BAB II

LANDASAN TEORI

2.1 Audit

Definisi *audit* menurut terminologi adalah pemeriksaan sistematis terhadap catatan–catatan dengan melibatkan analisa, pengujian bukti dan konfirmasi (Cannon, 2011:17). Sedangkan menurut ISACA, definisi audit adalah proses sistematis oleh tim independen atau individu berkualitas dan berkompeten untuk memperoleh dan mengevaluasi bukti secara obyektif mengenai pernyataan suatu proses dengan tujuan menunjukkan pendapat atau opini dan melaporkan sejauh mana pernyataan proses tersebut diimplementasikan (ISACA: *CISA Review Manual*, 2012).

Audit menurut ISACA dapat dibedakan menjadi beberapa jenis, yaitu (ISACA, 2012: 51):

a. Audit Finansial (*Financial Audit*), adalah audit yang bertujuan untuk menilai kebenaran laporan keuangan organisasi.
b. Audit Operasional (*Operational Audit*), adalah audit yang dirancang untuk mengevaluasi struktur pengendalian intern pada area proses tertentu.
c. Audit Terpadu (*Integrated Audit*), adalah audit yang menggabungkan tahapan audit keuangan dan operasional. Audit terpadu dilakukan untuk menilai tujuan keseluruhan dalam organisasi, yang terkait dengan pengamanan aset informasi keuangan, efisiensi dan kepatuhan.

d. Audit Administratif (*Administrative Audit*), adalah audit yang berorientasi untuk menilai atau mengkaji permasalahan yang terkait dengan efisiensi produktivitas operasional dalam sebuah organisasi.

e. Audit Sistem Informasi (*Information System Audit*), adalah audit yang bertujuan untuk menentukan apakah sistem informasi dan sumber daya terkait telah melindungi aset dan integritas sistem, memberikan informasi yang relevan dan dapat diandalkan, mencapai tujuan organisasi secara efektif dan efisien serta memiliki kontrol internal yang dapat memberikan keyakinan bahwa bisnis, operasional dan pengendalian telah terpenuhi.

f. Audit Khusus (*Specialized Audit*), merupakan bagian dari *Information System Audit* yang bertujuan untuk melakukan tinjauan / penelitian terhadap area tertentu seperti layanan yang diberikan oleh pihak ketiga.

g. Audit Forensik (*Forensic Audit*), didefinisikan sebagai audit khusus untuk menemukan, mengungkapkan dan menindaklanjuti penipuan dan kejahatan. Tujuan dari tindaklanjut tersebut adalah pengembangan atau pemeriksaan bukti–bukti oleh penegak hukum dan otoritas pengadilan.

Kerangka kerja untuk pelaksanaan audit yang dikembangkan oleh ISACA menetapkan beberapa tingkatan panduan berupa (ISACA, 2009: 6):

a) *Standard*, mendefinisikan persyaratan minimum dalam pelaksanaan dan pelaporan audit.

b) *Guideline*, menyediakan panduan tentang penerapan standar (poin a).

c) *Procedure*, menyediakan contoh–contoh prosedur yang dapat diikuti oleh auditor selama penugasan audit.

Tabel 2.1 berikut adalah standar–standar audit yang dipublikasikan oleh ISACA di dalam *Information System Standars, Guidelines and Procedures for Auditing and Control Professionals*.

Tabel 2.1. Standar Audit *IS Standards, Guidelines and Procedures for Auditing and Control Professionals* (Sumber: ISACA, 2009)

S1	*Audit Charter*	S9	*Irregularities and Illegal Acts*
S2	*Independence*	S10	*IT Governance*
S3	*Professional Ethics and Standards*	S11	*Use of Risk Assessment in Audit Planning*
S4	*Professional Competence*	S12	*Audit Materiality*
S5	*Planning*	S13	*Using the Work of Other Experts*
S6	*Performance of Audit Work*	S14	*Audit Evidence*
S7	*Reporting*	S15	*IT Controls*
S8	*Follow–up Activities*	S16	*E–Commerce*

Masing–masing standar yang disebutkan pada Tabel 2.1 mengandung kriteria–kriteria persyaratan minimum yang harus dipenuhi oleh auditor selama proses penugasan audit. Berikut adalah penjelasan kriteria–kriteria persyaratan minimum standar audit ISACA (ISACA, 2009: 13):

1. *S5 Planning* (Perencanaan Audit)

   Tujuan dari standar ini adalah untuk menetapkan dan menyediakan petunjuk dalam tahapan perencanaan audit. Adapun persyaratan minimum yang harus dilakukan oleh auditor menurut standar ini adalah:

   a. Merencanakan ruang lingkup audit untuk menentukan tujuan dari audit serta mematuhi hukum yang berlaku dan standar profesional audit.
   b. Membuat dan mendokumentasikan pendekatan audit berbasis risiko.

c. Membuat dan mendokumentasikan rencana kerja audit yang menjelaskan dasar dan tujuan, waktu serta *resource* yang dibutuhkan dalam pelaksanaan audit.

d. Membuat program dan/atau rencana audit yang menjelaskan sifat, waktu serta ruang lingkup prosedur audit yang diperlukan untuk menyelesaikan audit.

2. *S6 Performance of Audit Work* (Pelaksanaan Audit)

Tujuan dari standar ini adalah untuk menetapkan dan menyediakan panduan dalam tahapan pelaksanaan audit. Persyaratan minimum yang harus dilakukan oleh auditor menurut standar ini adalah:

a. Melakukan pengawasan kepada staf audit guna memastikan tujuan audit telah tercapai dan standar profesional audit yang ditetapkan telah terpenuhi.

b. Memperoleh bukti audit yang cukup, *reliable* dan relevan sesuai dengan tujuan audit yang dilakukan. Temuan dan kesimpulan audit harus didukung oleh analisa dan interpretasi yang tepat.

c. Mendokumentasikan proses audit terutama bukti audit yang akan digunakan sebagai acuan dalam penyusunan temuan dan kesimpulan audit.

3. *S7 Reporting* (Pelaporan Audit)

Tujuan dari standar ini adalah untuk menetapkan dan menyediakan panduan dalam tahap pelaporan audit. Persyaratan minimum yang harus dilakukan oleh auditor menurut standar ini adalah sebagai berikut:

a. Menyajikan laporan audit dalam bentuk yang tepat. Laporan audit berisi identifikasi organisasi, penerima yang dimaksudkan dan pembatasan sirkulasi.

b. Laporan audit menyatakan ruang lingkup, tujuan, periode, sifat, waktu dan batas pengerjaan audit.
c. Laporan audit menyatakan temuan, kesimpulan, rekomendasi, reservasi, kualifikasi atau keterbatasan ruang lingkup.
d. Auditor memiliki bukti audit yang cukup dan tepat guna mendukung hasil yang akan dilaporkan.
e. Laporan audit harus ditandatangani dan didistribusikan sesuai dengan ketentuan di dalam *audit charter* atau *engagement letter*.

2.2 Pengelolaan Layanan Teknologi Informasi

Pengelolaan Layanan Teknologi Informasi atau disebut juga dengan *Information Technology Service Management* (ITSM) didefinisikan sebagai pemanfaatan terencana dan terkendali terhadap aset TI, sumber daya manusia dan proses untuk mendukung kebutuhan operasional bisnis seefisien mungkin dan memastikan bahwa organisasi memiliki kemampuan secara cepat dan efektif untuk menanggapi kejadian atau situasi yang tidak diinginkan serta terus menerus mengevaluasi proses dan kinerja dalam rangka mengidentifikasi dan menetapkan peluang perbaikan (Addy, 2007: 46). ITSM merupakan disiplin proses yang berorientasi pada penggabungan pengelolaan proses dan praktik terbaik industri dalam suatu pendekatan standar untuk mengoptimalkan layanan TI. ITSM menyediakan kerangka kerja dalam penyusunan operasional TI agar organisasi dapat memberikan kualitas pelayanan sesuai kebutuhan bisnis dan kesepakatan tingkat layanan. Beberapa standar ITSM yang paling diakui secara internasional adalah ITIL, ISO/IEC 20000 dan CMMI Service (Mesquida et al., 2012).

Sedangkan menurut *Information Technology Service Management Forum* (itSMF), ITSM dikenal sebagai sebuah pendekatan proses dan layanan yang berfokus pada pengelolaan TI. Tujuan dari proses ITSM adalah untuk memberikan kontribusi terhadap kualitas layanan TI (itSMF, 2004: 29). Layanan TI dapat diartikan sebagai seperangkat atau serangkaian fungsi terkait yang disediakan oleh sistem TI dalam mendukung satu atau lebih unit bisnis. Layanan yang dimaksud dapat terdiri dari perangkat lunak, perangkat keras, fasilitas komunikasi serta tenaga kerja (Izza, 2010: 424).

Ruang lingkup layanan TI yang diperlukan atau dilakukan oleh sebuah organisasi TI sangat bervariasi. Peppard (2003) membagi layanan TI dalam beberapa kategori sebagai berikut:

1. *Application Service,* mengacu pada layanan yang disampaikan melalui perangkat lunak.
2. *Operational Service*, adalah layanan yang berhubungan dengan perakitan dan pengoperasian inti lingkungan teknologi informasi.
3. *Value enabling Service*, adalah layanan yang disediakan untuk meningkatkan nilai aset–aset informasi, atau mengidentifikasi peluang yang disediakan oleh teknologi informasi dalam mengelola informasi.
4. *Infrastructure Service* adalah layanan yang diperoleh secara langsung dari investasi infrastruktur teknologi.

Terdapat empat perspektif atau atribut untuk menjelaskan konsep ITSM menurut Ivanka Menken's (2009: 9). Keempat perspektif atau atribut tersebut adalah:

1) *Partners/Suppliers Perspective*, memperhatikan pentingnya hubungan mitra dan pemasok eksternal dan kontribusinya dalam penyampaian layanan.
2) *People Perspective*, terkait dengan sisi non teknis ITSM, meliputi staf TI, pelanggan, pemegang saham dan lainnya.
3) *Product/Technology Perspective*, memperhatikan pentingnya peran dari layanan TI, perangkat keras, perangkat lunak, anggaran dan alat yang digunakan.
4) *Process Perspective*, terkait rangkaian tahapan penyampaian layanan berdasarkan aliran proses.

Keempat perspektif tersebut perlu menjadi pertimbangan ketika membangun sebuah layanan guna mencapai keberhasilan dalam hal rancangan, transisi dan implementasi. Manfaat dari penerapan proses pengelolaan layanan TI secara efektif dapat (Ady, 2007: 34):

(1) Meningkatkan produktivitas/efisiensi operasional dan mendorong efisiensi penggunaan sumber daya.
(2) Memungkinkan staf TI untuk mengelola/mengatur beban kerja agar lebih efektif.
(3) Meningkatkan kepuasan pelanggan dan mengurangi volume insiden/gangguan.
(4) Memungkinkan akses akurasi data secara *real time* untuk mempermudah pengambilan keputusan secara efektif oleh manajemen.

2.3 Teknologi Informasi

ITIL mendefinisikan teknologi informasi sebagai pemanfaatan teknologi untuk penyimpanan, komunikasi atau pemrosesan informasi. Teknologi ini pada umumnya meliputi komputer, telekomunikasi, aplikasi dan perangkat lunak. Sedangkan informasi dapat mencakup data bisnis, suara, gambar, video dan sebagainya. Teknologi informasi sering digunakan untuk mendukung proses bisnis melalui layanan TI (TSO, 2011).

Adapun definisi teknologi informasi menurut beberapa pakar teknologi yaitu (Kadir dan Terra, 2003):

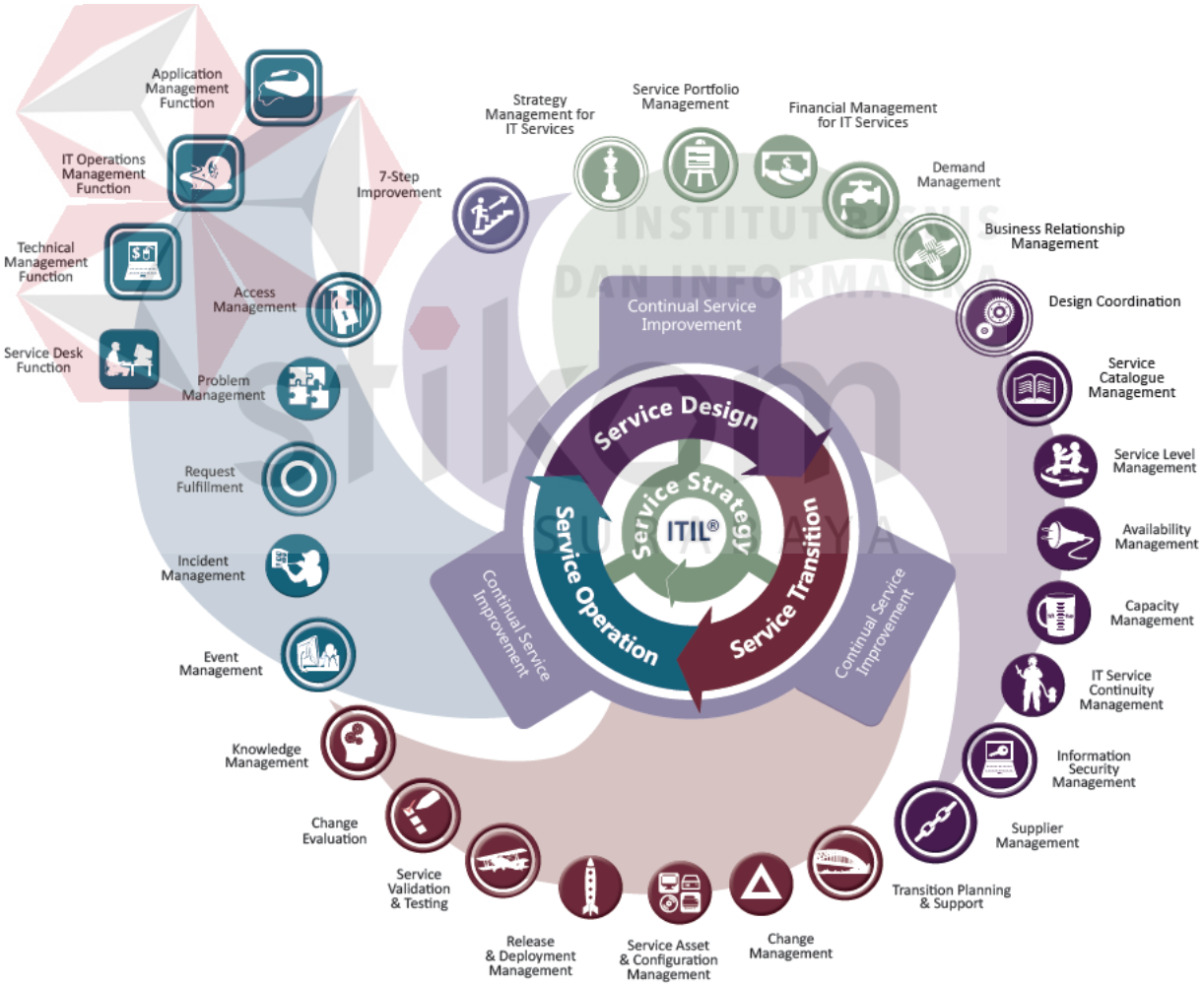
a. Martin, teknologi informasi adalah hal yang tidak hanya terbatas pada teknologi komputer yang digunakan untuk memproses dan menyimpan informasi, melainkan juga mencakup teknologi komunikasi untuk mengirimkan informasi.
b. Rahardjo, teknologi informasi adalah sama dengan teknologi lainnya, hanya informasi merupakan komoditas yang diolah dengan teknologi tersebut. Dalam hal ini, teknologi mengandung konotasi memiliki nilai ekonomi yang mempunyai nilai jual.

2.4 *Information Technology Infrastructure Library* (ITIL)

Information Technology Infrastructure Library adalah kerangka kerja berisi praktik terbaik yang dapat digunakan untuk membantu organisasi dalam mengembangkan proses pengelolaan layanan teknologi informasi (itSMF, 2007: 8). Kerangka kerja ITIL bertujuan secara berkelanjutan meningkatkan efisiensi operasional teknologi informasi dan kualitas layanan pelanggan (Sarno, 2009: 20).

Nama ITIL dan *IT Infrastructure Library* adalah merek dagang terdaftar atas milik *United Kingdom's Office of Government Commerce* (OGC). ITIL khususnya di Eropa telah menjadi standar *de–facto* tata kelola layanan TI (Brenner, 2006).

Pada saat ini kerangka kerja ITIL versi 3 merupakan pengembangan dari ITIL versi 2 berupa 7 seri buku yang diterbitkan pada tahun 2000–2004. ITIL versi 3 terdiri dari 5 buku utama (*core publication*) yang membahas tentang tahapan–tahapan siklus hidup layanan (*service lifecycle*) seperti yang terlihat pada Gambar 2.1.



Gambar 2.1. *ITIL 2011 Edition Service Lifecycle*
(Sumber: Pultorak & Associates, Ltd., 2011)

Kelima buku utama ITIL pada Gambar 2.1 di halaman 16 menjelaskan tahapan–tahapan siklus layanan dimulai dari pendefinisian awal dan analisa persyaratan bisnis yang dijelaskan dalam *service strategy* dan *service design*, peralihan layanan baru atau layanan yang diubah dalam *service transition*, operasional dan perbaikan layanan yang dijelaskan dalam *service operation* dan *continual service improvement*. Berikut adalah penjelasan dari masing–masing modul siklus layanan ITIL Versi 3 Edisi Tahun 2011 (TSO, 2011: 05):

2.4.1 *Service Strategy* (Strategi Layanan)

Service strategy menyediakan panduan tentang bagaimana pengelolaan layanan tidak hanya sebagai sebuah kapabilitas organisasi tetapi juga sebagai aset strategis. Aset strategis organisasi meliputi *people*, *process*, *product* dan *technology*. Topik penting dalam *service strategy* meliputi pendefinisian ruang pasar, karakteristik tipe penyedia layanan internal dan eksternal, aset layanan, portofolio layanan dan pelaksanaan strategi melalui siklus layanan. Adapun proses utama dalam *service strategy* meliputi *Strategy Management for IT Services*, *Service Portfolio Management, Demand Management, Financial Management for IT Services* dan *Business Relationship Management*.

2.4.2 *Service Design* (Desain Layanan)

Service design menyediakan panduan dalam perancangan dan pengembangan layanan serta praktik pengelolaan layanan, mencakup prinsip perancangan dan metode untuk mengubah tujuan strategis organisasi menjadi portofolio dan aset layanan. Ruang lingkup *service design* tidak terbatas pada layanan baru tetapi juga mencakup perubahan dan perbaikan yang diperlukan untuk meningkatkan dan memelihara nilai pelanggan melalui siklus layanan,

kelangsungan layanan, pencapaian tingkat layanan dan kesesuaiannya terhadap standar dan regulasi layanan. Adapun proses utama dalam *service design* yaitu *Design Coordination*, *Service Catalogue Management*, *Service Level Management*, *Information Security Management*, *Capacity Management*, *IT Service Continuity Management*, *Availability Management* dan *Supplier Management*.

2.4.3 *Service Transition* (Transisi Layanan)

Service transition menyediakan panduan dalam pengembangan dan peningkatan kemampuan untuk mengenalkan layanan baru atau layanan yang diubah ke dalam lingkungan yang mendukung. *Service transition* juga memastikan nilai–nilai yang teridentifikasi dalam *service strategy*, dan dikembangkan dalam *service design*, dapat diwujudkan secara efektif ke dalam lingkungan operasional layanan sekaligus mengontrol risiko kegagalan dan membantu dalam pengambilan keputusan. Adapun proses utama dalam *service transition* meliputi *Transition Planning and Support*, *Change Management*, *Service Asset and Configuration Management*, *Release and Deployment Management*, *Knowledge Management*, *Service Validation and Testing* dan *Change Evaluation*.

2.4.4 *Service Operation* (Operasional Layanan)

Service operation menggambarkan praktik terbaik dalam pengelolaan layanan ke dalam lingkungan yang mendukung, serta mencakup panduan dalam pencapaian efektivitas dan efisiensi penyampaian dan dukungan layanan untuk memastikan nilai pelanggan, pengguna dan penyedia layanan. Disamping itu, *service operation* juga menyediakan panduan dalam menjaga kestabilan operasional layanan, pengelolaan perubahan desain, skala, ruang lingkup dan tingkat kinerja layanan.

Adapun proses–proses inti dari operasional layanan adalah *Event Management*, *Incident Management, Request Fulfillment, Problem Management* dan *Access Management*. Topik *service operation* juga membahas sejumlah aktivitas–aktivitas operasional untuk memastikan keselarasan teknologi dengan layanan dan tujuan proses secara keseluruhan, seperti *Monitoring and Control, Network Management, Desktop and Mobile Device Support, Internet/Web Management* dan sebagainya.

Di samping itu, pembahasan topik *service operation* juga menjelaskan konsep–konsep umum pengorganisasian operasional layanan dan praktek terkait meliputi organisasi, fungsi, grup, tim, departemen, divisi, peran, tanggung jawab dan kompetensi serta aspek–aspek proses yang dapat diterapkan di seluruh siklus layanan. Adapun fungsi–fungsi utama operasional layanan meliputi *Service Desk, IT Operation Management, Technical Management* dan *Application Management*. Berikut adalah penjelasan lebih detil terkait proses–proses yang terdapat di dalam ITIL *Service Operation*:

1. Pengelolaan Peristiwa (*Event Management*)

Definisi *event* adalah segala perubahan yang berdampak terhadap pengelolaan layanan maupun komponen pendukungnya. Umumnya *event* dapat diketahui melalui notifikasi layanan, *configuration item* (CI) atau alat pemantau.

Pengelolaan *event* dapat diartikan sebagai proses yang dilakukan untuk mengelola *event* di seluruh siklus layanan. Pengelolaan *event* dapat diterapkan dalam segala aspek layanan yang memerlukan pengendalian seperti kondisi lingkungan, *configuration item*, pemantauan lisensi perangkat, keamanan dan aktivitas normal.

Berikut merupakan penjelasan aktivitas–aktivitas yang terdapat di dalam proses pengelolaan *event*:

1. Peristiwa Terjadi (*Event Occurs*)

   Peristiwa (*event*) terjadi secara terus menerus akan tetapi tidak semuanya dapat terdeteksi atau tercatat. Oleh karena itu, peran manajemen sangat dibutuhkan dalam merumuskan jenis–jenis *event* seperti apa yang perlu dikendalikan.

2. Notifikasi Peristiwa (*Event Notification*)

   Prinsip umum notifikasi *event* bergantung pada definisi data yang diperlukan untuk membuat keputusan. Definisi data, definisi peran dan tanggung jawab dalam proses pengelolaan *event* terlebih dahulu harus ditetapkan/ditentukan pada tahap desain dan transisi layanan. Demikian juga penggunaan perangkat pendukung (*tool*) yang diperlukan untuk mengkonfigurasi, mengoperasikan dan mengontrol komponen layanan.

3. Pendeteksian Peristiwa (*Event Detection*)

   Sebuah *event* dapat dideteksi oleh *agent* sistem atau ditransmisikan melalui perangkat yang secara khusus dirancang untuk membaca dan menafsirkan arti dari *event* tersebut.

4. Pencatatan Peristiwa (*Event Logged*)

   Setiap *event* harus tercatat melalui perangkat pengelola *event*, atau dapat dibiarkan sebagai entri dalam *log* sistem perangkat atau aplikasi. Jika hal ini terjadi, maka perlu ditetapkan standar terkait berapa lama *event* dapat tersimpan di dalam *log* tersebut sebelum akhirnya diarsipkan atau dihapuskan.

5. Korelasi Peristiwa dan Filterisasi Tingkat Pertama (*First–Level Event Correlation and Filtering*)

   Tujuan dari korelasi *event* dan filterisasi tingkat pertama ini adalah untuk memutuskan apakah *event* akan ditransmisikan melalui perangkat pendukung (*tool*) atau mengabaikannya. Jika diabaikan, maka *event* akan tercatat sebagai *log file* dalam perangkat. Korelasi *event* biasanya dilakukan oleh *agent* atau mesin korelasi (*correlation engine*) yang melekat pada *configuration item* (CI) atau CI yang terhubung dengan server.

6. Signifikansi Peristiwa (*Significance of Events*)

   Tiap organisasi memiliki kategorisasi tersendiri dalam menetapkan makna atau signifikansi peristiwa. Kategori *event* dapat diklasifikasikan menjadi tiga hal, yaitu:

   a. *Informational*, adalah suatu *event* yang tidak memerlukan tindak lanjut dikarenakan *event* tersebut bukan merupakan pemicu terjadinya insiden atau masalah. *Informational event* biasanya digunakan untuk memeriksa status perangkat atau layanan, atau mengkonfirmasikan keberhasilan suatu aktivitas.

   b. *Warning*, adalah *event* yang dihasilkan dari kondisi layanan atau perangkat yang telah mencapai ambang batas (*threshold*) dan memerlukan tindakan pemeriksaan segera. Hal ini dikhawatirkan *event* tersebut dapat menjadi pemicu terjadinya insiden atau masalah.

   c. *Exception*, adalah *event* dimana kondisi layanan atau perangkat tidak beroperasi secara normal dan dipastikan merupakan *trigger* terjadinya insiden atau masalah. Dalam kondisi *event* seperti ini umumnya telah terjadi

pelanggaran terhadap *Service Level Agreement* (SLA) atau *Operational Level Agreement* (OLA).

7. Korelasi Peristiwa Tingkat Kedua (*Second–Level Event Correlation*)

   Korelasi *event* tingkat kedua dilakukan jika *event* termasuk dalam kategori *warning*. Normalnya, korelasi dilakukan oleh mesin penghubung dengan cara membandingkan *event* pada seperangkat aturan bisnis.

8. Tindak Lanjut yang Diperlukan (*Further Action Required*)

   Aktivitas tindak lanjut diperlukan jika *event* yang terdeteksi pada korelasi tingkat kedua memerlukan suatu respon, baik respon dilakukan secara otomatis (*auto respo*n) ataupun melalui peringatan (*alert*).

9. Pilihan Respon (*Response Selection*)

   Dalam proses ini, pemberian respon dapat dilakukan dengan berbagai macam pilihan respon atau kombinasi. Pilihan respon dapat dilakukan melalui *auto respon*, *alert*, relasi dengan catatan insiden/masalah atau melalui prosedur *request for change* (RFC).

10. Tindakan Pengkajian (*Review Action*)

    Tindakan pengkajian bertujuan untuk memeriksa keakuratan informasi *event*, meliputi kategori dan jenis *event* serta relasinya dengan proses insiden, masalah atau perubahan. Langkah ini bertujuan untuk menghilangkan duplikasi informasi *event* dengan catatan pengkajian sebelumnya.

11. Penutupan Peristiwa (*Close Event*)

    Beberapa *event* akan tetap terbuka hingga dilakukan tindakan pada proses terkait. Oleh sebab itu, diperlukan penggunaan perangkat yang sama pada infrastruktur pengelola *event*.

2. Pengelolaan Insiden (*Incident Management*)

Definisi *incident* adalah segala sesuatu yang dapat mengganggu layanan, menurunkan kualitas layanan atau menyebabkan kegagalan komponen layanan (CI). Pengelolaan insiden dapat diartikan sebagai suatu proses yang dilakukan untuk mengelola *lifecycle* insiden. Proses terjadinya insiden dapat diidentifikasi melalui laporan staf teknisi, alat pemantau *event*, pemberitahuan oleh pengguna serta laporan dari pihak ketiga.

Tujuan pengelolaan insiden adalah untuk mengembalikan operasional layanan pada keadaan normal secepat mungkin dan meminimalisasi dampak negatif terhadap bisnis organisasi. Keadaan normal operasional layanan didefinisikan sebagai keadaan dimana layanan dan komponennya berjalan sesuai dengan SLA dan OLA yang ditetapkan.

Berikut adalah penjelasan dari aktivitas–aktivitas di dalam proses pengelolaan insiden:

1. Identifikasi Insiden (*Incident Identification*)

   Insiden dapat diidentifikasi melalui berbagai macam sumber seperti *service desk, technical staff* ataupun sistem (*event/alert tool*). Kondisi ideal, insiden harus dapat teridentifikasi sebelum mempengaruhi pengguna.

2. Pencatatan Insiden (*Incident Logging*)

   Pencatatan insiden meliputi detil informasi tiap jenis insiden baik yang berskala kecil maupun berskala besar (*major*). Adapun detil informasi insiden meliputi nomor referensi (id), kategori insiden, prioritas insiden, waktu insiden, nama/staf/grup yang bertanggung jawab dalam penanganan,

nama/departemen/telepon/lokasi pengguna, deskripsi insiden, resolusi dan waktu penutupan insiden

3. Kategorisasi Insiden (*Incident Categorization*)

   Kategorisasi insiden pada masing–masing organisasi berbeda, begitu juga dengan pedoman atau panduan yang digunakan sebagai referensi dalam menetapkan kategori insiden. Sehingga dibutuhkan teknik pengkodean khusus dalam menyusun kategori insiden.

4. Prioritas Insiden (*Incident Prioritization*)

   Prioritas insiden dapat dirancang dengan melakukan pengkodean prioritas berdasarkan urgensi dan tingkat dampak insiden terhadap kegiatan bisnis organisasi. Indikasi dampak insiden seringkali berkaitan dengan jumlah pengguna yang terpengaruh. Adapun contoh pengkodean prioritas insiden dapat dilihat pada Tabel 2.2.

Tabel 2.2 Contoh Sistem Pengkodean Prioritas Insiden

	Impact		
Urgency		High	Medium	Low
	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

Priority code	Description	Target resolution time
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

5. Diagnosis Awal (*Initial Diagnosis*)

   Diagnosis insiden dapat dilakukan oleh *service desk* maupun *technical staff* melalui prosedur pencocokan insiden terhadap catatan masalah dan informasi *known error*. Prosedur pencocokan ini dapat membantu penyelesaian insiden dengan lebih cepat.

6. Eskalasi Insiden (*Incident Escalation*)

   Eskalasi diartikan sebagai suatu kegiatan untuk memperoleh sumber daya tambahan yang diperlukan agar target layanan (SLA) atau harapan *customer* dapat tercapai. Terdapat 2 (dua) macam eskalasi insiden, yaitu eskalasi fungsional dan eskalasi hirarki. Definisi eskalasi fungsional adalah tindakan mengalihkan sebuah insiden, masalah atau perubahan kepada *technical staff* dengan tingkat keahlian yang lebih tinggi (*2nd level*, *3rd level* dan seterusnya). Sedangkan eskalasi hirarki adalah tindakan penanganan insiden, masalah atau perubahan dengan melibatkan rantai manajemen (struktural organisasi).

7. Investigasi dan Diagnosis (*Investigation and Diagnosis*)

   Tindakan investigasi dan diagnosis dilakukan oleh *service desk* maupun *support group* guna mencari dan menemukan penyebab terjadinya insiden melalui pemeriksaan terhadap catatan insiden/masalah, *known error database* (KEDB), dan *error log* dari pihak ketiga.

8. Resolusi dan Pemulihan (*Resolution and Recovery*)

   Definisi resolusi adalah segala tindakan yang diperlukan untuk memperbaiki akar masalah (*root cause*) insiden/masalah atau menetapkan *workaround*. Tindakan pemulihan dapat dilakukan dengan berbagai cara, misalnya dengan memandu pengguna melalui telepon, menggunakan perangkat pendukung

yang dikendalikan secara *remote* atau meminta penanganan kepada pihak terkait (*support group*/*3rd party*/*supplier*).

9. Penutupan Insiden (*Incident Closure*)

   Definisi penutupan adalah tindakan yang dilakukan untuk mengubah status insiden, masalah dan perubahan. Penutupan insiden sepenuhnya dilakukan oleh *service desk* sebagai *single point of contact* antara organisasi penyedia layanan dengan pengguna. Beberapa hal yang harus dilakukan oleh *service desk* sebelum melakukan penutupan insiden yaitu memeriksa akurasi kategori insiden, melakukan survei kepuasan dan mendokumentasikan detil informasi insiden.

3. Pemenuhan Permintaan (*Request Fulfilment*)

Definisi *service request* mengacu pada jenis–jenis permintaan layanan yang disediakan oleh organisasi TI bagi para pengguna/pelanggan. Sedangkan *request fulfilment* dapat diartikan sebagai suatu proses yang dilakukan untuk mengelola semua jenis permintaan layanan. Pada beberapa organisasi, permintaan layanan dikelola melalui proses dan perangkat pengelola insiden.

Aktivitas–aktivitas yang terdapat di dalam proses pemenuhan permintaan adalah sebagai berikut:

1. Penerimaan Permintaan (*Receive Request*)

   Pemenuhan permintaan layanan hanya dapat dilakukan melalui permintaan resmi yang disampaikan kepada sumber permintaan. Sumber tersebut dapat berasal dari *service desk* sebagai dukungan lini pertama, *request for change*, *specialist group* dan pihak ketiga (*supplier*).

2. Pencatatan dan Validasi Permintaan (*Request Logging and Validation*)

   Informasi permintaan layanan harus tercatat sesuai dengan ruang lingkup layanan yang disediakan oleh organisasi. Permintaan juga harus disahkan oleh sumber permintaan, baik oleh *service desk*, proses *request for change* atau *specialist group*. Adapun detil informasi permintaan yang dicatat meliputi nomor referensi (id), kategori permintaan, prioritas permintaan, waktu permintaan, nama/id staf/grup yang bertanggung jawab dalam penanganan permintaan, nama/departemen/telepon/lokasi pengguna, pusat anggaran, deskripsi permintaan, waktu pemenuhan dan penutupan permintaan.

3. Kategorisasi Permintaan (*Request Categorization*)

   Kategorisasi permintaan pada tiap–tiap organisasi berbeda, begitu juga dengan pedoman dalam perancangan kategorisasi permintaan. Jenis permintaan dapat dikategorikan berdasarkan layanan (*by service*), aktivitas (*by activity*), tipe (*by type*), fungsi (*by function*) dan jenis CI (*by CI type*).

4. Prioritas Permintaan (*Request Prioritization*)

   Prioritas permintaan dapat ditentukan berdasarkan urgensi dan tingkat dampak yang ditimbulkan terhadap kegiatan bisnis organisasi. Diantara faktor–faktor yang dapat mempengaruhi tingkat dampak permintaan adalah jumlah layanan atau pengguna yang terpengaruh, status pemohon layanan (*executive*/*lower level*), besar keuntungan atau kerugian finansial serta reputasi organisasi jika permintaan tidak terpenuhi.

5. Otorisasi Permintaan (*Request Authorization*)

   Otorisasi permintaan dapat dilakukan melalui *service desk* atau proses yang lebih rumit melalui koordinasi dengan sumber–sumber yang lain seperti manajemen akses dan manajemen keuangan.

6. Pengkajian Permintaan (*Request Review*)

   Pengkajian permintaan bertujuan untuk menentukan fungsi khusus yang akan melakukan aktivitas pemenuhan permintaan. Catatan permintaan harus dikaji dan diperbaharui agar histori permintaan selalu terpelihara.

7. Pelaksanaan Model Permintaan (*Request Model Execution*)

   Setiap aktivitas pemenuhan permintaan harus mengacu pada model permintaan yang berisikan standar alur proses, peran dan tanggung jawab. Hal ini bertujuan untuk memastikan konsistensi tindakan pemenuhan permintaan layanan.

8. Penutupan Permintaan (*Request Closure*)

   Diantara hal–hal yang harus diperhatikan dalam penutupan permintaan adalah melakukan pemeriksaan ulang terhadap kategori permintaan, melakukan survei kepuasan dan mendokumentasikan detil informasi permintaan.

9. Aturan Membuka Kembali Permintaan (*Rules for Reopening Request*)

   Kebijakan pembukaan kembali permintaan pada tiap organisasi berbeda–beda, tergantung pada aturan (*threshold*) serta pedoman yang ditetapkan. Jika aturan ini diterapkan, maka implikasi pada pelacakan data dan laporan permintaan menjadi pertimbangan penting.

4. Pengelolaan Masalah (*Problem Management*)

ITIL mendefinisikan masalah sebagai penyebab terjadinya satu atau lebih insiden. Pengelolaan masalah dapat diartikan sebagai suatu proses yang dilakukan untuk mengelola siklus (*lifecycle*) masalah.

Tujuan dari pengelolaan masalah adalah untuk mengelola siklus masalah sejak pertama kali teridentifikasi melalui investigasi, pencatatan hingga dilakukan penghapusan. Pengelolaan masalah juga bertujuan untuk meminimalkan dampak negatif dari insiden/masalah yang disebabkan kesalahan infrastruktur serta secara proaktif mencegah terulang kembali. Selain itu, aktivitas pengelolaan masalah meliputi langkah–langkah yang diperlukan untuk mendiagnosa *root cause* insiden serta menentukan *workaround* dan resolusi sesuai dengan prosedur pengendalian, khususnya *change management, release* dan *deployment management*.

Adapun proses–proses yang terdapat di dalam pengelolaan masalah adalah sebagai berikut:

1. Pendeteksian Masalah (*Problem Detection*)

   Tiap organisasi memiliki banyak cara dalam mendeteksi masalah, diantaranya adalah faktor pemicu (*trigger*) reaktif dan proaktif pengelolaan masalah. Faktor pemicu reaktif meliputi analisa penyebab insiden yang dilakukan oleh *service desk*, teknisi pendukung, alat otomatis dan pihak ketiga (*supplier/contractor*). Sedangkan faktor proaktif mencakup tindakan analisa insiden yang merujuk pada catatan masalah, tren catatan histori insiden maupun aktivitas–aktivitas perbaikan kualitas layanan.

2. Pencatatan Masalah (*Problem Logging*)

   Informasi masalah harus tercatat dengan jelas termasuk rincian yang terkait dengan catatan insiden. Adapun detil informasi yang harus dicatat meliputi id pengguna, layanan, komponen, waktu pencatatan, detil prioritas dan kategori, deskripsi insiden, jumlah catatan insiden dan detil diagnosis atau langkah pencegahan yang dilakukan.

3. Kategorisasi Masalah (*Problem Categorization*)

   Jenis masalah dikategorikan berdasarkan pedoman atau panduan yang telah ditetapkan oleh organisasi sebagaimana pada kategori insiden, termasuk teknik pengkodean yang digunakan dalam penyusunan kategori masalah.

4. Prioritas Masalah (*Problem Prioritization*)

   Perancangan prioritas masalah dapat dilakukan dengan cara yang sama seperti pada proses penentuan prioritas insiden. Prioritas juga harus memperhitungkan tingkat keparahan masalah dari perspektif layanan, pengguna dan infrastruktur.

5. Investigasi dan Diagnosis Masalah (*Problem Investigation and Diagnosis*)

   Aktivitas investigasi dilakukan untuk mendiagnosa akar masalah (*root cause*). Ketepatan dan kecepatan aktivitas investigasi tergantung pada keahlian sumber daya, kode prioritas dan tingkat keparahan masalah. Terdapat sejumlah teknik pemecahan masalah yang dapat digunakan sebagai rujukan guna membantu diagnosis dan penyelesaian masalah, diantaranya adalah *pain value analysis*, *kepner and tregoe*, *brainstorming*, *5–whys*, *fault isolation*, *ishikawa diagram* dan *pareto analysis*.

6. *Workaround*

   Definisi *workaround* adalah suatu kegiatan yang dilakukan untuk mengurangi atau menghilangkan dampak dari sebuah insiden atau masalah jika resolusi yang bersifat permanen belum ditemukan. Adapun *workaround* masalah didokumentasikan di dalam catatan *known error*, sedangkan *workaround* insiden tetap berada di dalam catatan insiden apabila tidak memiliki keterkaitan dengan catatan masalah.

7. Pembangkitan Catatan *Known Error* (*Raising Known Error Record*)

   Definisi *known error* adalah masalah yang terdokumentasikan beserta akar masalah dan *workaround/resolution*. Sedangkan definisi *known error record* adalah catatan yang berisi detil *known error*. Apabila diagnosis masalah telah selesai dilakukan, terutama ketika *workaround* ditemukan, maka catatan *known error* yang terdapat di dalam *Known Error Database* (KEDB) harus selalu dimutakhirkan. Hal ini bertujuan untuk mempercepat proses identifikasi dan pemulihan layanan.

8. Resolusi Masalah (*Problem Resolution*)

   Resolusi masalah diterapkan jika akar masalah dan solusi telah ditemukan kecuali jika masalah tersebut sangat serius dan memerlukan perbaikan segera maka harus dilakukan penyelesaian melalui prosedur *emergency change*. Pada kasus tertentu, masalah bisa dimungkinkan hanya memiliki *workaround* saja tanpa harus mempunyai resolusi.

9. Penutupan Masalah (*Problem Closure*)

   Hal–hal yang harus diperhatikan sebelum dilakukan penutupan adalah melakukan pemeriksaan dan pemutakhiran histori/deskripsi semua *event*.

10. Pengkajian Masalah Penting (*Major Problem Review*)

    Setiap organisasi memiliki aturan/pedoman tersendiri dalam menentukan prioritas masalah, begitu juga dalam menetapkan kriteria *major problem*. Disamping itu, organisasi juga perlu mengkaji ulang *major problem* yang pernah terjadi agar dapat mempelajari hal–hal yang bisa dijadikan sumber perbaikan. Kegiatan pengkajian dapat dilakukan melalui pelatihan staf teknisi ataupun kegiatan lain, dan setiap pelajaran yang diperoleh (*lessons learned*) harus selalu didokumentasikan dalam sebuah prosedur, instruksi kerja, skrip diagnosis atau catatan *known error*.

5. Pengelolaan Akses (*Access Management*)

Pengelolaan akses adalah suatu proses yang bertujuan untuk mengelola hak pengguna agar dapat menggunakan layanan, data atau aset TI. Selain itu, pengelolaan akses juga bertujuan untuk melindungi kerahasiaan, integritas dan ketersediaan aset layanan. Oleh karena itu, pengelolaan akses berhubungan erat dengan pengelolaan keamanan informasi.

Berkut adalah penjelasan dari proses–proses yang terdapat di dalam pengelolaan akses:

1. Permintaan Akses (*Request Access*)

   Permintaan atau pembatasan akses dapat dilakukan dengan berbagai cara, diantaranya melalui sistem (*human resource*/*request fulfilment system*), s*cript* atau prosedur *request for change* (RFC). Aturan permintaan akses dapat didokumentasikan sebagai bagian dari *request fulfilment* atau penjelasan dalam katalog layanan.

2. Verifikasi (*Verification*)

   Verifikasi permintaan akses layanan dapat dilakukan berdasarkan kebijakan keamanan pada suatu organisasi atau verifikasi independen dari jajaran fungsi/manajemen.

3. Pemberian Akses (*Provide Right*)

   Pemberian akses dilakukan melalui verifikasi hak pengguna dengan jenis layanan yang diminta untuk menghindari terjadinya konflik. Seringkali konflik peran terjadi disebabkan oleh kebijakan dan keputusan diluar operasional layanan. Oleh karena itu, katalog peran sangat diperlukan untuk menghindari konflik kepentingan dalam organisasi serta dilakukan pengkajian ulang untuk memastikan kekinian katalog peran tersebut.

4. Pemeriksaan dan Pemantauan Status Identitas (*Check and Monitor Identity Status*)

   Proses pemeriksaan dan pemantauan status pengguna mencakup perubahan peran dan akses layanan. Perubahan tersebut dapat dipengaruhi oleh hal–hal seperti perubahan jabatan, transfer/mutasi, pengunduran diri, kematian, pensiun, tindakan indisipliner dan pemberhentian kerja.

5. Pencatatan dan Pelacakan Akses (*Log and Track Access*)

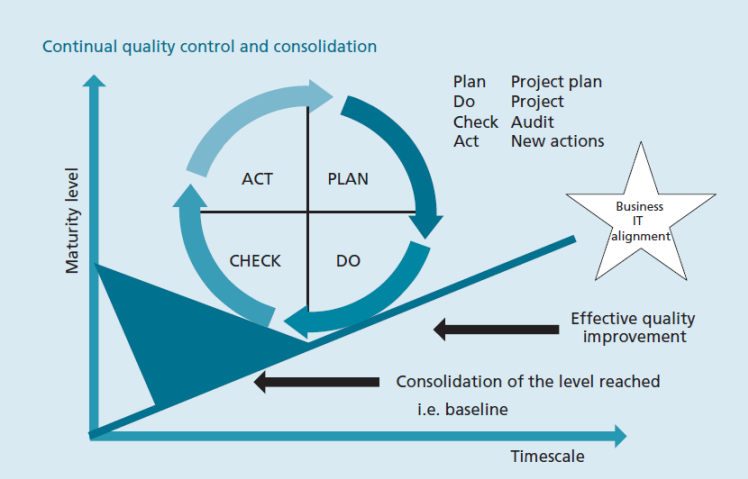
   Aktivitas pemantauan dan pelacakan akses dilakukan pada semua fungsi pengelola aplikasi, teknik dan proses operasional layanan. Pengelolaan akses harus dapat memberikan histori (*record*) akses untuk layanan tertentu seperti bukti hari/waktu dan konten yang diakses selama proses investigasi.

6. Penghapusan atau Pelarangan Akses (*Remove or Restrict Access*)

   Penghapusan dan pelarangan akses tergantung pada kebijakan serta aturan yang telah ditetapkan dalam strategi dan desain layanan. Pada umumnya, penghapusan akses pengguna dilakukan ketika berada dalam kondisi seperti kematian, pengunduran diri, pemberhentian kerja, perubahan peran dan transfer/perjalanan menuju regional yang berbeda.

2.4.5 *Continual Service Improvement* (Perbaikan Layanan Berkelanjutan)

Continual Service Improvement (CSI) berisi panduan penyusunan dan pemeliharaan kualitas layanan TI melalui perpaduan 4 (empat) tahapan layanan yang telah dijelaskan sebelumnya; *strategy*, *design*, *transition* dan *operation*. CSI juga berisi penjelasan praktik terbaik dalam pencapaian perbaikan kualitas layanan secara global, efisensi operasional, kelangsungan bisnis dan memastikan portofolio layanan selaras dengan kebutuhan bisnis dalam setiap tahapan siklus layanan berdasarkan model *Plan–Do–Check–Act (PDCA)* atau *Deming Quality Cycle* seperti yang ditunjukkan pada Gambar 2.2. Adapun proses utama yang terdapat dalam CSI yaitu *The Seven–Step Improvement Process*.



Gambar 2.2. *Deming Quality Cycle* (Sumber: TSO, 2011: 27)

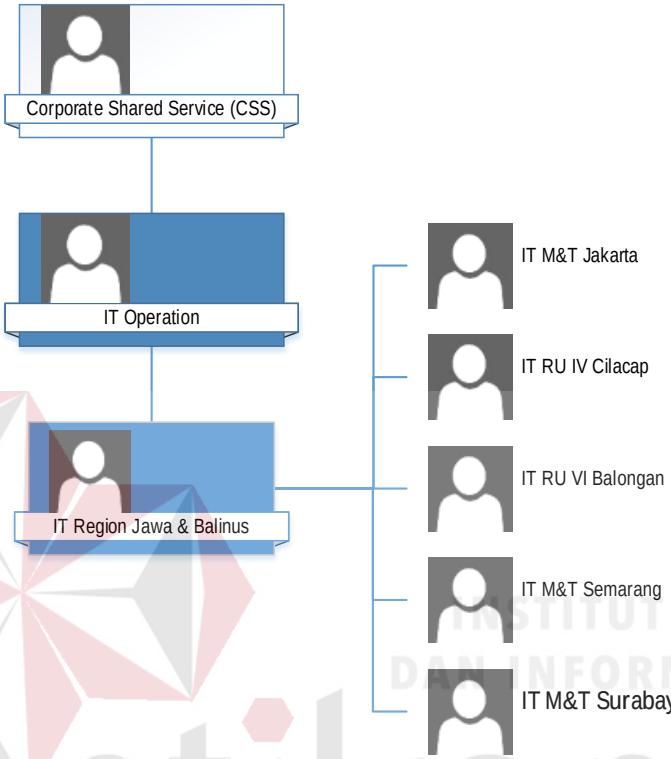
Manfaat penerapan *best practice* ITIL bagi penyedia layanan TI menurut Kneller (2010: 4), adalah:

a) Layanan TI yang selaras dengan prioritas dan tujuan bisnis memberi pengertian bahwa bisnis dapat mencapai lebih banyak hal dalam tujuan strategisnya.
b) Biaya TI dapat diketahui dan dikelola untuk memastikan perencanaan keuangan bisnis menjadi lebih baik.
c) Meningkatkan produktivitas, efisiensi dan efektivitas bisnis dikarenakan layanan TI lebih dapat diandalkan dan bekerja lebih baik bagi pengguna bisnis.
d) Penghematan keuangan terhadap pengelolaan sumber daya dan mengurangi pengerjaan yang berulang.
e) Pengelolaan perubahan menjadi lebih efektif sehingga memungkinkan bisnis untuk mengikuti perubahan dan mendorong perubahan bisnis menjadi suatu keuntungan (*advantage*).
f) Meningkatkan pelayanan dan kepuasan pelanggan melalui TI.
g) Meningkatkan citra dan persepsi pelanggan terhadap organisasi.

2.5 *Information Technology Marketing & Trading* (IT M&T) PT. Pertamina (Persero) Marketing Operation Region V Surabaya

IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya merupakan bagian dari fungsi operasional TI *Corporate Shared Service* (CSS) PT. Pertamina (Persero) seperti yang terlihat pada Gambar 2.3 di halaman 36. Tugas dari IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya adalah sebagai penyelenggara atau penyedia layanan

teknologi informasi dan komunikasi untuk mendukung unit bisnis PT. Pertamina (Persero) di wilayah Jatim, Bali, Nusa Tenggara dan Timor Leste.



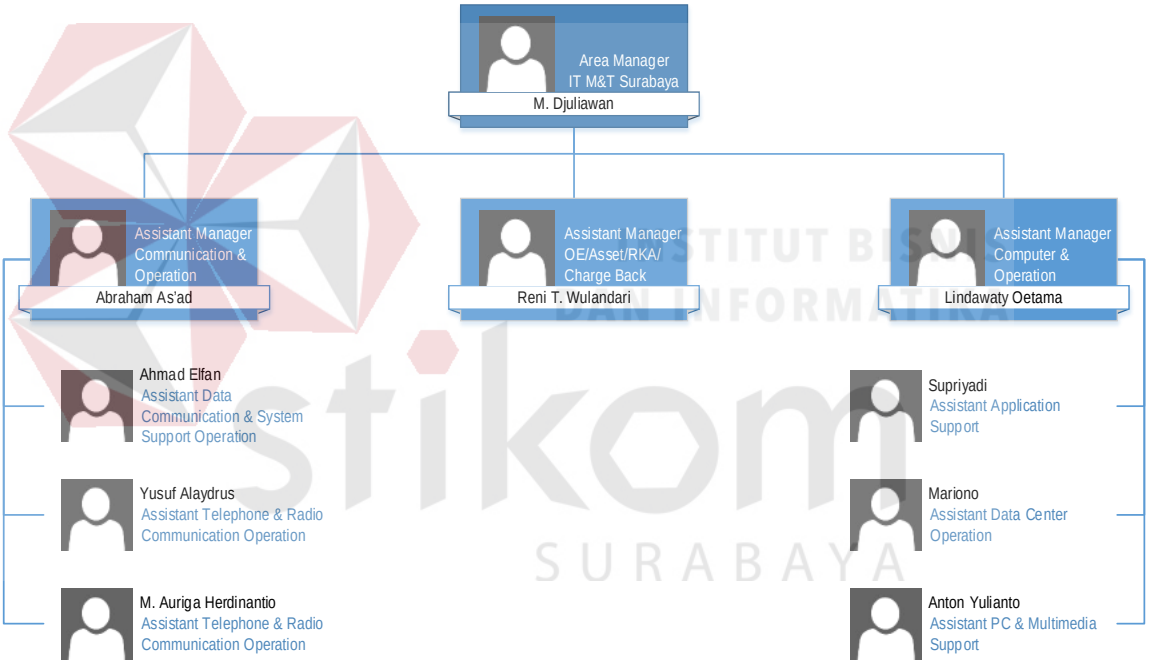
Gambar 2.3. Alur Struktur Organisasi IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya

Adapun visi dari IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya merujuk pada visi CSS PT. Pertamina (Persero), yaitu menjadi penyelenggara layanan teknologi informasi berkelas dunia untuk industri minyak dan gas bumi di kawasan regional. Sedangkan Misi dari IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya adalah sebagai berikut:

1. Memposisikan Teknologi Informasi dan Komunikasi (TIK) sebagai pendaya strategis untuk mencapai sasaran bisnis dengan berfokus pada efektivitas, efisiensi, kerahasiaan, integritas, ketersediaan, kepatuhan, dan kehandalan.

2. Secara terus menerus meningkatkan kontribusi dan *value* Teknologi Informasi dan Komunikasi (TIK) bagi bisnis Pertamina dan anak perusahaan.
3. Menyediakan teknologi informasi, pengembangan, dan pemeliharaan aplikasi serta memproses proses bisnis Pertamina dan anak perusahaan dengan model *outsourcing.*

Berikut adalah struktur organisasi IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya seperti yang terlihat pada Gambar 2.4.



Gambar 2.4. Struktur Organisasi IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya

Kebijakan pengelolaan layanan TI dalam suatu organisasi mutlak diperlukan untuk mengarahkan dan memastikan kinerja perusahaan dalam memberikan layanan TI secara konsisten, handal dan fokus pada kepuasan pelanggan berdasarkan portofolio yang telah ditetapkan. Oleh sebab itu, dibutuhkan mekanisme untuk memvalidasi kemampuan organisasi dalam mendukung

penyampaian layanan TI berdasarkan standar atau *framework* tertentu guna mencapai efisiensi dan efektivitas layanan TI.

Berikut adalah kebijakan–kebijakan manajemen layanan TI yang ditetapkan di lingkungan IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya:

1. Meningkatkan nilai tambah tambah, daya saing dan efisiensi perusahaan.
2. Mengutamakan mutu dan kepuasan pelanggan.
3. Mengutamakan keselamatan dan kesehatan kerja.
4. Mentaati semua peraturan dan prosedur yang berlaku.
5. Menghormati semua etika yang berlaku.
6. Bekerja secara profesional dan penuh tanggung jawab.
7. Senantiasa melakukan perbaikan berkesinambungan di segala lini, dengan berpedoman pada *ICT Master Plan* dan *Enterprise Architecture*.
8. Menggunakan secara optimal seluruh aset milik perusahaan.

Adapun jenis–jenis layanan yang disediakan oleh IT M&T PT. Pertamina (Persero) Marketing Operation Region V Surabaya bagi para pengguna/pelanggan layanan berdasarkan referensi katalog layanan adalah sebagai berikut:

1) Layanan Dukungan *Enterprise Resource Planning* (ERP), yaitu fungsi–fungsi dukungan bagi pengguna aplikasi terkait dengan penyelesaian masalah teknis maupun permohonan bantuan untuk proses transaksi dan penggunaan aplikasi ERP beserta seluruh fungsi–fungsi aplikasi atau *interface* yang terkait.
2) Layanan Dukungan Aplikasi Non–ERP, adalah fungsi–fungsi dukungan bagi pengguna aplikasi terkait dengan penyelesaian masalah teknis maupun permohonan bantuan untuk penggunaan aplikasi Non–ERP.

3) Layanan Pemeliharaan Aplikasi Non–ERP, adalah peningkatan fungsi (*enhancement*) serta modifikasi aplikasi Non–ERP, pembuatan laporan (*report*), beserta seluruh fungsi–fungsi aplikasi atau *interface* yang tidak merubah bisnis.
4) Layanan Konsultasi Teknologi Informasi, meliputi penyusunan atau pembuatan pelaporan hasil kajian tren dan alternatif solusi teknologi informasi sesuai dengan kebutuhan bisnis perusahaan.
5) Layanan Email & File Sharing, mencakup permintaan *file sharing*, dan permintaan akun domain pertamina.com beserta fitur–fiturnya (email, akses internet, akses VPN), serta dukungan atas gangguan atau permasalahan yang terjadi.
6) Layanan Jaringan & Internet, mencakup permintaan instalasi jaringan baik per komputer maupun lokasi kerja tertentu, baik *wired* maupun *wireless*, serta dukungan atas gangguan atau permasalahan yang terjadi dalam lingkup lokal maupun internet.
7) Layanan Telekomunikasi, mencakup permintaan layanan telepon meja, *facsimile*, *SIM card corporate*, *push mail*, HT, serta dukungan atas gangguan atau permasalahan yang terjadi.
8) Layanan Multimedia, mencakup permintaan sarana multimedia untuk keperluan acara dan rapat meliputi proyektor, *sound system*, *teleconference*, *video conference*, serta dukungan atas gangguan atau permasalahan yang terjadi.

9) Layanan *Desktop*, mencakup permintaan perangkat PC, *notebook*, tablet komputer, *printer* beserta *software* resmi, *IT supplies*, perbaikan atas perangkat yang bermasalah, serta peminjaman perangkat.