Sertifikat ISO/IEC 20000 dapat meningkatkan citra perusahaan akan komitmennya terhadap kualitas layanan TI yang diberikan. Jika standar ISO 9000 menunjukkan komitmen perusahaan akan sistem manajemen mutu yang baik, maka ISO/IEC 20000 merupakan komitmen mutu yang baik dalam penyelenggaraan layanan TI. Pencapaian ini akan meningkatkan daya saing perusahaan di mata pelanggan.

(2) Menunjukkan kemampuan perusahaan dalam audit.

Sertifikat ISO/IEC 20000 membuktikan bahwa penyedia layanan TI mampu memberikan layanan yang memenuhi kebutuhan pengguna. Di dalam standar ISO/IEC 20000 terdapat spesifikasi agar layanan yang diberikan memiliki kualitas yang dapat diterima oleh pelanggan. Sertifikat ISO 20000 mampu membuktikan kepada *auditor* bahwa layanan TI dikelola dengan baik dan kualitasnya dapat diterima oleh pelanggan. ISO 20000 menekankan pendekatan proses pada pengelolaan layanan TI, sehingga hal ini memberikan jaminan bahwa data yang dihasilkan oleh proses yang benar adalah data yang valid dan mereduksi keraguan auditor atas data yang diaudit.

(3) Memenuhi persyaratan tender.

Standar ini wajib dimiliki oleh penyedia layanan eksternal yang ingin mengikuti tender. Beberapa tender mensyaratkan agar penyedia layanan telah tersertifikasi ISO/IEC 20000.

(4) Memberikan kerangka kerja peningkatan layanan TI, mengurangi risiko dan biaya layanan TI.

Dengan mempraktikkan manajemen sistem layanan yang baik seperti yang ditetapkan dalam ISO/IEC 20000, diharapkan perusahaan dapat melakukan peningkatan dalam kualitas layanannya, melakukan penghematan biaya dan meningkatkan efisiensi, menghasilkan pengurangan resiko yang mungkin ditimbulkan oleh layanan TI dan mendorong perbaikan layanan TI secara terus-menerus.

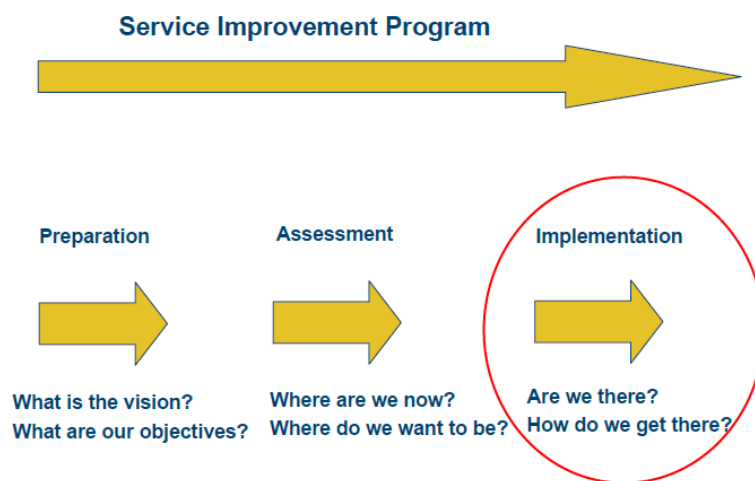
3.1.4 Langkah-Langkah Sertifikasi ISO/IEC 20000

Standar ISO/IEC 20000 mengatur prosedur dan proses dari ITSM, sehingga diperlukan pemahaman dan implementasi ITSM. Perusahaan yang telah sadar akan pentingnya sertifikasi ISO/IEC 20000 untuk menjamin mutu layanan TI harus mendefinisikan visi dan misi yang dibantu dengan panduan batasan pengembangan kualitas. Kemudian dilakukan penilaian awal atas keadaan yang saat ini dialami perusahaan, dilanjutkan dengan *gap analysis* kondisi sekarang dengan kondisi yang ingin dicapai. Perusahaan selanjutnya perlu menyiapkan berbagai program perbaikan layanan berdasarkan temuan yang didapat dalam fase persiapan, penilaian, dan implementasi. Hal tersebut merupakan tahap awal mencapai ketentuan sertifikasi ISO/IEC 20000, lihat gambar 4 (Monica, Hindarto, & Widyastuti, 2014).

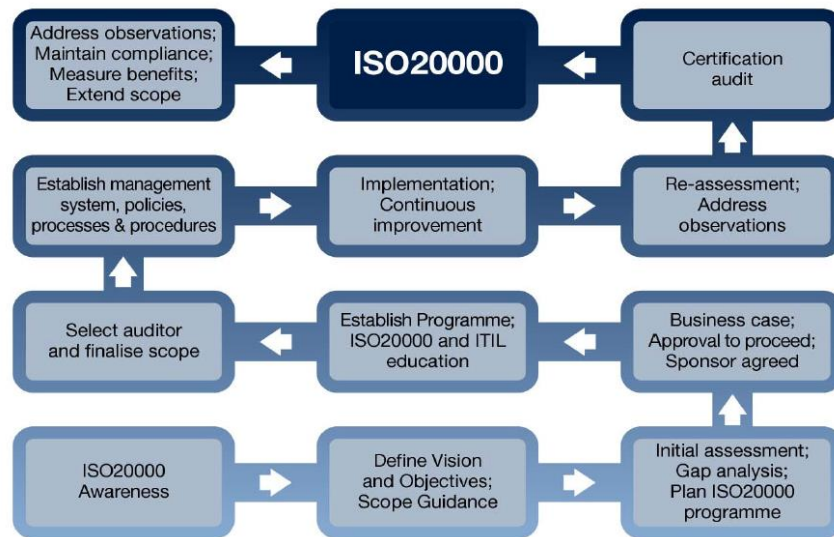
Setelah perusahaan merencanakan manajemen layanan yang baik dan sesuai dengan *best practice* dan *good practice* yang ada, perusahaan mulai melakukan studi kasus agar persetujuan bisa diperoleh dan disetujui oleh sponsor.

Langkah selanjutnya adalah menetapkan program yang berbasis pada ketentuan dan kriteria dalam ISO/IEC 20000. Diperlukan pemilihan *auditor* dan finalisasi lingkup layanan untuk kemudian dilanjutkan ke penetapan sistem manajemen, kebijakan-kebijakan, proses dan prosedur. Setelah proses dan prosedur ditetapkan, dimulailah implementasi manajemen layanan TI dan dilanjutkan dengan evaluasi dan perbaikan terus-menerus.

Setelah beberapa waktu menjalankan program manajemen layanan, dilakukan penilaian ulang dan pembahasan atas observasi yang dilakukan pihak *auditor*. Untuk dapat dikatakan *certified*, perusahaan perlu melakukan *certification audit*. *Auditor* atau tim audit akan memberikan serangkaian pertanyaan terkait dengan standar ISO/IEC 20000. Jika layanan dinyatakan telah layak dan mampu memberikan *value* bagi pelanggan, maka perusahaan akan mendapatkan sertifikat ISO 20000. Namun tidak berhenti sampai disini, perusahaan harus terus menerus melakukan observasi, mempertahankan kesesuaian layanan, mengukur manfaat dan memperluas lingkup manajemen layanan. Secara ringkas, langkah-langkah ini dapat dilihat dalam gambar 5.



Gambar 4 Tahapan Implementasi Program Perbaikan Layanan (John, DiMaria, 2006)



Gambar 5 Langkah-Langkah Mencapai Sertifikat ISO/IEC 20000

3.1.5 Lama Implementasi Sertifikasi ISO/IEC 20000

Implementasi program manajemen layanan TI tentu membutuhkan waktu yang relatif lama. Bagi perusahaan yang belum menerapkan ITIL®, dibutuhkan waktu sekitar 18 bulan untuk bisa mencapai ISO 20000. Sedangkan untuk perusahaan yang telah menerapkan ITIL® dengan baik, dibutuhkan waktu sekitar 9 bulan. Yang perlu diperhatikan adalah, ketika suatu proses didesain dan didokumentasikan, proses tersebut butuh diluncurkan dan dijalankan selama 3 bulan sebelum memasuki proses audit untuk membuktikan kesesuaian. Beberapa hal penting juga perlu diperhatikan, diantisipasi dan ditangani dalam implementasi, yaitu:

- (1) Proses dan prosedur yang ada tidak selalu sejalan.
- (2) Terdapat beberapa proses yang tidak ada atau bahkan tidak diperlukan.
- (3) Karyawan tidak mengerti perbedaan antara proses dan prosedur.
- (4) Sumber daya untuk implementasi manajemen layanan, kadang karyawan punya kesibukan lain dalam pekerjaannya.
- (5) Karyawan enggan untuk mengakui bahwa mereka tidak tahu atau paham akan kebutuhan.

- (6) Ruang lingkupnya belum jelas.
- (7) Tidak semua proses terdokumentasi dan terukur, terutama untuk performa perbaikan yang teridentifikasi.
- (8) Konsentrasi lebih terarah pada alat dan bukan pada implementasi proses.

3.1.6 Contoh Studi Kasus

PT. Astra Graphia Information Technology (AGIT) adalah contoh studi kasus perusahaan yang menerapkan sertifikasi ISO/IEC 20000 (APM Group, 2015).

(1) Profil singkat AGIT (APM Group, 2015)

1 *Company Name* : PT. Astra Graphia Information Technology

2 *Country* : Indonesia

3 *Certified Under* : The APM Group

4 *Version of ISO/IEC 20000* : 2011

5 *Certification Status* : Issued

6 *Certification Start Date*: 03 Sep 2013

7 *Certification Expiry Date* : 02 Sep 2016

8 *RCB Certified by* : British Standards Institution

9 *The Scope of the certification is* :

IT SMS that supports the provision of IT Services (Colocation, Helpdesk and CCTV) to AGIT's internal and external customers, including the IT Infrastructure operational support from its sites in Jakarta (Sudirman, Kramat and TB Simatupang)

10 *The Location covered by the certification is* :

ANZ Tower, 22nd floor,
JL. Jenderal Sudirman Kav. 33A
Jakarta 10220
Indonesia

(2) Sejarah singkat AGIT

- 1 1971 : Mulai beroperasi pada tahun 1971 sebagai divisi Xerox di PT. Astra International.
- 2 1976 : PT. Astra Graphia berdiri sebagai badan hukum (perseroan).
- 3 1983 : Memasuki bisnis TI dengan ditunjuknya sebagai distributor eksklusif Digital Equipment Corporation. USA.
- 4 1989 : Menjadi perusahaan publik dengan mencatatkan sahamnya di BEJ dan BES.
- 5 2004 : Membentuk kemitraan strategis dengan SCS atas unit bisnis IT *Solution* menjadi PT. SAT (49% saham dimiliki Astragraphia).
- 6 2008 : Melakukan akuisisi 50.99% saham PT SAT dari SCS, kepemilikan saham Astragraphia menjadi 99.99%.
- 7 2010 : Unit bisnis Solusi Dokumen (AGDS) mencapai pendapatan bersih Rp 1 Triliun pertama.
- 8 2011 : AGIT JV dengan Monitise Asia Pacific Ltd, HongKong, membentuk PT. AGIT Monitise Indonesia (PT. AMI).

(3) Sertifikasi AGIT

Pada tahun 2013, Manajemen Pengendalian Mutu dan Keselamatan Kerja AGIT telah menunjukkan komitmennya dalam melakukan perbaikan secara berkala yaitu dengan melakukan uji sertifikasi menggunakan standar ISO 9001 dan OHSAS 18001. Selain itu, pada tahun 2013 AGIT berhasil lulus dalam sertifikasi ISO/IEC 20000-1, yaitu *Service Management*. Sertifikasi ini semakin melengkapi kompetensi AGIT untuk menjaga kualitas mutu dan layanan, setelah sebelumnya juga telah lulus uji sertifikasi ISO/IEC 27001 yang menunjang prosedur keamanan infrastruktur teknologi informasi di *Data Center*.

Sementara itu untuk segmen usaha teknologi informasi dan komunikasi, AGIT menggunakan *Customer Satisfaction Index* (CS Index) untuk mengukur kepuasan pelanggan. Pada akhir tahun, AGIT mencapai CS Index 3,96 dari skala

5. Hal ini membuktikan bahwa CSC AGIT memberikan kualitas layanan yang sesuai dengan sertifikasi ISO 20000:1 untuk layanan pelanggan, layanan *hosting* dan layanan CCTV. Selain itu, CSC AGIT melakukan implementasi aplikasi *Services Desk* yaitu alat untuk pencatatan semua keluhan pelanggan sehingga tim *Helpdesk* dapat memantau tahap penanganan pengaduan yang diterima.

Berdasarkan *annual report* 2013, AGIT telah memenuhi syarat dan telah membuktikan bahwa AGIT mampu berkompetensi di bidang ITSM secara global atau internasional, sedangkan melalui analisa R.Purwedi Darminto yang menjabat sebagai *Section Head of Oracle Development, Oracle Partners Ecosystem and Project Delivery at Astragraphia Information Technology*, AGIT telah mengalami banyak kemajuan semenjak memegang ISO/ICE 20000-1 dan ISO 27001, dan pada gambar 6 di bawah merupakan hasil analisis yang dipaparkan oleh beliau atas sertifikasi ISO/IEC yang diperoleh oleh AGIT.

Management System



Page 10

Gambar 6 Hasil Sertifikasi ISO/IEC AGIT
(Haekal, Darminto, & Baby, 2015)

Pada gambar 7, dipaparkan bahwa AGIT Business Strategy mengalami peningkatan dari tahun 2011 hingga 2014, diperkirakan lagi bahwa pada tahun 2015 akan melebihi ekspektasi atau sesuai pada strategi awal.

Business & Operation Strategy... Guidance



Gambar 7 AGIT Business Strategy 2013-2015
(Haekal, Darminto, & Baby, 2015)

3.2 ISO/IEC 27001

3.2.1 Gambaran ISO/IEC 27001

Standar ISO/IEC 27001 membantu organisasi untuk menjaga keamanan aset informasi, seperti informasi keuangan, kekayaan intelektual, rincian karyawan, dan informasi pihak ketiga atau pelanggan. ISO/IEC 27001 adalah standar paling terkenal dalam memberikan persyaratan untuk manajemen keamanan informasi (ISMS) (ISO, 2015).

Sejak tahun 2005, ISO telah mengembangkan sejumlah standar tentang ISMS baik dalam bentuk persyaratan maupun panduan. Standar ISMS ini dikelompokkan sebagai keluarga atau seri ISO 27000, diantaranya (Tim Direktorat Keamanan Informasi, 2011).

- (1) ISO/IEC 27000:2009 – *ISMS Overview and Vocabulary*
- (2) ISO/IEC 27001:2005 – *ISMS Requirements*
- (3) ISO/IEC 27002:2005 – *Code of Practice for ISMS*
- (4) ISO/IEC 27003:2010 – *ISMS Implementation Guidance*
- (5) ISO/IEC 27004:2009 – *ISMS Measurements*
- (6) ISO/IEC 27005:2008 – *Information Security Risk Management*
- (7) ISO/IEC 27006:2007 – *ISMS Certification Body Requirements*
- (8) ISO/IEC 27007 - *Guidelines for ISMS Auditing*

Standar ISO/IEC 27001 sendiri merupakan sebuah standar keamanan informasi yang memiliki beberapa versi dimana versi yang paling baru yaitu ISO 27001:2013 disahkan pada tanggal 25 September 2013 oleh *International Organization for Standardization* (ISO) yang kemudian digunakan untuk menggantikan peran standar versi terdahulu (ISO 27001:2005) tujuannya menanggapi perubahan-perubahan teknologi yang banyak berdampak pada kelangsungan bisnis pada masa kini. Standar ISO/IEC 27001 berisikan spesifikasi bagi sistem manajemen keamanan informasi atau *Information Security Management System* (ISMS) serta menentukan persyaratan pelaksanaan kontrol keamanan yang kemudian dapat disesuaikan dengan kebutuhan organisasi.

Manfaat yang dimiliki ISO/IEC 27001 dalam penerapannya sendiri cukup banyak, diantaranya digunakan oleh organisasi untuk merumuskan persyaratan dan tujuan keamanan, memastikan bahwa suatu risiko keamanan dapat dikelola dengan biaya yang seefektif mungkin, dan memastikan organisasi telah patuh pada hukum dan peraturan yang ada (ISO, 2015).

ISO/IEC 27001 dibagi menjadi dua standar dalam implementasi ISMS, diantaranya.

(1) ISO/IEC 27001:2005 (Bagian pertama)

Standar ini berisikan prasyarat (*requirements*) sistem manajemen ISMS dan kontrol keamanan informasi yang harus dipenuhi (*shall*). Standar ini merupakan kriteria audit dalam proses audit sertifikasi (*auditable*).

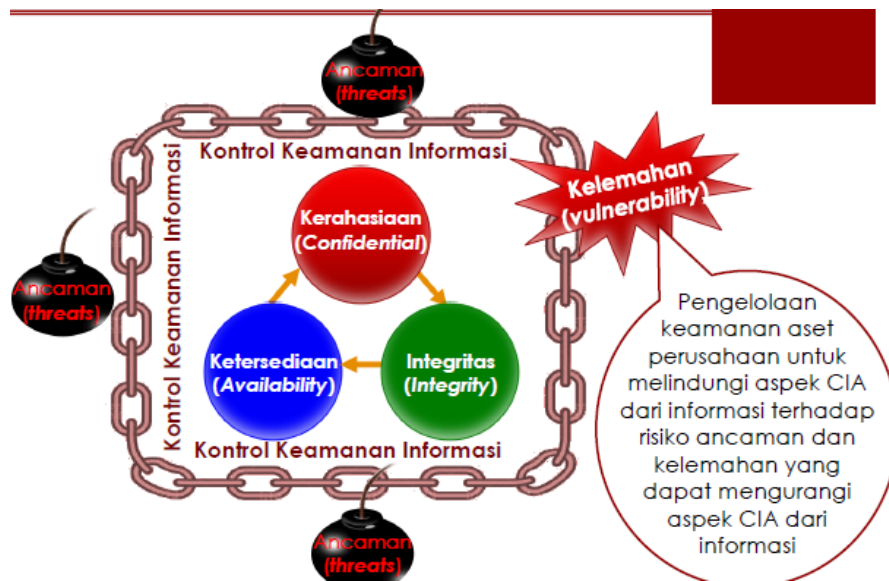
(2) ISO/IEC 27001:2005 (Bagian kedua)

Standar ini berisi panduan (*code of practice*) terkait proses *assessment* risiko dan kontrol keamanan informasi yang sebaiknya dilakukan (*should*). Standar ini bukan merupakan kriteria audit dalam proses audit sertifikasi (*non-auditable*).

Untuk menjaga keamanan informasi, ISO/IEC 27001 mempertahankan 3 aspek dari informasi, yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan), lihat gambar 8. Ketiga aspek ini tidak terpisahkan pada saat melakukan pengembangan sistem untuk mengamankan informasi, fasilitas pengolahan informasi, dan fasilitas pendukungnya. Pada gambar 9 dijelaskan bahwa ancaman terhadap informasi sangat rentan terjadi disetiap sudut. Maka dibutuhkan pengamanan yang baik dan terkontrol.



Gambar 8 Aspek Keamanan Informasi



Gambar 9 Ancaman Keamanan Informasi

3.2.2 Fungsi ISO/IEC 27001

ISO/IEC 27001: 2005 ditujukan untuk beberapa jenis penggunaan, diantaranya.

- (1) Digunakan dalam organisasi untuk merumuskan persyaratan keamanan dan tujuan.
- (2) Digunakan dalam organisasi sebagai cara untuk memastikan bahwa pendanaan risiko keamanan dikelola secara efektif.
- (3) Digunakan dalam organisasi untuk memastikan kepatuhan terhadap hukum dan peraturan yang ada.
- (4) Digunakan dalam sebuah organisasi sebagai kerangka proses untuk pelaksanaan dan manajemen kontrol dan memastikan tujuan keamanan secara *specific* dari suatu organisasi dapat terpenuhi.
- (5) Definisi proses manajemen keamanan informasi yang terbaru.
- (6) Identifikasi dan klarifikasi proses manajemen keamanan informasi yang ada.
- (7) Digunakan oleh manajemen organisasi untuk menentukan status kegiatan manajemen keamanan informasi.

- (8) Digunakan oleh pekerja auditor internal dan eksternal dalam sebuah organisasi untuk menentukan tingkat kepatuhan terhadap kebijakan, arahan dan standar yang diadopsi oleh organisasi.
- (9) Digunakan oleh organisasi untuk memberikan informasi yang relevan tentang kebijakan keamanan informasi, arahan, standar dan prosedur untuk mitra dagang dan organisasi lain dengan siapa mereka berinteraksi untuk alasan operasional atau komersial.
- (10) Pelaksanaan keamanan informasi-memungkinkan bisnis.
- (11) Digunakan oleh organisasi untuk memberikan informasi yang relevan tentang keamanan informasi kepada pelanggan.

3.2.3 Sertifikasi ISO/IEC 27001

Sebuah ISMS dapat memenuhi persyaratan sertifikasi ISO/IEC 27001 oleh sejumlah Terakreditasi Registrars di seluruh dunia. ISO/IEC 27001 sertifikasi biasanya melibatkan tiga tahap proses audit, yaitu (Ideafshift, 2015).

(1) Tahap 1 pendahuluan

Pada tahap ini meliputi tinjauan informal dari ISMS, misalnya memeriksa keberadaan dan kelengkapan dokumentasi kunci seperti organisasi kebijakan keamanan informasi. Tahap ini berfungsi untuk membiasakan para *auditor* dengan organisasi dan sebaliknya.

(2) Tahap 2

Pada tahap ini akan dipaparkan lebih rinci dan kepatuhan formal audit, menguji secara independen ISMS terhadap persyaratan yang ditetapkan dalam ISO/IEC 27001. Para auditor akan mencari tau bukti-bukti untuk mengkonfirmasi bahwa sistem pengelolaan telah dirancang dan dilaksanakan. Sertifikasi audit biasanya dilakukan oleh ISO/IEC 27001 *Lead Auditor*. Setelah melewati tahap ini, hasil ISMS bersertifikat sesuai dengan ISO/IEC 27001.

(3) Tahap 3

Pada tahap ini melibatkan tindak lanjut tinjauan atau audit untuk memastikan bahwa organisasi tetap sesuai dengan standar. Pemeliharaan sertifikasi memerlukan kembali secara periodic audit untuk memastikan bahwa ISMS terus beroperasi seperti yang ditentukan. Keadaan ini harus terjadi setidaknya setiap tahun.

3.2.4 Langkah-Langkah Sertifikasi ISO/IEC 27001

Langkah-langkah untuk melakukan sertifikasi ISO/IEC 27001:2013 saat ini terbagi menjadi 3 tahap, yaitu *gap analysis*, *formal assessment*, dan sertifikasi serta tahap-tahap selanjutnya.

(1) Gap Analysis

Analisa celah, layanan ISO pada tahap awal akan melihat lebih dekat pada sistem yang ada, keamanan informasi, manajemen dan melihat dari syarat-syarat ISO/IEC 27001:2013 Annex A. Hal ini membantu ISO untuk mengidentifikasi daerah yang dibutuhkan lebih banyak pekerjaan sebelum ISO melaksanakan penilaian formal untuk menghemat waktu dan uang.

Dokumen-dokumen yang dibutuhkan berdasarkan standar Annex A ada 114 dokumen dari organisasi namun, hanya ada 41 dokumen yang sangat mereka tinjau atau lebih penting dari lainnya, diantara 42 dokumen tersebut, 24 dokumen sangat diwajibkan ketersediaannya, dan 18 dokumen yang lain menjadi opsi peninjauan saja. 24 dokumen tersebut diantaranya.

- 1 *Scope of the ISMS (clause 4.3)*
- 2 *Information security policy and objectives (clauses 5.2 and 6.2)*
- 3 *Risk assessment and risk treatment methodology (clause 6.1.2)*
- 4 *Statement of Applicability (clause 6.1.3 d)*
- 5 *Risk treatment plan (clauses 6.1.3 e and 6.2)*
- 6 *Risk assessment report (clause 8.2)*
- 7 *Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)*

- 8 *Inventory of assets (clause A.8.1.1)*
- 9 *Acceptable use of assets (clause A.8.1.3)*
- 10 *Access control policy (clause A.9.1.1)*
- 11 *Operating procedures for IT management (clause A.12.1.1)*
- 12 *Secure system engineering principles (clause A.14.2.5)*
- 13 *Supplier security policy (clause A.15.1.1)*
- 14 *Incident management procedure (clause A.16.1.5)*
- 15 *Business continuity procedures (clause A.17.1.2)*
- 16 *Statutory, regulatory, and contractual requirements (clause A.18.1.1)*
- 17 *And here are the mandatory records.*
- 18 *Records of training, skills, experience and qualifications (clause 7.2)*
- 19 *Monitoring and measurement results (clause 9.1)*
- 20 *Internal audit program (clause 9.2)*
- 21 *Results of internal audits (clause 9.2)*
- 22 *Results of the management review (clause 9.3)*
- 23 *Results of corrective actions (clause 10.1)*
- 24 *Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)*

Sedangkan 18 dokumen yang lainnya terbagi menjadi sebagai berikut.

- 1 *Procedure for document control (clause 7.5)*
- 2 *Controls for managing records (clause 7.5)*
- 3 *Procedure for internal audit (clause 9.2)*
- 4 *Procedure for corrective action (clause 10.1)*
- 5 *Bring your own device (BYOD) policy (clause A.6.2.1)*
- 6 *Mobile device and teleworking policy (clause A.6.2.1)*
- 7 *Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)*

- 8 *Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)*
- 9 *Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)*
- 10 *Procedures for working in secure areas (clause A.11.1.5)*
- 11 *Clear desk and clear screen policy (clause A.11.2.9)*
- 12 *Change management policy (clauses A.12.1.2 and A.14.2.4)*
- 13 *Backup policy (clause A.12.3.1)*
- 14 *Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)*
- 15 *Business impact analysis (clause A.17.1.1)*
- 16 *Exercising and testing plan (clause A.17.1.3)*
- 17 *Maintenance and review plan (clause A.17.1.3)*
- 18 *Business continuity strategy (clause A.17.2.1)*

(2) Formal Assessment

Tahap penilaian formal terjadi pada dua tahap, yaitu.

- 1 ISO akan meninjau dari kesiapan organisasi untuk penilaian dengan memeriksa jika diperlukan ISO/IEC 27001 prosedur dan kontrol yang akan di *deploy* pada tahap selanjutnya, ISO akan membagikan detail apa yang mereka temukan untuk menemukan celah yang kurang, agar dapat diselesaikan tanpa adanya masalah.
- 2 Ketika sudah ditemukan kesenjangannya, maka akan ditutup, kemudian ISO akan melaksanakan prosedur dan kontrol dalam organisasi untuk memastikan bahwa ISMS telah berkerja secara efektif seperti yang ditentukan untuk sertifikasi.

(3) Sertifikasi dan tahap selanjutnya

Bila organisasi telah lulus pada tahap analisa dan penilaian maka organisasi akan menerima sertifikasi ISO/IEC 27001 yang akan berlaku selama tiga tahun, Manajer klien organisasi akan tetap berhubungan bersama ISO, untuk melakukan kunjungan rutin untuk memastikan sistem berjalan sesuai atandar, tidak hanya sekedar berada di level sebelumnya namun berkembang ke level yang lebih baik.

3.2.5 Lama Implementasi Sertifikasi ISO/IEC 27001

Setelah melalui tahap penilaian dan dokumen-dokumen yang dibutuhkan ISO untuk analisis penyesuaian dan kelayakan organisasi untuk memiliki sertifikasi ISO/IEC 27001, maka waktu yang dibutuhkan untuk implementasi pada organisasi akan berbeda-beda sesuai besar dan kecilnya sebuah organisasi tersebut. Sebagai contoh standar ISO ialah sebagai berikut :

1 Organisasi kecil

Menurut ISO, pada kategori ini jumlah karyawan mencapai 50 karyawan. Standar waktu minimal yang dibutuhkan lembaga sertifikasi minimal 6 hingga 8 bulan.

2 Organisasi menengah

Menurut ISO, pada kategori ini jumlah karyawan mencapai 500 karyawan. Standar waktu minimal yang dibutuhkan lembaga sertifikasi minimal 8 hingga 12 bulan.

3 Organisasi besar

Menurut ISO, pada kategori ini jumlah karyawan berkisar 500 lebih karyawan. Standar waktu minimal yang dibutuhkan lembaga sertifikasi minimal 12 hingga 15 bulan ataupun lebih.

Menurut Dejan Kosutic, seorang pakar akademis ISO, berpendapat bahwa selama ia berkarir dalam bidang ISO, ia mengatakan perusahaan atau organisasi yang melebihi standar kurun waktu implementasi ISO, tidak akan

menyelesaikan implementasi tersebut, dan organisasi tersebut dapat di cap atau di *brand* oleh para pakar ISO, untuk tidak dapat dipercaya baik dari sisi SDM maupun finansial organisasi tersebut tidak akan dapat menutupi *budget* fase-fase ISO atau lembaga sertifikasi setelah penerapan sertifikasi ISO / IEC 27001.

3.2.6 Contoh Studi Kasus

PT. Visionet Internasional ('VisioNet') adalah perusahaan anak dari PT. Multi Polar, yang menguatkan kesuksesan dari PT. Multi Polar. VisioNet merupakan anak usaha Perusahaan yang menyediakan layanan IT Outsourcing/Managed Services. Mulai beroperasi di tahun 2006, dengan fokus pada Layanan EDC *operation*, dalam waktu singkat VisioNet berhasil mengalami perkembangan yang luar biasa pada area tersebut. VisioNet telah memperoleh sertifikasi ISO 9001:2008 untuk tiga bidang utamanya, yaitu *Electronic Draft Capture Operation and Maintenance Services*, *Desktop Server Network Operation and Maintenance Services*, dan *Information Technology Operation and Maintenance Services*. Layanan VisioNet juga telah diakui dengan mendapatkan sertifikasi ISO 27001:2005 yang merupakan standarisasi dalam cakupan *Development, Implementation, Controlling, Management & Improvement of Information Security Management System (ISMS) for Data Center*; dan *PCI DSS (Payment Card Industry Data Security Standard)* (PT. Mutipolar, 2013).

(1) *Development, Implementation, Controlling*

Perusahaan sudah tersertifikasi mampu mengembangkan, mengimplementasi, serta mengontrol layanan TI yang diberikan. Layanan TI yang diberikan sudah memenuhi standar internasional yang mampu dipercaya oleh seluruh dunia.

(2) *Management & Improvement of Information Security Management System (ISMS) for Data Center*

Perusahaan tersertifikasi mampu manajemen keamanan dan ketersediaan informasi perusahaan yang disimpan di dalam *data center*. Jadi keamanan data sangat mampu dihandalkan.

(3) *PCI DSS (Payment Card Industry Data Security Standard)*

Perusahaan mampu menjamin keamanan pemegang kartu pembayaran yang mengacu pada standar internasional.

Dan untuk menambah kepercayaan dari pelanggan terkait keamanan transaksi pembayaran, VisioNet juga telah berhasil mendapatkan sertifikasi *PCI DSS Certificate* (*PCI Data Security Standard*). Hal tersebut menjadikan Perusahaan optimis bahwa layanan *IT Managed Services* akan semakin tumbuh dan berkembang di masa mendatang seiring dengan permintaan pelanggan untuk mendelegasikan fungsi-fungsi pekerjaan TI mereka kepada VisioNet. Sampai dengan akhir 2013, VisioNet didukung oleh lebih dari 1.100 personil, serta memiliki lebih dari 112 titik layanan yang tersebar di 107 kota di seluruh Indonesia dan termasuk layanan *Contact Center* yang beroperasi 24 jam guna mendukung kegiatan operasional VisioNet pada umumnya serta pelanggan pada khususnya. Untuk menambah kepercayaan dan peningkatan mutu dan kualitas layanan terhadap pelanggan, maka di tahun 2014 VisioNet bertransformasi dari penyedia layanan *IT Services* menjadi penyedia layanan *Business Process Managed Service* yang fokus kepada 6 (enam) pilar layanan utama antara lain *Branch IT Services*, *Merchant IT Services*, *Field Operation*, *IT Managed Services*, *Application Managed Services*, dan *Contact Center & CRM Services*. Diharapkan dengan orientasi fokus kepada layanan proses bisnis ini akan membawa VisioNet sebagai penyedia layanan yang lengkap dan handal.

3.3 Perbandingan ISO/IEC 20000 dan ISO/IEC 27001

Tabel 1 memaparkan beberapa perbedaan manajemen ISO/IEC 20000 dengan ISO/IEC 27001 (Coral, 2015).

Tabel 1 Perbedaan ISO/IEC 20000 dan ISO/IEC 27001

<i>International Standard</i>	<i>Coverage</i>	<i>Why should I choose this one?</i>	<i>What is the name of the risk register /record?</i>
ISO 27001 – information security management system	Standar ISO 27001 fokus kepada proteksi dari informasi perusahaan. Semua informasi yang memiliki <i>value</i> pada perusahaan, bukan hanya infrastruktur TI. Jika perusahaan ingin melindungi semua informasi yang memiliki <i>value</i> dari <i>unathourized access (confidentiality)</i> , hilang dan hancurnya informasi (<i>availability</i>), standard ISO 27001 menyediakan beberapa kontrol yang bisa menekan resiko – resiko tersebut. Sertifikasi ISO 27001 meliputi 114 kontrol yang bertujuan untuk membuat arsitektur yang aman, mencegah hal-hal yang tidak diinginkan, mengontrol prosedur yang ada, juga meningkatkan prosedur, infrastruktur, dan personel perusahaan.	Jika perusahaan memperhatikan proteksi dari informasi perusahaan, sangat perlu dilakukan sertifikasi ISO 27001. ISO 27001 juga bisa sangat spesifik, misalna hanya ada beberapa hal yang ingin disertifikasi.	<i>Information risk register</i> – Dimana perusahaan bisa melihat resiko yang bisa mengancam informasi perusahaan.

Tabel 1 Perbedaan ISO/IEC 20000 dan ISO/IEC 27001 (lanjutan)

<i>International Standard</i>	<i>Coverage</i>	<i>Why should I choose this one?</i>	<i>What is the name of the risk register /record?</i>
ISO 20000-1 – (IT) service management system	Standar ITSM – ISO 20000 certification lebih diarahkan bagaimana layanan TI yang di berikan oleh perusahaan, Standar ITSM – ISO 20000 mengarah kepada <i>best practice</i> dari proses layanan TI.	Mengarahkan layanan TI yang dimiliki perusahaan bisa mencapai <i>best practice</i> yang mengacu pada ITIL. Perusahaan perlu melakukan sertifikasi ISO 20000 jika perusahaan bergerak pada jasa di bidang TI.	IT (<i>service</i>) <i>risk register</i> . ISO 20000: 2005 memiliki referensi rencana untuk meningkatkan kualitas layanan TI yang akan memperbaiki kekurangan layanan.

BAB IV

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. Persaingan ini didukung oleh kemajuan teknologi informasi yang selaras ikut berkembang pada saat ini.. Perkembangan teknologi ini semakin hari semakin kompleks yang memungkinkan segala sesuatu menjadi lebih cepat dan terjangkau hingga menyebabkan pelanggan juga memiliki hak atas permintaan yang lebih beragam. Keadaan ini membuat perusahaan memerlukan pendekatan yang lebih fleksibel untuk integrasi antara layanan TI dengan layanan konvensional perusahaan agar dapat bersaing dengan perusahaan lainnya yang serupa.

Usaha untuk meningkatkan layanan TI ini tentunya bukan hal yang mudah, oleh karena itu dibutuhkan manajemen TI yang baik serta pengolahan informasi yang aman agar pemenuhan kebutuhan pelanggan oleh perusahaan dapat disampaikan tepat sasaran dan dapat memberikan solusi serta *value* bagi pelanggan.

Saat ini, manajemen seperti ini sudah dapat dipaparkan dalam bentuk yang lebih terstruktur dengan menggunakan manajemen teknologi informasi (ITSM) dan juga manajemen keamanan informasi (ISMS). Pada setiap manajemen ini, terdapat beberapa standar sendiri yang digunakan, dalam hal ini adalah ISO/IEC 20000 untuk ITSM dan ISO/IEC 27001 untuk ISMS. Kedua standar ini sudah bertingkat internasional, sehingga tidak diragukan lagi keakuratannya. PT. Astra Graphia Information Technology dan PT. Visionet Internasional adalah salah satu perusahaan yang sudah menerapkan standar kedua ISO tersebut.

DAFTAR PUSTAKA

- Andgaa. (2015, Oktober 14). *IT Service Management (ITSM)*. Source: IT Service Management (ITSM): <http://andgaa.web.id/it-service-management-itsm/>
- APM Group. (2015, Oktober 15). *ISO/IEC 20000 Certified Organizations*. Source: http://www.isoiec20000certification.com/home/ISOCertifiedOrganizations/ISOCountryListings.aspx?CO_CompanyName=&CO_Country=Indonesia&Cert_Version=&RCB_cert=&view2order=&view2direction=&dosearch=y
- APM Group. (2015, Oktober 15). *PT. Astra Graphia Information Technology*. Source: Certified Organizations: <http://www.isoiec20000certification.com/home/ISOCertifiedOrganizations/PTAstraGraphia.aspx>
- APMG International. (2015, Oktober 15). *ISO/IEC 20000 Certification*. Source: <http://www.apmg-international.com/en/qualifications/isoiec20000/iso-iec-20000.aspx>
- Carapedia. (2015, Oktober 14). *Pengertian dan Definisi Layanan*. Source: Definisi: https://carapedia.com/pengertian_definisi_layanan_info2148.html
- Coral. (2015, Oktober 15). *Difference Between ISO 27001 and ISO 20000*. Source: source <http://www.coralesecure.com/blog/tag/difference-between-iso-27001-and-iso-20000/>
- Correia, A., & Brito e Abreu, F. (2010). *Defining and Observing the Compliance of Service Level Agreements: A Model Driven Approach*. 2010 7th International Conference on the Quality of Information and Communication Technology. IEEE Computer Society.
- cybersecurity. (2015, Oktober 14). *Information Security Management System (ISMS)*. Source: <http://cnii.cybersecurity.my/main/resources/ISMS.pdf>
- Haekal, E., Darminto, R. P., & Baby, V. (2015, Oktober 15). *Introductory Economics of Managers : Chapter 7 Yhe Nature of Industry*. Source: <http://www.slideshare.net/purwedidarmino/the-nature-of-industry-32434531>
- Ideaofshift. (2015, Oktober 15). *Sekilas tentang Iso 27001/ISMS*. Source: <https://ideaofshift.wordpress.com/2012/06/20/sekilas-tentang-iso-27001-isms/>
- ISO. (2015, Oktober 15). *ISO/IEC 20000-1:2005*. Source: http://www.iso.org/iso/catalogue_detail?csnumber=41332
- ISO. (2015, Oktober 15). *ISO/IEC 27001-Information Security Management*. Source: Standar:Management System Standards:ISO/IEC 27001: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>
- ISO. (2015, Oktober 15). *Management System Standards*. Source: Standards: Managements System Standards: <http://www.iso.org/iso/home/standards/management-standards.htm>
- ISO. (2015, Oktober 2015). *Standards Catalogue*. Source: <http://www.iso.org/>

- kemkes. (2015, Oktober 14). *Pengenalan Standard ISO 27001*. Source: <http://e-report.alkes.kemkes.go.id/dat/97ef50cb90499632b3502ce9a7521b93/berita/2014/BERITA-0000000000000013.pdf>
- Kuller, P., Grabowski, M., PetrSames, & Vogt, M. (2010). *IT Service Management Methods and Frameworks Systematization*. Europe: Innovation Training IT Central Europe.
- Kurnia. (2015, Oktober 15). *Sertifikasi ISO 20000 : Mengapa Menjadi Begitu Penting?* Source: Value IT Consulting: Delivering Integrated Through IT: http://www.ivitc.com/index.php?option=com_content&view=article&id=37:sertifikasi-iso-20000-mengapa-menjadi-begitu-penting&catid=24:it-service-management&Itemid=8
- Lepmets, M., Ras, E., & Renault, A. (2011). *A Quality Measurement Framework for IT Services. 2011 Annual SRII Global Conference*. IEEE Computer Society.
- Monica, Hindarto, V. D., & Widyastuti, Y. M. (2014). *ISO/IEC 2000: An IT Service Management Standard (Studi Kasus pada Oxford University Press)*. *Makalah*.
- PT. Mutipolar. (2013). *Investing For The Future Through Strong Commitment And Continuous*. Jakarta: PT. Multipolar Technology Tbk.
- Tim Direktorat Keamanan Informasi. (2011). *Panduan Penerapan Tata kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*.
- Wardani, K. (2007). *Penggunaan Microsoft Operations Framework (MOF) Untuk Mencapai Standar ISO 20000*. hal:1.
- Wikipedia. (2015, Oktober 14). *Information Technology Service Management*. Source: ITSM: <https://id.wikipedia.org/wiki/ITSM>
- Zhang, S., Ding, Z., & Zong, Y. (2009). *ITIL Process Integration in the Context of Organization Environment. 2009 World Congress on Computer Science and Information Engineering*. IEEE Computer Society.