



**TATA KELOLA INFRASTRUKTUR INFORMASI**  
**BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI**

---

---

**UNDANG-UNDANG REPUBLIK INDONESIA  
NOMOR 28 TAHUN 2014  
TENTANG HAK CIPTA**

**Pasal 113**

- (1) Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
- (2) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
- (3) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (4) Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

# **TATA KELOLA INFRASTRUKTUR INFORMASI**

## **BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI**

**Penyusun:**

Taslim Rochmadi

Ahmad Ismed Yanuar

Amir Dahlan

Noviyanah Farhanah



Jakarta, 2019

## **TATA KELOLA INFRASTRUKTUR INFORMASI BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI**

**Penulis:** Taslim Rochmadi, Ahmad Ismed Yanuar, Amir Dahlan, Noviyannah Farhanah

**Copy Editor** : Ria Ariani

**Layout Editor** : Lisda Rahayu

**Proofread** : Eka Meifrina Suminarsih

**Desain Sampul** : S. Imam Setyawan

Cetakan ke-1, Mei 2019

Cetakan ke-2, November 2019



Diterbitkan oleh:

**BPPT Press**

Badan Pengkajian dan Penerapan Teknologi (BPPT)

Anggota IKAPI, No.476/DKI/III/2014

### **Alamat Redaksi:**

- Gd. BPPT 2 Lt. 4  
Jl. MH Thamrin No.8 Jakarta
  - Gedung Teknologi 3 Lantai 2  
Kawasan Puspiptek Serpong  
Tangerang Selatan, Banten 15314
- Telp.(021) 75791260-262; Fax. (021) 75791218  
Email: [bpptpress@bppt.go.id](mailto:bpptpress@bppt.go.id)

Perpustakaan Nasional: Katalog dalam Terbitan (KDT)

Tata Kelola Infrastruktur Informasi Badan Pengkajian dan Penerapan Teknologi/ disusun oleh Taslim Rochmadi, dkk.,-- Jakarta: BPPT Press, 2019.

x+114 hlm.; 21 x 29,7 cm

ISBN: 978-602-410-155-8

- 
1. Infrastruktur Informasi
    - I. Badan Pengkajian dan Penerapan Teknologi
    - II. Taslim Rochmadi
    - III. Ahmad Ismed Yanuar

## KATA PENGANTAR

Dalam rangka penyelenggaraan *e-government* di BPPT guna meningkatkan kualitas layanan publik secara efektif dan efisien, diperlukan suatu perencanaan yang terkoordinir dan penerapan sesuai dengan tugas dan tanggung jawab pihak-pihak terkait. Terlebih lagi pada Infrastruktur informasi yang menjadi dasar pemanfaatan Teknologi Informasi dan Komunikasi (TIK). Pokok-pokok yang menjadi dasar penyelenggaraan *e-government* ini perlu dikelola dalam suatu sistem tata kelola yang tepat dan dilakukan secara profesional.

TIK yang diimplementasikan oleh Bidang Infrastruktur Informasi - Pusat Manajemen Informasi, merupakan pekerjaan terkait dengan penyimpanan data, pengolahan data, penyelenggaraan pertukaran informasi, serta pelaksanaan sistem manajemen baik operasional layanan maupun pengembangan layanan serta manajemen risiko dan manajemen pengetahuan. Guna pelaksanaan pekerjaan tersebut perlu adanya suatu arahan, rujukan serta tata kelola yang tepat sesuai dengan perkembangan teknologi informasi, dimana TIK diimplementasikan.

Buku Sistem Tata Kelola Infrastruktur Informasi BPPT ini disusun mengikuti peraturan perundangan yang berlaku, Rencana Strategis (Renstra) BPPT dan Rencana Induk Teknologi Informasi (RITI) BPPT, serta *framework* standar internasional, yang disesuaikan dengan kondisi di BPPT. Sehingga proses yang berhubungan dengan Infrastruktur informasi ini dapat dilaksanakan, mulai dari perencanaan, penerapan hingga pelaksanaan evaluasi, sehingga pelaksanaannya terkelola dalam sistem tata kelola yang baik, terstruktur serta terukur.

Di samping itu buku ini dilengkapi dengan panduan sistem manajemen lainnya yang telah berjalan sebelumnya, yang mendukung tata kelola infrastruktur informasi, seperti Sistem Manajemen Risiko, Sistem Manajemen Pengetahuan dan Rencana Keberlangsungan Layanan (*Business Continuity Plan – BCP*).

Serpong, Maret 2019

Tim Penulis



## DAFTAR GAMBAR

Gambar 2.1 Tata Kelola IT berdasarkan Level Kebijakan COBIT 5 .....	4
Gambar 2.2 Representasi Level taktis di Tata Kelola TI .....	5
Gambar 2.3 Hubungan Eksternal Tata kelola di Bidang Infrastruktur Informasi PMI.....	9
Gambar 3.1 Proses Bisnis BII dalam lingkup BPPT .....	13
Gambar 3.2 Diagram Proses Layanan Infrastruktur .....	13
Gambar 3.3 Proses Bisnis Pengembangan Infrastruktur .....	14
Gambar 3.4 Proses Bisnis Optimasi Infrastruktur .....	15
Gambar 3.5 Bagan Perencanaan Adopsi ITIL untuk Perbaikan .....	16
Gambar 3.6 Struktur organisasi CSIRT .....	17
Gambar 3.7 Tipikal Jaringan di Gedung Bertingkat.....	18
Gambar 3.8 Tipikal Jaringan di Gedung Sistem Cluster .....	18
Gambar 3.9 Arsitektur Sistem Keamanan di <i>Data Center</i> .....	19
Gambar 3.10 Arsitektur Desain Dasar <i>Backup DC-DRC</i> .....	19
Gambar 3.11 Arsitektur LAN .....	20
Gambar 3.12 Arsitektur WLAN .....	21
Gambar 4.1 Pemisahan <i>Governance</i> (Tata kelola) dan <i>Management</i> (Manajemen).....	25
Gambar 4.2 Proses yang terdiri dari 37 item .....	27
Gambar 4.3 Lima Bagian ITIL.....	28
Gambar 4.4 Gambar Lengkap Siklus Hidup Layanan .....	29
Gambar 4.5 Lima Prinsip COBIT .....	30
Gambar 4.6 Siklus Hidup Layanan .....	31
Gambar 4.7 Rangkuman Siklus Hidup Layanan .....	31
Gambar 4.8 Infografis COBIT vs ITIL (1 dari 3) .....	32
Gambar 4.9 Infografis COBIT vs ITIL (2 dari 3) .....	33
Gambar 4.10 Infografis COBIT vs ITIL (3 dari 3) .....	34
Gambar 4.11 Urutan Pengembangan Tata Kelola, Pemilihan Tema Utama .....	51
Gambar 5.1 Diagram Proses <i>Service Design</i> (ITIL).....	58
Gambar 5.2 <i>Service Level Management</i> dalam Lingkungan <i>Service Design</i> .....	61
Gambar 5.3 <i>IT Service Management</i> dalam Interaksi dengan Kerekayasaan.....	62
Gambar 5.4 Diagram Alur Pelaksanaan Manajemen Kapasitas .....	67
Gambar 5.5 <i>Flow</i> diagram proses manajemen Kapasitas Infrastruktur informasidi BII .....	69
Gambar 5.6 Diagram Alur Manajemen Ketersediaan .....	70
Gambar 5.7 Diagram Alur Manajemen Ketersediaan Layanan Infrastruktur informasi BII.....	71
Gambar 6.1 <i>Service Transition</i> menurut ITIL.....	74
Gambar 6.2 <i>Service Transition</i> yang dilakukan di BII mengadopsi ITIL .....	77
Gambar 7.1 Ruang Lingkup <i>Service Operation</i> .....	82
Gambar 7.2 Ruang Lingkup <i>Service Operation</i> di BII.....	83
Gambar 7.3 Ruang lingkup Fungsi IT <i>Operation Management</i> .....	89
Gambar 7.4 Manajemen Pengoperasian TI di BII .....	90
Gambar 8.1 Kerangka Kerja Manajemen Risiko .....	94

Gambar 8.2 Proses Manajemen Risiko .....	95
Gambar 8.3 Proses Identifikasi Risiko .....	96
Gambar 8.4 Hubungan Dampak dan Kemungkinan Peningkatan Risiko .....	96
Gambar 8.5 Rencana Penanganan Risiko .....	98

## DAFTAR ISI

KATA PENGANTAR.....	v
DAFTAR ISI .....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xi
BAB I PENDAHULUAN.....	1
A. Rencana Induk Teknologi Informasi (RITI) BPPT .....	3
B. Pengembangan Tata Kelola Infrastruktur Informasi BPPT.....	6
BAB III PENGELOLAAN INFRASTRUKTUR INFORMASI .....	11
A. Bidang Infrastruktur Informasi – Pusat Manajemen Informasi .....	11
B. Proses Bisnis Bidang Infrastruktur Informasi .....	12
C. CSIRT ( <i>Computer Security Incident Response Team</i> ) BPPT .....	16
D. Konsep Dasar Infrastruktur Informasi BPPT.....	17
BAB IV STRATEGI LAYANAN ( <i>SERVICE STRATEGY</i> ).....	23
A. Strategi Penerapan Tata Kelola Teknologi Informasi.....	23
B. Referensi <i>Framework</i> COBIT dan ITIL.....	24
C. Pemisahan Tata Kelola Dari Manajemen .....	26
D. <i>Information Technology Infrastructure Library</i> (ITIL).....	27
E. Penerapan COBIT 5 Bidang Infrastruktur Informasi.....	38
F. Penerapan ITIL V3 Bidang Infrastruktur Informasi.....	50
BAB V DESAIN LAYANAN ( <i>SERVICE DESIGN</i> ).....	57
A. Manajemen Katalog Layanan ( <i>Service Catalogue Management</i> ) .....	59
B. Manajemen Tingkat Layanan ( <i>Service Level Management</i> ) .....	60
C. Manajemen Pemasok ( <i>Supplier Management</i> ) .....	64
D. Manajemen Kapasitas ( <i>Capacity Management</i> ).....	66
E. Manajemen Ketersediaan ( <i>Availability Management</i> ).....	69
BAB VI TRANSISI LAYANAN ( <i>SERVICE TRANSITION</i> ).....	73
A. Manajemen Perubahan ( <i>Change Management</i> ) .....	75
B. <i>Release and Deployment Management</i> .....	77
C. Manajemen Aset dan Konfigurasi Layanan.....	78
D. Manajemen Pengetahuan ( <i>Knowledge Management</i> ).....	80
BAB VII PENGOPERASIAN LAYANAN ( <i>SERVICE OPERATION</i> ).....	81
A. Manajemen Even ( <i>Event Management</i> ) .....	83

B.	Manajemen Insiden ( <i>Incident Management</i> ) .....	84
C.	Manajemen Masalah ( <i>Problem Management</i> ).....	86
D.	Manajemen Akses ( <i>Access Management</i> ) .....	87
E.	Pemenuhan Permintaan ( <i>Request Fulfillment</i> ).....	88
F.	Manajemen Pengoperasian TI ( <i>IT Operation Management</i> ).....	88
BAB VIII SISTEM MANAJEMEN PENDUKUNG TATA KELOLA INFRASTRUKTUR INFORMASI.....		93
A.	Manajemen Risiko.....	93
B.	Manajemen Pengetahuan.....	98
C.	Manajemen Keamanan Informasi.....	100
D.	<i>Business Continuity Plan</i> (BCP).....	100
BAB IX MONITORING DAN EVALUASI.....		105
A.	Monitoring .....	105
B.	Evaluasi.....	106
C.	Audit Internal .....	106
D.	Kaji Ulang Manajemen .....	107
BAB X PENUTUP.....		109
REFERENSI .....		110
INDEKS.....		111

## DAFTAR TABEL

Tabel 4.1 Keterangan Infografis COBIT vs ITIL .....	35
Tabel 4.2 Pemetaan COBIT dan ITIL .....	36
Tabel 4.3 Tabel Dokumen Kebijakan Eksisting .....	39
Tabel 4.4 Tabel SOP Eksisting .....	40
Tabel 4.5 Tabel Standar Instruksi Kerja Eksisting .....	41
Tabel 4.7 Deskripsi Proses DSS 01 .....	42
Tabel 4.8 Raci Chart DSS 01 .....	43
Tabel 4.9 Proses, Input, Output dan Aktivitas DSS01 .....	44
Tabel 4.10 Standar Terkait DSS 01 .....	47
Tabel 4.11 Tabel Pemetaan DSS 01.01 .....	47
Tabel 4.12 Tabel Rekomendasi Kategori Kebijakan .....	48
Tabel 4.13 Tabel Rekomendasi Kategori Prosedur, Formulir, Instruksi Kerja .....	49
Tabel 4.14 Tabel Rekomendasi Kategori Sistem, Fitur, <i>Tools</i> .....	49
Tabel 4.15 Tabel Rekomendasi Kategori Tindakan Lainnya .....	49
Tabel 4.16 Tabel Prioritas Pengembangan .....	49
Tabel 4.17 Tabel <i>Service Catalog</i> Layanan BII .....	52
Tabel 4.18 Detail Layanan <i>Service Catalog</i> Layanan BII .....	53
Tabel 9.1 Daftar Peralatan Monitoring .....	105
Tabel 9.2 Tabel Evaluasi Layanan BII .....	106



## BAB I PENDAHULUAN

Sebagaimana diketahui BPPT adalah Lembaga Pemerintahan Nonkementerian, suatu lembaga yang dibentuk di dalam sistem pemerintahan Indonesia, untuk membantu Presiden dalam melaksanakan mandat di bidang pengkajian dan penerapan teknologi. Dalam melaksanakan perannya di bidang pengkajian dan penerapan teknologi, BPPT mengikuti peraturan dan perundang-undangan yang berlaku di Indonesia. Khusus untuk tata kelola dalam manajemen teknologi informasi ini mengacu pada Peraturan Menteri Komunikasi dan Informatika Nomor 41 Tahun 2007 tentang "Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional".

Kebijakan dan arahan aturan tata kelola untuk teknologi informasi sangat dibutuhkan dan penting dalam rangka untuk melaksanakan tugas dan fungsi terkait dengan pengelolaan teknologi informasi di internal lembaga. Oleh karena itu, kebijakan akan acuan dalam perencanaan pelaksanaan pekerjaan. Dalam buku ini, permasalahan dibatasi khusus tentang pedoman tata kelola terkait dengan infrastruktur informasi di BPPT.

Dalam menyusun tata kelola infrastuktur informasi ini, Pusat Manajemen Informasi (PMI) yang secara fungsional berada di bawah dan bertanggung jawab kepada Kepala BPPT, serta secara administratif dikoordinasikan oleh Sekretaris Utama, mempunyai tugas untuk melaksanakan pengelolaan infrastruktur informasi, penerapan *e-government*, manajemen pengetahuan dan perpustakaan, dan standarisasi hasil inovasi dan layanan teknologi. Dengan demikian PMI perlu menyusun suatu sistem tata kelola sebagai acuan dalam bekerja sesuai tugas tersebut dengan BPPT sebagai ruang lingkup tugasnya, sehingga *output* yang dihasilkan dapat mendukung dan menguatkan sistem Teknologi Informasi dan Komunikasi di BPPT.

Penyusunan tata kelola teknologi informasi dan komunikasi ini ditekankan untuk selalu diperbaiki dan ditingkatkan, sehingga perlu mengikuti berbagai kebijakan terkait seperti Keputusan Menteri Komunikasi dan Informasi Nomor 57 Tahun 2003 tentang "Penyusunan Rencana Induk Pengembangan *e-Government*", juga mengikuti pemeringkatan *e-government* di Indonesia (PeGI) oleh Kementerian Komunikasi dan Informatika serta pemeringkatan Keamanan Informasi (KAMI) oleh Badan Siber dan Sandi Negara (BSSN).

Kebijakan yang disusun untuk infrastruktur informasi ini, merupakan acuan bagi Bidang Infrastruktur Informasi - Pusat Manajemen Informasi BPPT dan pemangku kepentingannya dalam melaksanakan pengelolaan Teknologi Informasi khususnya terkait dengan infrastruktur informasi. Dalam pengembangan tata kelola infrastruktur informasi ini, selain yang telah disebutkan di atas, perlu juga diselaraskan *state the art of technology* dengan standar internasional terkait dengan pengelolaan infrastruktur teknologi informasi.

Salah satu standar yang banyak digunakan sebagai acuan adalah standar *Control Objective for Information & Related Technology* (COBIT) yaitu panduan standar praktik untuk tata kelola TI yang dapat membantu auditor, pengguna (*user*), dan manajemen, untuk menjembatani gap

antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI. Versi terakhir standar COBIT adalah COBIT versi 5 atau COBIT 5 yaitu edisi terbaru dari *Framework COBIT ISACA* yang menyediakan penjabaran bisnis secara *end-to-end* dari tata kelola teknologi informasi untuk menggambarkan peran utama dari informasi dan teknologi dalam menciptakan nilai organisasi. COBIT 5 dibangun berdasarkan pengembangan dari COBIT 4.1 dengan mengintegrasikan Val IT dan *Risk IT* dari ISACA, ITIL, dan standar-standar yang relevan dari ISO.

Kemudian dalam level praktis pengelolaan infrastruktur informasi mengikuti ITSM (*IT Service Management*) yang umum dijadikan sebagai acuan adalah *Information Technology Infrastructure Library* (ITIL) yaitu suatu rangkaian konsep dan teknik pengelolaan infrastruktur, pengembangan, serta operasi teknologi informasi (TI). Standar ITIL yang diacu adalah ITIL versi 3.

Buku ini disusun untuk memberikan arahan yang lebih detail serta terfokus pada pengelolaan infrastruktur informasi yang diterapkan di BPPT, dalam rangka meningkatkan kemampuan pengelolaan, memperbaiki proses yang berjalan serta melaksanakan layanan yang dilakukan oleh Bidang Infrastruktur Informasi dari Pusat Manajemen Informasi.

## BAB II

### TATA KELOLA TEKNOLOGI INFORMASI BPPT

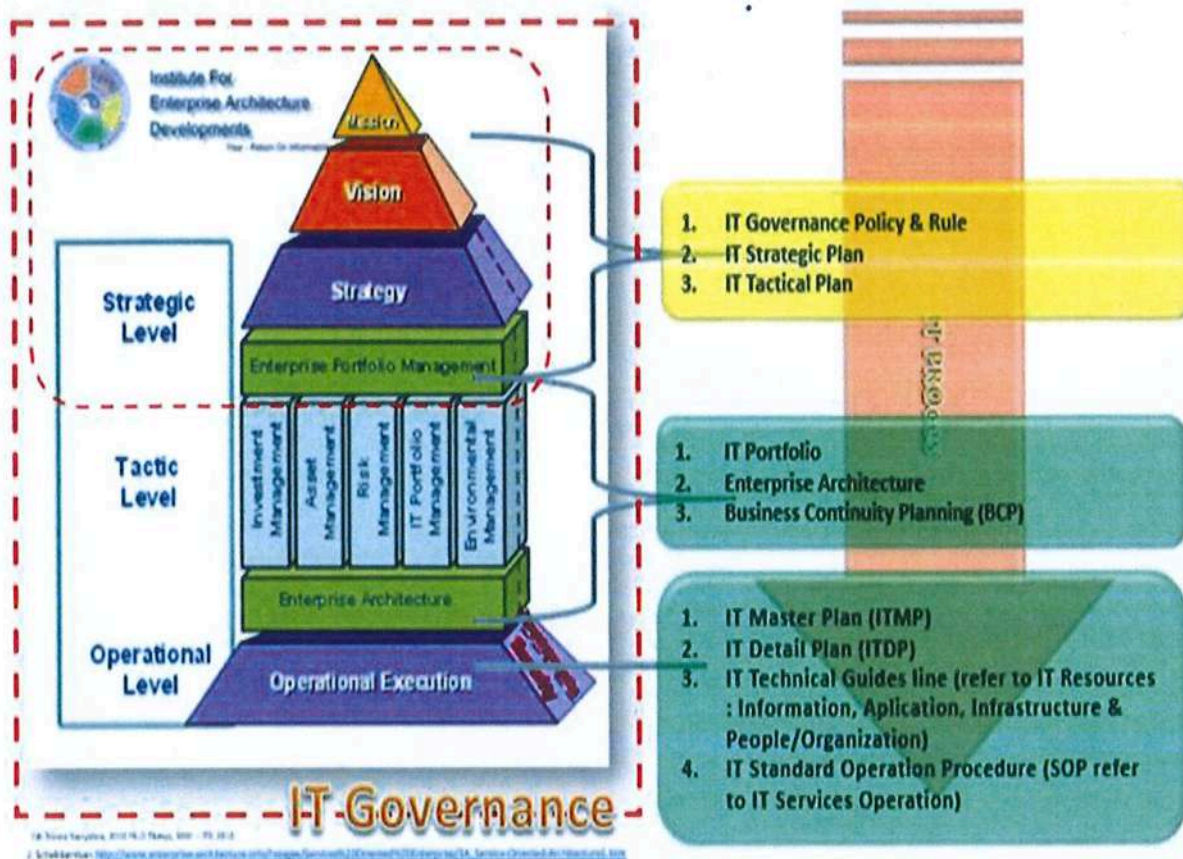
Dalam rangka pengelolaan dan pengembangan infrastruktur informasi BPPT, terdapat arahan dan batasan yang secara prinsip bertujuan untuk menjadikan sistem informasi yang ada di BPPT tetap dalam jangkauan yang terkendali, dapat diaudit, serta mengoptimalkan sumber daya secara efektif dan efisien. Dengan demikian Bidang Infrastruktur Informasi dalam mengimplementasikan teknologi informasi terbaru dalam menjalankan *e-government* secara baik dan benar, disertai dengan penggunaan sumber daya yang ada dengan tepat sasaran sesuai dengan beban kerja yang diberikan.

Infrastruktur informasi BPPT merupakan komponen penting agar *e-government* BPPT bisa dilaksanakan dengan handal, karenanya harus dipersiapkan dan direncanakan dengan baik. Secara manajerial memiliki prinsip manajemen PDCA yang secara terus menerus memungkinkan untuk dikembangkan dan diperbaiki sehingga dapat berfungsi dalam sistem manajemen yang lebih baik secara berkelanjutan. Untuk itu pada pengembangan tata kelola diatur sedemikian rupa agar ada keteraturan dan kepastian manfaat yang akan diperoleh. Selain untuk mengikuti perkembangan teknologi juga agar sesuai dengan *framework* yang tepat. Namun, dalam level aplikatif atau praktis masih memerlukan suatu contoh atau *framework* yang memberi arahan yang dapat menjangkau pelaksanaan pengelolaan infrastruktur yang baik dan memenuhi syarat teknis. Untuk itu *framework* dan konsepnya perlu dijadikan acuan, yang kemudian dapat secara mudah untuk diadopsi dan dijalankan. Artinya tata kelola sistem infrastruktur yang terpasang, khususnya yang telah beroperasi, dapat dikelola dalam lingkup praktis yang terkontrol serta mampu mengikuti perkembangan teknologi.

Untuk menyusun tata kelola tersebut, Pusat Manajemen Informasi (PMI) yang bertanggung jawab sebagai pelaksana manajemen infrastruktur informasi, yang juga harus melaksanakan Rencana Strategis (Renstra) dan Rencana Induk Teknologi Informasi (RITI) BPPT, perlu menetapkan tata kelola teknologi informasi yang mapan dan dapat dipertanggung jawabkan. Adapun *framework* yang diacu dalam tata kelola infrastruktur informasi BPPT adalah COBIT 5, serta *framework* ITSM (*IT Service Management*) yaitu ITIL versi 3.

#### A. Rencana Induk Teknologi Informasi (RITI) BPPT

Rencana Induk Teknologi Informasi (RITI) BPPT menjelaskan hal-hal pada level strategis, yaitu membahas tentang visi, misi dan strategi, serta manajemen portofolio lembaga dari tata kelola teknologi informasi. Dimana hal tersebut merupakan kebijakan, yang merupakan acuan pada level taktis yang diwakili manajemen investasi, manajemen aset, manajemen portofolio dan manajemen risiko, serta *enterprise architecture*. Sehingga apabila RITI BPPT disejajarkan dengan COBIT 5 pada level kebijakan, maka dapat digambarkan sebagai berikut.

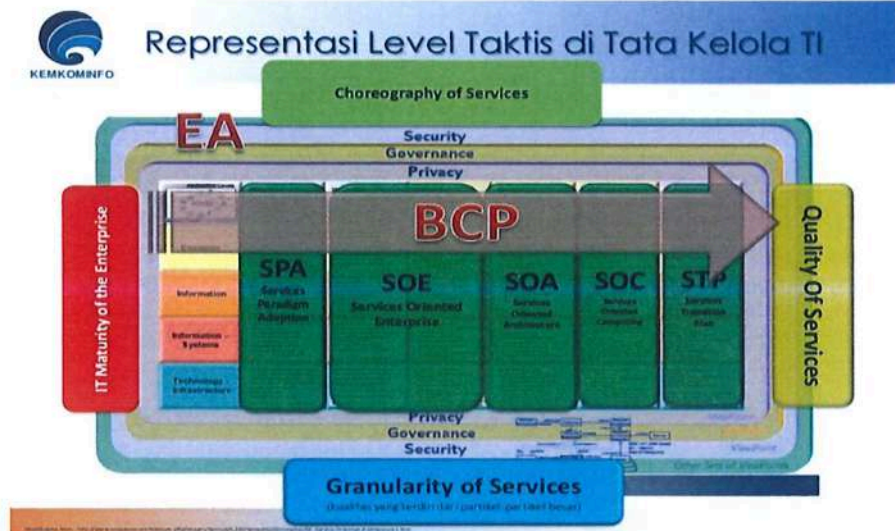


Gambar 2.1 Tata Kelola IT berdasarkan Level Kebijakan COBIT 5

Sumber : Rencana Induk Teknologi Informasi Badan Pengkajian dan Penerapan Teknologi 2015-2019 (RITI-BPPT)

Dalam implementasi tata kelola dan pengembangan infrastruktur di BPPT yang secara langsung dilaksanakan oleh Bidang Infrastruktur Informasi – Pusat Manajemen Informasi (PMI), tata kelola tersebut harus disusun dengan perencanaan yang baik serta dijalankan melalui suatu tahapan dan langkah langkah yang sesuai *framework* yang dapat diadopsi sebagaimana tersebut di atas.

Dalam penyusunan tata kelola sebagaimana prinsip yang ada pada level taktis, perlu untuk mengadopsi representasi level taktis tata kelola dari Kementerian Komunikasi dan Informatika seperti diagram berikut.



Gambar 2.2 Representasi Level taktis di Tata Kelola TI

Sumber : Bahan presentasi panduan penyusunan Rencana Induk TIK  
Kementerian dan Komunikasi Informatika, 2012

Sebagaimana prinsip yang ada pada Level taktis, untuk menyusun perencanaan ini PMI perlu untuk mengadopsi representasi level taktis tata kelola dari Kementerian Komunikasi dan Informatika. Prinsip tata kelola yang ada pada level taktis disusun dalam panduan mutu PMI, dimana layanan terbagi dalam bidang-bidang yang ada di PMI. Sehingga dalam perencanaan dalam level taktis ini tergantung pada ruang lingkup layanan yang diberikan. Untuk Bidang Infrastruktur Informasi, maka dalam memberikan layanan infrastruktur informasi perlu disusun perencanaan infrastruktur yang menjangkau seluruh kebutuhan unit kerja di BPPT terhadap layanan infrastruktur informasi. Untuk itu perlu disusun secara lebih mendetail tentang perencanaan layanan yang diberikan oleh Bidang Infrastruktur Informasi yang telah diberikan sampai dengan tahun 2019 serta perencanaan struktur infrastruktur itu sendiri yang dapat mendukung layanan yang diberikan Bidang Infrastruktur Informasi .

Pada penyusunan buku “Tata Kelola Infrastruktur Informasi” ini dibatasi pada bidang operasional, atau level operasional, dimana di dalamnya terdapat ‘Operational Execution’. Hal ini disusun guna menerjemahkan level strategis dan level taktis pada RITI BPPT 2014-2019 dan panduan mutu PMI ke dalam hal-hal yang bersifat operasional. Adapun pelaksana tata kelola yang menyangkut infrastruktur informasi adalah Bidang Infrastruktur Informasi, sehingga pelaksanaan praktis ini harus diatur lebih lanjut dengan suatu *framework* yang tepat.

Secara struktur Bidang Infrastruktur Informasi (BII) dalam melaksanakan level operasional. harus melengkapi dirinya dengan *IT Master Plan* (ITMP), *IT Detail Plan* (ITDP), *IT Guides Line* dan *IT Standard Operation Procedure*. *IT Master Plan* sudah tercantum pada RITI BPPT (2015-2019), *detail plan* ada pada Rencana Tindak IT BPPT 2015-2019. Rencana yang lebih detail lagi dijelaskan buku ini, sehingga dalam melaksanakan pekerjaan dan mengembangkan infrastruktur informasi lebih lanjut, BII sudah memiliki pedoman yang dapat digunakan untuk level operasional.

Adapun tanggung jawab dokumen yang lebih tinggi yaitu level strategis dan level taktis pengelolaannya oleh unsur kelembagaan seperti *Chief Information Officer* (CIO). Artinya *IT*

*Governance Policy & Rule, IT Strategic Plan, IT Tactical Plan, IT Portofolio, Enterprise Architecture, dan Business Continuity Planning*, diharapkan sudah tercakup pada dokumen lain, yang dikerjakan pada level di atas BII.

## **B. Pengembangan Tata Kelola Infrastruktur Informasi BPPT**

Untuk melaksanakan perencanaan infrastruktur informasi perlu diperhatikan beberapa poin penting yang perlu dikemukakan disini. Perencanaan tersebut harus dapat mempertahankan beberapa sifat utama yang menjadi kekuatan inti dari infrastruktur informasi, yaitu:

1. Keandalan sistem;
2. Ketersediaan sistem;
3. Keamanan sistem; serta
4. Keberlanjutan sistem.

Mengingat hal tersebut di atas, maka perencanaan itu diharapkan selalu mempunyai arahan yang dalam pelaksanaan operasional dapat menjadi rujukan. Bidang Infrastruktur Informasi bertindak untuk melaksanakan perencanaan infrastruktur, dan juga membuat perencanaan tata kelola yang disusun hingga detail sampai dengan SOP dan instruksi teknisnya.

Dalam menyusun tata kelola infrastruktur informasi, BII secara berkesinambungan mempunyai fase-fase yang secara siklus dilakukan yaitu fase evaluasi, fase desain, fase implementasi, dan fase kontrol (Pengendalian). Hal ini merupakan manajemen yang menyesuaikan dengan konsep PDCA yang diterapkan pada teknologi informasi. Secara singkat masing-masing fase yang dilaksanakan dijelaskan sebagai berikut :

### **Fase 1 : Evaluasi**

Fase evaluasi bertujuan untuk mengevaluasi tata kelola TI yang sudah ada dalam organisasi saat ini. Tahapannya terdiri dari :

- Tahap1, yaitu melakukan konfirmasi kepada tim;
- Tahap 2, yaitu melakukan karakterisasi umum organisasi;
- Tahap 3, yaitu menganalisis penyelarasan sumber daya TI dengan tujuan bisnis organisasi, mengusulkan satu set alat untuk melaksanakan penilaian ini;
- Tahap 4, yaitu mengusulkan prosedur khusus untuk menganalisis manajemen risiko TI, untuk mendapatkan penilaian risiko dalam organisasi;
- Tahap 5, yaitu mengidentifikasi tingkat kepuasan karyawan terhadap layanan TI dan sumber daya;
- Tahap 6, yaitu melakukan diagnosa kematangan terhadap objek kontrol TI;
- Tahap 7, yaitu memberikan pemahaman tata kelola TI yang sedang berlangsung di organisasi;
- Tahap 8, yaitu memberikan usulan tindakan perbaikan, pencegahan dan/atau peningkatan layanan.

## **Fase 2 : Desain**

Fase desain dari proses tata kelola TI didefinisikan dengan pendekatan *Business Process Management* (BPM). Tahapannya terdiri dari :

- Tahap 9, yaitu melakukan pemodelan dan analisis proses *As-Is*;
- Tahap 10, yaitu melakukan identifikasi peluang untuk perbaikan dalam proses, dari hasil fase sebelumnya;
- Tahap 11, yaitu menjelaskan secara rinci pemilihan dan desain subproses. Fase ini berakhir dengan desain proses *To-Be* (yang diinginkan).

## **Fase 3 : Implementasi**

Fase implementasi melaksanakan proses dengan merancang prosedur umum penerapan dan diikuti dengan penerapan bertahap pada masing-masing *subprocess*.

## **Fase 4 : Kontrol**

Fase kontrol melakukan pengendalian pada tiap subproses, diikuti pengembangan alat bantu pengelolaan pengendalian berdasarkan prinsip-prinsip IT BSC (*Business Service Continuity*), dan diakhiri dengan proses evaluasi TI secara keseluruhan.

Keempat fase ini menjadikan teknologi informasi dapat diimplementasikan pada bidang yang luas baik untuk membantu berbagai bentuk layanan, serta untuk menjadikan adanya keselarasan kerja yang secara *life cycle* berlanjut dan berkembang.

Dalam pengembangan tata kelola infrastruktur informasi ini, tahap pertama adalah mengenal *stakeholder*, lingkungan dan kebutuhan yang ada di BPPT, selain itu juga mengenal perkembangan atau evolusi teknologi, sekurang-kurangnya teknologi yang dapat diaplikasikan dalam waktu dekat. *Stakeholder* dan lingkungan yang terbentuk berdasarkan dokumen perencanaan Renstra BPPT periode 2015-2019 (saat ini menggunakan revisi ke-lima) yang disusun dengan berpedoman pada Rencana Pembangunan Jangka Menengah Nasional (RPJMN), dimana menurut dokumen Renstra tersebut *stakeholder* atau pemangku kepentingan yang dimaksud adalah sebagai berikut.

Tabel 2.1 Ekspektasi pemangku kepentingan dan pengguna (Renstra BPPT)

	Pemangku Kepentingan	Lembaga	Ekspektasi/Perspektif
1.	<b>Lembaga Pemerintah</b> Pihak-pihak yang berkepentingan atau memiliki harapan terhadap perkembangan kinerja dan program BPPT	Presiden dan Kabinet	Kontribusi BPPT terhadap perkembangan ekonomi untuk meningkatkan daya saing dan kemandirian bangsa
2.	<b>Pelanggan (Customer)/aliansi</b>  a. <b>Pelanggan/Customer</b> Pihak yang menggunakan produk dan pelayan BPPT  b. <b>Aliansi</b> Lembaga yang bekerjasama dengan BPPT sebagai partner yang mempunyai tujuan, sasaran dan interes bersama	Industri  Pemerintah  Lembaga, Litbangyasa, Perguruan Tinggi	Ketersediaan sumber daya teknologi untuk melakukan inovasi, pendalaman proses pertambahan nilai, dan pembaruan proses produksi untuk meningkatkan keuntungan.  ketersediaan sumber daya teknologi/rekomendasi kebijakan untuk meningkatkan pelayanan publik  Efektivitas melakukan pembaruan ilmu pengetahuan dan teknologi
3.	<b>Masyarakat</b>	DPR, Masyarakat Umum	Keluaran dan produk BPPT dapat dimanfaatkan secara luas, meningkatkan kualitas hidup, lingkungan dan ekonomi secara keseluruhan.

Agar dapat memenuhi informasi kepada stakeholder tersebut Bidang Infrastruktur Informasi (BII) perlu menyusun infrastruktur yang dapat menjangkau seluruh *stakeholder*.

Secara teknologi dapat dilakukan dengan penggunaan *IP Base*, maka informasi dapat disampaikan melewati internet maupun intranet, serta telekomunikasi digital lainnya.

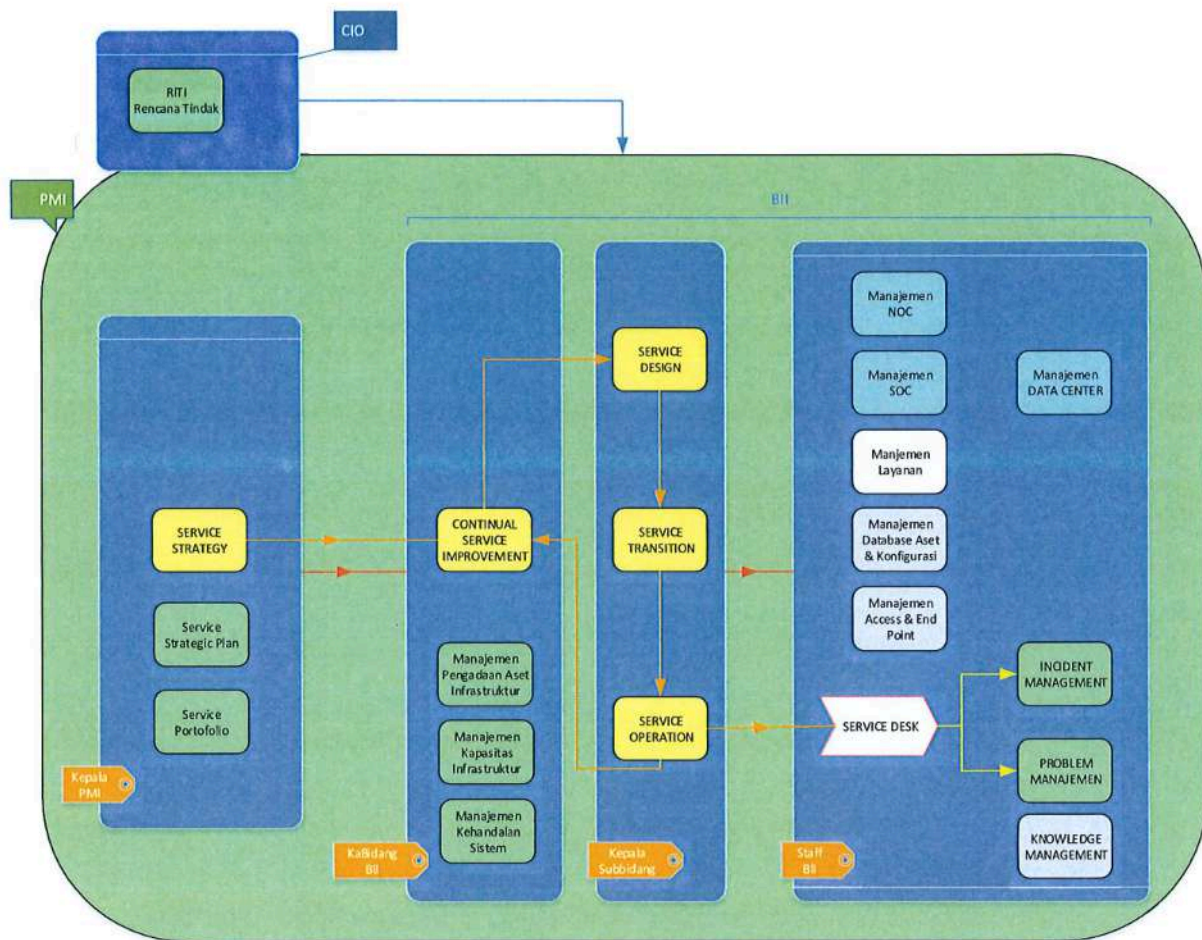
Disamping itu juga diperhatikan lingkup area organisasi, dimana dan apa saja yang diperlukan secara garis besar dalam mengelola infrastruktur ini. BII yang berada di Pusat Manajemen Informasi (PMI) melaksanakan tugas secara komprehensif, yaitu melaksanakan pengembangan dan optimasi pemanfaatan infrastruktur informasi BPPT. Dengan penyelenggaraan fungsi untuk:

- a. Pengembangan infrastruktur teknologi informasi komunikasi untuk penerapan *e-government* di lingkungan BPPT; dan
- b. Pelaksanaan optimasi pemanfaatan infrastruktur teknologi informasi komunikasi untuk penerapan *e-government* di lingkungan BPPT.

Rangkaian pekerjaan atau proses bisnis akan memberi gambaran yang lebih jelas dalam menyusun tata kelola yang baik dari pengembangan infrastruktur dan pelaksanaan optimasi

dalam sistem organisasi PMI, dengan mengenal *interface* atau interaksi dengan pihak luar atau hubungannya dengan organisasi di atasnya.

Gambaran ruang lingkup eksternal tata kelola yang akan dilaksanakan BII sebagai berikut :



Gambar 2.3 Hubungan eksternal Tata kelola di Bidang Infrastruktur Informasi PMI

Proses ini dimulai dari arahan CIO BPPT, yang memberikan kepada PMI untuk melaksanakan fungsinya, baik dalam ruang lingkup Rencana Induk Teknologi Informasi (RITI) maupun Rencana Tindak yang perlu dilaksanakan dalam tahun berjalan. Terkait dengan infrastruktur informasi, Kepala PMI memberikan tugas kepada Bidang Infrastruktur Informasi untuk memberikan layanan, disertai target yang ditetapkan setiap tahun atau penugasan lainnya yang harus dilaksanakan. Kepala Bidang Infrastruktur Informasi merencanakan peningkatan layanan yang akan dilaksanakan, atau mengembangkan serta membangun layanan tertentu sesuai kebutuhan atau arahan Kepala PMI. Selanjutnya tugas pengembangan didelegasikan kepada Sub Bidang Pengembangan Infrastruktur. Sedangkan untuk pengoperasian layanan infrastruktur atau peningkatan kapasitas dan kualitasnya didelegasikan kepada Sub Bidang Optimasi Infrastruktur.

Kemudian dikembangkan pula sistem manajemen pendukung lainnya guna memudahkan pelaksanaan pengelolaan infrastruktur informasi agar mencapai tujuan dengan berbagai parameter yang harus dipenuhi, seperti keamanan informasi, manajemen risiko dan *Business Continuity Plan* (BCP). Pelaksanaan sistem manajemen yang ada ini disusun dalam sistem tata kelola dengan mendokumentasikannya ke dalam dokumen terdiri dari :

1. Pedoman atau Kebijakan
2. SOP (Standar Operasi Prosedur)
3. SIK (Standar Instruksi Kerja)
4. SFK (Standar Formulir Kerja)

Sebagai inisiasi dari beberapa Pedoman atau Kebijakan yang ada untuk dapat dipakai sebagai acuan kerja di BII diantaranya adalah:

1. Buku Kebijakan Keamanan Informasi BPPT No:2106000.02.00.00.00.01.14 PDIS -BPPT yang berisi kebijakan keamanan informasi termasuk dalam penyelenggaraan infrastruktur;
2. Buku Panduan Manajemen Resiko No 2106000.PMR.2.01.13; PDIS- BPPT
3. Buku Panduan Manajemen *Business Continuity Plan* (BCP) PDIS; No:2106000.03.00.00.00.01.14, dan
4. Buku Panduan Manajemen Penyimpanan, *Backup* dan *Recovery*, No:2106000.01.09.00.00.01.13, PDIS - BPPT.

Dengan demikian buku "Tata Kelola Infrastruktur Informasi" ini disusun dengan harapan dapat memberikan arahan pada Bidang Infrastruktur Informasi dalam rangka memperbaiki tata kelola yang sudah ada.

## BAB III

### PENGELOLAAN INFRASTRUKTUR INFORMASI

Infrastruktur informasi didefinisikan sebagai sumber daya teknologi, yang secara bersama-sama dapat menyediakan *platform* (tempat dimana perangkat lunak dapat dijalankan) sehingga dengan demikian akan bisa diterapkan di atasnya berbagai aplikasi sistem informasi untuk berbagai kegunaan.

Di dalam infrastruktur teknologi informasi ada berbagai bentuk perangkat keras, perangkat lunak serta layanan, yang tersebar atau disusun sedemikian rupa sehingga memberikan manfaat tertentu sesuai dengan yang direncanakan.

Pengelolaan infrastruktur informasi adalah usaha yang dilakukan guna menjadikan infrastruktur yang ada menjadi lebih efisien dan bermanfaat bagi seluruh pemangku kepentingan, diantaranya adalah untuk mengurangi biaya, untuk menjadikan layanan organisasi selalu tersedia serta produktivitas selalu berjalan. Dengan pengelolaan infrastruktur informasi ini dapat meningkatkan berbagai pengetahuan dan pengalaman pengguna, mempermudah mengelola lingkungan TI, mengurangi risiko serta mempermudah memutuskan masalah TI dan dapat mencegah atau meminimalkan dampak bencana terhadap organisasi.

#### **Bidang Infrastruktur Informasi – Pusat Manajemen Informasi**

Bidang Infrastruktur Informasi telah menyusun tata kelola dalam melaksanakan operasional dan pengembangan infrastruktur, yang disusun berdasarkan pelaksanaan praktis dengan standar ISO 9001 sebagai framework kerja di PMI. Dalam perjalanan waktu ditambahkan dengan berbagai hal yang berusaha memenuhi aturan pemerintahan yang berlaku. Perbaikan atau penambahan tata kelola yang pernah terjadi adalah dalam rangka memenuhi Pemingkatan *e-Government* Indonesia (PeGI) dan memenuhi persyaratan Keamanan Informasi (KAMI).

Layanan Infrastruktur informasi adalah layanan yang diberikan baik untuk mendukung berbagai bentuk aplikasi yang ada di BPPT, juga untuk melancarkan komunikasi berbagai bentuk peralatan, serta mengikuti perencanaan dan tugas PMI.

Bentuk layanan dengan demikian terbentuk dalam jenis golongan besar sebagai berikut:

- a. Layanan di atas sistem Internet dan Intranet
- b. Layanan *email* dan sistem kolaborasi
- c. Layanan *cloud* dan sistem server lainnya
- d. Layanan *streaming* dan sistem komunikasi berbasis IP
- e. Layanan komunikasi khusus.

Jenis atau golongan besar layanan tersebut adalah dalam rangka menjadikan infrastruktur serta *resources* yang ada di BPPT dapat dioperasionalkan sebaik-baiknya, dan dengan biaya yang ada dapat melayani berbagai kebutuhan yang ada di BPPT.

Sistem infrastruktur yang terpasang ini diaplikasikan untuk melayani baik komunikasi yang ada di kantor BPPT maupun untuk mendukung terlaksananya *e-government* melalui teknologi informatika dan telekomunikasi yang telah berkembang saat ini. Implementasi operasional infrastruktur dengan demikian merupakan dasar penyelenggaraan *e-government*, yang berarti pula infrastruktur informasi ini harus bisa melayani kebutuhan yang saat ini demikian mulai banyak bermunculan berbagai aplikasi yang menggantikan sistem manual yang sudah ada, serta berbagai bentuk sistem komunikasi, *sharing* informasi, dan penggunaan berbagai macam sensor yang di implementasikan secara terus menerus.

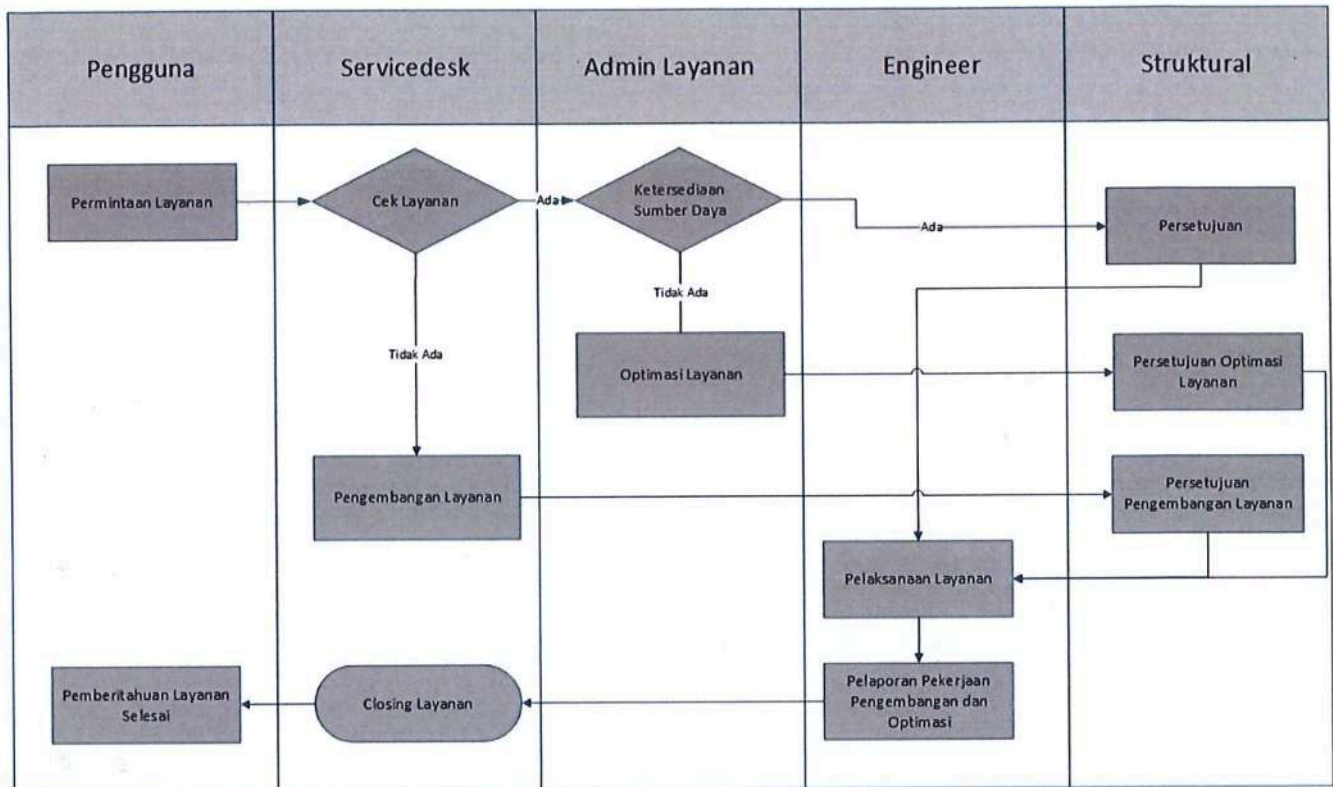
Dalam mengimplementasikan infrastruktur ini selain secara teknis harus mempunyai ketrampilan, juga dalam pelaksanaannya harus diatur dengan manajemen yang baik. Adapun implementasi operasional infrastruktur itu mempunyai ruang lingkup yang tersusun atas peralatan yang saling terkait satu sama lain, yang pada saat ini dapat diurut dalam tabel berikut.

### **Proses Bisnis Bidang Infrastruktur Informasi**

Agar proses bisnis dalam pengelolaan infrastruktur informasi dilakukan dengan konsep yang terkelola dengan baik maka harus disusun tata kelola yang mengacu pada *framework* yang diakui secara internasional, melengkapi acuan yang selama ini digunakan yaitu PeGI dan KAMI, yaitu dengan mengacu standar COBIT versi 5, serta pada level praktis dirujuk pula ITSM yaitu menggunakan ITIL versi 3.

Alasan penggunaan Standar COBIT dan ITIL adalah karena untuk dapat mengikuti terus perkembangan teknologi serta kemudahan implementasi pada masa mendatang, terutama untuk memudahkan audit, serta Sistem Infrastruktur bisa memberikan layanan sebaik baiknya, terukur serta dilaksanakan oleh Bidang Infrastruktur Informasi dalam tata kelola yang baik (*good governance*) dalam pengelolaan Infrastruktur Informasi.

Terimplementasinya *good governance* dalam Proses Bisnis di Bidang Infrastruktur Informasi dapat dilihat dari urutan proses pelaksanaan sebagai berikut:

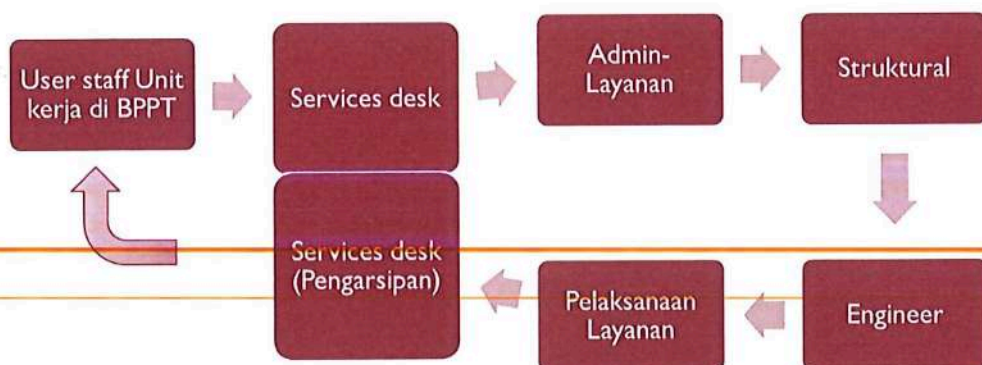


Gambar 3.1 Proses Bisnis BII dalam lingkup BPPT

Bidang Infrastruktur Informasi (BII) bertanggung jawab secara operasional dari Layanan Infrastruktur, sehingga fungsi infrastruktur untuk memenuhi kebutuhan dari sistem informasi di atasnya dapat terlaksana.

Sudut pandang proses bisnis ini dapat dibagi dua, yaitu:

- Proses pelaksanaan layanan infrastruktur yang diberikan ke pihak luar BII dan yang kedua dari sudut pandang pelaksanaan dan pengelolaan infrastruktur sehingga dapat memberikan layanan, proses ini kita sebut proses bisnis pengelolaan infrastruktur. Proses bisnis layanan infrastruktur mempunyai pintu tunggal yaitu *Service Desk*, proses ini mempunyai alur sebagai berikut:



Gambar 3.2 Diagram Proses Layanan Infrastruktur

- Proses bisnis pengelolaan infrastruktur kemudian lebih detail dapat dibagi menjadi proses pengembangan infrastruktur, yaitu dimulai dengan proses desain layanan dan

proses pembangunan layanan, proses instalasi dan *testing*. Ini disebut Pengembangan dan secara operasional dipertanggungjawabkan dan dilakukan oleh sub bidang pengembangan infrastruktur.

Adapun di sisi lainya adalah proses optimasi layanan, dimana sub bidang optimasi infrastruktur melakukan dan bertanggung jawab proses operasional dengan selalu melakukan optimasi layanan, yaitu melanjutkan proses *testing* pada transisi ke operasional, dimulai dari sosialisasi, penanganan operasional, perawatan, penanganan *evidence* dan *problem*, serta melakukan monitoring terus menerus. Layanan ditangani dengan pengertian bahwa proses operasional layanan tersebut berfungsi baik, mampu untuk membantu bagian atau bidang yang lain, sehingga dalam memproses aplikasi di atas infrastrukturnya juga berjalan baik.

Bidang Infrastruktur Informasi (BII) akan memenuhi fungsinya, bila proses *life cycle* manajemen infrastruktur berjalan baik, bisa melakukan monitoring dan melaksanakan evaluasi sesuai dengan jadwal waktu yang dibutuhkan, baik bulanan maupun triwulan, serta melakukan kontrol terhadap infrastruktur informasi dengan baik, dalam rangka untuk meningkatkan layanan serta menjamin kontinuitasnya.

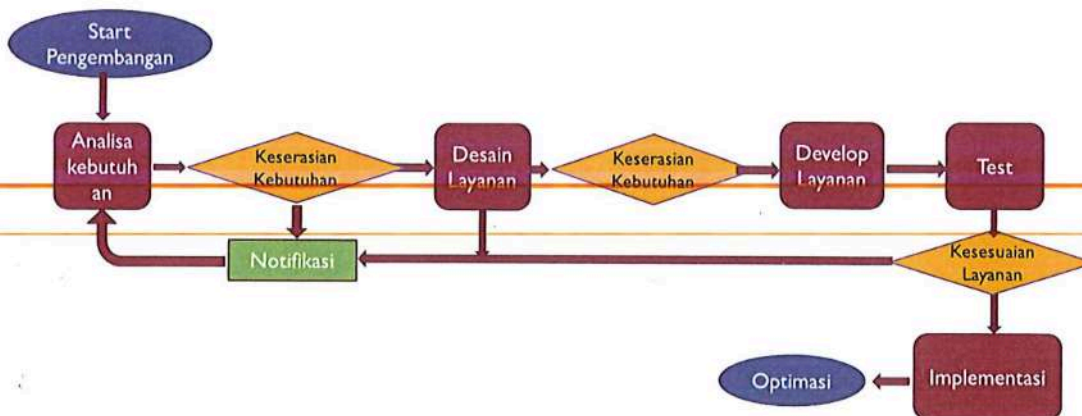
Sebagaimana yang tercantum dalam Renstra PMI, Bidang Infrastruktur Informasi mempunyai sasaran kegiatan untuk terpenuhinya kebutuhan infrastruktur dan layanan sistem untuk terlaksananya *e-government* BPPT. Dengan indikator kinerja kegiatan dalam tiga hal sebagai berikut:

1. Tersedianya infrastruktur yang aman, handal dan kapasitas yang cukup sesuai kriteria PeGI;
2. Tersedianya layanan infrastruktur yang cepat, efektif, dan nyaman sesuai kriteria penilaian PeGI;
3. Tersedianya kebijakan Bidang TIK BPPT.

Untuk merealisasikan hal tersebut maka proses bisnis pengelolaan infrastruktur di Bidang Infrastruktur Informasi (BII) disusun proses bisnis sebagai berikut:

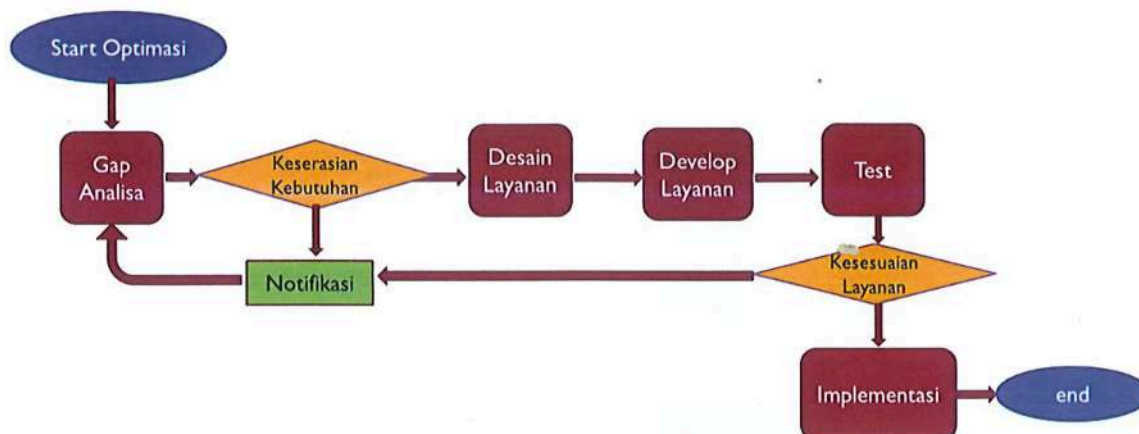
1. Proses bisnis pengembangan infrastruktur yang dilakukan oleh sub bidang pengembangan infrastruktur.

Proses ini dimulai dari analisa kebutuhan layanan yang ingin dibuat atau dikembangkan dan diakhiri sampai selesainya *testing* layanan untuk siap di implementasikan.



Gambar 3.3 Proses Bisnis Pengembangan Infrastruktur

## 2 Proses bisnis optimasi infrastruktur yang dilakukan oleh sub bidang optimasi infrastruktur



Gambar 3.4 Proses Bisnis Optimasi Infrastruktur

## 3 Monitoring dan evaluasi

Proses monitoring dan evaluasi adalah proses yang dilakukan Bidang Infrastruktur Informasi dalam rangka menjaga kontinuitas layanan dan meningkatkan layanan serta keadaan dari keamanan, kehandalan, kapasitas infrastruktur, serta kecepatan dan efektifitas serta kenyamanan layanan.

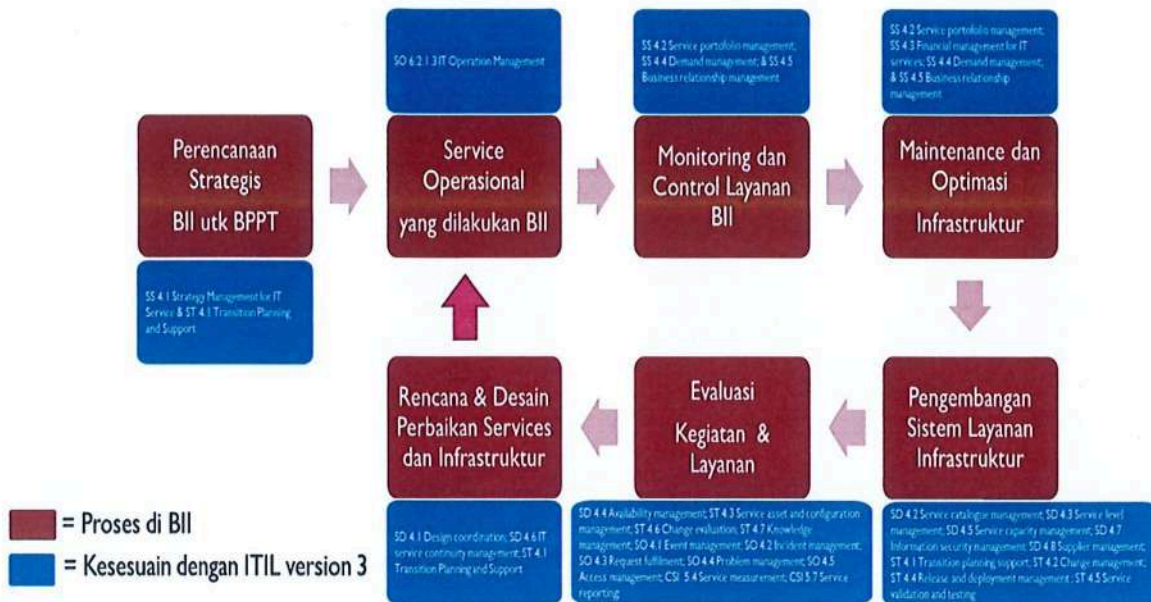
Monitoring dibantu dengan peralatan atau *tools* monitoring baik bersifat otomatis maupun manual. Hasil monitoring ini dilaporkan baik tertulis maupun lisan dilakukan agar kondisi yang ada diketahui dan dipakai sebagai input kebijakan atau tindakan yang harus dilakukan dalam pengelolaan infrastruktur tersebut.

Sedangkan untuk evaluasi diperlukan data dan sistem analisis lebih lanjut, sesuai dengan layanan dan objek yang menjadi perhatian untuk dievaluasi. Luasnya ruang lingkup disesuaikan dengan cakupan laporan yang diinginkan.

Untuk melaksanakan perbaikan proses bisnis tersebut di atas perlu tata kelola yang tersusun dengan baik. Dalam rangka perbaikan tata kelola ini diperlukan referensi dan *framework* yang tepat agar tercapai peningkatan sistem tata kelola itu sendiri maupun peningkatan kualitas layanan infrastruktur yang ada. Sebagai arahan kebijakan, maka diputuskan mengadopsi COBIT versi 5 untuk dipakai sebagai *framework* dalam menyusun tata kelola pada level atas atau level kebijakan, dimana untuk mencapai keamanan, kehandalan, dan kapasitas dari infrastruktur informasi diperlukan sebagian dari komponen BAI seperti BAI-04, BAI-09 dan BAI-10. Sedangkan dalam operasionalnya diperlukan berbagai bagian di seluruh DSS dari COBIT versi 5.

Adapun dalam level praktis, penyusunan tata kelola dipersiapkan pula sebagai *framework* ITILv3 yang dalam hal ini dapat membantu perbaikan sistem layanan dapat lebih bisa dipastikan pelaksanaan akan membantu untuk peningkatannya.

Dalam menyusun pengembangan tata kelola di BII ini maka sebagai arahan selanjutnya dapat diputuskan untuk dapat melengkapinya sesuai diagram berikut.



Gambar 3.5 Bagian Perencanaan Adopsi ITIL untuk Perbaikan

### CSIRT (*Computer Security Incident Response Team*) BPPT

CERT (*Computer Emergency Response Team*) merupakan tim koordinasi teknis terkait insiden jaringan internet di seluruh dunia. Belakangan tim ini disempurnakan lagi melalui RFC 2350 dengan nama CSIRT (*Computer Security Incident Response Team*). CERT/CSIRT yang dibangun memiliki ruang lingkup yang terbatas untuk kalangan tertutup, seperti GovCSIRT (Institusi Pemerintah) dan lain sebagainya.

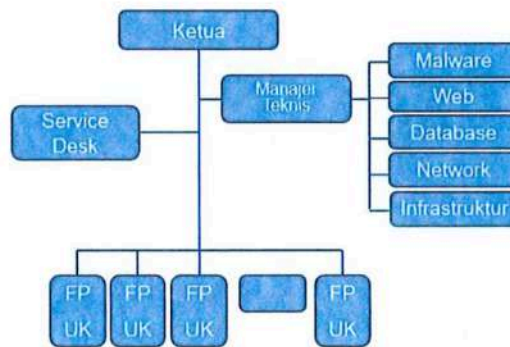
GovCSIRT merupakan tim koordinasi teknis terkait insiden jaringan internet dengan ruang lingkup terbatas untuk kalangan tertutup yang dibangun oleh institusi-institusi pemerintah. GovCSIRT di Indonesia diluncurkan pertama kali oleh Direktorat Keamanan Informasi (Subdit Monitoring, Evaluasi dan Tanggap Darurat) Kementerian Komunikasi dan Informatika berdasarkan Surat Keputusan Direktorat Jenderal Aplikasi Informatika Nomor: 01/SK/DJAI/KOMINFO/01/2012, tanggal 17 September 2012 di Jakarta. Ditandai dengan launchingnya website resmi CSIRT ([insting.kominfo.go.id](http://insting.kominfo.go.id)) kemudian berubah nama domain menjadi [govcsirt.kominfo.go.id](http://govcsirt.kominfo.go.id).

CSIRT BPPT atau *Government Computer Security Incident Respon Team* adalah merupakan suatu tim yang dibentuk BPPT dalam rangka melakukan respon atas berbagai permasalahan dalam bidang teknologi informasi, terutama dalam menangani masalah keamanannya. Keamanan informasi adalah suatu bagian yang sangat penting untuk mendapatkan perhatian khusus mengingat pentingnya dan berharganya informasi di BPPT. Adanya CSIRT ini adalah dalam rangka mewedahi serta mengatur suatu cara penanganan berbagai insiden di bidang teknologi informasi agar masalah yang terjadi di BPPT dalam bidang ini dapat diselesaikan secara cepat, tepat serta bisa melaksanakan dengan baik dalam rangka pengamanan informasi.

CSIRT BPPT dibentuk mengingat lokasi sebaran pengelolaan teknologi informasi BPPT demikian luas, sehingga perlu membangun institusi yang baik, mempunyai daya jangkauan luas namun

tetap efektif. Bentuk institusi CSIRT ini adalah sebuah kesatuan penanganan teknologi informasi yang anggotanya adalah personil yang kompeten dan berpengalaman dalam bidang teknologi informasi, mampu menangani masalah yang dihadapi dalam bidang ini, serta membentuk suatu kelompok yang saling bantu membantu untuk melakukan perbaikan sistem dan pengamanan informasi di BPPT.

## Struktur Organisasi



BPPT CSIRT

Gambar 3.6 Struktur organisasi CSIRT

### Konsep Dasar Infrastruktur Informasi BPPT

Bidang Infrastruktur Informasi bertanggung jawab secara operasional agar fungsi infrastruktur bisa terlaksana, maka dalam memberikan layanan infrastruktur informasi perlu disusun Perencanaan Struktur – Arsitektur Infrastruktur yang bisa menjangkau seluruh kebutuhan perencanaan infrastruktur di BPPT. Struktur – Arsitektur Infrastruktur yang dimaksudkan disini terbagi pada empat bentuk yang digolongkan menjadi:

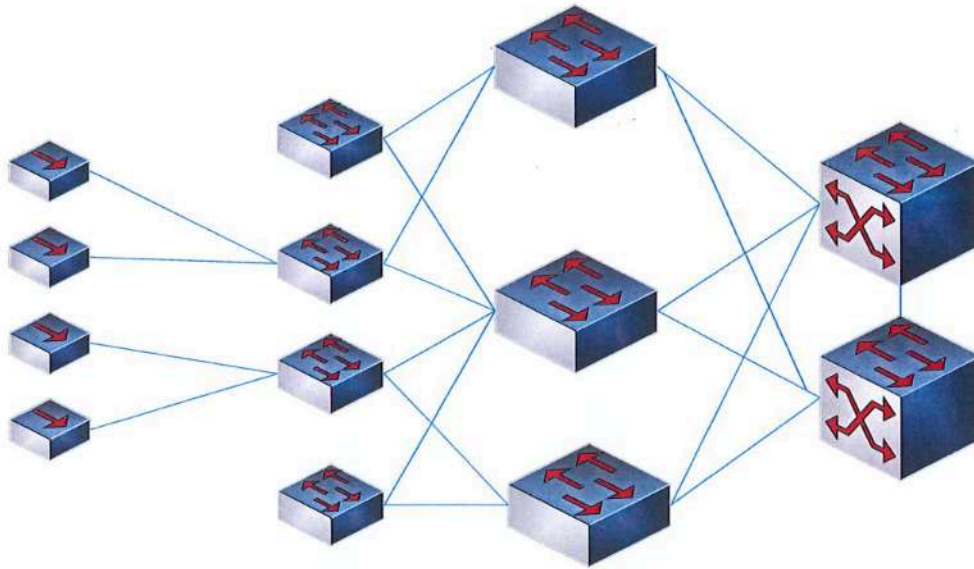
- 1) Arsitektur *Backbone*
- 2) Arsitektur *Data Center*
- 3) Arsitektur LAN (*Local Area Network*)
- 4) Arsitektur WLAN (*Wireless Local Area Network*)

#### 1. Arsitektur *Backbone*

*Backbone* adalah jaringan pokok atau jaringan utama yang terdiri dari jalur saluran *fiber optic* dan sistem *switch* yang direncanakan berdasarkan lokasi dan struktur gedung, maka sesuai keadaan dibagi dalam Sistem Gedung Bertingkat, Sistem *Cluster* dan WAN.

##### a. Sistem gedung bertingkat

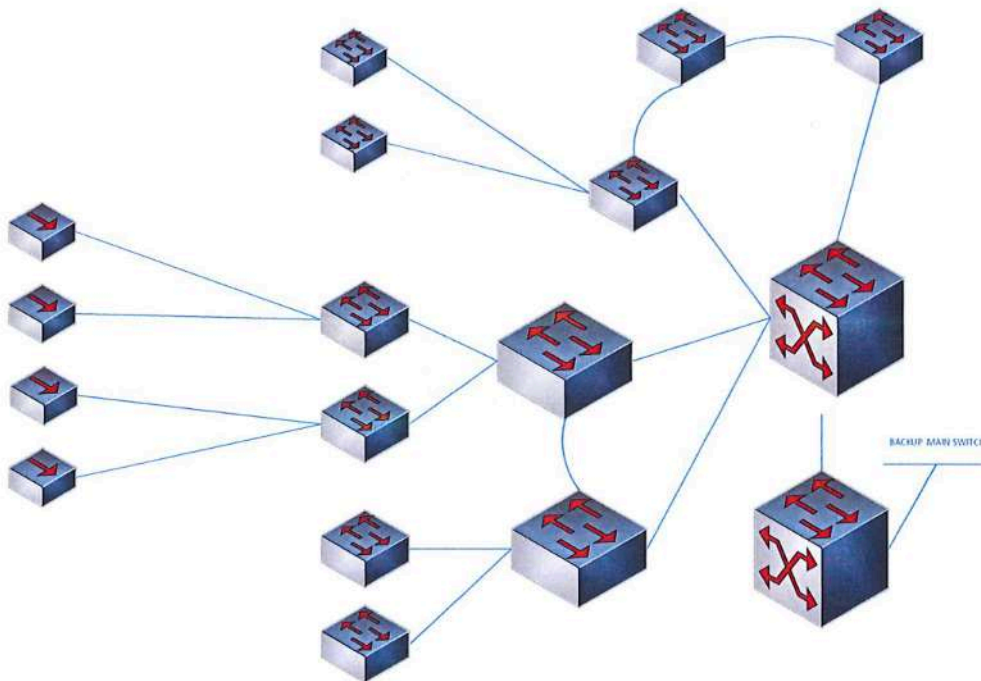
Sistem ini untuk gedung bertingkat seperti di kawasan perkantoran BPPT Jl. M.H. Thamrin Jakarta.



Gambar 3.7 Tipikal Jaringan di Gedung Bertingkat

**b. Sistem cluster**

Sistem ini untuk gedung yang tersebar seperti di Kawasan Puspiptek Serpong.



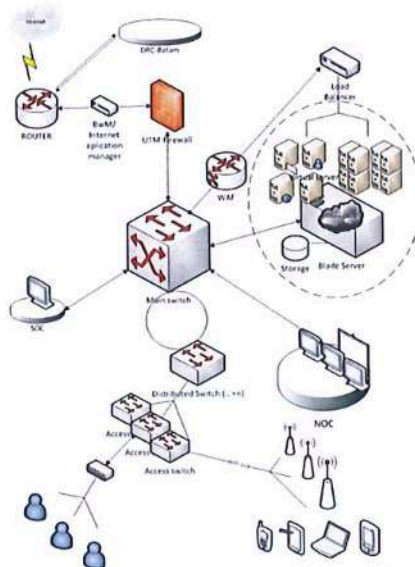
Gambar 3.8 Tipikal Jaringan di Gedung Sistem Cluster

**c. Sistem WAN**

Sistem ini diaplikasikan untuk komunikasi dengan Kantor BPPT yang berada di luar kota dan berjauhan dengan Jakarta. Implementasinya adalah dengan penggunaan internet ditambah dengan sistem sekuriti khusus.

## 2. Arsitektur Data Center

Sistem *Data Center* direncanakan untuk dibangun dengan sistem keamanan yang tinggi, dengan sistem *Cloud* sehingga bisa melayani secara **laaS**.



Gambar 3.9 Arsitektur Sistem Keamanan di Data Center

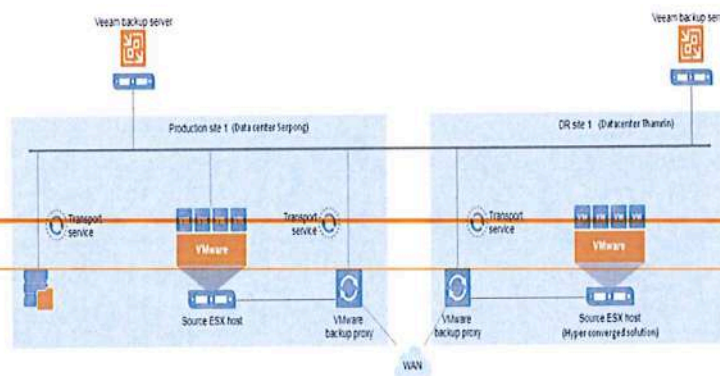
Arsitektur ini merupakan *High Level Design*, yang menggambarkan peralatan yang dipasang agar tercapai suatu infrastruktur yang cukup handal, *available* dan aman. Rangkaian sistem ini terpasang dengan prinsip penggunaan sistem *Cloud* serta dilengkapi sistem *Backup*.

### Arsitektur Sistem Backup

Untuk BPPT agar Sistem Informasi dengan aman maka sistem *Backup* digunakan tergambar sebagai berikut:

#### a. Backup server dan data

*Backup* ini mempunyai arsitektur desain dasar diantara *Data Center* dan DRC sebagai berikut.



Gambar 3.4 Arsitektur Desain Dasar Backup DC-DRC

Dari rancangan *backup* di atas, main *data center* berada di Serpong dan DR atau *Disaster Recovery site* berada di Thamrin. Pada site thamrin digunakan sistem *Hyperconverged solution*.

#### b. Backup Sistem Backbone Network

*Backup* ini bertujuan agar sistem beroperasi secara *high availability* dimana sistem sistem utama seharusnya mempunyai *backup* peralatan, yang siap bekerja 24x7, untuk itu selalu dijaga dan siap dengan kemudahan sistem *switch* yang cepat sesuai kebutuhan BPPT.

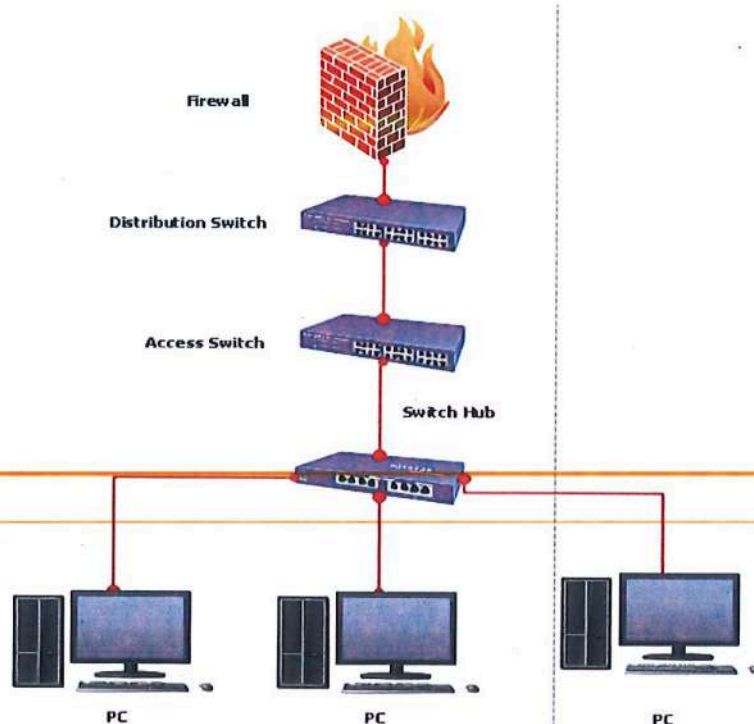
#### c. Backup Fasilitas

*Backup* ini meliputi berbagai fasilitas utama, yang amat penting, diantaranya *Power Listrik* dan *Air Conditioning*, kedua hal ini secara sistem perlu desain yang mampu untuk bisa bekerja terus menerus, sehingga *backup* diperlukan untuk kedua fasilitas ini.

Untuk melaksanakan *backup* fasilitas ini kemungkinan perlu koordinasi yang erat dengan Biro Umum - BPPT sebagai pemegang otoritas pelayanan fasilitas itu sehingga mendapatkan pelayanan khusus.

### 3. Arsitektur LAN (Local Area Network)

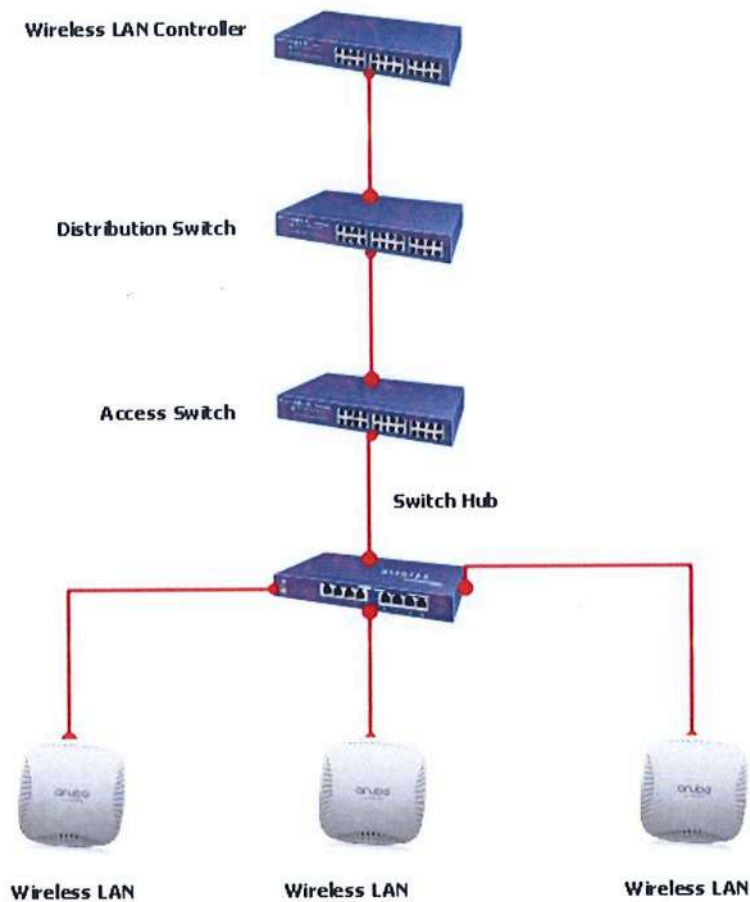
LAN (*Local Area Network*) mempunyai arsitektur yang mengarah pada layanan langsung ke *user/pengguna* sehingga akses *user* terkelola dengan baik. Untuk memastikan posisi *user* dalam sistem, *control access*, penggunaan dan layanan yang diberikan sesuai dengan kebutuhan *user*. Secara struktur LAN disusun sebagai gambar 3.11 di bawah, dengan level *user* terdapat beberapa tingkatan penggunaan, seperti penggunaan *user* biasa, penggunaan *user* dengan spesifikasi khusus.



Gambar 3.11 Arsitektur LAN

#### 4. Arsitektur WLAN (*Wireless Local Area Network*)

WLAN atau *Wireless LAN* adalah sistem LAN yang komunikasinya lebih *mobile*, mudah bergerak, sehingga sistem akses dan layanan yang ada di dalamnya terdapat memerlukan kontrol yang berbeda dengan sistem LAN biasa. WLAN direncanakan untuk dapat melayani sebanyak mungkin user, dengan control yang terpusat, yaitu dengan *Wireless LAN Controller*. Disamping itu, area layanan juga harus terkontrol atau mempunyai batasan tertentu agar tidak terlalu menyebar sehingga digunakan oleh yang tidak berhak. Struktur WLAN yang terpasang di BPPT tergambar sebagai gambar 3.12 berikut:



Gambar 3.5 Arsitektur WLAN

Untuk itu dalam perancangannya perlu digunakan beberapa peralatan yang dengan mudah dan presisi untuk mengetahui daya pancar dan penerimaan *access point* (AP), sehingga pancaran/penerimaan terlokalisasi.



## BAB IV

### STRATEGI LAYANAN (*SERVICE STRATEGY*)

Pembahasan *service strategy* dimaksudkan untuk menjelaskan secara praktis, bahwa pelaksanaan tata kelola atau *governance* membutuhkan strategi, mulai dari awal perencanaan, hingga penerapan, kebutuhan referensi dan *framework*, menyusunnya dalam kaidah yang mudah, serta bagaimana layanan itu hingga dapat diberikan secara nyata adalah proses yang membutuhkan strategi.

Mengingat BII relatif lebih mengutamakan agar bisa memberikan layanan dasar dari TI, maka dalam *service strategy* ini bentuk layanan dasar TI itu terlihat sangat jelas, atau jenis layanannya sudah dapat dipastikan kebutuhannya, seperti jaringan intranet dan jaringan internet, server, *storage*, *e-mail* dan seterusnya. Maka strategi layanan selanjutnya adalah bagaimana layanan itu selalu dapat ditingkatkan, baik *availabilitas*, kapasitas, aksesibilitas dan berbagai parameter lainnya. Namun demikian tetap tidak memungkiri adanya layanan baru sehingga dalam membangun layanan baru itu diperlukan strategi dari awal.

#### **Strategi Penerapan Tata Kelola Teknologi Informasi**

Penerapan tata kelola teknologi informasi selama ini telah dilakukan sesuai dengan arahan serta mengikuti peraturan yang berlaku, serta berusaha untuk dapat memenuhi kriteria PeGI. Bidang Infrastruktur Informasi sesuai tugas dan fungsinya mempunyai langkah-langkah untuk terpenuhinya kebutuhan infrastruktur dan layanan teknologi informasi sehingga terlaksananya *e-government* BPPT.

Dalam melaksanakan tata kelola teknologi informasi, ternyata dengan semakin meningkatnya kebutuhan serta kompleksitas infrastruktur yang ditangani, maka pelaksanaannya memerlukan *framework* tata kelola yang lebih baik dan lebih teratur untuk bisa lebih terarah serta mudah terkontrol serta secara praktis bisa dilaksanakan sesuai dengan keadaan saat ini.

Dalam rangka membentuk tata kelola yang baik tersebut, diperlukan strategi yang tepat untuk menjadikan hasil yang baik, mulai dari pemilihan *framework* tata kelola serta untuk kemudahan proses penerapannya. Sebagaimana diketahui dalam lingkungan organisasi besar seperti BPPT, pengelolaan TI tersebar serta belum adanya keteraturan, yang bisa menjangkau seluruh organisasi, maka pelaksanaan tata kelola akan berat bila tidak memiliki strategi yang tepat.

Untuk infrastruktur informasi disiapkan suatu strategi penerapan tata kelola terutama untuk dapat dilaksanakan di internal Bidang Infrastruktur Informasi (BII) serta menyebar berpengaruh di seluruh lingkungan BPPT.

Starategi pertama adalah memilih *framework* yang sesuai dan mampu dilaksanakan di BPPT. *Framework* ini lebih umum menyeluruh serta mendefinisikan kontrol yang teratur, kemudian menganalisis kecocokan dengan lingkungan serta kebutuhan yang ada di BII dan BPPT. Kedua perlu pula memilih suatu *framework* yang mudah diPraktikkan, ada *tools* yang sudah siap diimplementasi serta memberi kemudahan praktis dalam melaksanakannya. Atas hasil kajian dan analisis tersebut, dibuat pemilihan *framework* dan arahan kebijakan, maka diputuskan

mengadopsi COBIT versi 5 untuk dipakai sebagai *framework* dalam rangka mendapatkan pokok-pokok kontrol dalam menyusun tata kelola pada level tertentu atau level kebijakan, dimana untuk mencapai keamanan, kehandalan dan kapasitas dari infrastruktur informasi diperlukan kontrol dari COBIT versi 5.

Misalkan pada BII dibutuhkan kontrol di sebagian dari komponen BAI seperti BAI-04, BAI-09 dan BAI-10, maka pada problematika itu untuk diperhatikan kontrol dan tujuan pengaturannya, kemudian disusun aturan atau SOP (*Standard Operational Procedure*) yang dibutuhkan. Sedangkan, dalam operasionalnya diperlukan berbagai bagian pada keseluruhan DSS dari COBIT versi 5. Maka berbagai kontrol untuk operasionalnya diperhatikan, dihubungkan dengan faktor yang telah ditentukan dalam BAI serta disesuaikan dengan Praktik kerja yang ada di BPPT, dimana ada level struktural serta pekerjaan perekayasaan.

Adapun untuk dapat dilaksanakan dalam level praktis, penyusunan tata kelola dipersiapkan pula dengan derajat kepraktisan yang lebih baik yaitu dengan *framework* ITIL v3. *Framework* ini diambil agar dapat membantu lingkup cakupan tata kelola serta perbaikan tata kelola dari sistem layanan yang diberikan. Penyusunan organisasi, pemenuhan personil serta kompetensinya, sehingga dapat lebih bisa dipastikan pelaksanaan kesehariannya akan membantu untuk selalu terjadi peningkatannya.

## Referensi *Framework* COBIT dan ITIL

### 1. *Control Objectives for Information and related Technology* (COBIT)

COBIT adalah suatu panduan standar Praktik manajemen teknologi informasi dan sekumpulan dokumentasi *best practices* untuk tata kelola TI yang dapat membantu auditor, manajemen dan pengguna untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan pengendalian dan permasalahan-permasalahan teknis. COBIT dikembangkan oleh *IT Governance Institute* (ITGI), yang merupakan bagian dari *Information Systems Audit and Control Association* (ISACA). COBIT memberikan arahan (*guidelines*) yang berorientasi pada bisnis, dan karena itu *business process owners* dan manajer, termasuk juga auditor dan pengguna, diharapkan dapat memanfaatkan arahan ini dengan sebaik-baiknya.

COBIT merupakan suatu cara untuk menerapkan tata kelola TI. COBIT berupa kerangka kerja yang digunakan oleh suatu organisasi bersamaan dengan sumberdaya lainnya untuk membentuk suatu standar yang umum berupa panduan pada lingkungan yang lebih spesifik. Secara terstruktur, COBIT terdiri dari seperangkat *control objectives* untuk bidang teknologi informasi, dirancang untuk memudahkan tahapan-tahapan audit bagi auditor. Kelebihan COBIT adalah adanya pemisahan tata kelola dari manajemen.

Kerangka COBIT 5 memuat suatu perbedaan yang jelas antara tata kelola dan manajemen. Dua disiplin yang berbeda ini juga meliputi aktivitas yang berbeda, memerlukan struktur organisasi yang berbeda dan melayani tujuan yang berbeda pula. Kunci perbedaan antara tata kelola dan manajemen menurut COBIT 5 adalah:

- Tata kelola menjamin kebutuhan *stakeholder*, kondisi-kondisi, dan pilihan-pilihan selalu dievaluasi untuk menentukan tujuan organisasi yang seimbang dan disepakati untuk dicapai, menentukan arah melalui penentuan prioritas dan pengambilan keputusan, dan

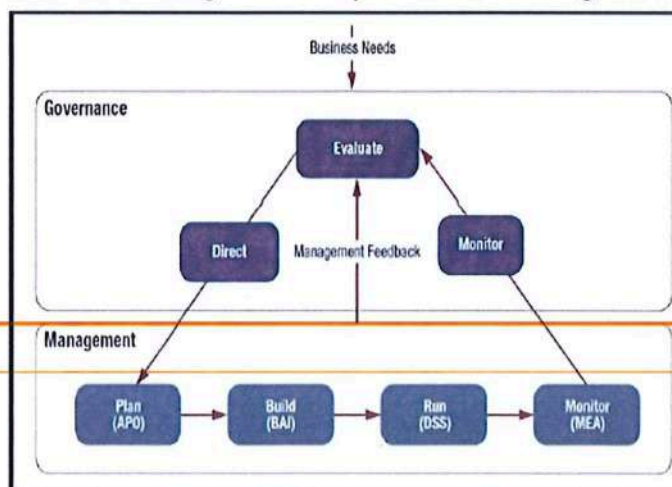
memantau pemenuhan unjuk kerja terhadap tujuan dan arah yang disepakati. Pada kebanyakan organisasi, tata kelola secara menyeluruh adalah tanggung jawab para eksekutif di bawah pimpinan seorang *chair person*. Tanggung jawab tata kelola yang lebih spesifik dapat didelegasikan kepada sebuah struktur organisasi khusus pada sebuah tingkatan yang lebih memerlukannya, biasanya pada organisasi yang besar dan kompleks.

- o Manajemen bertugas untuk merencanakan, membangun, menjalankan dan memantau aktivitas dalam rangka penyelarasan dengan arah organisasi yang telah ditentukan oleh badan pengelola (tata kelola), untuk mencapai tujuan perusahaan. Pada kebanyakan organisasi, manajemen adalah tanggung jawab manajemen eksekutif di bawah pimpinan seorang CEO.

Model referensi proses dalam COBIT 5 membagi proses tata kelola dan manajemen TI organisasi menjadi dua domain proses utama, yaitu:

1. Tata kelola, memuat lima proses tata kelola, dimana akan ditentukan praktik- praktik dalam setiap proses *Evaluate*, *Direct*, dan *Monitor* (EDM).
2. Manajemen, memuat empat domain, sejajar dengan area tanggung jawab dari *Plan*, *Build*, *Run* and *Monitor* (PBRM), dan menyediakan ruang lingkup TI yang menyeluruh dari ujung ke ujung. Domain ini merupakan evolusi dari domain dan struktur proses dalam COBIT 4.1., yang terdiri dari :
  - a. *Align, Plan, and Organize* (APO) – Penyelarasan, Perencanaan, dan Pengaturan.
  - b. *Build, Acquire, and Implement* (BAI) – Membangun, Memperoleh, dan Mengimplementasikan.
  - c. *Deliver, Service and Support* (DSS) – Mengirimkan, Layanan, dan Dukungan.
  - d. *Monitor, Evaluate, and Assess* (MEA) – Pengawasan, Evaluasi, dan Penilaian.

Model proses referensi dalam COBIT 5 adalah suksesor dari model proses COBIT 4.1, dengan mengintegrasikan model proses dari *Risk IT* dan *Val IT*. Secara total ada 37 proses tata kelola dan manajemen dalam COBIT 5 sebagaimana dapat dilihat dalam gambar berikut:



Gambar 4.6 Pemisahan Governance (Tata kelola) dan Management (Manajemen)  
 Sumber: COBIT 5 *governance and management keys areas*, Isaca-COBIT 5 *Framework A Business Framework for the Governance and Management of Enterprise IT*-Isaca (2012)

## Pemisahan Tata Kelola Dari Manajemen

Kerangka COBIT 5 memuat suatu perbedaan yang jelas antara tata kelola dan manajemen. Dua disiplin yang berbeda ini juga meliputi aktivitas yang berbeda, memerlukan struktur organisasi yang berbeda dan melayani tujuan yang berbeda pula. Kunci perbedaan antara tata kelola dan manajemen menurut COBIT 5 adalah:

**Tata kelola** menjamin kebutuhan *stakeholder*, kondisi-kondisi, dan pilihan-pilihan selalu dievaluasi untuk menentukan tujuan organisasi yang seimbang dan disepakati untuk dicapai, menentukan arah melalui penentuan prioritas dan pengambilan keputusan, dan memantau pemenuhan unjuk kerja terhadap tujuan dan arah yang disepakati. Pada kebanyakan organisasi, tata kelola secara menyeluruh adalah tanggung jawab para direksi di bawah pimpinan seorang *chair person*. Tanggung jawab tata kelola yang lebih spesifik dapat didelegasikan kepada sebuah struktur organisasi khusus pada sebuah tingkatan yang lebih memerlukannya, biasanya pada organisasi yang besar dan kompleks.

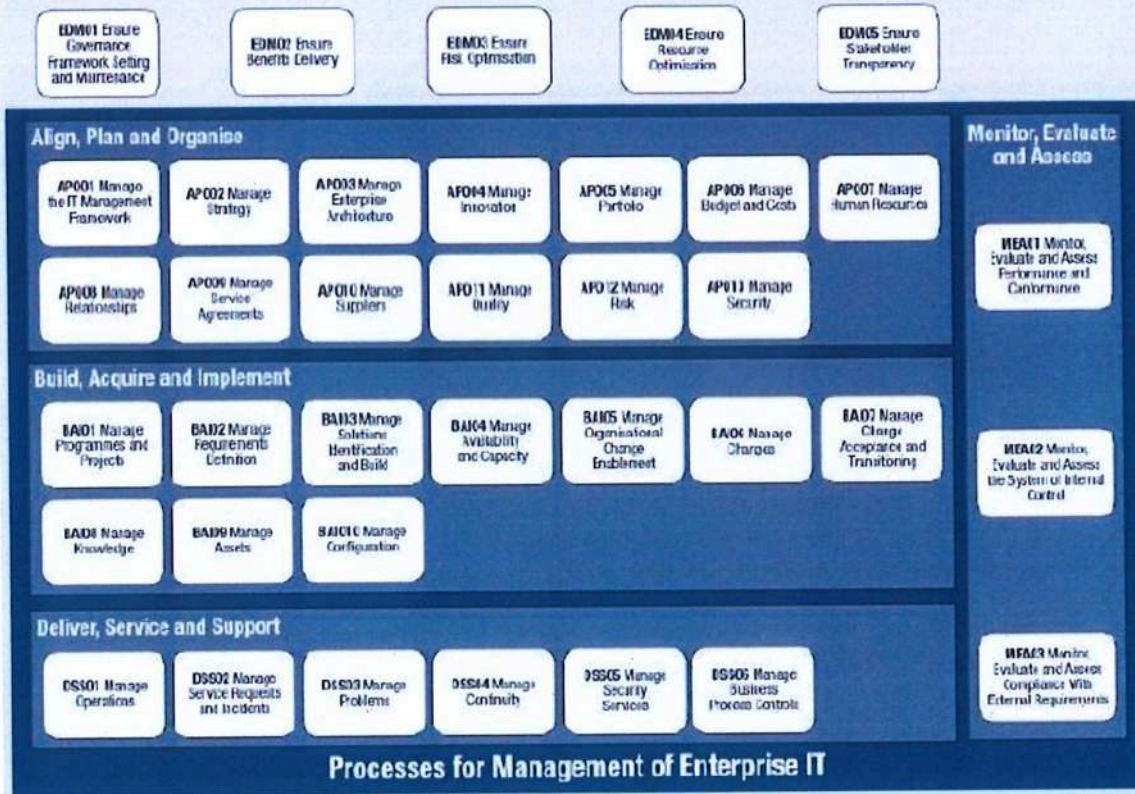
**Manajemen** bertugas untuk merencanakan, membangun, menjalankan, dan memantau aktivitas dalam rangka penyelarasan dengan arah organisasi yang telah ditentukan oleh badan pengelola (tata kelola), untuk mencapai tujuan organisasi. Pada kebanyakan perusahaan, manajemen adalah tanggung jawab manajemen eksekutif di bawah pimpinan seorang CEO.

Berdasarkan definisi tata kelola dan manajemen, jelas terlihat bahwa keduanya meliputi aktivitas-aktivitas yang berbeda dengan tanggung jawab yang berbeda. Bagaimanapun juga, berdasarkan peranan tata kelola untuk mengevaluasi, mengarahkan, dan memantau diperlukan suatu interaksi antara tata kelola dan manajemen untuk menghasilkan sistem tata kelola yang efektif dan efisien.

Model proses referensi dalam COBIT 5 adalah suksesor dari model proses COBIT 4.1, dengan mengintegrasikan model proses dari *Risk IT* dan *Val IT*. Secara total ada 37 proses tata kelola dan manajemen dalam COBIT 5 sebagaimana dapat dilihat dalam gambar 4.2.

## Processes for Governance of Enterprise IT

### Evaluate, Direct and Monitor



Gambar 4.2 Proses yang terdiri dari 37 item

Sumber: COBIT 5 *Process Reference Model*, Isaca-COBIT 5 *Framework A Business Framework for the Governance and Management of Enterprise IT*-Isaca (2012)

### Information Technology Infrastructure Library (ITIL)

ITIL adalah suatu rangkaian konsep dan teknik pengelolaan infrastruktur, pengembangan, serta operasi teknologi informasi (TI). ITIL diterbitkan dalam suatu rangkaian buku yang masing-masing membahas suatu topik pengelolaan TI. Nama ITIL dan *IT Infrastructure Library* merupakan merek dagang terdaftar dari *Office of Government Commerce* (OGC) Britania Raya. ITIL memberikan deskripsi detail tentang beberapa praktik TI penting dengan daftar pemeriksaan, tugas, serta prosedur yang menyeluruh yang dapat disesuaikan dengan segala jenis organisasi TI.

Walaupun dikembangkan sejak dasawarsa 1980-an, penggunaan ITIL baru meluas pada pertengahan 1990-an dengan spesifikasi versi keduanya (ITIL v2) yang paling dikenal dengan dua set bukunya yang berhubungan dengan ITSM (*IT Service Management*), yaitu *Service Delivery* (Antar Layanan) dan *Service Support* (Dukungan Layanan).

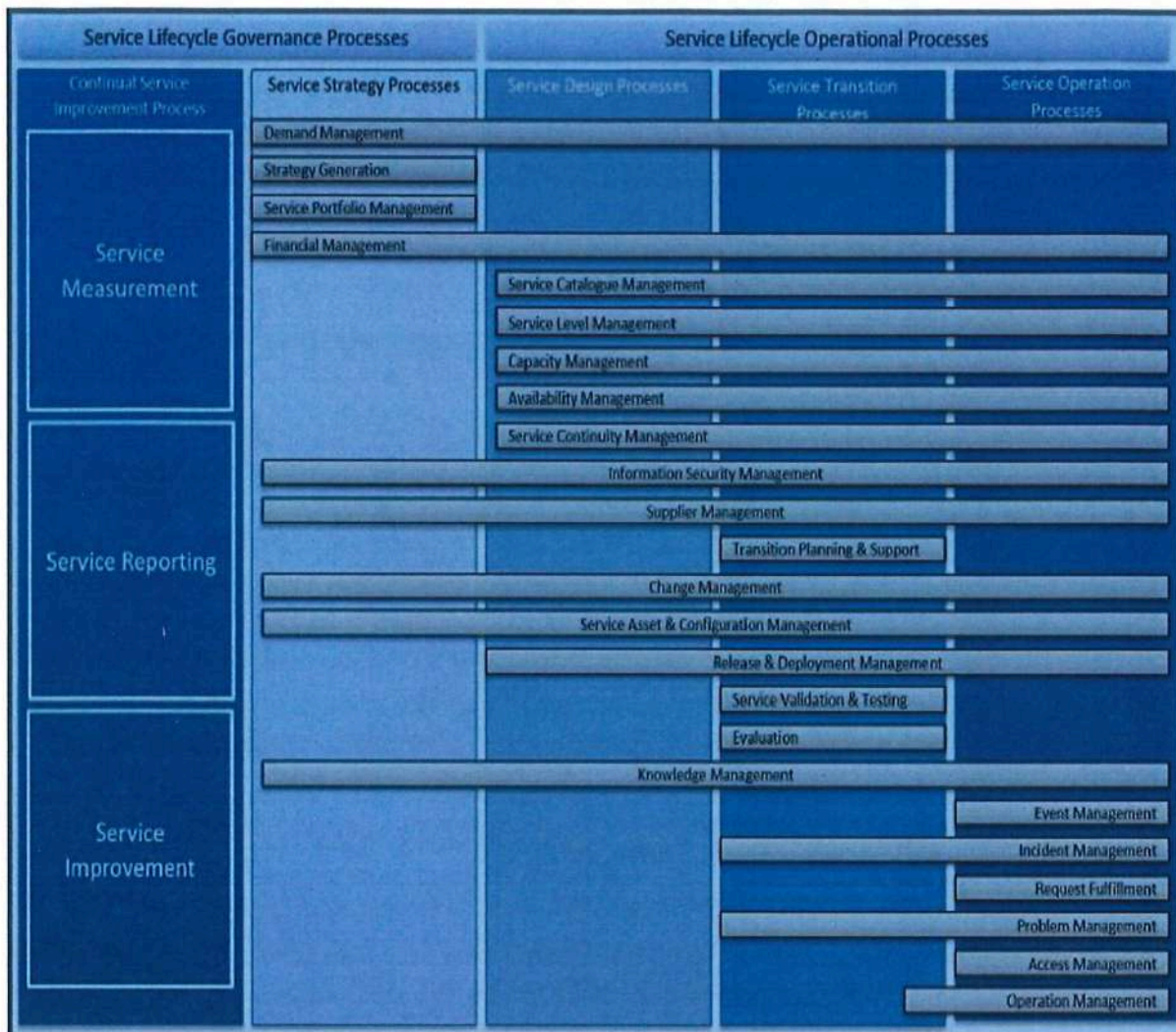


Gambar 4.3 Lima Bagian ITIL

Sumber: Kajian Pengembangan Tata Kelola Infrastruktur TIK BPPT berdasarkan COBIT 5, 2017

Pada 30 Juni 2007, OGC menerbitkan versi ketiga ITIL (ITIL v3) yang intinya terdiri dari lima bagian dan lebih menekankan pada pengelolaan siklus hidup layanan yang disediakan oleh teknologi informasi. Kelima bagian tersebut adalah:

1. *Service Strategy*
2. *Service Design*
3. *Service Transition*
4. *Service Operation*
5. *Continual Service Improvement*



Gambar 4.4 Gambar Lengkap Siklus Hidup Layanan

Sumber: Kajian Pengembangan Tata Kelola Infrastruktur TIK BPPT berdasarkan COBIT 5, 2017, *Business Procees Framework –ITIL Service Process Lansscape*

### 1. Pemetaan COBIT 5 Ke ITIL v3

Secara keseluruhan, pada pelaksanaannya, organisasi tidak harus memilih hanya satu kerangka karena ternyata COBIT dan ITIL saling melengkapi satu sama lain. Misalnya COBIT, dimana di dalam COBIT yang sering menjelaskan "mengapa" sesuatu dilakukan atau diperlukan, dan dimana ITIL menyediakan "bagaimana" hal tersebut dilaksanakan. Beberapa organisasi telah menggunakan COBIT dan COSO, bersama dengan standar ISO 27001 (untuk mengelola keamanan informasi).

Dua kerangka yang paling banyak digunakan adalah COBIT dan ITIL. COBIT sering digambarkan sebagai sistem manajemen yang menyediakan "mengapa", sementara ITIL dikatakan untuk memberikan "bagaimana".

## 2. Alasan Diperlukannya Penggunaan Dua *Framework*

COBIT merupakan suatu cara untuk menerapkan tata kelola TI. Berupa kerangka kerja yang digunakan oleh suatu organisasi bersamaan dengan sumber daya lainnya untuk membentuk suatu standar yang umum berupa panduan pada lingkungan yang lebih spesifik. Secara terstruktur, COBIT terdiri dari seperangkat *control objectives* untuk bidang Teknologi Informasi, dirancang untuk memudahkan tahapan-tahapan audit bagi auditor.



Gambar 4.5 Lima Prinsip COBIT

Dalam COBIT 5 terdapat suatu model referensi proses yang menentukan dan menjelaskan secara detail mengenai proses tata kelola dan manajemen. Model tersebut mewakili semua proses yang biasa ditemukan dalam perusahaan yang berhubungan dengan aktivitas TI, serta menyediakan model sebagai referensi yang mudah dipahami dalam operasional TI dan oleh manajer bisnis. Model proses yang diberikan merupakan suatu model yang lengkap dan menyeluruh, tapi bukan merupakan satu-satunya model proses yang bisa digunakan. Setiap perusahaan harus menentukan rangkaian prosesnya sendiri sesuai dengan situasinya yang spesifik.

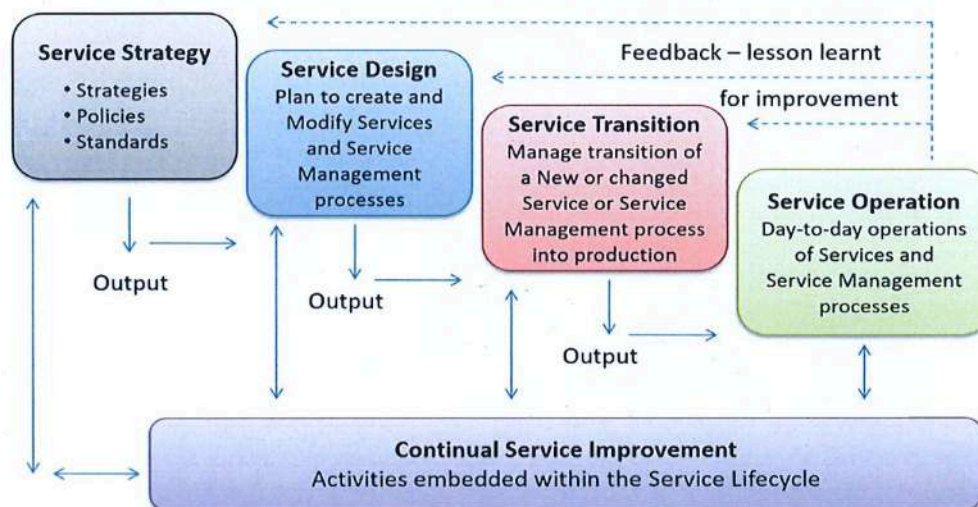
**Framework ITIL** (*Information Technology Infrastructure Library*) adalah suatu rangkaian konsep dan teknik pengelolaan infrastruktur, pengembangan, serta operasi teknologi informasi (TI). ITIL diterbitkan dalam suatu rangkaian buku yang masing-masing membahas suatu topik pengelolaan TI. Penggunaan ITIL baru meluas pada pertengahan 1990-an dengan spesifikasi versi keduanya (ITIL v2) yang paling dikenal dengan dua set bukunya yang berhubungan dengan ITSM (*IT Service Management*), yaitu *Service Delivery* (Antar Layanan) dan *Service Support* (Dukungan Layanan).

**Continual Service Improvement** (CSI) memberikan panduan penting dalam menyusun serta memelihara kualitas layanan dari proses desain, transisi dan pengoperasiannya. CSI mengkombinasikan berbagai prinsip dan metode dari manajemen kualitas, salah satunya adalah *Plan-Do-Check-Act* (PDCA) atau yang dikenal sebagai *Deming Quality Cycle*.



Gambar 4.6 Siklus Hidup Layanan

Sebagai rangkuman, siklus hidup layanan dapat digambarkan sebagai berikut :



Gambar 4.7 Rangkuman Siklus Hidup Layanan

Sumber: Kajian Pengembangan Tata Kelola Infrastruktur TIK BPPT berdasarkan COBIT 5, 2017, hal 52

Untuk organisasi dan profesional TI, penting untuk mengetahui kekuatan dan kelemahan masing-masing sistem manajemen layanan. Memiliki pemahaman yang baik dari perbedaan ini memungkinkan untuk memutuskan mana kerangka paling sesuai yang akan menghasilkan nilai yang paling bagus sekaligus mengoptimalkan anggaran dan mengatasi terbatasnya sumber daya perusahaan.

Pemilihan *framework* memerlukan banyak usaha untuk menentukannya. Penelitian atau kajian atas *framework* untuk pengelolaan TI telah dilakukan dalam beberapa waktu yang lalu. Para ahli juga telah mempelajari beberapa *framework* serta standar yang ada sehingga hasilnya bisa memberikan suatu arahan atau rekomendasi apa yang sebaiknya digunakan di BPPT. Hal ini dilakukan dalam rangka menyesuaikan dengan apa yang diinginkan atau kebutuhan BPPT, serta untuk memberikan dasar membangun sistem tata kelola yang baik, memungkinkan audit, serta mempunyai kesesuaian dengan beberapa standar.

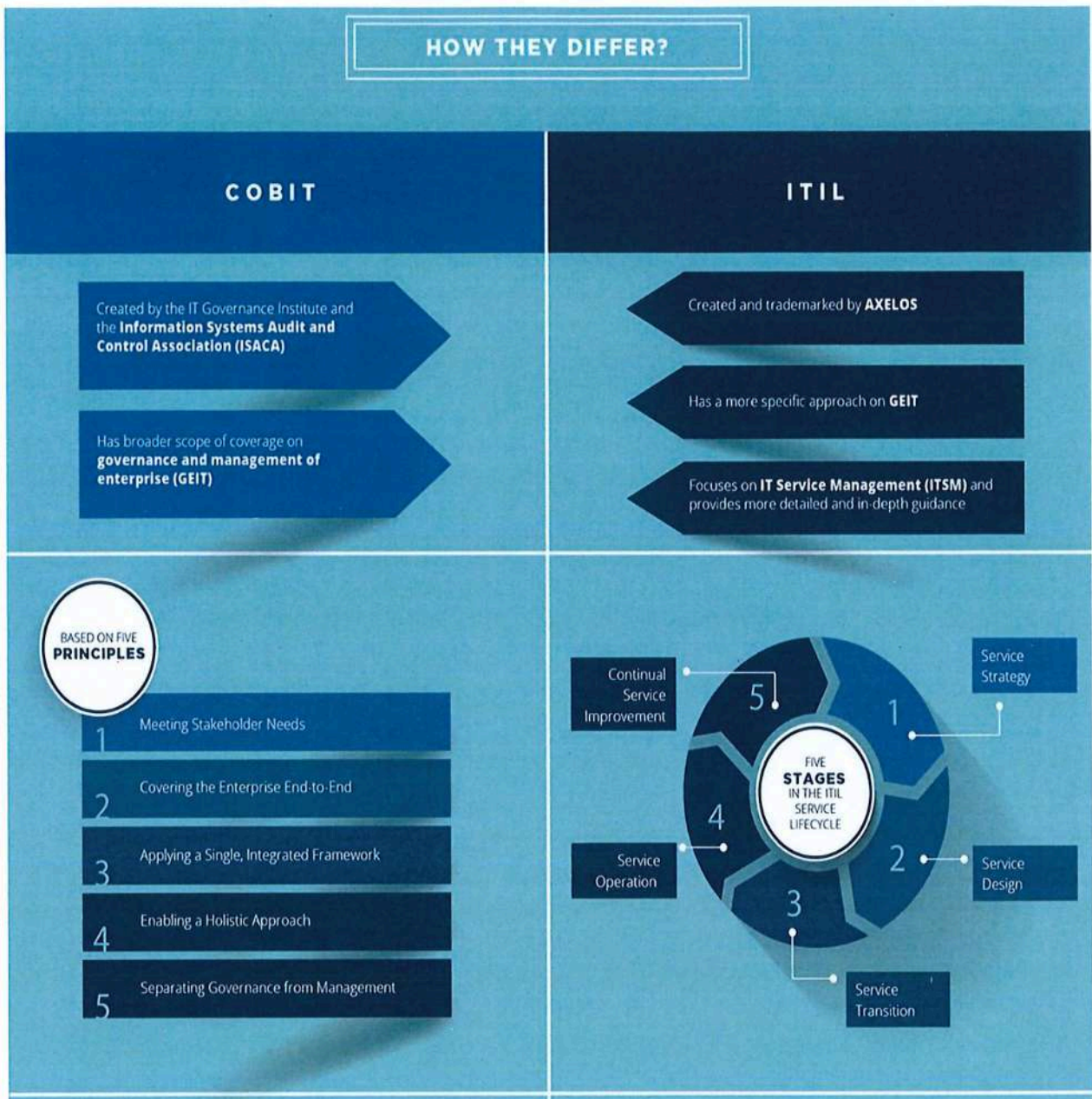
Dengan pertimbangan yang ada maka pilihan jatuh pada COBIT 5 dan ITIL, dimana keduanya selaras dalam pendekatan masing-masing kerangka untuk IT Service Management (ITSM). ITIL, bagaimanapun, sering dianggap sebagai cara untuk mengelola layanan TI di seluruh siklus hidup mereka dengan penekanan pada nilai bagi pengguna, sementara COBIT difokuskan pada

prinsip-prinsip dan *enabler* yang mendukung perusahaan untuk memenuhi kebutuhan dan persyaratan *stakeholder*.



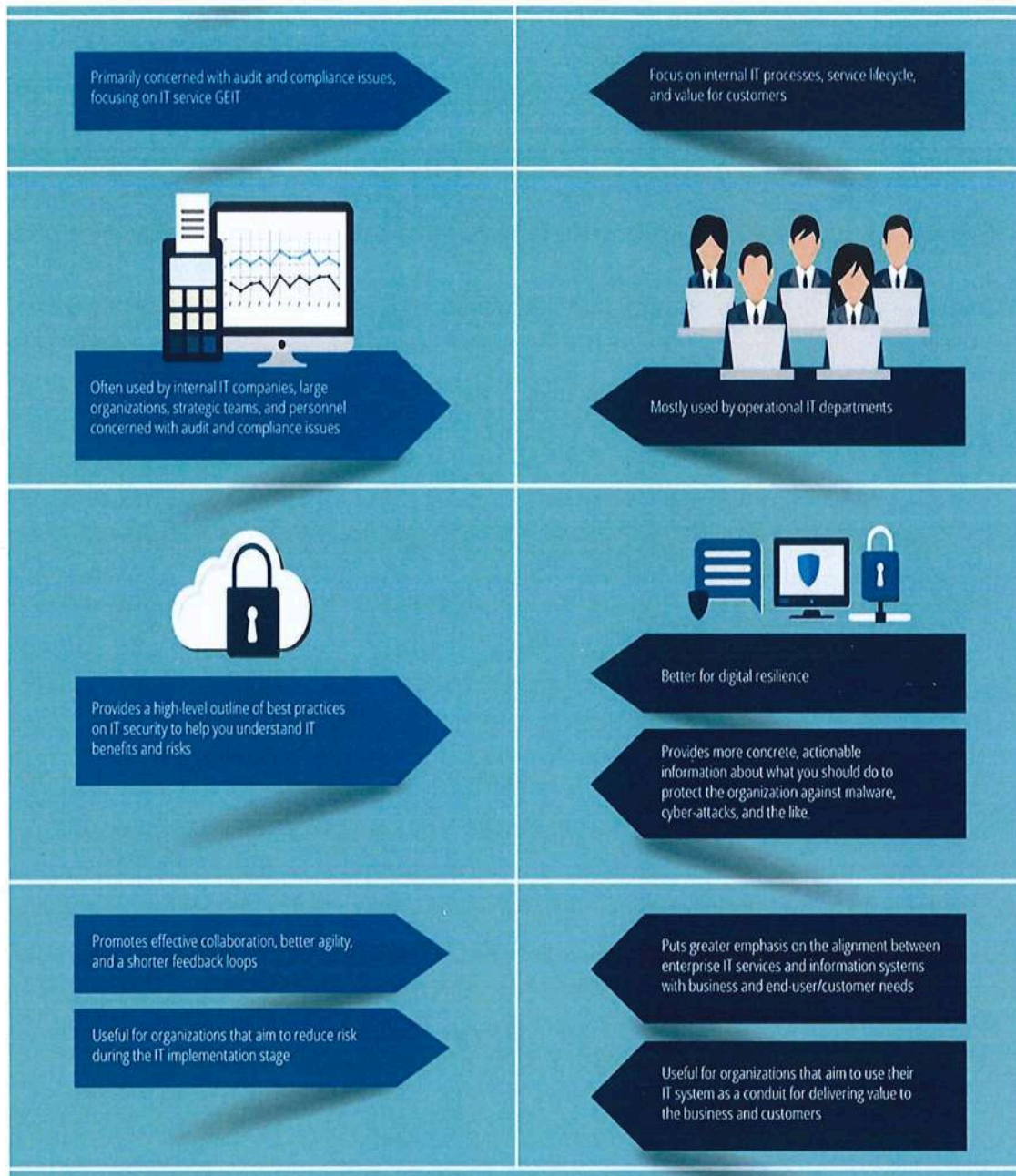
Gambar 4.8 Infografis COBIT vs ITIL (1 dari 3)

Sumber: Kajian Pengembangan Tata Kelola Infrastruktur TIK BPPT berdasarkan COBIT 5, 2017, hal 53



Gambar 4.9 Infografis COBIT vs ITIL (2 dari 3)

Sumber: Kajian Pengembangan Tata Kelola Infrastruktur TIK BPPT berdasarkan COBIT 5, 2017, hal 54



Gambar 4.10 Infografis COBIT vs ITIL (3 dari 3)

Sumber: Kajian Pengembangan Tata Kelola Infrastruktur TIK BPPT berdasarkan COBIT 5, 2017, hal 55

Dari keterangan gambar berikut, perbandingan antara COBIT dan ITIL dijelaskan pada tabel berikut:

Tabel 4.1 Keterangan Infografis COBIT vs ITIL

	COBIT	ITIL
<b>Fungsi</b>	Biasa digunakan organisasi untuk membuat, memantau dan melakukan pemeliharaan secara menyeluruh pada tata kelola dan manajemen TI	Pada dasarnya menyediakan sebuah perangkat <i>best practice</i> dan panduan yang saling berhubungan untuk membangun, menyampaikan dan mengelola layanan TI untuk mengaktifkan sebagian besar nilai bisnis
<b>Tujuan</b>	Bertujuan untuk memandu perusahaan pada implementasi, operasi dan peningkatan pengaturan sistem secara keseluruhan sesuai kebutuhan	Bertujuan memberikan deskripsi yang lebih rinci tentang manajemen layanan untuk kegiatan TI seperti proses, struktur organisasi dan sejenisnya
<b>Badan Pembentuk</b>	Dibentuk oleh Intitusi Pengatur TI Information Systems Audit and Control Association (ISACA)	Dibentuk dan berlabel ALEXOS
<b>Ruang Lingkup</b>	Ruang lingkungnya luas, dimana meliputi tata kelola dan manajemen perusahaan	Ruang lingkup pada tata kelola dan manajemen perusahaan lebih spesifik, serta fokus pada manajemen pelayanan TI dan menyediakan arahan yang lebih dalam serta detail
<b>Komponen</b>	Berdasarkan 5 prinsip: 1 Memenuhi kebutuhan pemangku kepentingan 2 Meliputi end-to-end perusahaan 3 Menerapkan single integrated framework 4 Memungkinkan pendekatan holistic 5 Memisahkan tata kelola dari manajemen	Memiliki 5 tahap yang saling berurutan, bertahap, serta terulang kembali layaknya siklus pelayanan ITIL: 1 Strategi Pelayanan 2 Desain Pelayanan 3 Transisi Pelayanan 4 Operasi Pelayanan 5 Peningkatan Pelayanan secara Berkelanjutan
<b>Konsentrasi</b>	Secara garis besar lebih memperhatikan audit dan isu-isu kepatuhan, serta fokus pada pelayanan tata kelola dan manajemen perusahaan	Fokus pada proses-proses internal TI, siklus hidup pelayanan, serta nilai untuk para pengguna
<b>Pengguna</b>	Seringkali digunakan oleh perusahaan internal TI, organisasi-organisasi besar,	Sebagian besar digunakan oleh bagian operasional TI

	tim-tim strategis, serta kebutuhan pribadi terkait isu-isu audit dan kepatuhan	
<b>Keamanan</b>	Menyediakan high level outline dengan Praktik-Praktik terbaik pada keamanan TI yang membantu pengguna untuk memahami keuntungan serta resiko TI	Lebih sesuai untuk keamanan digital, serta menyediakan informasi yang lebih actionable, konkrit, mengenai apa yang perlu dilakukan pengguna untuk mengamankan organisasinya terhadap malware, serangan siber, dan sejenisnya
<b>Keunggulan</b>	Mempromosikan kolaborasi yang efektif, kelincahan yang lebih baik, dan loops umpan balik yang lebih pendek	Lebih mengedepankan keselarasan antara pelayanan perusahaan TI serta sistem informasi dengan bisnis serta kebutuhan pengguna / end user
<b>Kegunaan</b>	Digunakan untuk organisasi yang memiliki tujuan untuk mengurangi resiko selama tahap implementasi TI	Digunakan untuk organisasi yang memiliki tujuan untuk menggunakan sistem TI mereka sebagai sarana untuk membawa nilai kepada bisnis dan juga pengguna-pengguna

### 3. PEMETAAN COBIT DAN ITIL

Tabel 4.2 Pemetaan COBIT dan ITIL

COBIT	ITIL
<b>Rekonsiliasi Fase</b>	
Planning and Organizing (PO)	Service strategy
Acquiring And Implementing (AI)	Service conception
Delivering and Supporting (DS)	Transition and operation of service
Monitoring and evaluating (ME)	Continuous improvement of service
<b>Rekonsiliasi Proses</b>	
PO1: Define a strategic IT plan	Set service strategy (Strategy service)
PO2: Define the information architecture	-
PO3: Determine technological direction	-
PO4: Define the processes, organization and labor relations	-
PO5: Manage IT investment	Financial Management of service (strategy of service)

COBIT	ITIL
PO6: Communicate the goals and management guidelines	-
PO7: Managing IT human resources	-
PO8: Managing Quality	-
PO9: Assess and manage risk	-
PO10: Manage projects	-
AI1: Find IT solutions	Management and deployment into production (Phase transition of service)
AI2: Purchase applications and maintain them	-
AI3: Purchase a technical infrastructure and maintain it	-
AI4: Facilitate the operation and use	-
AI5: Purchase IT resources	-
AI6: Manage change	Change Management (Phase transition of service)
AI7: Install and validate changes and solutions	Management and deployment into production (Phase transition of service)
DS1: Define and manage service levels	Service Level Management (Design Phase)
DS2: Manage third - party services	Supplier Management (Design Phase)
DS3: Manage performance and capacity	Capacity Management (Design Phase)
DS4: Ensure continuous service	Continuity Management (Design Phase)
DS5: Ensure security of systems	Security Management (Design Phase)
DS6: Identify and allocate costs	Financial Management Service (Strategy service)
DS7: Educate and train users	Management and deployment into production (Phase transition of service)
DS8: Manage support to clients and incidents	Incident Management (Operation Phase)

COBIT	ITIL
DS9: Manage configuration	Asset management and configuration (phase transition)
DS10: Manage problems	Problem Management (Operation Phase)
DS11: Manage data	-
DS12: Manage the physical environment	-
DS13: Manage operations	(This is a phase according to ITIL)
ME1: Monitor and evaluate the performance of IS	Phase of continuous improvement of service
ME2: Monitor and evaluate internal control	Phase of continuous improvement of service
ME3: Ensure compliance with external obligations	-
ME4: Implement a governance of IS	Portfolio Management Service (Phase service strategy)

### Penerapan COBIT 5 Bidang Infrastruktur Informasi

Bidang Infrastruktur Informasi adalah pelaksana dari kebijakan level manajemen di atasnya, melaksanakan tugas setingkat eselon 3 yang merealisasikan layanan infrastruktur. Oleh karena itu, pelaksanaan pekerjaan layanan dilakukan di level yang setingkat dengan manajemen yang mampu untuk membangun, mendapatkan atau memperoleh serta mengimplementasikan suatu layanan. Dimana layanan yang bisa dilakukan itu memang sudah mendapat persetujuan atau telah diarahkan oleh level di atasnya.

Untuk realisasi yang menjadi tanggung jawab eselon 3 ini dibebankan pada level eselon Praktiknya yaitu eselon 4 beserta dengan para ahli ataupun perekayasa. Maka, penerapan COBIT 5 ini di level eselon 3 adalah pada tingkatan BAI, sedangkan pelaksanaan DSS dan MEA diletakkan pada eselon 4 dan para perekayasa, yang mampu merealisasikan dengan berbagai SOP serta peralatan, yang pada akhirnya eselon 3 dapat memanfaatkan hasil monitoring secara riil serta mampu mengontrol layanan infrastruktur.

Adapun *Align, Plan, and Organize (APO)* – Penyelarasan, Perencanaan, dan Pengaturan. Pelaksanaan jelas pada level di atas BII, dan untuk itu maka dalam melaksanakan hal di atas BII mengacu pada dokumen RITI (Rencana Induk Teknologi Informasi) BPPT, aturan di atasnya, Keputusan CIO, serta menjalankan perencanaan dan pengaturan yang selaras dengan perubahan teknologi dan perubahan kebutuhan yang ada.

Tingkat penerapan operasional COBIT 5 pada BII dengan demikian menyesuaikan, dan mengikuti apa yang ada, dengan demikian tidak mengganggu keterbatasan untuk selalu meningkatkan baik kualitas layanan maupun pengembangan jenis layanan yang baru. Beberapa SOP yang disesuaikan dengan DSS di COBIT 5 diimplementasikan terutama untuk memenuhi standar keamanan Informasi yang tinggi misalnya diletakkan di Buku Kebijakan Keamanan Informasi.

### Tahapan Dalam Pengembangan COBIT 5

#### A. Pemetaan Kondisi Eksisting

Setelah mendapatkan pilihan *framework* tata kelola yang paling sesuai diterapkan di Bidang Infrastruktur Informasi, maka langkah selanjutnya adalah mengumpulkan data layanan infrastruktur yang bertujuan untuk mengetahui objek pengamatan data dukung yang terkait dalam tata kelola infrastruktur.

Bidang Infrastuktur Informasi sampai dengan awal tahun 2017 telah memiliki 18 (delapan belas) dokumen kebijakan, baik berupa panduan maupun petunjuk teknis, 16 (enam belas) standar operasional prosedur (SOP), 5 (lima) standar instruksi kerja (SIK) dan 12 (dua belas) standar formulir kerja (SFK).

##### a) Dokumen Kebijakan

Dokumen Kebijakan merupakan acuan yang dibuat oleh Pengambil Kebijakan (biasanya CIO – *Chief Information Officer*) yang akan mengatur dan menentukan tingkat layanan dan teknis secara global. Di BII, dokumen kebijakan yang diacu dapat berupa rencana induk, *blue print*, panduan, maupun petunjuk teknis. Tabel Praktik ini menunjukkan daftar dokumen kebijakan yang dimiliki dan dijadikan acuan oleh Bidang Infrastruktur Informasi.

Tabel 4.3 Tabel Dokumen Kebijakan Eksisting

No	Nama Dokumen	Nomer Dokumen
1	Rencana Induk Teknologi Informasi BPPT	-
2	Rencana Induk Teknologi Informasi BPPT 2015-2019	-
3	Rencana Tindak CIO BPPT 2015-2019	-
4	Blue Print Sistem e-government	-
5	ICT Outlook Indonesia 2013	-
6	Panduan Manajemen Resiko	2106000.PMR.2.01.13
7	Panduan Kebijakan Keamanan Informasi	2106000.02.00.00.00.01.14
8	Panduan Penyimpanan Back up dan Recovery	2106000.01.09.00.00.01.13
9	Panduan Manajemen BCP	2106000.03.00.00.00.01.14
10	Panduan Penanganan Insiden Malware	-

11	Panduan Penanganan Insiden Keamanan Jaringan	-
12	Panduan Penanganan Insiden Infrastruktur Fisik	-
13	Panduan Penanganan Insiden Web Defacement	-
14	Panduan Penanganan Insiden Database	-
15	Petunjuk Teknis Kebijakan Infrastruktur TI	ISBN 978-978-22-3092-0
16	Petunjuk Teknis Implementasi e-government	ISBN 978-979-3733-92-0
17	Petunjuk Teknis Implementasi KIP	ISBN 978-979-3733-94-4
18	Petunjuk Teknis Implementasi Aplikasi Perangkat Lunak dan FOSS	ISBN 978-979-3733-93-7

b) Dokumen Standar Operasional Prosedur (SOP)

Dokumen Standar Operasional Prosedur atau SOP merupakan turunan dari dokumen kebijakan yang dibuat oleh penanggung jawab operasional kegiatan (biasanya setingkat eselon 3 atau kepala bidang) yang akan mengatur dan menentukan pelaksanaan operasional di lapangan agar tidak terjadi kesalahan. Di BII para pelaksana lapangan akan melaksanakan kegiatan sesuai ketentuan yang ada di SOP.

Tabel 4.4 Tabel SOP Eksisting

No	Nama Dokumen	Nomer Dokumen
1	SOP Penambahan Akun Email	2106210.01.01.00.00.02.14
2	SOP Perubahan Password	2106210.01.02.00.00.02.14
3	SOP Penambahan Milis	2106210.01.03.00.00.02.14
4	SOP Cloud Computing	2106210.01.04.00.00.02.14
5	SOP Video Conference	2106210.01.05.00.00.02.14
6	SOP Penambahan Konten IPTV	2106210.01.06.00.00.02.14
7	SOP Broadcasting Digital	2106210.01.07.00.00.02.14
8	SOP Layanan Mobile Wireless	2106210.01.08.00.00.02.14
9	SOP Penambahan Jaringan Intranet Dan Internet BPPT	2106210.01.09.00.00.02.14
10	SOP Pengadaan IP Publik Dan Sub Domain	2106210.01.10.00.00.02.14
11	SOP Pemantauan Fasilitas TIK	2106200.01.02.00.00.01.14
12	SOP Teleworking	2106200.01.01.00.00.01.14
13	SOP Penanganan Insiden Yang Terdeteksi Oleh Tim	2106200.01.03.00.00.01.14

	Teknis	
14	SOP Penanganan Insiden Yang Terdeteksi Oleh Pengguna	2106200.01.04.00.00.01.14
15	SOP Penanganan Insiden Yang Terdeteksi Oleh Pihak Luar	2106200.01.05.00.00.01.14
16	SOP Kerja Di Daerah Aman	2106200.01.06.00.00.01.14

c) Dokumen Standar Instruksi Kerja (SIK)

Dokumen standard instruksi kerja atau SIK juga merupakan turunan dari dokumen SOP yang dibuat oleh *engineer* senior untuk menjadi panduan bagi pekerja di lapangan dalam menjalankan tugasnya. SIK berisi panduan atau manual kerja yang akan memandu petugas di lapangan untuk menginstalasi, mengkonfigurasi, maupun melakukan *troubleshooting* suatu perangkat atau sistem infrastruktur. SIK harus selalu di-*update* sesuai perkembangan teknologi agar tidak ketinggalan jaman.

Tabel 4.5 Standar Instruksi Kerja Eksisting

No	Nama Dokumen	Nomer Dokumen
1	SIK Layanan Penambahan Akun Email	2106210.01.01.01.00.02.14
2	SIK Layanan Perubahan Password	2106210.01.02.01.00.02.14
3	SIK sistem LDAP	2106200.01.01.01.00.01.14
4	SIK Back up sistem mail	2106200.01.01.02.00.01.14
5	SIK Hak Akses	2106200.01.01.03.00.01.14

d) Dokumen Standar Formulir Kerja

Dokumen standar formulir kerja atau SFK merupakan turunan dari dokumen SOP yang dibuat oleh Penanggung jawab operasional kegiatan (biasanya setingkat eselon 3 atau kepala bidang) bersama dengan para petugas lapangan yang akan mengatur dan menentukan item dan *checklist* apa saja yang harus diperiksa, diisi dan diukur oleh pemohon dan pelaksanaan lapangan agar proses permintaan, pemeriksaan dan pelayanan lengkap sesuai yang dibutuhkan.

Tabel 4.6 Tabel Standar Formulir Kerja Eksisting

No	Nama Dokumen	Nomer Dokumen
1	SFK Permohonan Layanan Pendaftaran e-Mail	4.01-0.01.01-PLP-B2.PMI
2	SFK Permohonan Reset Password	4.02-0.01-PRS-B2.PMI
3	SFK Pendaftaran Milis	4.03-0.01-PLPM-B2.PMI
4	SFK Layanan Infrastruktur Cloud	4.04-0.01-PLIC-B2.PMI
5	SFK Layanan Video Conference	4.05-0.01-PLVC-B2.PMI
6	SFK Penambahan Konten IPTV	4.06-0.01-PLIPTV-B2.PMI
7	SFK Layanan Broadcast Digital	4.07-0.01-PLBD-B2.PMI
8	SFK Layanan Wireless On Demand	4.08-0.01-PLW-B2.PMI
9	SFK Penambahan Akses Jaringan	4.10-0.01-PLPAJ-B2.PMI
10	SFK Pengadaan Nama Sub Domain	4.11-0.01-PLPSD-B2.PMI
11	SFK Pengadaan IP BPPT	4.09-0.01-PLIB-B2.PMI
12	SFK Keamanan Perangkat Pengguna	2106200.01.07.00.01.01.15

B. Rincian Domain Area *Deliver, Service and Support* (DSS) Sesuai Lingkup Kerja Bidang Infrastruktur Informasi

Ruang lingkup kajian tata kelola infrastruktur TI ini dibatasi pada domain area DSS yang akan dikembangkan terlebih dahulu, karena kelompok ini lebih banyak mengatur tata kelola layanan dan operasional, yang sesuai dengan salah satu tupoksi dari BII sehingga meningkatkan operasional Infrastruktur bisa terkelola dengan lebih rapi dan tersistematis.

Domain area DSS sendiri terbagi menjadi 6 proses pengelolaan yaitu : **DSS 01 Manage operations, DSS 02 Manage service requests and incidents, DSS 03 Manage problems, DSS 04 Manage continuity, DSS 05 Manage security services, DSS 06 Manage business process controls.** Contoh rincian proses dari domain area DSS:

Tabel 4.4 Deskripsi Proses DSS 01

DSS01 Pengelolaan Operasional	Area: Manajemen Domain : Deliver, Service and Support
Deskripsi proses <b>Mengkoordinasikan dan melaksanakan kegiatan dan prosedur operasional yang dibutuhkan untuk memberikan layanan IT internal dan layanan IT pihak ke 3, termasuk pelaksanaan prosedur yang telah ditetapkan dan kegiatan monitoring yang diperlukan.</b>	
Tujuan proses <b>Memberikan layanan TI sesuai yang direncanakan.</b>	

Proses yang mendukung tercapainya sekumpulan tujuan utama yang berhubungan dengan TI:	
Tujuan terkait TI	
04 Mengelola TI terkait risiko bisnis	<b>Ukuran terkait</b>
	<ul style="list-style-type: none"> <li>• Persentase Porses Bisnis Kritis Layanan TI Dan Program Bisnis terkait TI yang telah dilakukan pengkajian risikonya.</li> <li>• Jumlah Kejadian Penting Terkait Yang Tidak teridentifikasi dalam Asesmen resiko.</li> <li>• Persentase Risiko organisasi Termasuk Risiko Terkait TI.</li> <li>• Frekuensi pemutakhiran Profil Risiko</li> </ul>
07 Pemberian layanan TI sejalan dengan kebutuhan bisnis	<ul style="list-style-type: none"> <li>• Jumlah Gangguan Bisnis Akibat kejadian layanan TI.</li> <li>• Persentase kepuasan Stakeholders terhadap layanan TI yang memenuhi SLA. Persentase kepuasan Pengguna terhadap layanan TI.</li> </ul>
11 Optimisi aset TI, sumber daya dan kemampuan/kapabilitas	<ul style="list-style-type: none"> <li>• Frekuensi asesmen Kematangan Kemampuan Dan Optimasi biaya.</li> <li>• Trend Hasil asesmen.</li> <li>• Tingkat Kepuasan eksekutif Bisnis Dan TI terkait dengan Biaya Dan Kemampuan.</li> </ul>
Tujuan proses dan Ukuran	
Tujuan Proses	Metrik terkait
1. Kegiatan operasional dilakukan sesuai kebutuhan dan jadwal	<p>Jumlah prosedur operasional tidak Standar yang dilakukan.</p> <p>Jumlah kejadian yang diakibatkan Akibat Masalah Operasional.</p>
2. Operasi dimonitor, diukur, dilaporkan dan di perbaiki.	<p>Perbandingan kegiatan terhadap jumlah kejadian.</p> <p>Persentase event operasional Kritis yang di cover oleh Sistem Deteksi Automatic.</p>

Tabel 4.5 Raci Chart DSS 01

DSS01 RACI CHART							
	Ka. PMI	Ka. BII	Kasubbid pengembangan	Kasubbid optimasi	Helpdesk	Admin Jaringan	Teknisi lapangan
Key Management Practice							
DSS01.01 melakukan prosedur operasional		√					

DSS01.02 Mengelola layanan TI outsourcing			√				
DSS01.03 Memonitor infrastruktur TI			√				
DSS01.04 Mengelola lingkungan							
DSS01.05 Mengelola fasilitas							

Tabel 4.6 Proses, input, output dan Aktivitas DSS01

DSS01 Proses, input, output dan Aktivitas				
Praktik manajemen	Input		Output	
DSS 01. Melakukan prosedur operasional. Memelihara dan melakukan prosedur operasional dan tugas operasional handal dan konsisten	From	Description	Description	To
		BAI05.05	rencana operasi dan penggunaan	jadwal operasional Back up log
Activities				
1. Mengembangkan dan memelihara prosedur operasional dan kegiatan terkait untuk mendukung semua layanan yang diberikan.				
2. Memelihara jadwal kegiatan operasional, melakukan kegiatan, dan mengelola kinerja dan <i>throughput</i> dari kegiatan yang dijadwalkan.				
3. Verifikasi semua Data Yang dibutuhkan untuk diproses telah diterima dan diproses secara lengkap, akurat dan tepat waktu. Memberikan Output Sesuai Dengan Kebutuhan Organisasi. Dukungan Restart Dan Kebutuhan Pengolahan. Memastikan Bahwa Pengguna Menerima Output Yang Tepat Dengan Cara Yang Aman Dan Tepat Waktu.				
4. Memastikan standar keamanan yang berlaku dalam menerima, memproses, mengolah data dan mengeluarkan output data dipastikan sesuai standar keamanan yang diterapkan juga dipastikan dan sesuai dengan tujuan perusahaan dan aturan yang berlaku.				
5. Menjadwalkan pengambilan dan pencatatan backup sesuai dengan kebijakan dan prosedur yang telah ditetapkan.				
Praktik Manajemen	Inputs		Outputs	
Input output	Dari	Deskripsi	Deskripsi	Kepada
DSS01.02 Mengelola layanan TI outsourcing. Mengelola operasi outsourcing layanan TI untuk menjaga perlindungan informasi perusahaan dan keandalan pelayanan.	APO09.03	OLAs SLAs	jaminan rencana independen	MEA02.06
	BAI05.05	rencana operasi dan penggunaan		
Kegiatan				
1. Mengembangkan dan memelihara prosedur operasional dan kegiatan terkait untuk mendukung semua layanan yang diberikan				

2. Memelihara jadwal kegiatan operasional, melakukan kegiatan, dan mengelola kinerja dari kegiatan yang dijadwalkan.				
3. Memverifikasi semua data yang diterima untuk pengolahan dan diproses secara akurat dan dengan tepat waktu untuk memberikan output sesuai dengan kebutuhan instansi. Memastikan bahwa pengguna menerima output yang tepat dengan cara yang aman dan tepat waktu.				
4. Memastikan standar keamanan yang berlaku untuk penerimaan, pengolahan, penyimpanan data sesuai dengan persyaratan kebijakan dan persyaratan regulasi.				
5. Membuat jadwal untuk mengambil dan membuat catatan backup data sesuai dengan kebijakan dan prosedur yang telah ditetapkan. Membuat jadwal, mengambil dan <i>log backup</i> sesuai dengan kebijakan dan prosedur yang telah ditetapkan.				
Praktik manajemen	Inputs		Outputs	
DSS01.03 Memonitor infrastruktur TI. Memonitor infrastruktur TI dan peristiwa terkait. Mencatat informasi kronologis cukup untuk melakukan review dan pemeriksaan mulai dari pencatatan waktu dan kegiatan yang dilakukan.	Dari	Deskripsi	Deskripsi aturan pemantauan aset dan kondisi acara	Untuk DSS02.01 DSS02.02
	BAI03.11	definisi layanan	event log	Intern
			tiket insiden	DSS02.02
Kegiatan				
1. Log peristiwa, mengidentifikasi tingkat informasi yang akan dicatat berdasarkan pertimbangan risiko dan kinerja				
2. Mengidentifikasi dan memelihara daftar aset infrastruktur yang perlu dipantau berdasarkan pada layanan kekritisan dan hubungan antara konfigurasi item dan layanan yang diberikan.				
3. Mendefinisikan dan menerapkan aturan yang mengidentifikasi dan merekam pelanggaran batas dan kondisi kegiatan. Menemukan keseimbangan antara kekurangan dari suatu kegiatan/kejadian yang signifikan.				
4. Memelihara catatan kegiatan untuk jangka waktu tertentu yang tepat untuk membantu dalam menganalisa kekurangan pada waktu yang akan datang.				
5. Menetapkan prosedur untuk pemantauan dan melakukan tinjauan rutin.				
6. Memastikan catatan kegiatan dibuat pada saat yang tepat untuk memantau pengidentifikasi penyimpangan dari batas yang ditentukan.				
Praktik manajemen	Inputs		Outputs	
DSS01.04 Mengelola lingkungan hidup. Mempertahankan langkah-langkah untuk perlindungan terhadap faktor lingkungan. Memasang peralatan khusus dan perangkat untuk memonitor dan mengontrol lingkungan.	Dari	Diskripsi	Diskripsi	Untuk
			kebijakan lingkungan	<b>APO01.08</b>
			laporan polis asuransi	<b>MEA03.03</b>
Kegiatan				
1. Mengidentifikasi bencana alam dan bencana buatan manusia yang mungkin terjadi di daerah di mana fasilitas TI berada. Menilai efek potensial pada fasilitas TI.				
2. Mengidentifikasi bagaimana peralatan TI, termasuk peralatan mobile dan off-site, dilindungi terhadap ancaman lingkungan. Pastikan bahwa batas kebijakan atau tidak termasuk makan, minum dan merokok di daerah sensitif, dan melarang penyimpanan alat tulis dan perlengkapan lainnya berpose bahaya kebakaran dalam ruang komputer.				

3. Menempatkan dan membangun fasilitas TI untuk meminimalkan dan mengurangi kerentanan terhadap ancaman lingkungan					
4. Secara teratur memonitor dan memelihara perangkat yang secara proaktif mendeteksi ancaman lingkungan (misalnya, api, air, asap, kelembaban).					
5. Menanggapi alarm lingkungan dan pemberitahuan lainnya. Dokumen dan uji prosedur, yang harus mencakup prioritas alarm dan kontak dengan pemerintah tanggap darurat lokal, dan melatih personil dalam prosedur ini.					
6. Membandingkan langkah-langkah dan rencana kontingensi terhadap persyaratan polis asuransi dan hasil laporan. Membuat catatan dari ketidakpatuhan dalam waktu yang tepat.					
7. Pastikan Bahwa Situs TI yang dibangun dan dirancang untuk meminimalkan dampak risiko lingkungan (Misalnya, Pencurian, Udara, Api, Asap, Air, Getaran, Teror, Vandalisme, Kimia, Bahan Peledak) .Consider Khusus Kawasan Keamanan Dan Atau Kebakaran Sel Proof (misal: Penempatan Produksi Dan Pengembangan Lingkungan Server Jauh Dari Satu Orang Ke Orang Lainnya).					
8. Jauhkan situs TI dan ruang server bersih dan dalam kondisi aman setiap saat (tidak berantakan, tidak ada kertas atau karton kotak, tidak diisi sampah, tidak ada bahan kimia yang mudah terbakar atau bahan)					
Praktik manajemen		Inputs		Outputs	
DSS01.05 Mengelola fasilitas. Mengelola fasilitas, termasuk listrik dan komunikasi peralatan, sejalan dengan hukum dan peraturan, teknis dan kebutuhan bisnis, spesifikasi vendor, dan kesehatan dan pedoman keselamatan.				penilaian fasilitas laporan	MEA01.03
				kesadaran Kesehatan dan keselamatan	Internal
Kegiatan					
1. Memeriksa Fasilitas Persyaratan Untuk Perlindungan Terhadap Fluktuasi Daya Dan Usia, Perencanaan persyaratan pengadaan peralatan yang sesuai (Misalnya, Baterai, Generator) untuk mendukung kelangsungan pekerjaan.					
2. Teratur menguji <i>uninterruptible power supply</i> mekanisme dan memastikan daya yang dapat beralih ke penawaran tanpa pending effecton operasi bisnis.					
3. Pastikan bahwa fasilitas sistem TI memiliki lebih dari satu sumber untuk kemandirian (seperti Listrik, telekomunikasi, air, gas). Memisahkan pintu masuk fisik setiap utilitas.					
4. Konfirmasikan bahwa kabel eksternal ke situs TI terletak Praktik tanah atau memiliki perlindungan alternatif yang sesuai. Menentukan kabel yang dalam situs TI terkandung dalam saluran aman, dan kabel lemari memiliki akses terbatas ke petugas yang berwenang. Pengamanan secara baik dan benar untuk melindungi kabel terhadap kerusakan yang disebabkan oleh api, asap, air, intersepsi dan gangguan.					
5. Pastikan bahwa kabel dan patching fisik (data dan telepon) yang terstruktur dan terorganisir. Kabel dan saluran struktur harus didokumentasikan (Misal, rencana pembangunan cetak biru dan diagram <i>wiring</i> ).					
6. Analisis fasilitas perumahan tinggi sistem ketersediaan untuk redundansi dan gagal lebih persyaratan cabling eksternal dan internal.					
7. Pastikan bahwa situs IT dan fasilitas yang sesuai berlangsung dengan hukum kesehatan dan keselamatan, peraturan, pedoman, dan spesifikasi vendor					
8. Mendidik personel secara teratur pada hukum kesehatan dan keselamatan, peraturan, dan pedoman yang relevan. Mendidik personel terbakar dan penyelamatan latihan untuk memastikan pengetahuan dan tindakan yang diambil dalam kasus kebakaran atau insiden serupa.					
9. Rekam, memantau, mengelola dan menyelesaikan fasilitas insiden sejalan dengan proses manajemen insiden TI. Membuat laporan yang tersedia pada fasilitas insiden di mana pengungkapan diperlukan dalam					

hal hukum dan peraturan.
10. Memastikan bahwa situs dan peralatan yang dikelola menurut pemasok direkomendasikan interval service dan spesifikasi perawatan the harus dilakukan hanya oleh petugas yang berwenang.
11. Menganalisis perubahan fisik untuk situs IT atau tempat untuk menilai kembali risiko lingkungan (misalnya, kebakaran atau kerusakan air). hasil laporan analisis ini untuk kelangsungan bisnis dan fasilitas manajemen

Tabel 4.7 Standar Terkait DSS 01

<b>DSS01 Standar Terkait</b>	
<b>Standar terkait</b>	rinci Referensi
<b>ITIL V3 2011</b>	19 EVENT-ANAGEMENT 24 OPERATION MANAGEMENT

C. Melaksanakan Pemetaan (GAP analisis)

Analisis kesenjangan (*gap analysis*) dilakukan untuk mengetahui sejauh mana kesenjangan antara kondisi saat ini (*as-is condition*) dengan kondisi yang diharapkan (*to-be condition*), serta upaya (*effort*) yang harus dilakukan untuk meminimalisasi kesenjangan tersebut. Hasil analisis ini dapat diketahui dengan cara pemetaan kondisi saat ini (*kondisi eksisting*) berdasarkan aktifitas COBIT proses DSS dari DSS 01 - 06 per klausul sehingga menghasilkan Rekomendasi untuk menghasilkan kondisi yang diharapkan (*to-be condition*). Contoh GAP analisis DSS 01 adalah sebagai berikut:

Tabel 4.8 Tabel Pemetaan DSS 01.01

DSS01.01 Menjalankan prosedur operasional		
Aktifitas COBIT	Kondisi eksisting	Rekomendasi
1. Mengembangkan dan memelihara prosedur operasional dan kegiatan terkait untuk mendukung semua layanan yang diberikan	Prosedur operasional layanan yang sudah ada: <ol style="list-style-type: none"> <li>1. SOP penambahan akun email</li> <li>2. SOP perubahan password</li> <li>3. Penambahan milis</li> <li>4. <i>Cloud Computing</i></li> <li>5. <i>Video Conference</i></li> <li>6. Penambahan contain IP TV.</li> <li>7. <i>Broadcasting Digital</i></li> <li>8. <i>Mobile Wireless</i></li> <li>9. Penambahan jaringan intranet dan internet BPPT.</li> <li>10. Pengadaan IP Publik dan sub domain.</li> </ol>	<ol style="list-style-type: none"> <li>1. Menyusun SOP layanan End Point security.</li> <li>2. Memperbaiki format SOP sesuai dengan nama Unit Kerja baru.</li> </ol>
2. Memelihara jadwal kegiatan operasional, melakukan kegiatan, dan mengelola kinerja dan <i>throughput</i> dari kegiatan yang dijadwalkan.	Pengukuran optimasi kinerja jaringan; <ol style="list-style-type: none"> <li>1. Kecepatan jaringan.</li> <li>2. Utilisasi bandwidth</li> </ol>	Dibuatkan jadwal dan melakukan pemeliharaan sesuai dengan jadwal yang dibuat.

	<p>3. Availability</p> <p>4. Pengecekan tiket helpdesk</p> <p>5. Dsb</p> <p>Pengukuran di atas sudah dilakukan namun belum ada jadwal.</p>	
<p>3. Verifikasi semua Data Yang dibutuhkan telah diterima dan diproses secara lengkap, akurat dan tepat waktu.</p> <p>Memberikan Output Sesuai Dengan Kebutuhan Organisasi. Dukungan Restart Dan Kebutuhan Pengolahan. Memastikan Bahwa Pengguna Menerima Output Yang Tepat Dengan Cara Yang Aman Dan Tepat Waktu.</p>	<p>Selama ini layanan yang diberikan hanya berdasarkan permintaan namun prosesnya tidak semua dilakukan perekaman.</p>	<p>Pembuatan rekaman semua proses layanan (permintaan dan proses pekerjaan).</p> <ul style="list-style-type: none"> <li>- SOP</li> <li>- SFK</li> </ul>
<p>4. Memastikan standar keamanan yang berlaku dalam menerima, memproses, mengolah data dan mengeluarkan output data dipastikan sesuai standar keamanan yang diterapkan juga dipastikan dan sesuai dengan tujuan perusahaan dan aturan yang berlaku</p>	<p>Belum tersusunnya standar keamanan terhadap masing-masing layanan.</p>	<p>Melengkapi buku keamanan Informasi dengan standar keamanan masing-masing layanan.</p>
<p>5. Menjadwalkan pengambilan dan pencatatan backup sesuai dengan kebijakan dan prosedur yang telah ditetapkan.</p>	<p>Sudah dilakukan backup untuk masing-masing layanan namun masih ada jadwal dan pemeliharaan backup data secara otomatis dan belum.</p>	<p>Pembuatan SOP dan SFK pemeliharaan backup data tiap-tiap layanan.</p>

#### D. Pembuatan Rekomendasi Berdasarkan Bidang Fokus

Tahapan selanjutnya adalah pengelompokan rekomendasi di klausul-klausul tiap proses DSS menjadi 4 (empat) kategori. Kategori tersebut terdiri dari **1. Kebijakan, 2. Prosedur, Formulir, Instruksi Kerja, 3. Sistem, Fitur, Tools dan 4. Tindakan Lainnya.**

Penjelasan rekomendasi tiap proses dapat dilihat pada contoh tabel-tabel berikut ini:

Tabel 4.9 Tabel Rekomendasi Kategori Kebijakan

NO	ISI REKOMENDASI	KLAUSUL
1	Dibuatkan SK personel matriks penugasan untuk kegiatan operasional	DSS 01.01.02
2	Melengkapi buku kebijakan keamanan Informasi untuk menerima,	DSS 01.01.04

	memproses, mengolah data dan mengeluarkan output data	
3	Dst...	

Tabel 4.10 Tabel Rekomendasi Kategori Prosedur, Formulir, Instruksi Kerja

NO	ISI REKOMENDASI	KLAUSUL
1	Menyusun SOP layanan End Point security.	DSS 01.01.01
2	Memperbaiki format SOP layanan sesuai dengan nama Unit Kerja baru.	DSS 01.01.01
3	Dst...	

Tabel 4.11 Tabel Rekomendasi Kategori Sistem, Fitur, Tools

NO	ISI REKOMENDASI	KLAUSUL
1	Update konten faq website Helpdesk secara berkala	DSS 02.01.01
2	Implementasi daftar prioritas berdasarkan risk management	DSS 02.01.01 DSS 02.02.03
3	Dst..	

Tabel 4.12 Tabel Rekomendasi Kategori Tindakan Lainnya

NO	ISI REKOMENDASI	KLAUSUL
1	Perlu memperhatikan serta di patuhi isi kontrak apakah telah mencakup keamanan informasi dan operasional	DSS 01.02.01 DSS 01.02.02
2	Menentukan standar audit yang sesuai.	DSS 01.02.04
3	Dst	

#### E. Pembuatan Prioritas Pengembangan

Tahapan Terakhir adalah membuat tabel prioritas dalam pengembangan tata kelola untuk mencapai sesuai kebutuhan standar, atau untuk mencapai level *maturity* sesuai dengan COBIT 5.

Tabel 4.13 Tabel Prioritas Pengembangan

NO	ISI REKOMENDASI	DSS	KETERANGAN	KODE
1	Menyusun identifikasi peralatan TI terhadap ancaman lingkungan.	DSS 01.04.02	Buku BCP	BCP
2	Membuat prioritas penanganan berdasarkan dampak bisnis dan urgensi	DSS 03.01.04		BCP
3	Perlu ada perbaikan BCP disesuaikan dengan organisasi yang baru.	DSS 04.01.03; DSS 04.02.01; DSS 04.02.02		BCP

4	Perlu dibuat perencanaan berkelanjutan untuk menunjang keberlanjutan bisnis TI.	DSS 04.01.03		BCP
5	Perlu perbaikan buku panduan manajemen BCP PMI.	DSS 04.02.03		BCP
6	Menambahkan Proses Bisnis TI di dokumen BCP	DSS 06.01.01	aliran proses bisnis	BCP
7	"Update secara berkala manajemen resiko, kegiatan kontrol, review triwulan, kaji ulang Identifikasi level didokumentasi Reviu dokumen manajemen resiko"	DSS 06.01.02; DSS 06.01.03; DSS 06.01.04; DSS 06.01.05		BCP
8	Dst.....			

### Penerapan ITIL V3 Bidang Infrastruktur Informasi

Penerapan ITIL v3 di BPPT khususnya di Bidang Infrastruktur Informasi , adalah dalam rangka kemudahan operasional infrastruktur, dimana peralatan semakin banyak dan tersebar, sehingga kompleksitas semakin tinggi. Untuk menerapkan maka diikuti langkah langkah sebagai berikut:

Memulai Penerapan ITIL di Bidang Infrastruktur Informasi , diawali dalam lingkup *service operation*, yang berhubungan secara intens, dengan pengguna infrastruktur informasi, dan saat ini yang telah dilaksanakan adalah pengelolaan insiden atau *Incident Management*. *Interface* untuk menaganinya adalah dengan adanya fungsional *service desk*.

**Where to start**

It is recommended starting with what are called with "Customer Facing" processes such as Incident, Service Level and Change Management, which have daily interaction and visibility with the Business.

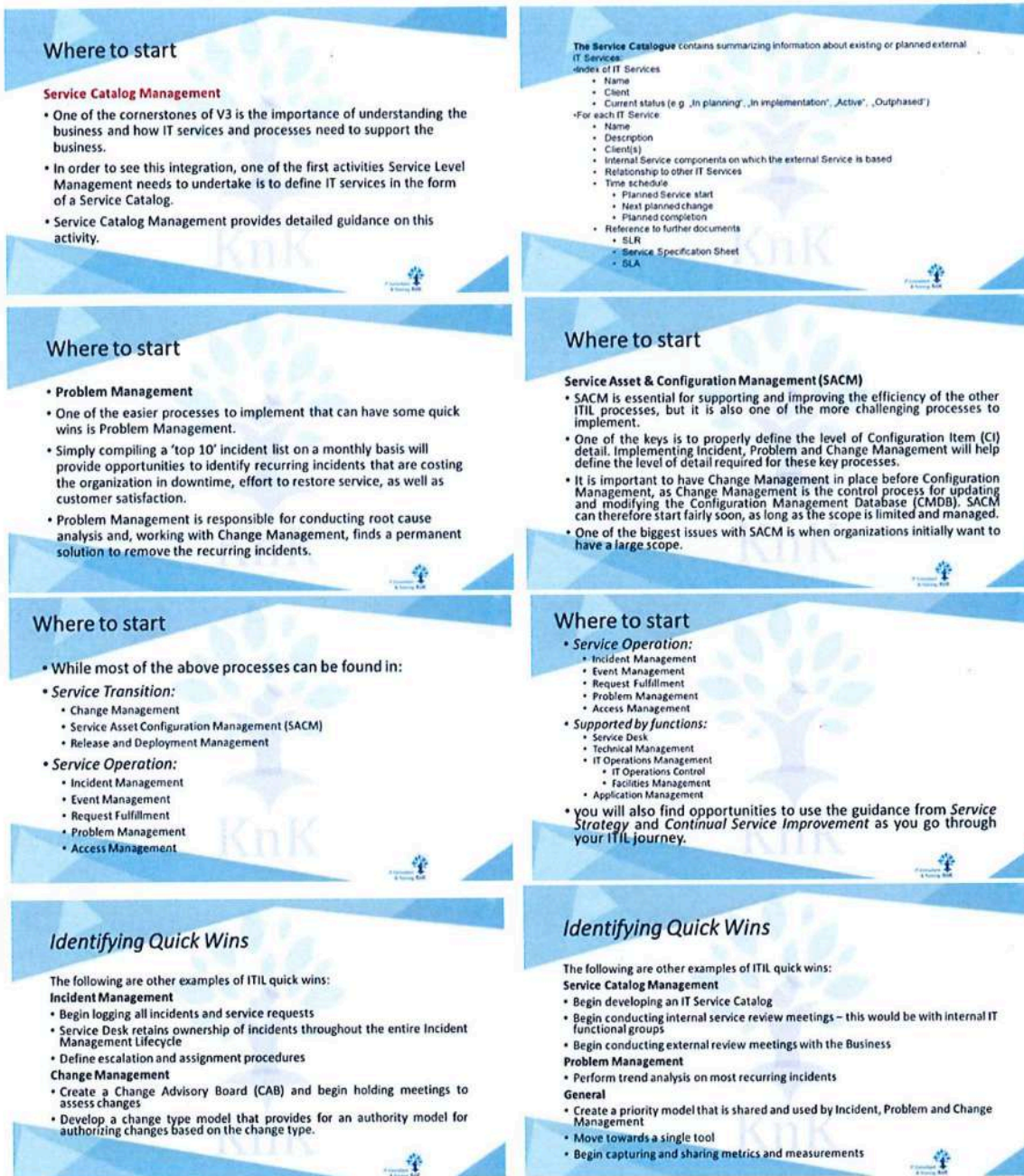
**Incident Management & Service Desk**

- Incident Management is responsible for restoring service and is considered a data gathering process that is critical to support other ITIL processes. The Service Desk is a functional group that plays a major role in Incident and Knowledge Management.
- As well, the Service Desk is a single point of contact for multiple process activities and for communication to the end user community and Business.

**Where to start**

**Change Management**

- Change Management, considered a control process, is important to gain a single view of all changes impacting an organization daily.
- The process is also responsible for properly assessing and authorizing changes based on change type criteria.
- Implementing a strong Change Management process will also help strengthen the Release and Deployment processes, as it will define certain requirements (including planning and testing) as a change moves through the lifecycle.



Gambar 4.11 Urutan Pengembangan Tata Kelola, Pemilihan Tema Utama  
 Sumber: Training Pengembangan Tata Kelola Infrastruktur TIK BPPT,  
 IT consultant and training KnK, 2017

Sesuai dengan keinginan pengembangan tata kelola yang mementingkan *service operation*, maka untuk ~~men-support insiden manajemen, operation manajemen dan problem manajemen~~ maka dibangun manajemen *service desk*.

### Manajemen *Service Desk*

*Service desk* adalah *group* fungsional yang mempunyai tugas sebagai *single point of contact* yaitu untuk memudahkan pengguna layanan infrastruktur berkomunikasi. Melalui *service desk* maka kebutuhan informasi, juga laporan insiden, serta manajemen pengetahuan dapat

dilaksanakan. *Service desk* mempunyai peran yang penting dalam pengelolaan insiden dan pengelolaan pengetahuan.

Layanan di Bidang Infrastruktur Informasi terbagi menjadi tiga kategori, dimana setiap kategori terdapat layanan yang cara penanganannya lewat *service desk*.

1. Kategori pertama yaitu layanan yang dapat diselesaikan sendiri oleh grup *service desk*. Saat ini ada 3 layanan yaitu layanan intranet, layanan *e-mail*, layanan keamanan informasi. Grup *service desk* sebagai pemilik layanan ini.
2. Kategori layanan kedua adalah server dan *data center*, yang dimiliki oleh suatu grup tersendiri yang lebih intens dengan server dan *data center*. Di dalamnya terdapat layanan kolaborasi dokumen dan layanan server *Cloud*.
3. Kategori ketiga adalah layanan yang lebih memerlukan ketelitian dan kemampuan dalam sistem pengaturan infrastruktur informasi yang disebut sebagai kategori infrastruktur akses internet. Di dalamnya ada layanan koneksi internet dan Layanan *IP Based Communication*.

Proses yang ada dalam manajemen *service desk* dalam proses layanan infrastruktur dapat dilihat pada Gambar 3.2. (Diagram proses layanan infrastruktur). *Service desk* merupakan ujung layanan atau sebagai *single point of contact* di Bidang Infrastruktur Informasi . Maka dalam pandangan tata kelola yang mengikuti ITIL v3, maka *service desk* berfungsi juga di dalamnya melaksanakan sebagian besar dari manajemen insiden dan manajemen pengetahuan. Terutama untuk layanan internet, layanan *e-mail* dan layanan keamanan informasi, *service desk* dapat melaksanakan manajemen insiden, dengan menerima informasi serta menagani insiden, untuk disampaikan kepada admin layanan terkait, atau memberikan solusi langsung ke pengguna untuk masalah yang sifatnya bukan masalah serius yang harus ditangani di manajemen *problem*. *Service desk* dengan peralatan atau *tools* manajemen pengetahuan, disamping digunakan bagi grup fungsional, hasilnya juga dapat digunakan oleh pengguna dalam menyelesaikan masalah sederhana.

Urutan kerja dari proses yang ada di *service desk* sebagian besar sudah diatur dalam SOP, dan SIK dari masing-masing tema layanan, serta formulir yang digunakanpun tersedia.

### Manajemen *Service Catalog*

Layanan infrastruktur informasi di BPPT dapat dicek di *service catalog*, dimana untuk tahun 2018 ini dapat dibagi dalam kategori layanan sebagai berikut.

Tabel 4.14 Tabel *Service Catalog* Layanan BII

Service Kategori	
<b>A Service Desk</b>	
1	Layanan Intranet
2	Layanan Email
3	Layanan Keamanan Informasi
<b>B Server dan Data Center</b>	

4	Layanan Kolaborasi Dokumen
5	Layanan Server Cloud
	i. Permintaan VPS
	ii. Permintaan Subdomain dan IP Address
	iii. Permintaan Colocation
	iv. Permintaan pengiriman Notifikasi dan peringatan event
	v. Permintaan SSL
	vi. Permintaan Load Balancing
	vii. Permintaan WAF dan Security Assessment
	viii. Permintaan koneksi ke SSO
<b>C Infrastruktur Akses Internet</b>	
6	Layanan Koneksi Internet
	i. Permintaan koneksi internet (wired)
	ii. Permintaan koneksi wifi adhoc
7	Layanan IP Based Communication
	i. Permintaan Video Conference
	ii. Permintaan IP Phone
	iii. Permintaan Dukungan Teknis IPTV / Live Streaming
	iv. Permintaan Video on Demand

Sebagai contoh detail dari layanan ini dapat disusun dalam tabel sebagai layanan yang lengkap menunjuk pada jenis service yang detail, didalamnya juga memberi informasi yang lengkap sebagai berikut.

Tabel 4.15 Detail Layanan *Service Catalog* Layanan BII

Service Category:		Service Desk					
Service Description:		Layanan penyediaan infrastruktur server berbasis <i>Virtual Machine</i> (VM) baik digunakan untuk Production ataupun Development dalam Sistem Cloud BPPT.					
Ref#	Service	Service Definition	Base Level Services	Services Not Included	Custom Services	Service Availability	Service Charge(s)
1.1	Reset Password Akun	Instruksi atau panduan untuk membantu pengguna yang mengalami lupa password	<ul style="list-style-type: none"> <li>- Membimbing dalam melakukan reset password mandiri</li> <li>- Membantu melakukan reset password akun SSO</li> <li>- Membantu dalam mengelola data di intranet</li> </ul>	<ul style="list-style-type: none"> <li>- Mengaktifkan kembali status nonaktif Sidadu</li> <li>- Meresetkan password selain akun pemohon</li> <li>- Meresetkan password akun jabatan atau kegiatan unit tanpa persetujuan Kepala Unit Kerja</li> </ul>		- Hari kerja (Senin - Jumat), pukul 7:30 - 15:00 WIB	Gratis
1.2	Permintaan Akun akses internet	Instruksi atau panduan untuk melakukan pembuatan	<ul style="list-style-type: none"> <li>- Membuat akun akses internet di firewall beserta</li> </ul>	<ul style="list-style-type: none"> <li>- Melakukan reset password akun akses internet</li> <li>- Membuat akun</li> </ul>		- Hari kerja (Senin - Jumat), pukul 7:30 - 15:00	Gratis

		atau perpanjangan waktu untuk akun akses internet di Firewall	password - Menambah masa aktif akun akses internet di firewall - Menghapus akun akses internet di Firewall	akses internet tanpa persetujuan Kepala Unit Kerja		WIB	
2.1	Pembuatan Akun Email BPPT	Layanan untuk memberikan fasilitas alamat surat elektronik kepada pegawai BPPT untuk kepentingan kelembagaan	- Membuat email baru dan passwordnya - Proses pembuatan email menunggu proses sinkronisasi pada tengah malam	- Mengganti username email ketika email sudah dibuat - Melakukan konfigurasi email lanjutan / preferences (seperti filtering, notifikasi, dsb.) - Memasukan isi kontak, task, calendar, dsb ke dashboard webmail. - Melakukan konfigurasi email client	- Peningkatan kuota email (hanya untuk email jabatan dan kegiatan) - Membuat username dan password yang tidak sesuai standar aturan yang telah ditetapkan penyedia layanan email - Email dibuat segera (kurang dari 24 jam)	- Peningkatan kuota email tergantung dari ketersediaan kapasitas mail server - Hari kerja (Senin - Jumat), pukul 7:30 - 15:00 WIB	Gratis

Seluruh layanan dikumpulkan dalam sistem katalog layanan dan hasil layanan kemudian diukur, misalnya berapa lama suatu layanan diselesaikan. Bilamana suatu penyelesaian layanan sudah terukur, maka dalam suatu layanan tersebut dapat dilakukan suatu bentuk SLA dengan suatu ukuran tertentu. Dengan demikian untuk integrasi dengan manajemen SLA, proses selanjutnya adalah menyeimbangkan antara kebutuhan bisnis yang ada di BPPT, sehubungan dengan kebutuhan layanan Infrastruktur yang bisa dilakukan dengan SLA yang sudah disepakati (ini dapat dilihat dari kolom *custome service*).

### Manajemen Perubahan

Kriteria perubahan Infrastruktur yang ada di BII dapat dibagi dalam 2 kelompok perubahan. Pertama perubahan besar yang mempengaruhi pelaksanaan kerja atau bisnis yang ada di BPPT. Jenis perubahan ini, baik yang diusulkan oleh manajemen tingkat atas maupun untuk keperluan khusus. Perubahan ini diperintah dan dipertanggungjawabkan oleh Kepala Bidang Infrastruktur Informasi.

Kedua perubahan kecil yang dilaksanakan oleh masing masing layanan, yang dilakukan dalam rangka permasalahan teknis, peningkatan teknologi, pelaksanaan optimasi sistem serta untuk menangani *problem* yang terjadi. Penanggungjawab perubahan ini adalah administrator layanan yang terkait. Adapun untuk integrasinya tergantung luasan cakupan perubahan, apakah pada level Sub Bidang Pengembangan atau Optimasi. Adapun bila pengaruhnya meluas, maka

Kepala Bidang Infrastruktur Informasi ikut mengetahui dan bertanggungjawab atas perubahan yang dilakukan.

Guna memberikan ketentuan dan urutan proses manajemen perubahan ini, maka Kepala Bidang Infrastruktur Informasi perlu memiliki alur proses perubahan bagi tiap layanan yang ada di Bidang Infrastruktur Informasi .

### Manajemen Masalah

Untuk manajemen masalah sebetulnya secara rutin sudah dilaksanakan. Adapun usaha untuk menyempurnakan dilakukan pendetailan dalam sub proses. Berikut ini adalah sub proses dari manajemen masalah:

- a. Mengidentifikasi Masalah Proaktif  
Pelaksanaan sub proses ini dilakukan dengan meningkatkan *tools* monitoring dan analisis terhadap masalah yang dihadapi. Tujuan proses adalah untuk meningkatkan ketersediaan layanan secara keseluruhan dengan mengidentifikasi masalah secara proaktif. Artinya untuk mengidentifikasi dan memecahkan masalah dan menyediakan solusi yang tepat sebelum insiden muncul kembali.
- b. Melakukan Kategorisasi dan Penetapan Prioritas, terhadap masalah yang perlu diselesaikan. Ini bertujuan untuk memprioritaskan masalah dengan ketelitian yang tepat, karena kebutuhan bisnis yang lebih besar, untuk memfasilitasi penyelesaian yang cepat dan efektif.
- c. Melaksanakan Diagnosis Masalah dan Resolusi, bila masalah terjadi dan perlu dicari solusi secepatnya. Ini bertujuan untuk mengidentifikasi akar penyebab masalah dan mulai memberi solusi yang paling tepat dan ekonomis. Jika memungkinkan, solusi sementara disediakan.
- d. Memantau Masalah dan Kontrol Kesalahan. Untuk selalu memantau masalah yang luar biasa terkait dengan status pemrosesan mereka. Kontrol kesalahan dilakukan dimana langkah-langkah perbaikan yang diperlukan atau dapat diperkenalkan.
- e. Pelaporan Manajemen Masalah, ini diperlukan bertujuan untuk memastikan bahwa proses 'Manajemen Layanan' berjalan dengan baik dan 'Manajemen Masalah' berhasil.

### Manajemen Aset dan Manajemen Konfigurasi

Manajemen aset dan konfigurasi di Bidang Infrastruktur Informasi sebagaimana telah dilakukan pencatatan aset dilakukan menggunakan software iTOP, maka dalam hal ini untuk merealisasikan dengan baik maka pencatatannya perlu terus dipantau, mengingat antara real perubahan yang di peralatan kadang kurang cepat dimasukkan ke *database* yang ada tersebut

Bilamana pencatatan telah dapat dipastikan, dan diatur dengan baik maka *database* itu dapat dipakai sebagai dasar manajemen lainnya. Dengan demikian maka penerapan *framework* ITIL dalam Bidang Infrastruktur Informasi dengan demikian akan tetap dapat diperluas dan tata kelolanya dapat diperbaiki dan disesuaikan.

## **Penggabungan *Framework* Tata Kelola Infrastruktur informasi**

Untuk menyusun tata kelola berdasarkan *framework* COBIT 5 dan ITIL v3 , maka secara prinsip perlu ditelusur secara lebih rinci apa yang harus dilakukan, yaitu dengan mensejajarkan antara kedua *framework* dan kemudian dicari rekomendasi apa yang harus dilakukan perubahan, atau perbaikan dari tata kelola yang sudah ada, atau membuat suatu SOP, SIK, maupun form yang dibutuhkan untuk proses tertentu.

## BAB V

### DESAIN LAYANAN (*SERVICE DESIGN*)

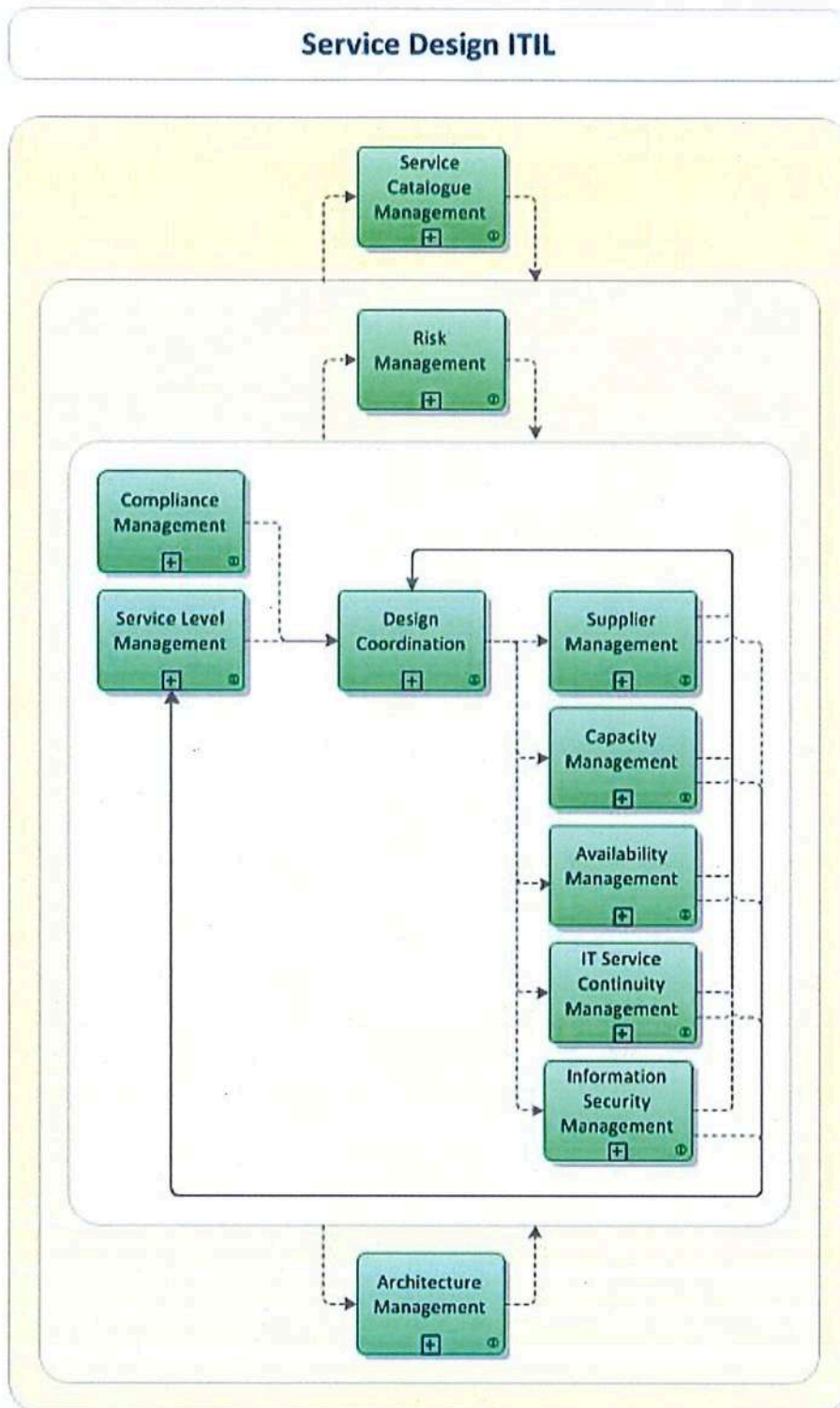
Agar layanan TI dapat memberikan manfaat kepada pengguna, layanan-layanan TI tersebut harus terlebih dahulu didesain dengan mengacu pada pemenuhan persyaratan pengguna. *Service design* memberikan panduan kepada organisasi TI untuk dapat secara sistematis dan *best practice* mendesain dan membangun layanan TI maupun implementasi ITSM itu sendiri. *Service design* berisi prinsip-prinsip dan metode-metode desain untuk mengkonversi tujuan-tujuan strategis organisasi yang memberikan layanan TI menjadi portofolio/koleksi layanan TI serta aset-aset layanan, seperti server, *storage* dan sebagainya.

Ruang lingkup *service design* tidak hanya untuk mendesain layanan TI baru, namun juga proses-proses perubahan maupun peningkatan kualitas layanan, kontinuitas layanan maupun kinerja dari layanan. Di lingkup pelaksanaan pekerjaan yang ada di BII, adalah mengembangkan infrastruktur terlebih dahulu sebelum mengembangkan layanan infrastruktur, dalam pengembangan infrastruktur itu sistem kerja kerekayasaan diterapkan. Proses pelaksanaan kerekayasaan adalah berurut dimulai dengan persiapan, perencanaan, perancangan atau desain, pengembangan atau pembangunan, testing, dan kemudian implementasi atau operasional, serta *maintenance*/pemeliharaan.

Dengan demikian untuk membentuk proses pelaksanaan yang dikendalikan oleh sub bidang pengembangan infrastruktur dan sub bidang optimasi infrastruktur, sehingga dalam implementasi secara detail akan terbagi disesuaikan dengan tugas dan fungsi masing-masing sub bidang.

Proses-proses yang dicakup dalam *service design* yaitu :

1. *Service Catalogue Management*
2. *Service Level Management*
3. *Supplier Management*
4. *Capacity Management*
5. *Availability Management*
6. *IT Service Continuity Management*
7. *Information Security Management*



Gambar 5.1 Diagram Proses *Service Design* (ITIL)

Beberapa proses yang penting perlu direalisasikan oleh BII, yang mengelola infrastruktur informasi, antara lain adalah *service catalogue management*, *service level management*, *capacity management* dan *availability management*.

Proses-proses yang sudah dilaksanakan di BII diantaranya adalah :

1. *Service Catalog Management*, yang dalam realisasi pelaksanaannya adalah
  - a. Adanya brosur daftar layanan
  - b. Selalu diperbaruhinya daftar layanan apabila ada layanan baru

c. Adanya dokumen *inventory service catalog*

Pengelolaan proses ini berada Praktik sub bidang optimasi infrastruktur.

2. *Service Level Management*, yang pada realisasinya yang terpenting adalah menyangkut availabilitas, dan kapasitas dari beberapa layanan. Karena layanan sifatnya internal masih banyak yang harus secara luas didokumentasi dan didiseminasikan. Juga masih banyak yang perlu dipersiapkan, oleh karena itu manajemen ini masih dipegang langsung oleh Kepala Bidang Infrastruktur Informasi .
3. *Supplier Management*, berhubungan dengan pemasok, baik untuk produk maupun jasa, dimana proses yang dilakukan di BPPT telah mempunyai aturan tersendiri dari mulai penganggaran hingga pelaksanaan. Dengan demikian BII tercatat sebagai *user*, atau pengguna dari barang dan jasa yang dipasok *supplier*. Dengan demikian proses manajemen ini menjadi tanggung jawab Kepala Bidang Infrastruktur Informasi .
4. *Information Security Management*, penanganan *security* disamping selalu dilakukan monitoring, adanya SOC (*Secure Operating Center*), serta dengan pembentukan organisasi CSIRT BPPT yang mempunyai tugas dan fungsi lebih luas, tidak saja memonitor keamanan juga menyebarkan informasi agar keamanan TI di BPPT tersebar luas dan termasuk informasi lain yang berkaitan dengan TI.

#### A. Manajemen Katalog Layanan (*Service Catalogue Management*)

Pada layanan infrastruktur yang diselenggarakan BII (Bidang Infrastruktur Informasi ), *service catalogue* adalah daftar layanan yang dapat lakukan atau diselesaikan dengan sebaik-baiknya oleh BII, dimana layanan itu dilaksanakan sesuai kebutuhan pengguna. Daftar layanan memberikan informasi serta penjelasan yang detail tentang layanan yang dimaksud. Dokumen tentang *service catalogue* ini terpisah dari buku ini, dipergunakan agar dapat memberikan informasi secara meluas kepada pengguna. Di dalamnya terdapat penjelasan tentang layanan apa yang bisa diberikan oleh BII. Dokumen yang terkait selanjutnya berupa dokumen tentang rencana layanan yang di dalamnya terdapat SAC (*Service Acceptance Criteria*) dan SLR (*Service Level Requirement*), dan dokumen yang berguna untuk keperluan internal BII yaitu *Inventory Service Catalogue*. *Inventory Service Catalogue* dipersiapkan untuk memberi kepastian pelayanan dapat dilaksanakan, sehingga layanan mempunyai SLA sesuai dengan yang telah dijanjikan. Selain itu tentang *Service Catalogue* ini dilengkapi pula informasi yang ada di *web* untuk dipergunakan agar dapat memberikan informasi secara meluas kepada pengguna.

Pelaksana yang bertanggung jawab dalam manajemen *service catalogue* adalah Kepala Sub Bidang Optimasi Infrastruktur. Adapun yang bertanggung jawab atas layanan adalah Kepala Bidang Infrastruktur Infomasi.

## B. Manajemen Tingkat Layanan (Service Level Management)

Manajemen tingkat layanan (SLM - *Service Level Management*) adalah pengelolaan dari tingkat layanan atau kualitas layanan agar ada kepastian yang lebih baik. Manajemen tingkat layanan (SLM) bertujuan untuk menegosiasikan perjanjian tingkat layanan dengan pengguna dan untuk merancang layanan sesuai dengan target tingkat layanan yang disepakati.

Proses yang ada dalam manajemen ini juga bertanggung jawab untuk memastikan bahwa semua perjanjian tingkat operasional dan kontrak pokok telah sesuai, serta memantau dan melaporkan tingkat layanan kepada atasannya. Manajemen tingkat layanan terutama bertanggung jawab untuk mengumpulkan persyaratan layanan, serta pemantauan dan pelaporan terkait dengan tingkat layanan yang disepakati.

Bagian proses terkait dengan manajemen tingkat layanan yang dilakukan adalah:

### a. Pemeliharaan Kerangka Kerja SLM

Pemeliharaan ini bertujuan untuk merancang dan memelihara struktur yang mendasari portofolio perjanjian pengguna, dan untuk menyediakan *template* untuk berbagai dokumen SLM.

Dasar kerangka kerja SLM diturunkan ke dalam program kerja kereyakasaan, terutama dalam perencanaan dan perancangan serta pengembangan. Dimana pada perencanaan dan pengembangan ini juga diawasi kesesuaiannya oleh Kepala Sub Bidang Pengembangan Infrastruktur. Kemudian penyiapan *testing* dan pemeliharaan serta optimasi layanan di bawah kendali sub b idang optimasiInfrastruktur.

Pada keadaan tertentu, sebagai yang dikenal dan realitas proses kerja, pelaksanaan *testing* dilakukan sebagai proses *service transition*, proses *testing* masih ada dalam tanggung jawab perekayasa dalam lingkup sub bidang pengembangan infrastruktur. Pemeliharaan kerangka kerja SLM menjadi tanggung jawab Kepala BII, dengan kerjasama Sub Bidang terkait.

### b. Identifikasi Persyaratan Layanan

Tujuan proses identifikasi adalah untuk memperoleh hasil yang diinginkan (persyaratan dari sudut pandang pengguna) untuk layanan baru atau modifikasi layanan utama. Persyaratan layanan harus didokumentasikan dan diserahkan pada evaluasi awal, sehingga alternatif dapat dicari pada tahap awal untuk persyaratan yang tidak layak secara teknis atau ekonomis.

Identifikasi persyaratan ini dilakukan oleh Kepala Bidang Infrastruktur Informasi atau struktur di atasnya, sebagai proses awal dan cara untuk mewakili pengguna yang ada di internal BPPT, disertai dengan input informasi maupun berdasarkan perkiraan kebutuhan yang bisa direalisasi. Identifikasi ini diperoleh berdasar perencanaan dan pengembangan infrastruktur yang ada di kereyakasaan.

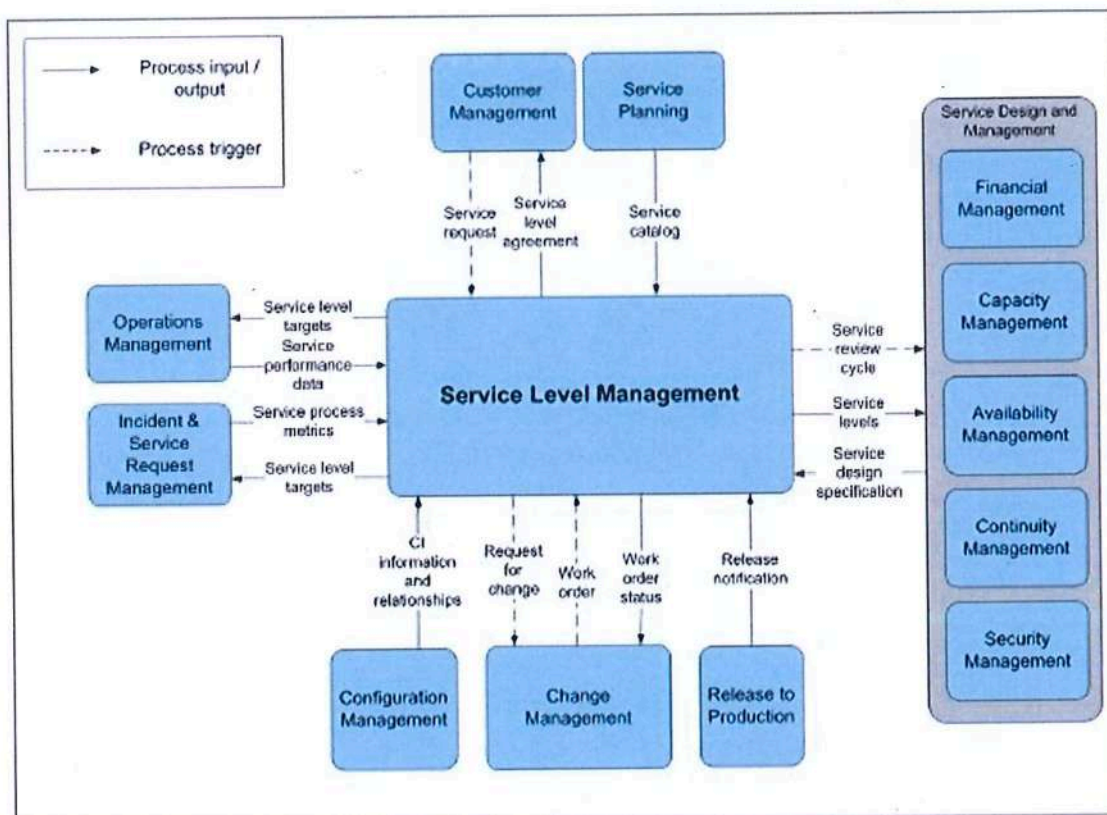
### c. Perjanjian *Sign-Off* dan Aktivasi Layanan

Tujuan proses ini adalah agar semua kontrak yang relevan ditandatangani setelah transisi layanan selesai, dan untuk memeriksa apakah kriteria penerimaan layanan terpenuhi. Secara khusus, proses ini memastikan bahwa semua *operating level agreement* (OLA)

yang relevan, dikontrak oleh pemilik layanan mereka, dan bahwa SLA ditandatangani oleh pengguna. Proses ini dilaksanakan untuk memberikan kepastian dan tanggung jawab layanan, sehingga perlu diusahakan adanya oleh Kepala BII, serta diatur secara internal oleh BII. Proses ini didasarkan dari hasil pengembangan infrastruktur, serta hasil *testing*.

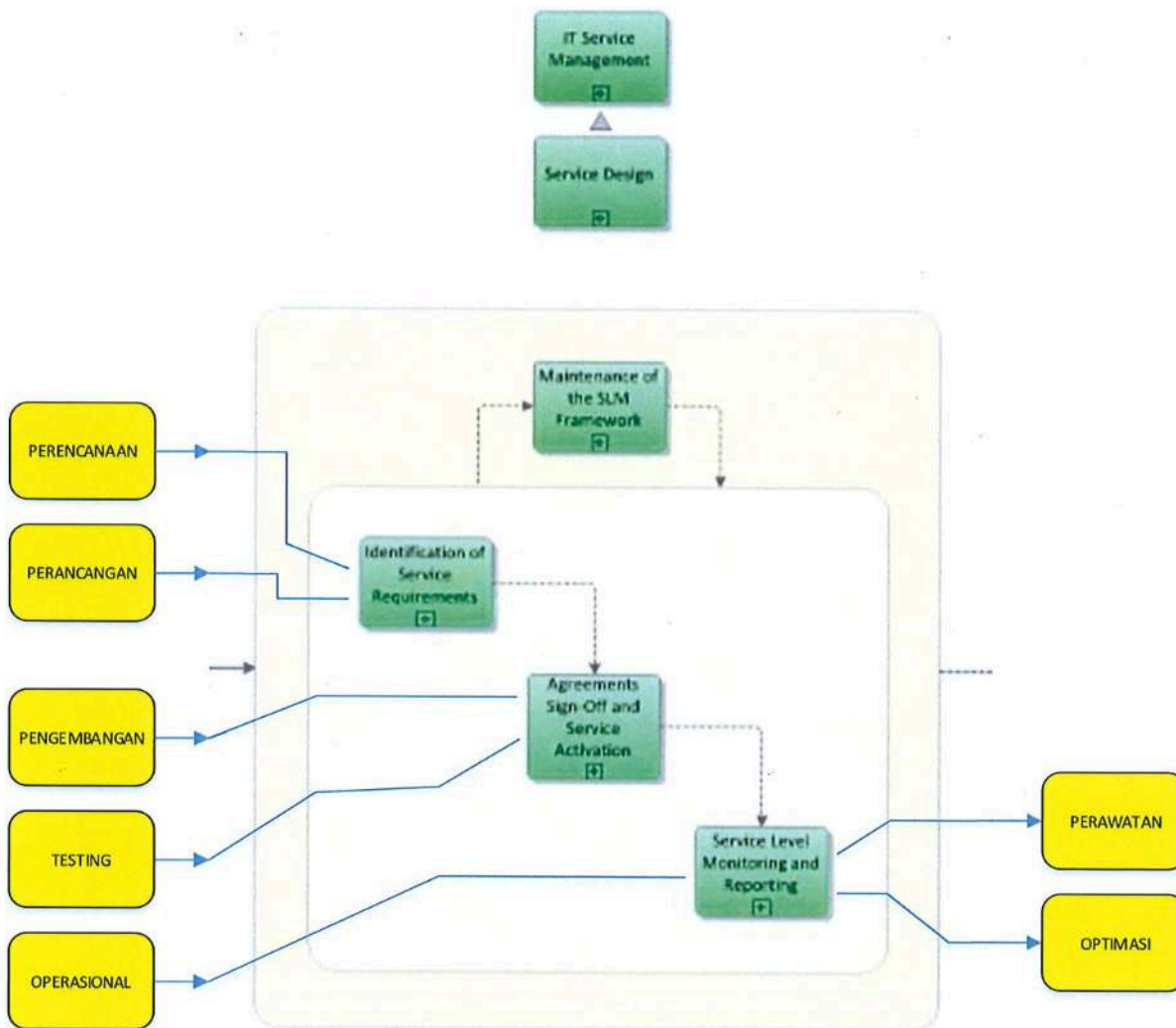
#### d. Pemantauan dan Pelaporan Tingkat Layanan

Tujuan proses pemantauan dan pelaporan adalah untuk memantau tingkat layanan yang dicapai dan dibandingkan dengan target tingkat layanan yang disepakati ("Laporan Tingkat Layanan"). Informasi ini diedarkan kepada pengguna dan semua pihak terkait lainnya, sebagai dasar untuk langkah-langkah untuk meningkatkan kualitas layanan. Pemantauan dan pelaporan ini mempunyai dasar dari proses pelaksanaan *testing* dan operasional dari infrastruktur, termasuk pula hasil *maintenance* dan optimasi Infrastruktur.



Gambar 5.7 *Service Level Management* dalam Lingkungan *Service Design*  
 Sumber: <http://tierrasalto.com/service-level-management/> 29 Juli, 2009

Untuk melengkapi ini maka BII perlu untuk melakukan pembuatan atau perbaikan *service level agreement*, dan pembuatan *operating level agreement* dari rekanan luar. Semua itu adalah dalam rangka untuk memenuhi keempat sub proses di atas.



Gambar 5.3 IT Service Management dalam Interaksi dengan Kerekayasaan  
 Sumber: *The ITIL Process Map v3 2011*, ditambah dimodifikasi

Sedang untuk melengkapi manajemen ini beberapa dokumen yang dapat berguna untuk manajemen ini antara lain :

### 1. Portofolio Perjanjian Pengguna

Meskipun katalog layanan memiliki daftar lengkap layanan yang dikelola oleh BII, namun portofolio perjanjian pengguna diperlukan karena memuat semua perjanjian layanan yang menyediakan kerangka kerja untuk memberikan layanan kepada pengguna tertentu. Portofolio perjanjian pengguna saat ini belum secara spesifik dibuat, karena layanan sifatnya internal, sehingga secara resmi belum diberikan arahan dengan karakteristik maupun batasan yang dapat dipakai sebagai acuan untuk memberikan layanan dengan kualitas tertentu. Akan tetapi, layanan tetap mempunyai dasar untuk selalu ditingkatkan sehubungan dengan perkembangan teknologi, kebutuhan, serta batasan biaya yang disediakan.

### 2. Perjanjian Tingkat Operasional (OLA)

Perjanjian antara penyedia layanan TI dan bagian lain dari organisasi yang sama. OLA mendukung pengiriman layanan penyedia layanan TI kepada pengguna. BII sebagai

penyedia layanan perlu untuk menyiapkan dokumen OLA, dengan beberapa unit kerja atau suatu bagian tertentu yang ada di BPPT, diantaranya dengan Biro Umum. OLA mendefinisikan barang atau jasa yang akan diberikan dan tanggung jawab kedua belah pihak.

Misalnya mungkin ada OLA – Layanan *Cloud* IaaS (*Infrastructure as a Service*) antara penyedia layanan TI (BII) dan beberapa organ seperti administrator, unit kerja lain seperti BJIK, dan sebagainya, untuk menjadikan layanan IaaS tersebut terjamin sampai pengguna. Contoh lain diantara adalah desk layanan (*Service Desk*) dan kelompok dukungan atau tim teknis untuk memberikan resolusi insiden dalam waktu yang disepakati (lebih detail lihat dokumen OLA). Dokumen ini dibuat terpisah dan dibagi per layanan agar mudah dan secara sistematis terbentuk serta mudah untuk ditelusur serta dirubah bila terdapat perubahan pada dokumen tersebut. Agar dokumen itu lengkap, maka garis besar persyaratan layanan, dan kriteria penerimaan layanan (SAC) bila memungkinkan sebaiknya juga tercantum di dalamnya.

### **3. Garis Besar Persyaratan Layanan**

Hasil yang diinginkan dari layanan, dinyatakan dalam hal fungsi layanan yang diperlukan (utilitas) dan tingkat layanan (garansi). Berdasarkan informasi ini, persyaratan layanan rinci ditentukan selama tahap desain layanan. Kepala Sub Bidang Pengembangan Infrastruktur bertanggung jawab untuk menyusun desain layanan.

### **4. Kriteria Penerimaan Layanan (SAC)**

SAC adalah seperangkat kriteria yang digunakan untuk pengujian penerimaan layanan, untuk memastikan bahwa layanan TI memenuhi fungsionalitas dan persyaratan kualitas, serta BII siap untuk mengoperasikan layanan baru yang siap dijalankan. Kriteria ini dipersiapkan, didokumentasikan pada OLA maupun SLA, dan dapat diajukan dan dipersyaratkan oleh Kepala Sub Bidang Optimasi Infrastruktur.

### **5. Perjanjian Tingkat Layanan (SLA)**

Perjanjian antara penyedia layanan TI (BII) dan pengguna. SLA menjelaskan layanan TI, mendokumentasikan target tingkat layanan, dan menetapkan tanggung jawab penyedia layanan TI dan pengguna. SLA tunggal dapat mencakup beberapa layanan atau beberapa pengguna (lihat juga daftar periksa ITIL SLA - OLA).

### **6. Laporan Tingkat Layanan**

Laporan Tingkat Layanan memberikan wawasan tentang kemampuan penyedia layanan untuk memberikan kualitas layanan yang disepakati. Untuk tujuan ini, perlu membandingkan tingkat layanan yang disetujui dan yang benar-benar dicapai, dan juga termasuk informasi tentang penggunaan layanan, langkah-langkah berkelanjutan untuk peningkatan layanan dan laporan setiap kejadian luar biasa. Laporan tingkat layanan dikeluarkan oleh penyedia layanan untuk penggunaannya, manajemen TI dan proses manajemen layanan lainnya. Laporan serupa juga dibuat oleh pemasok layanan eksternal untuk mendokumentasikan kinerja layanan yang dicapai.

### **7. Persyaratan Tingkat Layanan (SLR)**

Dokumen Persyaratan Tingkat Layanan berisi persyaratan untuk layanan dari sudut pandang pengguna, mendefinisikan target tingkat layanan terperinci, tanggung jawab bersama, dan persyaratan lainnya khusus untuk pengguna (kelompok) tertentu. Ketika layanan memasuki tahapan baru dari siklus hidupnya, dokumen SLR bisa berkembang menjadi sebuah rancangan perjanjian tingkat layanan. Persyaratan ini dapat dicantumkan di OLA maupun SLA sesuai kebutuhan dan urgensinya.

### C. Manajemen Pemasok (*Supplier Management*)

Tujuan dari manajemen pemasok adalah untuk memastikan bahwa semua kontrak dengan pemasok dapat mendukung kebutuhan bisnis. Proses ini juga bertanggung jawab untuk memastikan bahwa semua pemasok memenuhi komitmen kontraktual mereka.

Karena proses dan manajemen terkait dengan pemasok telah diatur di BPPT, maka BII tidak secara penuh melakukan manajemen ini. Manajemen pemasok ini sudah diatur dengan adanya berbagai bentuk aturan dan organisasi seperti LPSE, ULP dan sebagainya. Oleh karena itu manajemen pemasok yang dilakukan BII hanya terbatas terutama pemasok tertentu untuk menjaga layanan BII agar bisa didukung pemasok dan dijamin mempunyai hasil yang sebaik mungkin. Untuk itu secara praktis BPPT harus menyediakan, atau melakukan sub proses sebagai berikut. Untuk melaksanakan pengelolaan pemasok ini ada beberapa hal yang perlu di persiapkan antara lain:

a. Menyediakan Kerangka Manajemen Pemasok

Tujuan adanya kerangka manajemen pemasok untuk memberikan panduan dan standar untuk pengadaan layanan dan produk yang akan diterima. Ini termasuk penyediaan strategi pemasok dan persiapan syarat dan ketentuan standar baik pemasok maupun jasa dan produknya.

b. Evaluasi Pemasok dan Kontrak Baru

Tujuan proses ini untuk mengevaluasi calon pemasok sesuai dengan strategi pemasok, dan untuk memilih pemasok yang paling sesuai.

c. Menetapkan Pemasok dan Kontrak baru

Walaupun penetapan pemasok bisa terjadi pada lembaga lain, tujuan proses penetapan ini untuk membantu dalam bernegosiasi dan dasar menandatangani kontrak yang mengikat dengan pemasok. Proses ini terutama diterapkan untuk investasi yang signifikan, barang dan jasa yang sangat mempengaruhi layanan BII, baik layanan yang disediakan eksternal atau dalam bentuk teknologi tertentu.

d. Pemasok dan Tinjauan Kontrak

Tujuan Proses ini adalah untuk memverifikasi apakah kinerja yang disepakati kontrak benar-benar telah dikirim pemasok, dan untuk menentukan tindakan perbaikan jika diperlukan (lihat lebih detil pada contoh "Pemasok dan Tinjauan Kontrak" dan hasil verifikasi).

e. Pembaruan Kontrak atau Penghentian

Tujuan proses ini untuk melaksanakan perpanjangan kontrak secara berkala, menilai apakah kontrak tersebut masih relevan, dan untuk mengakhiri kontrak yang tidak lagi diperlukan.

Manajemen pemasok ini (butir a. sampai dengan e.) sudah diatur dengan adanya berbagai bentuk aturan di atas BII dan dilakukan oleh organisasi pengelolaan pengadaan di BPPT seperti LPSE, ULP dan seterusnya. BII sebagai *user*, yang menyiapkan beberapa dokumen yang perlu dipersiapkan berhubungan dengan *supplier management*. Untuk melaksanakan proses tersebut di atas maka dokumen yang dipersiapkan meliputi meliputi dokumen kontrak, dokumen SLA, dokumen RAB dan dokumen lain yang berkaitan.

Berikut ini beberapa objek informasi yang digunakan dalam manajemen pemasok untuk menjadikan proses di atas dapat dilaksanakan dengan baik, yaitu:

#### 1. Pesanan Pembelian

Pesanan untuk membeli barang atau jasa dari pemasok. Pesanan ini harus dipersiapkan terlebih dahulu, persiapan adalah dengan adanya perencanaan, sebagaimana proses yang berlaku di instansi pemerintahan, perencanaan atau pemesanan ini dilakukan di tahun sebelumnya. Tetapi bila dapat dilakukan revisi, maka pesanan dapat diperbaiki karena alasan tertentu. Jika pesanan untuk layanan pendukung yang disediakan secara eksternal, ini disertai dengan mendasari kontrak yang mendefinisikan target tingkat layanan.

Pesanan dapat pula didasari dari hasil kerja kerekayasaan yang memberikan usulan atas spesifikasi, maupun kriteria yang menjadi kebutuhan untuk meningkatkan ketersediaan, kehandalan dan kapasitas infrastruktur yang berpengaruh pada peningkatan layanan.

#### 2. Permintaan Pembelian

Permintaan untuk membeli layanan atau produk dari pemasok eksternal, yang dikeluarkan misalnya dari manajemen rilis selama pembuatan layanan. Permintaan pembelian produk barang maupun jasa, pertama ada kesesuaian dengan perencanaan besar di RITI, mengikuti konsep dasar arsitektur yang ada, serta memiliki kesesuaian dengan perencanaan yang dilaksanakan pada program kerekayasaan yang ada. Memproses permintaan pembelian biasanya akan dilanjutkan hanya jika pemohon juga memegang anggaran yang disetujui untuk pembelian.

#### 3. Syarat dan Ketentuan Standar

Seperangkat persyaratan dan ketentuan yang secara rutin dilampirkan pada kontrak dan pesanan saat mendapatkan layanan atau produk. Persyaratan ini minimal perlu diketahui oleh Kepala BII.

#### 4. Supplier dan Sistem Informasi Manajemen Kontrak (SCMIS)

Pemasok dan sistem informasi manajemen kontrak adalah *database* atau dokumen terstruktur yang digunakan untuk mengelola pemasok dan kontrak selama siklus hidup mereka. SCMIS berisi atribut kunci dari semua kontrak dengan pemasok, dan harus menjadi bagian dari sistem manajemen pengetahuan layanan. Sistem dikelola unit lain (LPSE dan yang lain).

#### 5. Laporan Pertemuan Ulasan Pemasok dan Kontrak

Untuk perpanjangan kontrak atau kontrak baru perlu pertemuan dengan pemasok dan rapat peninjauan ulang kontrak, dengan mengadakan dokumen yang telah dicapai dan kinerja pemasok yang disepakati. Dokumen juga berisi tentang kelemahan dan masalah pemasok yang teridentifikasi, serta saran tentang bagaimana situasi dapat ditingkatkan.

#### **6. Evaluasi Pemasok**

Dokumen ini dihasilkan dari proses evaluasi pemasok, menjelaskan secara rinci kriteria yang digunakan untuk mengevaluasi dan memilih pemasok yang sesuai. BII sebaiknya mengeluarkan dokumen ini agar dapat memberikan alasan yang memberikan data yang benar untuk perbaikan di tahun mendatang. Evaluasi pemasok ini dapat dibuat terpisah atau bisa pula dicantumkan atau digabung dengan laporan tingkat layanan pemasok.

#### **7. Laporan Tingkat Layanan Pemasok**

Laporan tingkat layanan pemasok memberikan wawasan tentang kemampuan pemasok eksternal penyedia layanan untuk memberikan kualitas layanan yang disepakati. Untuk tujuan ini, maka perlu membandingkan tingkat layanan yang disetujui dan yang benar-benar dicapai, dan juga termasuk informasi tentang penggunaan layanan, langkah-langkah berkelanjutan untuk peningkatan layanan, dan setiap kejadian luar biasa.

#### **8. Strategi Pemasok**

Dokumen ini untuk mencatat pengalaman dan cara yang harus dilakukan menghadapi Pemasok, yang spesifik untuk layanan tertentu yang sangat diperlukan BII, seperti ISP *bandwidth* internet. Strategi pemasok menetapkan pedoman untuk pengadaan layanan dan barang. Ini biasanya termasuk kriteria untuk pemilihan pemasok yang sesuai dan daftar pemasok yang disarankan.

#### **9. *Underpinning Contract* (UC)**

Sebuah kontrak antara penyedia layanan TI (BII) dan pihak ketiga. Pihak ketiga menyediakan layanan pendukung yang memungkinkan penyedia layanan untuk memberikan layanan kepada pengguna. Oleh karena itu, *Underpinning Contracts* harus diselaraskan dengan perjanjian tingkat layanan (SLA) yang disepakati pengguna dari BII.

### **D. Manajemen Kapasitas (*Capacity Management*)**

Manajemen kapasitas bertujuan untuk memastikan bahwa kapasitas layanan TI dan infrastruktur TI mampu memberikan target tingkat layanan yang disepakati dengan biaya yang efektif dan tepat waktu. Proses manajemen kapasitas mempertimbangkan semua sumber daya yang diperlukan untuk memberikan layanan TI, dan rencana untuk kebutuhan bisnis jangka pendek, menengah dan panjang.

Proses yang ada dalam manajemen kapasitas ini adalah:

- a. Manajemen Kapasitas Bisnis

Tujuan Proses: Untuk menerjemahkan kebutuhan bisnis dan rencana ke dalam kapasitas dan persyaratan kinerja untuk layanan dan infrastruktur TI, dan untuk memastikan bahwa kapasitas dan kinerja kebutuhan masa depan dapat terpenuhi.

b. Manajemen Kapasitas Layanan

Tujuan Proses: Untuk mengelola, mengendalikan dan memprediksi kinerja dan kapasitas layanan operasional. Ini termasuk memulai tindakan proaktif dan reaktif untuk memastikan bahwa kinerja dan kapasitas layanan memenuhi target yang disepakati.

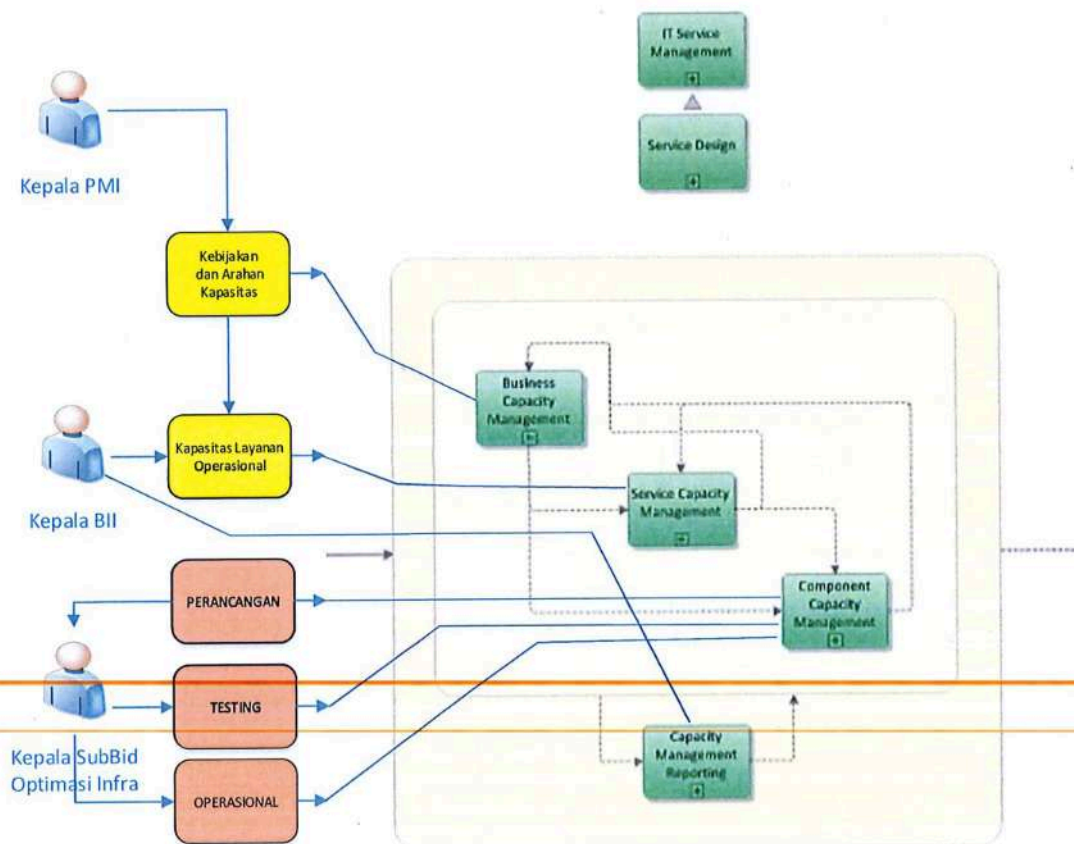
c. Manajemen Kapasitas Komponen

Tujuan Proses: Untuk mengelola, mengendalikan dan memprediksi kinerja, pemanfaatan dan kapasitas sumber daya TI dan komponen TI individu.

d. Pelaporan Manajemen Kapasitas

Tujuan Proses: Untuk menyediakan proses manajemen layanan dan manajemen TI lainnya dengan informasi yang terkait dengan layanan dan kapasitas sumber daya, pemanfaatan dan kinerja adapun hasil atau output pelaporan ini adalah "Laporan Kapasitas".

Dalam rangka memenuhi proses tersebut di atas maka untuk perencanaan, *forecast*, arahan kebijakan serta laporan dibuat suatu dokumen laporan kapasitas berdasarkan tahun kerja.



Gambar 5.4 Diagram Alur Pelaksanaan Manajemen Kapasitas

Pelaksanaan manajemen kapasitas oleh PMI diuraikan dalam rencana strategis PMI, atau arahan Kepala PMI, yang kemudian diterjemahkan dalam setiap layanan yang diberikan BII, untuk direncanakan dan diimplementasikan sebagai kapasitas layanan operasional. Karena setiap layanan bergantung pada komponen atau sumberdaya TI yang digunakan, seperti komponen *server, storage, bandwidth network*, dan komponen sistem jaringan lainnya, maka manajemen kapasitas akan diuraikan berdasarkan dari setiap komponen yang mempengaruhinya.

Untuk itu maka dalam pengelolaan kapasitas ini, komponen dan sumberdaya TI yang ada harus dimonitor setiap saat dan bila tren meningkat perlu diwaspadai untuk dipersiapkan atau direncanakan dalam antisipasinya. Kepala Sub Bidang Optimasi Infrastruktur bertanggung jawab dalam memonitor, menganalisis, serta memberikan rekomendasi, untuk menampilkan data yang ada.

Kepala Bidang BII melaporkan keadaan kapasitas, dan perkiraan ke depan untuk memberikan informasi kepada Kepala PMI sebagai bahan pertimbangan untuk memberikan arahan kebijakan agar dapat dilaksanakan.

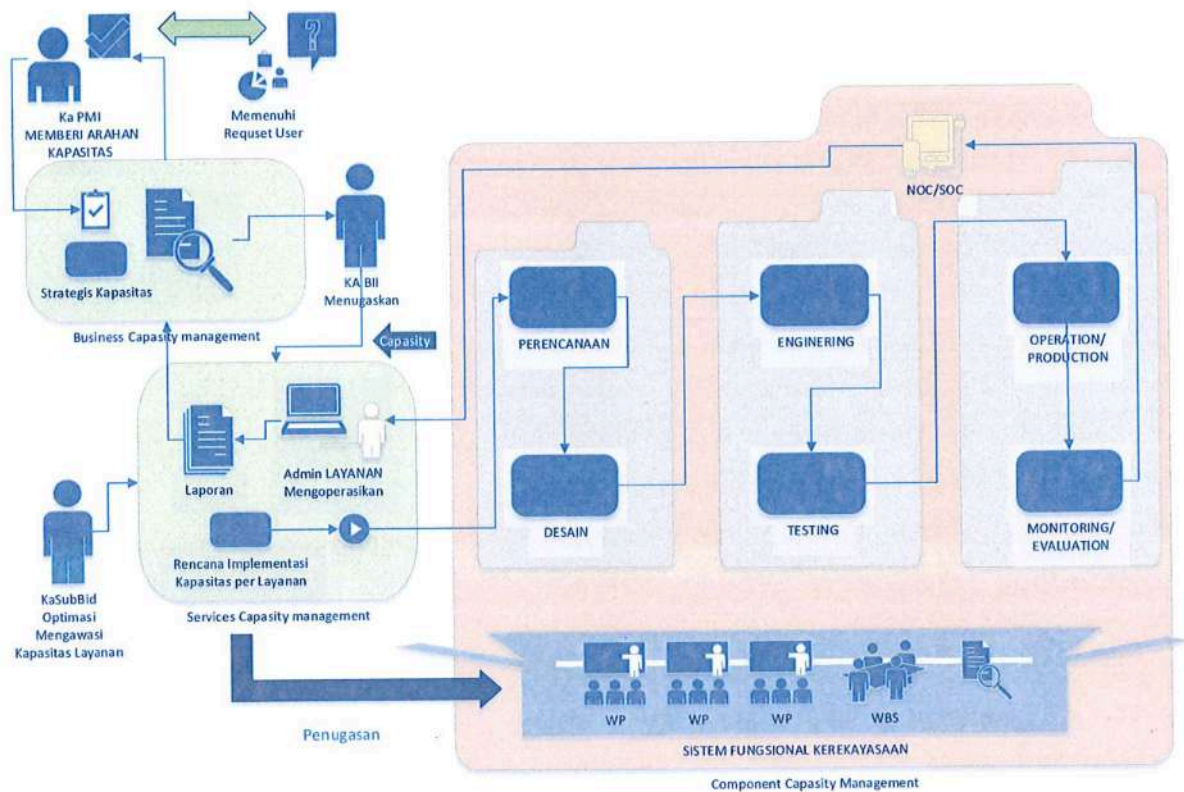
Berdasarkan pada uraian di atas maka susunan manajemen kapasitas untuk Infrastruktur Informasi, adalah dimulai dengan menterjemahkan *Business Capacity Management* yang diarahkan oleh Kepala PMI, baik berupa Renstra, Renja, PK serta berbagai bentuk sumber dana dan kemampuan personil yang diberikan. Menjadi kegiatan yang disebut sebagai '*Service Capacity Management*', berdasar arahan, diskusi dan ketetapan Kepala PMI dapat disusun sasaran strategis kapasitas layanan untuk dilaksanakan BII.

BII menterjemahkan arahan dari Kepala PMI untuk dilaksanakan sebagai suatu layanan tertentu, yang mempunyai kapasitas layanan dengan parameter tertentu, seperti alokasi kuota *inbox* dan *outbox*, jumlah alokasi *storage server*, kecepatan dan *bandwith* komunikasi dan seterusnya. Dimana dari setiap layanan mempunyai ukuran tertentu yang secara riil dibutuhkan, guna kenyamanan pengguna.

Manajemen kapasitas layanan ini dilakukan oleh Kepala Bidang Infrastruktur Informasi, dengan menentukan pada setiap layanan mempunyai parameter dengan kapasitas tertentu, serta pada pelaksanaannya akan diserahkan dan diidentifikasi ke dalam manajemen kapasitas dari setiap komponen infrastruktur yang dioperasikan di BPPT. Hasil kapasitas layanan dilaporkan kepada Kepala PMI. (Laporan Manajemen Kapasitas Layanan dilakukan setiap 3 bulan, dalam laporan hasil monitoring – *Capacity Report* ).

Untuk selanjutnya pelaksanaan manajemen kapasitas per komponen diserahkan kepada pengelola, dalam hal ini para perekayasa yang bekerja pada spesifik bidang kerjanya. Misalnya *Network, Cloud System, e-mail* dan sebagainya, baik pada level perancangan, level testing untuk bisa dilanjutkan pada level operasional, semua itu dilaksanakan menggunakan sistem kerja kerekayasaan.

Adapun untuk laporannya, terutama hasil monitoring operasional yang dilaksanakan, biasanya sudah mencakup di hasil monitoring tentang *capacity report*. Diagram alur dari proses yang dilakukan di BII dengan mengadopsi ITIL, serta menyesuaikan dengan keadaan dan cara kerja kerekayasaan dapat digambarkan sebagai berikut.



Gambar 5.5 Flow diagram proses manajemen Kapasitas Infrastruktur informasi di BII

### E. Manajemen Ketersediaan (*Availability Management*)

Manajemen ketersediaan bertujuan untuk mendefinisikan, menganalisis, merencanakan, mengukur dan meningkatkan semua aspek ketersediaan layanan TI. Hal ini bertanggung jawab untuk memastikan bahwa semua infrastruktur, proses, alat, peran dan lain-lain sesuai dengan target ketersediaan yang disepakati.

Sub-proses pada manajemen ketersediaan dapat disebutkan disini termasuk tujuan prosesnya adalah sebagai berikut:

a. Layanan Desain untuk Ketersediaan

Tujuan Proses: Untuk merancang prosedur dan fitur teknis yang diperlukan untuk memenuhi tingkat ketersediaan yang disepakati.

b. Pengujian Ketersediaan

Tujuan Proses: Untuk memastikan bahwa semua mekanisme ketersediaan, ketahanan dan pemulihan tunduk pada pengujian rutin.

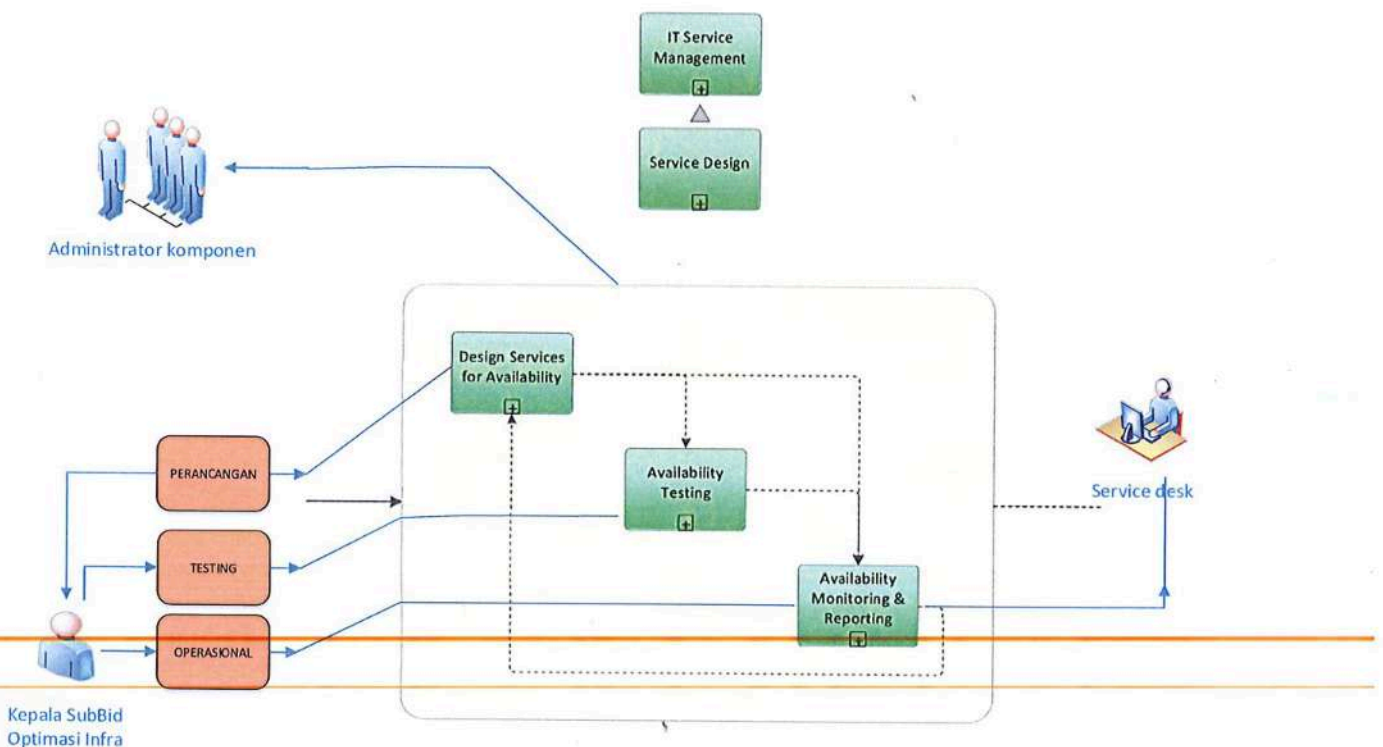
c. Pemantauan dan Pelaporan Ketersediaan

Tujuan Proses: Untuk menyediakan proses manajemen layanan dan manajemen TI lainnya dengan informasi yang terkait dengan layanan dan ketersediaan komponen. Ini termasuk membandingkan ketersediaan yang dicapai terhadap yang disepakati dan mengidentifikasi area dimana ketersediaan harus ditingkatkan.

Dalam rangka memenuhi proses tersebut di atas maka untuk perencanaan, arahan kebijakan, kriteria desain, analisa resiko serta laporan, dibuat suatu dokumen *service availability* atau ketersediaan layanan yang dikeluarkan berdasarkan tahun kerja.

Pelaksanaan manajemen ketersediaan diterjemahkan dalam setiap layanan yang dapat diberikan BII, untuk direncanakan dan diimplementasikan sebagai kapasitas layanan operasional. Karena setiap layanan bergantung pada komponen atau sumberdaya TI yang digunakan, seperti komponen server, *storage*, *bandwidth network*, dan komponen sistem jaringan lainnya, maka ketersediaan komponen tersebut akan mempengaruhi layanan yang diberikan. Manajemen ketersediaan akan diuraikan dari setiap komponen yang mempengaruhi. Untuk itu maka dalam pengelolaan komponen dan sumber daya TI yang ada harus dimonitor terus dan apabila ada kerusakan atau ketidakstabilan perlu diwaspadai untuk dipersiapkan atau direncanakan antisipasinya.

Kepala Sub Bidang Optimasi Infrastruktur bertanggung jawab dalam memonitor, menganalisis, serta memberikan rekomendasi, dibantu perekayasa untuk menampilkan data yang ada. Perekayasa yang bekerja pada fase perancangan, *testing* dan operasional, perlu membantu dan menginformasikan serta memperhatikan ketersediaan komponen atau sumber daya TI. Kepala Bidang BII melaporkan keadaan ketersediaan layanan dan kebutuhan untuk memberikan ketersediaan lebih baik serta informasi kepada Kepala PMI guna memudahkan arahan kebijakan dapat dilaksanakan.



Gambar 5.6 Diagram Alur Manajemen Ketersediaan

Manajemen ketersediaan yang diterapkan di BII, sesuai sebagai yang dijelaskan di atas mempunyai awal dengan melakukan desain ketersediaan, kemudian testing ketersediaan serta

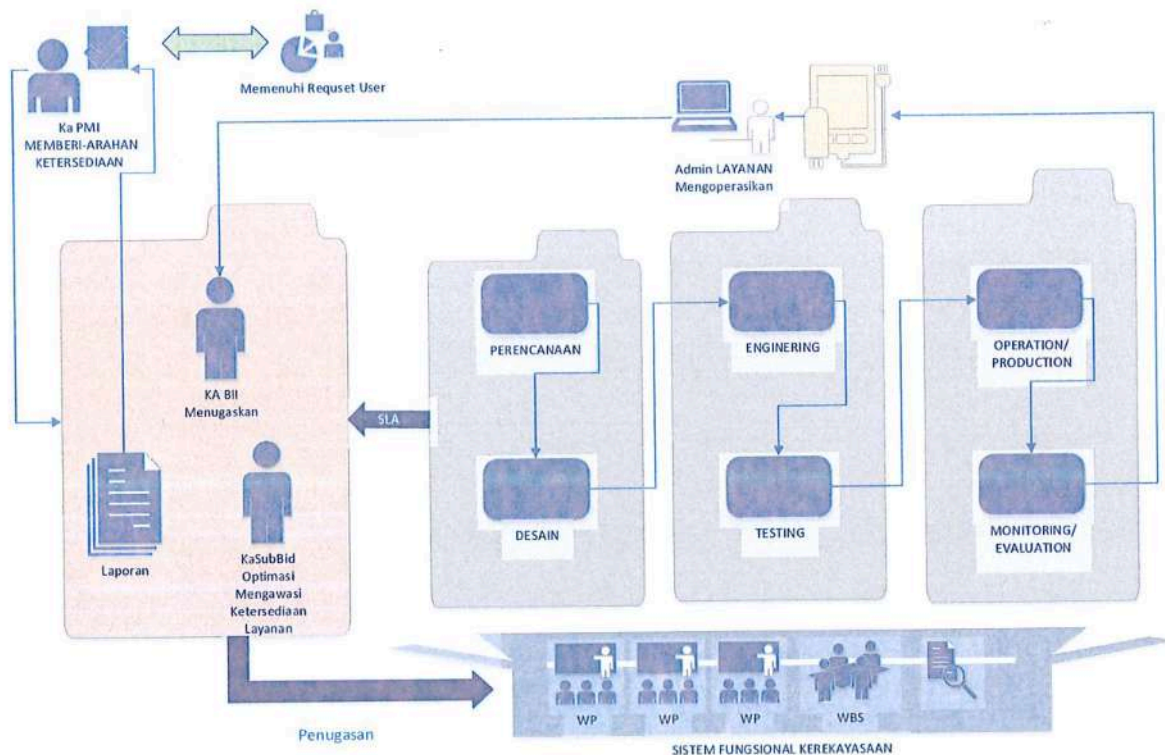
monitoring ketersediaan. Dalam mencukupi ketersediaan tersebut, setiap layanan tergantung pada ketersediaan komponen yang ada di bidang infrastruktur informasi.

Adapun ketersediaan setiap layanan ada ketergantungan terhadap komponen *resources* yang ada. Dengan demikian dalam setiap layanan sebagaimana diagram di atas, ketersediaan layanan itu akan dimonitor terus oleh administrator yang bersangkutan, ditambah dengan *service desk*.

Untuk mendukung ketersediaan itu maka perekrutan selalu dalam suatu proses yang sesuai dengan proses manajemen ketersediaan, yaitu dimulai dari *desain avability*, *testing availability*, serta dalam operasional pelaksanaan, meliputi pula untuk monitoring dan laporan tentang *availability* atau ketersediaan layanan.

Secara lebih baik lagi, manajemen sistem ketersediaan ini akan dapat memberikan layanan dengan mengeluarkan SLA dengan ukuran tertentu. Mestinya jika sudah dapat diukur kinerja yang dipersiapkan *input* yang diterima serta *output* yang dapat disampaikan.

### Manajemen Ketersediaan Layanan di BII



Gambar 5.7 Diagram Alur Manajemen Ketersediaan Layanan Infrastruktur informasi BII



## BAB VI

### TRANSISI LAYANAN (*SERVICE TRANSITION*)

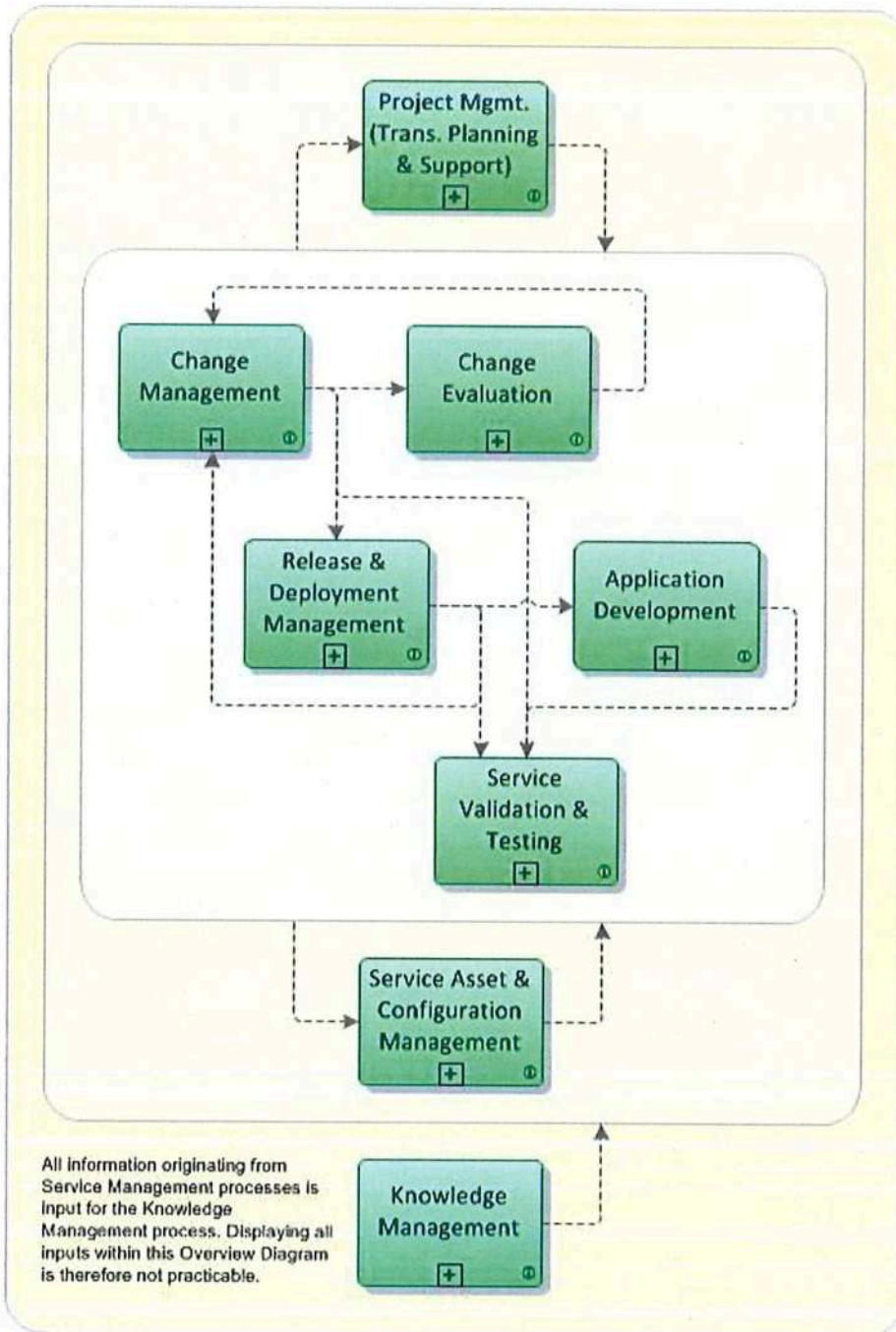
*Service transition* menyediakan panduan kepada organisasi TI untuk dapat mengembangkan kemampuan dalam mengubah hasil desain layanan TI baik yang baru maupun layanan TI yang diubah spesifikasinya ke dalam lingkungan operasional. Tahapan *lifecycle* ini memberikan gambaran bagaimana sebuah kebutuhan yang didefinisikan dalam *service strategy* kemudian dibentuk dalam *service design* untuk selanjutnya secara efektif direalisasikan dalam *service operation*.

Proses-proses yang dicakup dalam *service transition* yaitu :

1. *Transition Planning and Support*
2. *Change Management*
3. *Service Asset & Configuration Management*
4. *Release & Deployment Management*
5. *Service Validation*
6. *Evaluation*
7. *Knowledge Management*

Dari proses tersebut di atas tidak semua proses dilakukan oleh BII. *Transition Planning and Support* tidak secara mendetail ada, namun *planning* dan *support* itu dilaksanakan sesuai pada persiapan operasional suatu layanan yang baru. Adapun *Change Management*, *Release and Deployment Management*, *Service Asset and Configuration Management* sedang dalam pengembangan dan segera diusahakan sebaik baiknya. Sedangkan untuk meningkatkan layanan maka *Knowledge Management* juga sudah dapat dimulai.

## Service Transition ITIL



Gambar 6.1 *Service Transition* menurut ITIL

## A. Manajemen Perubahan (*Change Management*)

Manajemen perubahan bertujuan untuk mengontrol siklus hidup semua perubahan. Tujuan utama dari proses ini adalah untuk menjadikan perubahan yang bermanfaat itu dapat dilakukan, dengan kemungkinan gangguan terhadap operasional yang minimum terhadap layanan TI. Hal ini seharusnya dilaksanakan setelah adanya *planning* dan *support*, atau perencanaan dan persiapan *support*, baik dari adanya sumber daya serta tersedianya fasilitas untuk terjadinya perubahan.

Untuk melaksanakan manajemen perubahan ini beberapa subproses dapat disebutkan sebagai berikut:

### 1. Dukungan Manajemen Perubahan

Tujuan sub proses ini untuk menyediakan contoh atau *template*, dan panduan, untuk otorisasi perubahan. Juga untuk memberikan informasi atau memasok informasi kepada proses manajemen layanan TI lainnya, tentang adanya perubahan yang direncanakan dan berkelanjutan. Dukungan manajemen dalam proses perubahan, terutama didapat dari Kepala Bidang Infrastruktur Informasi, sebagai Manajer Perubahan, dari *decision sheet* atau *instruction sheet* yang diberikan.

Kemudian proses dilanjutkan oleh tim pelaksana perubahan, dengan membuat proposal perubahan, urutan proses perubahan, dan *testing* serta hasil penilaian perubahan.

### 2. Penilaian Proposal Perubahan

Tujuan sub proses ini untuk menilai proposal perubahan yang biasanya dikirimkan untuk perubahan signifikan oleh proses strategi layanan. Tujuan menilai Proposal Perubahan adalah untuk mengidentifikasi kemungkinan adanya masalah sebelum dimulainya kegiatan desain. Kepala Bidang Infrastruktur Informasi berhak menilai proposal perubahan dalam rangka melanjutkan atau menghentikan proses, atau memperbaiki strateginya.

### 3. Peninjauan Permintaan Perubahan

Tujuan sub proses ini untuk menyaring permintaan perubahan yang tidak mengandung semua informasi yang diperlukan untuk penilaian atau yang dianggap tidak praktis. Tim Perubahan yang dibentuk, menyaring terhadap permintaan perubahan, dengan pertimbangan teknis, kemampuan personil serta sumber daya yang ada.

### 4. Penilaian dan Implementasi Perubahan Darurat

Tujuan sub proses ini untuk menilai, mengesahkan, dan menerapkan perubahan darurat secepat mungkin. Proses ini dijalankan jika prosedur manajemen perubahan yang normal tidak dapat diterapkan karena keadaan darurat dan memerlukan tindakan segera. Perubahan darurat dapat dilaksanakan jika ada izin dan arahan Kepala Bidang Infrastruktur Informasi atau Kepala Sub Bidang Optimasi Infrastruktur. Keadaan darurat ini memerlukan informasi dan bisa disarankan oleh admin peralatan.

### 5. Penilaian Perubahan oleh Manajer Perubahan

Tujuan sub proses ini untuk menentukan tingkat otorisasi yang diperlukan untuk penilaian perubahan yang diusulkan. Perubahan signifikan diteruskan ke *Change Advisory Board*

(CAB) untuk penilaian, sementara perubahan kecil segera dinilai dan disahkan oleh Manajer Perubahan. Penilaian perubahan yang diusulkan baik untuk memenuhi RFC atau dari kebutuhan lain, dilakukan oleh Manajer Perubahan. Karena di BPPT tidak ada CAB, maka tingkat ini untuk perubahan infrastruktur akan diputuskan penyelesaiannya kepada Kepala PMI.

#### **6. Penilaian Perubahan oleh CAB**

Tujuan sub proses ini untuk menilai perubahan yang diusulkan dan mengotorisasi fase perencanaan perubahan. Jika diperlukan, tingkat otoritas yang lebih tinggi (misalnya pengelolaan TI) terlibat dalam proses otorisasi. Otorisasi perubahan yang lebih tinggi bagi Kepala Bidang Infrastruktur Informasi adalah Kepala PMI.

#### **7. Penjadwalan Perubahan dan Otorisasi**

Tujuan sub proses ini untuk mengotorisasi perencanaan perubahan dan menulis detail rincian, serta untuk menilai rencana proyek yang dihasilkan sebelum mengesahkan fase perubahan.

#### **8. Otorisasi Distribusi Perubahan**

Tujuan sub proses ini untuk menilai apakah semua komponen perubahan yang diperlukan telah dibangun dan diuji dengan benar, dan untuk mengotorisasi Fase penerapan perubahan.

#### **9. *Minor Change Deployment***

Tujuan sub proses ini untuk menerapkan perubahan yang berisiko rendah dan dipahami dengan baik yang tidak memerlukan keterlibatan 'Manajemen Rilis'.

#### **10. Tinjauan Implementasi dan Penutupan Perubahan**

Tujuan sub proses ini untuk menilai jalannya implementasi perubahan dan hasil yang dicapai, untuk memverifikasi secara lengkap sebagai referensi di masa mendatang, dan untuk memastikan bahwa kesalahan telah dianalisa sebagai pelajaran yang didapat.

**Peran dan tanggung jawab Manajer Perubahan - Pemilik Proses, terbagi sebagai berikut:**

##### **1) Mengontrol Siklus Hidup Semua Perubahan**

Tujuan utamanya adalah untuk memungkinkan perubahan yang bermanfaat dilakukan, dengan gangguan minimum terhadap layanan TI. Untuk perubahan penting, Manajer Perubahan akan merujuk otorisasi perubahan ke Dewan Penasihat Perubahan (CAB).

##### **2) *Change Advisory Board (CAB)***

Sekelompok orang yang menyarankan Manajer Perubahan dalam penilaian, penentuan prioritas dan penjadwalan perubahan. Dewan ini biasanya terdiri dari perwakilan dari semua area dalam organisasi TI, bisnis, dan pihak ketiga seperti pemasok.

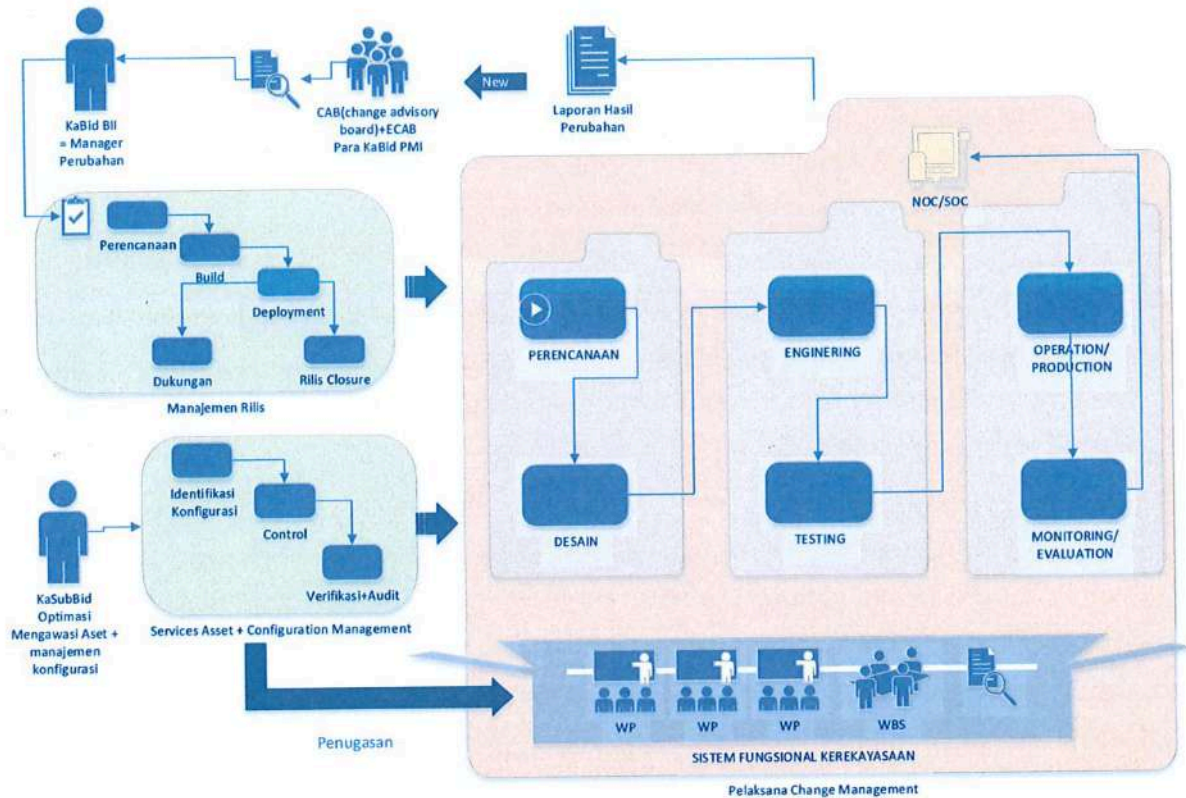
##### **3) Dewan Penasihat Perubahan Darurat (ECAB)**

Bagian dari *Change Advisory Board* yang membuat keputusan tentang Perubahan Darurat yang berdampak tinggi. Keanggotaan ECAB dapat diputuskan pada saat pertemuan dipanggil, dan tergantung pada sifat dari perubahan darurat.

Untuk memberikan informasi yang lebih kongkrit dapat disusun matrik *responsibility* untuk *Change Management*.

Kegiatan manajemen perubahan untuk Bidang Infrastruktur Informasi , dikepalai oleh Kepala Bidang BII. Adapun yang bertindak sebagai *Board Advisory Change (CAB)* dan Dewan Penasihat Perubahan Darurat (*ECAB*) adalah Kepala Bidang yang ada di lingkungan PMI. Hal ini disebabkan karena para Kepala Bidang merupakan bagian yang sangat terpengaruh oleh perubahan.

Manajemen perubahan ini dapat dipecah sebagai 'Manajemen Rilis' dan 'Manajemen Aset dan Konfigurasi', yang masing-masing dilaksanakan oleh Kepala Bidang BII dan Kepala Sub Bidang Optimasi dan Kepala Sub Bidang Pengembangan Infrastruktur.



Gambar 6.2 *Service Transition* yang dilakukan di BII mengadopsi ITIL

Namun, dalam pelaksanaannya ditugaskan ke pelaksana *Change Management*, yaitu para perekayasa yang tergabung dalam tugas di dalam sistem fungsional kerekayasaan. Sehingga pelaksanaannya diatur dengan keteraturan engineering yang dimulai dari perencanaan, desain, engineering, testing operation produksi dan monitoring dan evaluasi. Sehingga proses *management service* dan *validation testing* ada juga di dalam sistem kerekayasaan.

### B. Release and Deployment Management

*Release and deployment management* bertujuan untuk merencanakan, menjadwalkan, dan mengontrol pergerakan peluncuran. Peluncuran layanan ini adalah proses untuk menguji dan menjalani lingkungan yang ada. Tujuan utama dari proses ini adalah untuk memastikan bahwa keadaan integritas lingkungan bisa terlindungi dan komponen baru yang diluncurkan adalah hal yang benar.

Untuk melaksanakan *release and deployment management* ini beberapa sub proses dapat disebutkan sebagai berikut:

**a) Dukungan Manajemen Rilis**

Tujuan sub proses ini untuk memberikan pedoman dan dukungan untuk penyebaran rilis.

**b) Perencanaan Rilis**

Tujuan sub proses ini untuk menetapkan perubahan resmi paket yang diluncurkan dan untuk menentukan ruang lingkup dan isi peluncuran. Berdasarkan informasi ini, proses perencanaan rilis mengembangkan jadwal untuk membangun, menguji, dan menyebarkan rilis.

**c) Pembangunan Rilis**

Tujuan sub proses ini untuk mengeluarkan semua perintah kerja dan permintaan pembelian yang diperlukan agar komponen rilis yang dibeli dari vendor luar atau dikembangkan/disesuaikan di dalam. Pada akhir proses ini, semua komponen *release* yang dibutuhkan siap memasuki fase pengujian.

**d) Release Deployment**

Tujuan sub proses ini untuk menyebarkan komponen rilis ke dalam lingkungan produksi langsung. Proses ini juga bertanggung jawab untuk melatih pengguna akhir dan staf operasi dan menyebarkan informasi/dokumentasi tentang rilis yang baru dikerahkan atau layanan yang didukungnya.

**e) Dukungan Inisial Penerapan**

Tujuan sub proses ini untuk menyelesaikan masalah operasional dengan cepat selama periode awal setelah peluncuran rilis, dan untuk menghapus semua kesalahan atau kekurangan yang tersisa.

**f) Release Closure**

Tujuan sub proses ini untuk secara resmi menutup rilis setelah memverifikasi apakah log aktivitas dan konten CMS adalah yang terbaru.

Untuk membantu dalam kemudahan penanganan manajemen rilis ini perlu dibuat suatu dokumen yang memberi gambaran tentang rilis layanan yang telah dilakukan hingga saat ini, yang tercatat dalam rilis terkini yang pernah dikeluarkan beserta riwayatnya.

### **C. Manajemen Aset dan Konfigurasi Layanan**

Manajemen aset dan konfigurasi layanan bertujuan untuk menjaga informasi tentang *Item Konfigurasi (CI)* yang diperlukan untuk memberikan layanan TI, termasuk hubungan antar mereka (antar CI).

Untuk melaksanakan ‘Manajemen Aset dan Konfigurasi Layanan’ beberapa sub proses dapat disebutkan sebagai berikut :

**a. Identifikasi Konfigurasi**

Tujuan subproses ini untuk menentukan dan mempertahankan struktur dasar dari CMS (Model Konfigurasi), sehingga mampu menampung semua informasi tentang *Item Konfigurasi (CI)*. Termasuk pula menentukan atribut yang menggambarkan tipe CI dan subkomponennya, serta menentukan keterkaitannya.

## b. Kontrol Konfigurasi

Tujuan subproses ini untuk memastikan bahwa tidak ada *Item Konfigurasi* yang ditambahkan atau dimodifikasi tanpa otorisasi yang diperlukan, dan bahwa modifikasi tersebut dicatat secara memadai dalam CMS.

Catatan: Kontrol konfigurasi ITIL terutama berkaitan dengan peninjauan modifikasi pada Sistem Manajemen Konfigurasi (CMS), adalah guna memastikan informasi yang disimpan dalam CMS telah dilakukan dan modifikasi dilakukan oleh pihak yang berwenang. Proses lain yang juga mendukung tujuan kontrol konfigurasi adalah identifikasi konfigurasi yaitu menentukan siapa yang berwenang untuk membuat perubahan tertentu pada CMS. Dalam arti yang lebih luas, 'Manajemen Perubahan' dan 'Manajemen Rilis' dengan prosedur yang ditentukan, mereka juga membantu memastikan bahwa tidak ada perubahan yang tidak sah terjadi.

## c. Verifikasi dan Audit Konfigurasi

Tujuan subproses ini untuk melakukan pemeriksaan rutin, memastikan bahwa informasi yang terkandung dalam CMS merupakan representasi yang tepat dari *Item Konfigurasi (CI)* yang sebenarnya dan dipasang di lingkungan produksi langsung.

Beberapa hal penting yang perlu untuk dilengkapi dalam melakukan pengelolaan aset dan konfigurasi layanan adalah sebagai berikut:

### 1. Permintaan Perubahan ke Struktur CMS

Permintaan dari proses manajemen layanan untuk mengubah struktur CMS. Permintaan ini dikirim ke manajemen konfigurasi jika CI atau atribut baru harus dicatat tetapi struktur CMS tidak memadai untuk menyimpan data baru.

### 2. CMS / CMDB

*Configuration Management System (CMS)* adalah seperangkat alat dan data yang digunakan untuk mengumpulkan, menyimpan, mengelola, memperbarui, menganalisis dan menyajikan data tentang semua item konfigurasi dan hubungannya. CMS dapat mengelola lebih dari satu *Physical Configuration Management Databases (CMDBs)*. Struktur dasarnya ditentukan oleh model konfigurasi, model logis dari aset layanan organisasi TI. (Lihat juga: Daftar Periksa ITIL CMS - CMDB).

### 3. Kebijakan Perubahan CMS

Seperangkat aturan yang menentukan siapa yang berwenang untuk memodifikasi struktur dan isi dari CMS.

### 4. Laporan Audit Konfigurasi

Sebuah laporan yang merangkum hasil audit CMS, menyoroti perbedaan yang terungkap antara catatan CMS dan benar-benar menginstal CI.

### 5. Item Konfigurasi (CI)

Item konfigurasi (CI) dari berbagai jenis: CMS hampir selalu mencakup layanan dan infrastruktur TI, namun mungkin juga mencakup jenis item lain seperti kebijakan, dokumentasi proyek, karyawan, pemasok dan sebagainya. *Item konfigurasi* dicirikan oleh atributnya (dicatat dalam Catatan Konfigurasi CI) dan hubungannya dengan CI lain.

## 6. Perpustakaan Media Definitif (DML)

*Definitive Media Library* (DML) adalah pustaka logika yang aman di mana versi resmi dari semua CI media disimpan dan dilindungi. DML biasanya terdiri dari satu atau beberapa area penyimpanan file perangkat lunak, serta penyimpanan fisik misalnya master pada CD/ DVD.

Untuk pelaksanaan manajemen ini BII menggunakan *software* aplikasi iTOP, sehingga dengan aplikasi iTOP ini dapat mencapai hasil serta menggunakan proses-proses yang sesuai dengan 'Manajemen Aset dan Konfigurasi'.

### D. Manajemen Pengetahuan (Knowledge Management)

Untuk *knowledge management* dalam Praktiknya ada di *service desk*, dan menyatu dengan *service operation*. Mengenai 'Manajemen Pengetahuan' secara rinci akan dibahas lebih lanjut pada bab selanjutnya.

## BAB VII

### PENGOPERASIAN LAYANAN (*SERVICE OPERATION*)

*Service operation* atau pengoperasian layanan merupakan tahapan *lifecycle* yang mencakup semua kegiatan operasional harian pengelolaan layanan-layanan TI. Di dalamnya terdapat berbagai panduan bagaimana mengelola layanan TI secara efisien dan efektif serta menjamin tingkat kinerja yang telah dijanjikan dengan pengguna sebelumnya. Panduan-panduan ini mencakup bagaimana menjaga kestabilan operasional layanan TI serta pengelolaan perubahan desain, skala, ruang lingkup serta target kinerja layanan TI.

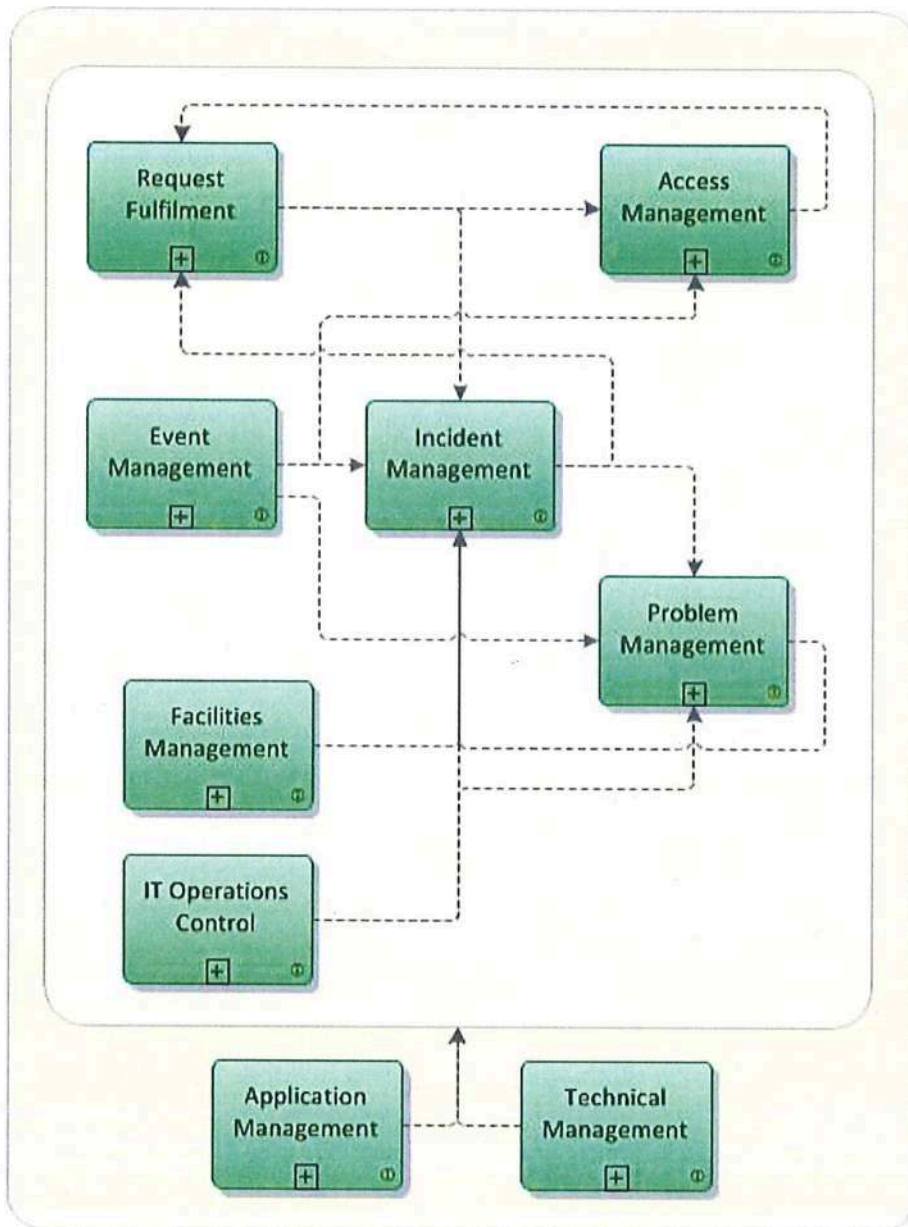
Proses-proses yang dicakup dalam 'Pengoperasian Layanan' yaitu :

1. *Event Management*
2. *Incident Management*
3. *Problem Management*
4. *Request Fulfillment*
5. *Access Management*
6. *IT Operation Management*
7. *Technical Management*
8. *Service Desk*

Dalam proses manajemen operasional dari layanan ini, proses yang ditangani terkumpul atau dimulai dari *service desk*, sehingga pelaksanaan cukup terintegrasi dengan manajemen yang ada di ITIL, namun demikian dalam realitasnya ada berbagai simplifikasi disebabkan keterbatasan personil serta kesederhanaan masalah yang dihadapi di BII.

Pertama dapat dilihat, dalam proses praktisnya dapat disusun sesuai dengan *framework* dari ITIL sebagai berikut:

## Service Operation ITIL



Gambar 7.1 Ruang Lingkup *Service Operation*

Dimulai dari *event management*, proses yang ada di pengoperasian layanan dapat dimulai dan ditelusur. Bila secara operasional telah melaksanakan berbagai layanan yang dalam pelaksanaan sehari-hari ingin mengadopsi ITIL, maka disusun proses sebagai berikut beserta tata kelola untuk melengkapinya.

Karena BII secara operasional terdiri dari para perekayasa yang tergabung dalam suatu sistem kerja kerekayasaan, maka *job* yang dilaksanakan untuk melakukan pengoperasian layanan itu menggunakan sistem kerekayasaan. Selain itu, pengoperasian layanan juga ditunjang dengan sistem *job* yang disebut *service desk*, dengan demikian antara otoritas pemberi pekerjaan yaitu pejabat struktural, para perekayasa serta *job* sebagai *service desk* perlu suatu kerjasama untuk pengoperasian seluruh layanan yang ada di BII.

Gambaran diagram sederhana manajemen yang ada di pengoperasian layanan dapat dibentuk dalam susunan berikut.



Gambar 7.2 Ruang Lingkup Service Operation di BII

### Manajemen Even (*Event Management*)

Tujuan proses dalam *event management* adalah untuk memastikan *Item* Konfigurasi (CI) dan layanan selalu dimonitor, dan untuk menyaring dan mengkategorikan suatu kondisi, untuk kemudian diputuskan tindakan yang tepat.

Untuk melaksanakan 'Manajemen Even', beberapa subproses dapat disebutkan sebagai berikut:

#### 1. Pemeliharaan Mekanisme dan Aturan Pemantauan Even

Tujuan subproses ini untuk mengatur dan memelihara mekanisme guna menghasilkan even yang bermakna dan aturan yang efektif untuk penyaringan dan hubungannya.

#### 2. Penyaringan Even dan Korelasi Tingkat 1

Tujuan subproses ini untuk menyaring even yang hanya bersifat informasi dan dapat diabaikan, dan untuk mengkomunikasikan peringatan dan even pengecualian/yang tidak biasa.

#### 3. Korelasi Tingkat 2 dan Pilihan Tanggapan

Tujuan subproses ini untuk menginterpretasikan makna dari suatu even dan memilih respon yang sesuai jika diperlukan.

#### 4. Tinjauan Even dan Penutupan

Tujuan subproses ini untuk memeriksa apakah even telah ditangani secara tepat dan dapat ditutup penyelesaian. Proses ini juga memastikan bahwa *log* peristiwa dianalisis untuk mengidentifikasi tren atau pola, yang dapat menyarankan tindakan korektif yang harus dilakukan.

BII dalam melaksanakan 'Manajemen Even' mempunyai mekanisme dan aturan pemantauan, dimana dalam pemantauan atau memonitor titik-titik yang krusial menggunakan peralatan monitor, baik dengan *software* maupun *hardware* tertentu (lihat peralatan monitoring) yang berguna untuk melihat keadaan operasional layanan yang diberikan. Untuk satuan waktu tertentu diberikan hasil laporan tentang peristiwa yang terjadi.

Adapun bilamana ada insiden maka penyelesaian insiden masuk pada 'Manajemen Insiden'. Yang secara prinsip telah diatur dengan suatu SOP. Sedangkan, bilamana hal tersebut merupakan hal yang cukup besar dengan resolusi yang memakan waktu, maka masuk pada proses 'Manajemen Problem'.

## **B. Manajemen Insiden (*Incident Management*)**

Manajemen Insiden bertujuan untuk mengelola siklus hidup semua Insiden (insiden ini bersifat gangguan yang tidak direncanakan atau penurunan kualitas layanan TI). Tujuan utama dari proses dalam manajemen ini adalah mengembalikan layanan TI kepada pengguna secepat mungkin. Manajemen insiden dibedakan dengan Insiden yang berarti Interupsi Layanan dan Permintaan Layanan. Permintaan Layanan tidak lagi dipenuhi oleh 'Manajemen Insiden', karena ada proses yang disebut 'Pemenuhan Permintaan'.

Ada proses khusus untuk menangani keadaan darurat ("Penanganan Insiden Utama"), juga peristiwa penting yang memicu penciptaan Insiden. Selanjutnya, antarmuka proses perlu ditambahkan antara 'Manajemen Even' dan 'Manajemen Insiden'. Serta memperbaiki 'Panduan Manajemen Insiden', untuk memprioritaskan insiden (Panduan Prioritas Insiden Daftar Periksa).

Untuk realisasinya maka dalam insiden manajemen ini, dimasukkan atau digabung dengan *service desk*, dengan maksud adanya insiden maupun untuk memenuhi permintaan dapat dimulai dari proses yang ada dalam *service desk*.

Langkah-langkah tambahan untuk penyelesaian insiden, yaitu dengan 'Dukungan Tingkat 1' untuk menjelaskan bahwa insiden harus dicocokkan (jika mungkin) dengan masalah yang ada dan kesalahan yang diketahui. Resolusi insiden oleh 'Dukungan Tingkat 1' dan resolusi insiden oleh 'Dukungan Tingkat 2', adalah langkah-langkah yang telah sangat diperluas untuk memberikan panduan yang lebih jelas tentang kapan 'Manajemen Insiden' dinaikkan menjadi 'Manajemen Masalah'.

Penekanan manajemen insiden adalah untuk memulihkan layanan secepat mungkin. Dan secepat mungkin dinaikkan menjadi 'Manajemen Masalah' jika penyebab yang mendasari suatu insiden tidak dapat diselesaikan dengan perubahan kecil dan / atau waktu resolusi yang lama atau yang dalam komitmen akan terlewati.

Subproses 'Insiden Manajemen, Insiden Penutupan dan Evaluasi' sekarang menyatakan lebih jelas bahwa penting untuk memeriksa apakah ada masalah baru. Kesalahan yang diketahui yang harus diserahkan ke 'Manajemen Masalah'.

---

Berikut ini adalah subproses 'Manajemen Insiden' dan tujuan prosesnya:

### **a. Dukungan Manajemen Insiden**

Tujuan subproses ini untuk menyediakan dan memelihara peralatan, proses, keterampilan dan aturan untuk penanganan insiden yang efektif dan efisien.

### **b. Insiden *Logging* dan Kategorisasi**

Tujuan subproses ini untuk mencatat dan memprioritaskan insiden dengan ketekunan yang tepat, serta untuk memfasilitasi resolusi yang cepat dan efektif.

**c. Resolusi Insiden Langsung oleh Dukungan Tingkat 1**

Tujuan subproses ini untuk menyelesaikan insiden (gangguan layanan) dalam jadwal waktu yang disepakati. Tujuannya adalah pemulihan layanan TI yang cepat, bila perlu dengan bantuan solusi. Segera setelah menjadi jelas bahwa 'Dukungan Tingkat 1' tidak dapat menyelesaikan Insiden itu sendiri atau ketika waktu target untuk tingkat resolusi 1 terlampaui, maka insiden akan ditransfer ke grup yang sesuai dalam 'Dukungan Tingkat 2'.

**d. Resolusi Insiden oleh Dukungan Tingkat 2**

Tujuan subproses ini untuk menyelesaikan insiden (gangguan layanan) dalam jadwal waktu yang disepakati. Tujuannya adalah pemulihan layanan yang cepat, jika perlu dengan menggunakan solusi. Jika diperlukan, kelompok dukungan khusus atau pemasok pihak ketiga (Dukungan Tingkat 3) dilibatkan. Jika koreksi akar penyebab tidak dimungkinkan, maka rekam masalah dibuat dan koreksi kesalahan ditransfer ke 'Manajemen Masalah'.

**e. Penanganan Insiden Mayor**

Tujuan sub proses ini untuk menyelesaikan insiden mayor. Insiden utama menyebabkan gangguan serius terhadap aktivitas bisnis dan harus diselesaikan dengan urgensi yang lebih besar. Tujuannya adalah pemulihan layanan yang cepat, jika perlu dengan menggunakan solusi. Jika diperlukan, kelompok dukungan khusus atau pemasok pihak ketiga (Dukungan Tingkat 3) dilibatkan. Jika koreksi akar penyebab tidak dimungkinkan, rekam masalah dibuat dan koreksi kesalahan ditransfer ke 'Manajemen Masalah'.

**f. Pemantauan Insiden dan Eskalasi**

Tujuan subproses ini untuk terus memantau status pemrosesan insiden yang luar biasa, sehingga tindakan dapat diperkenalkan sesegera mungkin apabila tingkat layanan kemungkinan dilanggar.

**g. Insiden Penutupan dan Evaluasi**

Tujuan subproses ini untuk menyerahkan catatan insiden ke kontrol kualitas akhir sebelum ditutup. Tujuannya adalah untuk memastikan bahwa Insiden itu benar-benar diselesaikan dan bahwa semua informasi yang diperlukan untuk menggambarkan siklus hidup Insiden disediakan secara cukup rinci. Selain ini, temuan dari resolusi Insiden harus direkam untuk digunakan di masa depan.

**h. Informasi Pengguna Proaktif**

Tujuan subproses ini untuk menginformasikan kepada pengguna tentang kegagalan layanan segera setelah ini diketahui oleh *service desk*, sehingga pengguna berada dalam posisi untuk menyesuaikan diri dengan gangguan. Informasi pengguna yang proaktif juga bertujuan untuk mengurangi jumlah pertanyaan oleh pengguna. Proses ini juga bertanggung jawab untuk mendistribusikan informasi lain kepada pengguna, misalnya peringatan keamanan.

**i. Pelaporan Manajemen Insiden**

Tujuan subproses ini untuk memasok informasi terkait insiden ke proses manajemen layanan lainnya, hal ini untuk memastikan bahwa potensi peningkatan atau penurunan berasal dari insiden sebelumnya.

BII dengan dilengkapi fungsi *service desk*, di dalamnya termasuk melaksanakan manajemen insiden dan manajemen *problem*, untuk itu maka dalam hal ini dilaksanakan proses itu dengan suatu SOP (SOP Manajemen Insiden dan SOP Manajemen Masalah).

### C. Manajemen Masalah (*Problem Management*)

Manajemen masalah bertujuan untuk mengelola siklus hidup masalah yang terjadi. Tujuan utama dari proses ini adalah untuk mencegah terjadinya insiden, dan untuk meminimalkan dampak insiden yang tidak dapat dicegah.

'Manajemen Masalah Proaktif' menganalisis data insiden, dan menggunakan data yang dikumpulkan oleh proses manajemen layanan TI lainnya untuk mengidentifikasi tren atau masalah yang signifikan. Subproses "*Major Issues Review*" adalah untuk meninjau riwayat solusi, untuk menghilangkan masalah utama, untuk mencegah terulangnya dan untuk belajar atau pelajaran di masa depan.

Berikut ini adalah subproses dari 'Manajemen Masalah' dan tujuan prosesnya:

#### 1. Mengidentifikasi Masalah Proaktif

Tujuan subproses ini untuk meningkatkan ketersediaan layanan secara keseluruhan dengan mengidentifikasi masalah secara proaktif. Manajemen masalah proaktif bertujuan untuk mengidentifikasi dan memecahkan masalah dan/atau menyediakan solusi yang tepat sebelum insiden muncul kembali.

#### 2. Kategorisasi dan Pertanyaan Penetapan Prioritas

Tujuan subproses ini untuk merekam dan memprioritaskan masalah dengan ketekunan yang tepat, untuk memfasilitasi penyelesaian yang cepat dan efektif.

#### 3. Diagnosis Masalah dan Resolusi

Tujuan subproses ini untuk mengidentifikasi akar penyebab masalah dan mulai solusi masalah yang paling tepat dan ekonomis. Jika memungkinkan, solusi sementara disediakan.

#### 4. Masalah dan Kontrol Kesalahan

Tujuan subproses ini untuk selalu memantau masalah yang luar biasa terkait dengan status pemrosesan mereka, jadi dimana langkah-langkah perbaikan yang diperlukan dapat diperkenalkan.

#### 5. Masalah Penutupan dan Evaluasi

Tujuan subproses ini untuk memastikan bahwa setelah solusi masalah yang berhasil, perekaman masalah mengandung uraian historis lengkap, dan bahwa catatan kesalahan terkait diperbarui.

## 6. Ikhtisar Masalah Utama

Tujuan subproses ini untuk meninjau resolusi masalah untuk mencegah kekambuhan dan belajar pelajaran untuk masa depan. Lebih jauh lagi, harus diverifikasi apakah masalah yang ditandai sebagai tertutup sebenarnya telah dihapuskan.

## 7. Pelaporan Manajemen Masalah

Tujuan subproses ini adalah untuk memastikan bahwa proses manajemen layanan dan manajemen TI lainnya diberitahukan tentang status pemrosesan mereka, yang bertujuan untuk mengelola siklus hidup semua masalah. Tujuan utama dari proses ini untuk mencegah terjadinya insiden, dan untuk meminimalkan dampak insiden. 'Manajemen Masalah Proaktif' menganalisis rekaman Insiden dan menggunakan data yang dikumpulkan oleh proses manajemen layanan TI lainnya untuk mengidentifikasi tren atau masalah yang signifikan.

### D. Manajemen Akses (Access Management)

Manajemen akses bertujuan untuk memberikan hak kepada pengguna yang sah guna menggunakan layanan, sambil mencegah akses ke pengguna yang tidak berwenang. Proses 'Manajemen Akses' pada dasarnya melaksanakan kebijakan yang didefinisikan dalam 'Manajemen Keamanan Informasi'. Manajemen akses disebut juga sebagai manajemen hak atau manajemen identitas. Manajemen akses sebagai suatu proses penanganan dengan alasan keamanan Informasi, karena pemberian akses ke layanan dan aplikasi TI hanya untuk pengguna yang berwenang sangat penting dari sudut pandang keamanan informasi.

Perlu ditambahkan sebuah antarmuka antara 'Manajemen Akses' dan 'Manajemen Even', adalah untuk menekankan bahwa penyaringan even dan aturan korelasi harus dirancang oleh 'Manajemen Akses' guna mendukung deteksi akses tidak sah ke layanan. Aktivitas khusus telah ditambahkan untuk mencabut hak akses jika diperlukan, guna memperjelas poin ini. Agar dibuat lebih jelas dalam proses 'Permintaan Pemenuhan' (*Request Fulfillment*) dan 'Manajemen Insiden' bahwa otorisasi pemohon harus diperiksa.

Berikut ini adalah subproses manajemen akses ITIL dan tujuan prosesnya:

#### 1. Pemeliharaan Katalog Peran Pengguna dan Profil Akses

Tujuan subproses ini untuk memastikan bahwa katalog peran pengguna dan profil akses masih sesuai untuk layanan yang diberikan kepada pengguna, dan untuk mencegah akumulasi hak akses yang tidak diinginkan.

#### 2. Memproses Permintaan Akses Pengguna

Tujuan subproses ini untuk memproses permintaan guna menambah, mengubah atau mencabut hak akses, dan memastikan bahwa hanya pengguna yang diberi wewenang diberikan hak untuk menggunakan layanan.

### 3. Pemenuhan Permintaan (*Request Fulfillment*)

Pemenuhan permintaan (*request fulfillment*) bertujuan untuk memenuhi permintaan layanan, yang dalam banyak kasus merupakan perubahan minor - misalnya permintaan untuk mengubah kata sandi atau permintaan informasi. Untuk mencerminkan 'Pemenuhan Permintaan', dibagi dan didetilkkan dalam 5 (lima) subproses, untuk memberikan penjelasan rinci tentang semua kegiatan dan titik-titik keputusan.

*Request fulfillment* berisi antarmuka dengan 'Manajemen Insiden' - jika permintaan layanan berubah menjadi insiden, dan dengan transisi layanan - jika penyelesaian permintaan layanan membutuhkan keterlibatan 'Manajemen Perubahan'. Ikhtisar subproses pemenuhan permintaan adalah sebagai berikut:

#### 1. Dukungan Pemenuhan Permintaan

Tujuan subproses ini untuk menyediakan dan memelihara alat, proses, ketrampilan, dan aturan untuk penanganan permintaan layanan yang efektif dan efisien.

#### 2. *Logging* dan Kategorisasi Permintaan

Tujuan subproses ini untuk mencatat dan mengkategorikan permintaan layanan dengan ketekunan yang tepat dan memeriksa otorisasi pemohon untuk mengajukan permintaan, untuk memfasilitasi pemrosesan yang cepat dan efektif.

#### 3. Eksekusi Model Permintaan

Tujuan subproses ini untuk memproses permintaan layanan dalam jadwal waktu yang disepakati.

#### 4. Pemantauan dan Eskalasi Permintaan

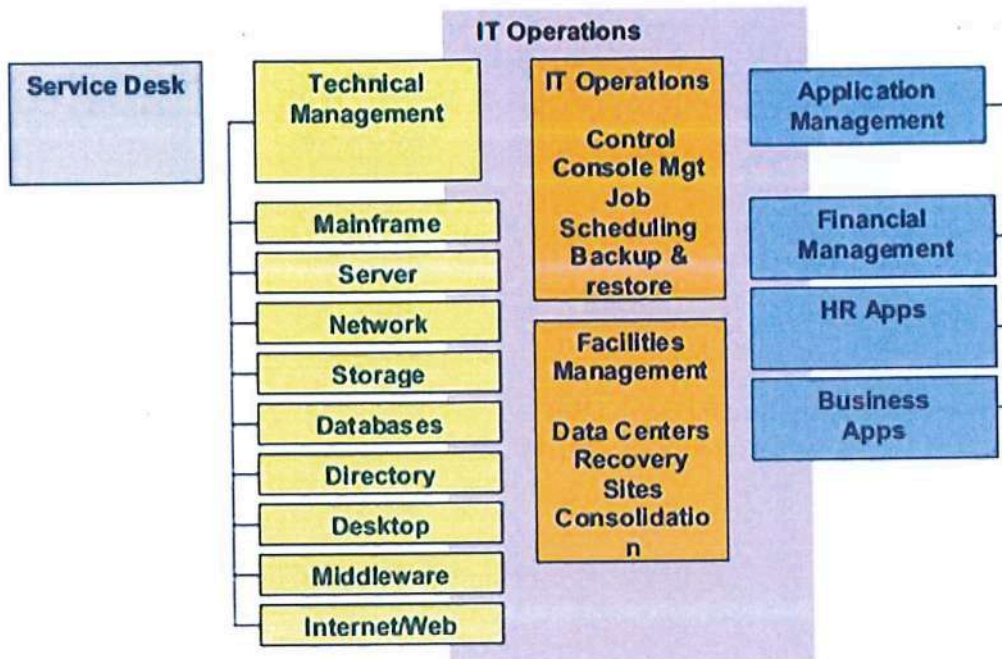
Tujuan subproses ini untuk terus memantau status pemrosesan permintaan layanan yang luar biasa, sehingga tindakan penanganan dapat diperkenalkan sesegera mungkin apabila terdapat tingkat layanan yang mungkin dilanggar.

#### 5. Penutupan dan Evaluasi Permintaan

Tujuan subproses ini untuk menyerahkan catatan permintaan ke kontrol kualitas akhir sebelum ditutup. Tujuannya adalah untuk memastikan bahwa permintaan layanan benar-benar diproses dan bahwa semua informasi yang diperlukan untuk menjelaskan siklus hidup permintaan disediakan secara cukup rinci. Selain itu, temuan dari pemrosesan permintaan harus dicatat untuk digunakan di masa mendatang. Penjelasan yang lebih lengkap tentang informasi yang menjelaskan permintaan layanan dan siklus hidupnya telah ditambahkan. Permintaan layanan dijelaskan secara lebih rinci dalam SOP pemenuhan permintaan.

## E. Manajemen Pengoperasian TI (*IT Operation Management*)

Manajemen pengoperasian TI meliputi manajemen fasilitas dan pengendalian pengoperasian TI. Untuk melengkapi proses dalam pengoperasian layanan, manajemen pengoperasian TI ini di dalamnya mencakup proses yang perlu dibantu fungsi-fungsi kerja antara lain *service desk*, *technical management* dan *application management*.



Gambar 7.8 Ruang lingkup Fungsi *IT Operation Management*

Pada *IT Operation* mempunyai dua fungsi yang mencakup diantaranya *IT operation control*, didalamnya ada *console management, job scheduling, backup and restore*. Sedangkan, *facility management* meliputi *data center, recovery sites* serta *consolidation*.

### (1) Pengendalian Pengoperasian TI

Pengendalian operasi TI bertujuan untuk memantau dan mengendalikan layanan TI dan infrastruktur dasarnya. Proses ini menjalankan tugas rutin sehari-hari yang terkait dengan pengoperasian komponen dan aplikasi infrastruktur. Ini termasuk penjadwalan pekerjaan, aktivitas pencadangan dan pemulihan, serta pemeliharaan rutin.

- a. *Console Management*
- b. *Job scheduling*
- c. *Backup and Restore*

### (2) Manajemen Fasilitas

Manajemen fasilitas ini mencakup pula penanganan *power supply, air condition*, pengamanan terhadap kebakaran, serta sistem *alert-nya*. Lebih dari itu manajemen fasilitas ini berlaku untuk tempat-tempat khusus yang ada di BPPT antara lain DC, DRC, NOC dan SOC, secara umum dapat terbagi pada lokasi berikut.

- a. *Data Center*
- b. *Recovery Sites*
- c. *Consolidation*

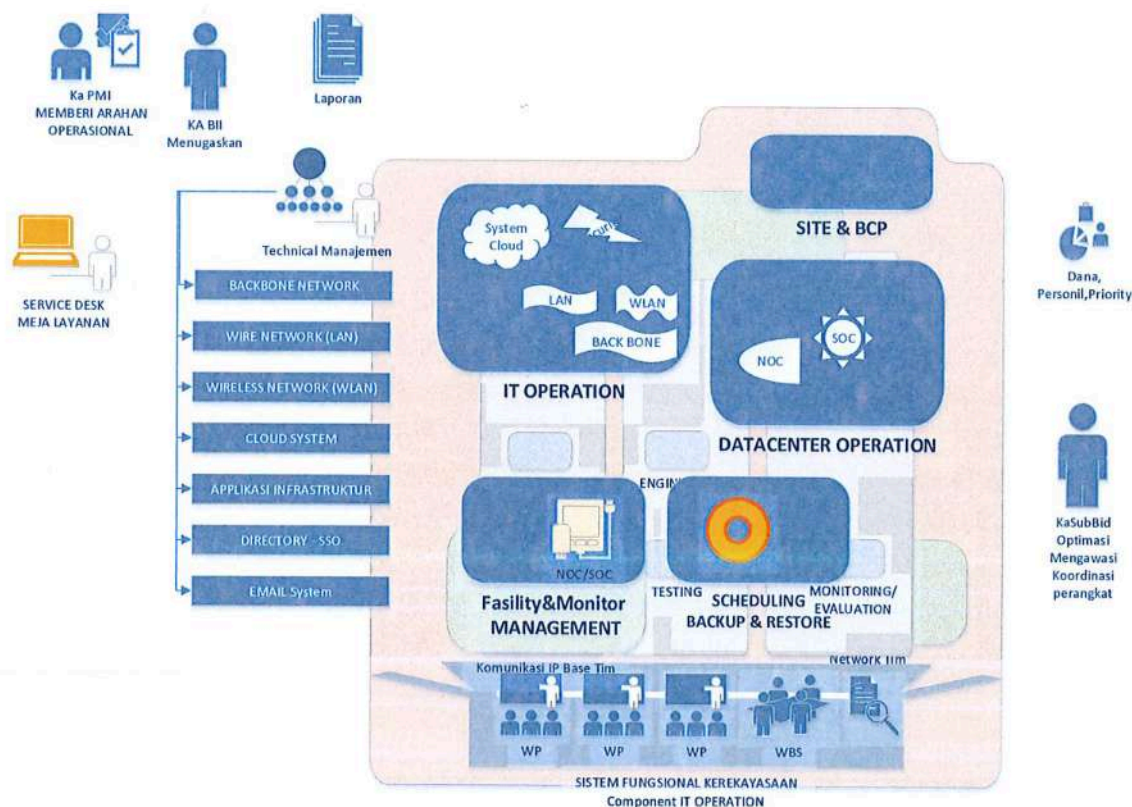
Adapun secara fungsi dalam *service operation*, BII telah menerapkan beberapa fungsi yang dilaksanakan yaitu:

- a. *Service desk* dengan SOP

b. *Technical management* dan *IT operation*, yang dilakukan secara manajemen kerekayasaan, yang dilaksanakan dan awasi oleh sub bidang pengembangan dan sub bidang optimasi. Sehingga perencanaan hingga pelaporannya telah tersusun dalam suatu sistem tersendiri.

Bidang Infrastruktur Informasi melaksanakan fungsi penanganan infrastruktur saja, sehingga ada beberapa yang tidak dilaksanakan, mengingat memang terbatas lingkup pekerjaan dan tanggung jawabnya. Sehingga di BII hanya ada *service desk*, *IT operation*, *technical management* dengan 'Tim Teknis' yang bekerja sesuai dengan sistem kerja kerekayasaan.

Pelaksanaan 'Manajemen Pengoperasian TI' di BII dengan demikian secara otomatis pekerjaannya terkoordinir antara *service desk*, yang memberikan informasi tentang insiden, problem dan kebutuhan pengguna, kemudian yang menggerakkan tim teknis yang menguasai secara spesifik perangkat, *hardware*, *software* dan perangkat spesifik lain, yang dilaksanakan melalui sistem kerekayasaan. Serta dengan dukungan struktural yang membantu penyelesaian di bidang *resources*, dana dan bentuk koordinasi dengan faktor eksternal.



Gambar 7.4 Manajemen Pengoperasian TI di BII

Di level operasional ini, Kepala Sub Bidang mengawasi, mengkoordinasi, sehingga operasional TI berlangsung dengan sebaik baiknya, karena ditangani oleh para *engineer* yang tepat, terutama dalam sistem kerja yang sudah teratur dalam sistem kerekayasaan.

Secara garis besar struktural berdasarkan objek teknis yang terkelola serta membagi dalam pekerjaan jenis optimasi operasional layanan serta jenis pengembangan infrastruktur. Yang pada kedua jenis ini dapat disatukan dalam sistem kerja kerekayasaan, dengan berbagai kelompok manajemen atau lingkup kerja tertentu yang spesifik. Misalnya pengelolaan

operasional IT yang optimal, pengelolaan data center yang memenuhi karakteristik tertentu, cara pengelolaan dan pelaksanaan fasilitas dan monitoring berbagai peralatan, maupun manajemen *backup*, agar peralatan ada kehandalan, maupun data dapat dijamin availabilitas atau ketersediaannya setiap saat.

Kesemuanya itu didukung dengan beberapa petunjuk teknis (Juknis) dan SOP yang mendukung operasional agar setiap personil mengetahui dan bertindak sesuai prosedur. Diantara Juknis dan SOP itu adalah SOP *Help Desk*, Juknis Perekayasa, Buku Pedoman Keamanan Informasi, Petunjuk Teknis *Backup* dan *Recovery* serta petunjuk teknis dan SOP yang terkait operasional TI.



## BAB VIII

### SISTEM MANAJEMEN PENDUKUNG TATA KELOLA INFRASTRUKTUR INFORMASI

Sebagaimana telah diketahui bahwa dalam penggunaan sistem elektronik atau sistem informasi untuk membantu suatu bisnis atau pekerjaan di suatu organisasi, maka dalam praktik pelaksanaannya ada berbagai kendala yang harus siap untuk ditangani. Dalam melaksanakan sistem ini harus punya keberlanjutan sebagaimana keberlanjutan proses bisnis yang dibantu. Untuk itu, maka perlu diketahui risiko yang dihadapi dan keamanan terhadap berbagai bentuk gangguan informasi yang ditangani.

Selain itu juga untuk keberlanjutan yang lebih baik lagi, atau menyusun suatu sistem yang selalu dapat dilaksanakan perbaikan (*improvement*), maka perlu pula manajemen pengetahuan serta keberlanjutan layanan yang disediakan.

Demikian pula bagi Bidang Infrastruktur Informasi selain dapat melaksanakan pengelolaan dan pengembangan secara terus menerus, maka perlu adanya perhatian pada permasalahan khusus tersebut. Sehingga pelaksanaan operasional ada bagian yang memperhatikan panduan dan arahan berikut.

Beberapa sistem manajemen yang mendukung atau saling melengkapi terhadap sistem tata kelola infrastruktur informasi BPPT diantaranya:

- Sistem Manajemen Risiko
- Sistem Manajemen Pengetahuan
- Sistem Manajemen Keamanan Informasi
- *Business Continuity Plan* (BCP)

Sistem tersebut di atas sudah diterapkan di lingkup PMI dilengkapi dengan dokumentasinya. Dalam buku panduan ini, selanjutnya akan dijelaskan secara singkat konsep masing-masing sistem tersebut di atas yang telah berjalan di PMI. Namun demikian, apabila ada hal-hal rinci yang perlu untuk diketahui dapat merujuk pada dokumen terkait dengan sistem yang dimaksud.

#### **Manajemen Risiko**

##### **Kebijakan Manajemen Risiko PMI**

Dalam rangka menerapkan *Good Corporate Governance* (GCG) serta meningkatkan kemampuan organisasi dalam menghadapi setiap perubahan, maka penerapan 'Manajemen Risiko' menjadi kebutuhan mutlak guna mengurangi dan mencegah terjadinya kerugian yang mengganggu kelangsungan layanan.

Kebijakan 'Manajemen Risiko' yang berlaku di lingkungan PMI adalah sebagai berikut:

1. Risiko merupakan bagian dari dinamika organisasi yang harus dikelola sebagai usaha memaksimalkan nilai organisasi serta memenuhi harapan pemangku kepentingan lainnya;
2. Menyatukan 'Manajemen Risiko' ke dalam budaya organisasi sehingga menjadi bagian integral dari praktik layanan dan pengambilan keputusan;

3. Kepala Bidang bertanggung jawab mengelola risiko di organisasinya masing-masing melalui proses penerapan manajemen risiko dan secara berkala melaporkan realisasi tindak lanjut pengendalian risiko dan segala peristiwa yang mengakibatkan kerugian organisasi.

### Kerangka Kerja Manajemen Risiko

Kerangka kerja 'Manajemen Risiko' menjadi dasar penataan yang mencakup seluruh kegiatan manajemen risiko di segala tingkatan di PMI. Kerangka kerja ini membantu PMI mengelola risiko secara efektif melalui penerapan proses manajemen risiko dalam berbagai tingkatan dan dalam konteks spesifik. Kerangka kerja ini memastikan bahwa informasi risiko yang lengkap dan memadai yang diperoleh dari proses manajemen risiko dilaporkan serta digunakan sebagai landasan untuk pengambilan keputusan. Hal ini dilakukan sesuai dengan kejelasan akuntabilitas pada setiap tingkatan organisasi.



Gambar 8.1 Kerangka Kerja Manajemen Risiko

Skema pada gambar di atas memperjelas gambaran umum mengenai kerangka kerja manajemen risiko sebagai induk dari proses manajemen risiko yang lebih bersifat teknis. Kerangka kerja ini tidak dimaksudkan untuk menggambarkan sebuah sistem manajemen baru, tetapi lebih ditujukan untuk membantu organisasi dalam mengintegrasikan manajemen risiko ke dalam sistem manajemen organisasi keseluruhan, khususnya melalui siklus manajemen PDCA (*Plan-Do-Check-Action*). Skema di atas menunjukkan gambaran mengenai bagaimana tata kelola risiko di PMI harus dilaksanakan, dimana dalam tata kelola risiko ini terdiri dari:

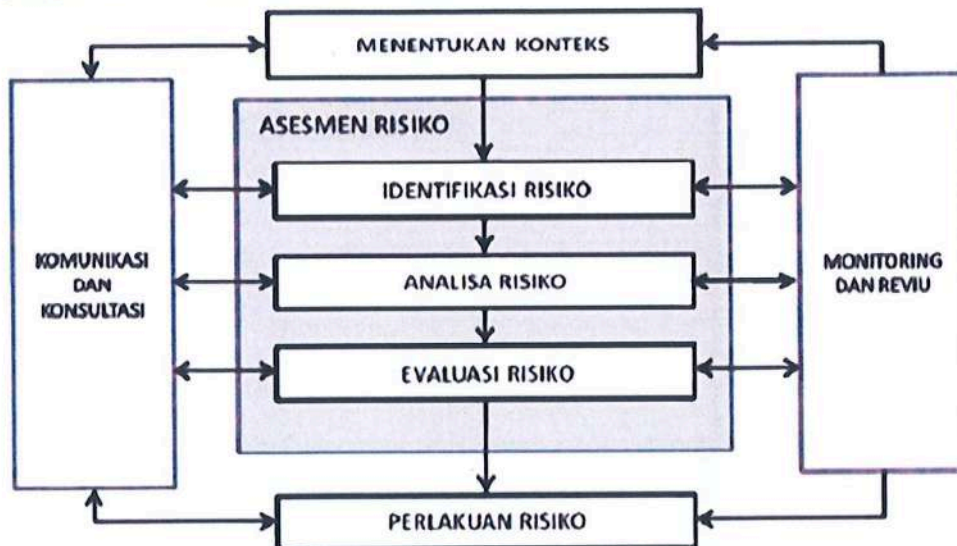
- aspek struktural
- aspek operasional
- aspek perawatan

### Proses Manajemen Risiko

Proses manajemen risiko adalah penerapan secara sistematis kebijakan manajemen, prosedur dan praktik manajemen dalam pelaksanaan tugas untuk melakukan komunikasi dan konsultasi; menetapkan konteks; melakukan asesmen risiko yang meliputi identifikasi; analisa dan evaluasi risiko; serta perlakuan risiko, dan diakhiri dengan pemantauan dan pengkajian risiko.

Proses manajemen risiko secara singkat adalah penerapan kerangka kerja manajemen risiko pada tiap-tiap jenis risiko yang secara spesifik mempunyai karakter yang berbeda-beda sesuai dengan konteksnya. Ini sesuai dengan prinsip manajemen risiko yang menyatakan bahwa manajemen risiko adalah khas bagi penggunaannya. Walaupun penerapan proses manajemen

risiko khas untuk masing-masing risiko, tetapi secara metodologis, penerapannya sesuai dengan sistem yang digambarkan pada gambar Praktik ini.



Gambar 8.2 Proses Manajemen Risiko

Proses manajemen risiko meliputi lima kegiatan, yaitu komunikasi dan konsultasi; menentukan konteks; asesmen risiko; perlakuan risiko; serta pemantauan dan kaji ulang, sebagaimana ditunjukkan pada gambar.

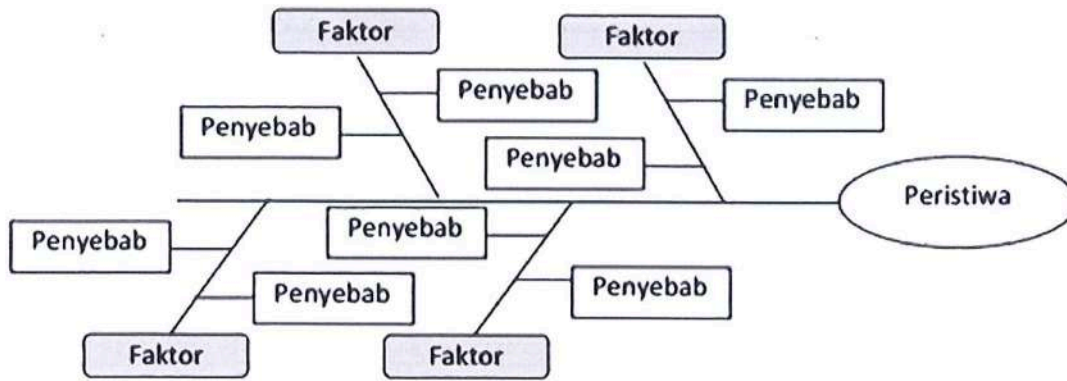
Proses manajemen risiko melibatkan banyak pihak dalam organisasi. Oleh karena itu, perlu kejelasan akuntabilitas untuk memastikan bahwa semua proses dapat berjalan dengan baik.

Untuk memperjelas akuntabilitas pemangku kepentingan dalam penerapan sistem manajemen risiko digunakan metode *RACI Matrix*. *RACI* adalah singkatan dari *Responsible*, *Accountable*, *Consulted*, dan *Informed*. *RACI Matrix* akan menjelaskan atau menentukan dalam setiap kegiatan yaitu:

- "R" siapa yang *responsible*, artinya siapa yang mengerjakan kegiatan tersebut;
- "A" siapa yang *accountable*, artinya siapa yang berhak membuat keputusan akhir atas kegiatan tersebut, serta menjawab pertanyaan-pertanyaan pihak lain;
- "C" siapa yang harus *consulted*, artinya harus diajak konsultasi atau dilibatkan sebelum atau saat kegiatan tersebut dilaksanakan atau dilanjutkan; serta
- "I" siapa yang harus *informed*, artinya siapa yang harus diberi informasi mengenai apa yang sedang terjadi atau sedang dilakukan tanpa harus menghentikan kegiatan tersebut.

### Identifikasi Risiko

Dalam mengidentifikasi risiko digunakan analisis sebab-akibat atau dikenal pula sebagai metoda diagram tulang ikan (*fishbone diagram*). Analisis sebab-akibat adalah suatu metode terstruktur untuk mengidentifikasi kemungkinan penyebab dari suatu peristiwa yang tidak diinginkan atau masalah. Metode ini mengeluarkan semua faktor penyebab yang mungkin terjadi sehingga semua hipotesis yang mungkin terjadi dapat dipertimbangkan. Metode ini digambarkan dalam diagram *fishbone* atau dalam sebuah diagram pohon, yang menggambarkan secara terstruktur dari daftar penyebab.



Gambar 8.3 Proses Identifikasi Risiko

Hasil akhir dari proses identifikasi risiko adalah dibuatnya daftar risiko. Daftar risiko adalah suatu rekaman data mengenai riwayat risiko dan perkembangan perlakuannya. Dengan demikian, daftar risiko merupakan data dasar dalam proses manajemen risiko yang harus selalu dimutakhirkan sesuai dengan perkembangan dan dinamika proses, serta konteks organisasi.

Secara umum, struktur isi dari daftar risiko meliputi lima hal yaitu nomor identifikasi risiko, Peristiwa, Penyebab, Dampak dan Penanganan.

### Analisa Risiko

Setelah proses identifikasi risiko selesai dilakukan, selanjutnya dilakukan analisis risiko. Analisis risiko adalah upaya untuk memahami risiko lebih dalam. Hasil analisis risiko ini akan menjadi masukan bagi evaluasi risiko dan untuk proses pengambilan keputusan mengenai perlakuan terhadap risiko tersebut.

Berdasarkan formulasi hubungan dampak dan kemungkinan yang dijadikan ukuran pemeringkatan risiko maka diperoleh gambaran hasil analisis risiko yang secara sederhana ditampilkan pada gambar berikut.

Kemungkinan	4	4	8	12	16	<b>Kemungkinan :</b> 1 : Jarang sekali 2 : Jarang 3 : Sering 4 : Sering sekali <b>Dampak :</b> 1 : Dapat diabaikan 2 : Serious 3 : Berbahaya 4 : Katastropik
	3	3	6	9	12	
	2	2	4	6	8	
	1	1	2	3	4	
		1	2	3	4	
		Dampak				

Gambar 8.9 Hubungan Dampak dan Kemungkinan Pemeringkatan Risiko

## Evaluasi Risiko

Tujuan dari evaluasi risiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut. Hasil evaluasi risiko akan menjadi masukan bagi proses perlakuan risiko.

Hasil analisis risiko menjadi masukan untuk dievaluasi lebih lanjut menjadi urutan prioritas perlakuan risiko, sekaligus menyaring risiko-risiko tertentu untuk tidak ditindaklanjuti atau diperlakukan khusus. Risiko-risiko yang perlu ditindaklanjuti untuk mendapat perlakuan khusus adalah risiko dengan peringkat enam sampai dengan enam belas hasil penilaian pada tahapan analisis risiko.

Hasil evaluasi risiko menunjukkan peringkat risiko yang memerlukan penanganan lebih lanjut atas dasar risiko yang tersisa dan efektifitas pengendalian risiko yang dituangkan dalam dokumen Rencana Penanganan Risiko / *Risk Treatment Plan* (RTP).

## Rencana Penanganan Risiko

Penanganan risiko adalah suatu proses untuk mengidentifikasi dan memilih opsi penanganan risiko, langkah penanganan dan jadwal pelaksanaannya melalui proses yang sistematis dan terstruktur, sehingga akan dihasilkan jenis penanganan yang efektif dan efisien untuk suatu risiko dan jadwal implementasinya.

Konsep dalam melakukan penanganan risiko adalah:

- a. Menggunakan pemahaman mendalam, pendekatan sistematis dan komprehensif antara lain:
  - Risiko-risiko yang perlu mendapatkan penanganan;
  - Prioritas penanganan;
  - Besarnya dampak penanganan tersebut terhadap konteks yang lebih luas.
- b. Mempertimbangkan analisa biaya dan keuntungan;
- c. Penanganan risiko diarahkan pada penanganan akar permasalahan (*root cause*) dan bukan hanya gejala.

Opsi yang dapat dipilih dalam penanganan risiko adalah:

- (1) Menghindari risiko
- (2) Menerima risiko
- (3) Mengurangi konsekuensi risiko
- (4) Mengurangi frekuensi risiko
- (5) Membagi / mengalihkan risiko

Contoh Rencana Penanganan Risiko

**Risk Treatment Plan**

<b>Subject :</b> Layanan Website BPPT	
<b>Information Asset</b>	<b>Asset Name :</b> Server website BPPT <b>Owner Division :</b> DATIN
<b>Risk Description :</b> Website BPPT diretas karena admin belum menutup hak akses ketika selesai mengubah konten pada website	
<b>Risk Point (or Gap from Baseline) :</b>	
<b>Treatment Option :</b> <b>REDUCE / AVOID / TRANSFER / ACCEPT</b>	
<b>Action Plan</b>	<b>1</b>
	<b>By Date :</b> <b>Action By :</b> Rachmat
	<b>Action Details</b>
	<ul style="list-style-type: none"> <li>✓ Memutuskan koneksi ke server</li> <li>✓ Mengalihkan ke server backup / restore sistem aplikasi dan database dari clean backup</li> <li>✓ Melokalisir website dan melihat log detection dan analisis</li> <li>✓ Mengobservasi dan mengidentifikasi website yang diretas</li> <li>✓ Installing patches dan mengganti password</li> <li>✓ Mengkonfigurasi ulang keamanan sistem server</li> </ul> <b>Estimated Cost :</b>
<b>2</b>	<b>By Date :</b> <b>Action By :</b> Trianita Hermawati
	<b>Action Details</b>
	<ul style="list-style-type: none"> <li>✓ Dibuatkan SOP untuk admin agar selalu menutup hak akses setiap selesai mengubah konten pada website</li> </ul> <b>Estimated Cost :</b>
<b>Risk Point After Action :</b> <b>Acceptability :</b> Acceptable / Unacceptable	
<b>Remarks</b>	
<b>Planner's Comment (if any) :</b>	
<b>Signature</b>	<b>Name (in block letter) :</b> DENNA ARFIANI
	<b>Signature :</b> <b>Date :</b>
<b>Approver's Comment (if any) :</b>	
<b>Approval :</b> <b>APPROVE / REVERT</b>	
<b>Signature</b>	<b>Name (in block letter) :</b> FACHRUDDIN RAHMAT
	<b>Signature :</b> <b>Date :</b>

Gambar 8.5 Rencana Penanganan Risiko

**B. Manajemen Pengetahuan**

Manajemen pengetahuan (KMS – *Knowledge Management System*) adalah untuk membuat berbagai kemudahan serta meningkatkan manfaat dari pengetahuan itu sendiri. Manfaat KMS antara lain mempermudah proses berbagi pengetahuan (*knowledge sharing*) dengan

melakukan diskusi sesuai dengan keterlibatan tiap pegawai dalam kategori komunitas keahlian yang diikutinya, hal ini bisa melalui Aplikasi Forum Komunitas Praktisi.

Manfaat dibangunnya forum komunitas praktisi adalah sebagai berikut :

- Mempermudah proses berbagi pengetahuan (*Knowledge Sharing*) dengan melakukan diskusi sesuai dengan keterlibatan tiap pegawai dalam kategori komunitas keahlian yang diikutinya.
- Mempermudah pencarian pegawai untuk diminta berbagi pengalaman, berdiskusi tentang suatu pengetahuan atau saling berkolaborasi sesuai dengan forum yang diikutinya, kemudian juga mempermudah penyampaian pendapat dan pemikiran dalam mencari solusi permasalahan teknologi dan sebagainya.
- Menjalin jejaring dan memperluas wawasan melalui keaktifan dalam berpartisipasi di forum komunitas praktisi.
- Mempermudah pencarian keahlian pegawai sesuai dengan kompetensi yang dimilikinya melalui aplikasi 'Data Kepakaran'.
- Mempermudah melakukan akses ke repositori *online* yang dimiliki BPPT yang berisikan seluruh koleksi dan sumber pengetahuan yang telah dikelola dengan baik melalui aplikasi 'Digital Library'. Ini akan mempermudah penelusuran jurnal-jurnal di BPPT hingga pengelolaan proses penerbitannya secara online, melalui aplikasi *Open Journal System*.

KMS yang mulai dibangun di BPPT adalah menggunakan komunitas praktisi bertujuan untuk mewujudkan "*create – expand - exchange knowledge*" hingga mampu untuk mengembangkan kapabilitas individu yang tergabung dalam forum tersebut. Faktor pengikat dalam komunitas tersebut adalah kesamaan minat, komitmen dan motivasi untuk berkembang kearah lebih baik. Selama masih ada relevansi dengan topik-topik, nilai-nilai yang dijunjung bersama serta kepentingan dan keminatan yang sama maka suatu forum komunitas akan tetap eksis sebagai salah satu sarana untuk saling bagi pengetahuan/*knowledge*.

Agar forum komunitas praktisi bisa menjadi sarana untuk berbagi pengetahuan, khususnya untuk pengetahuan tacit (*Implisit Knowledge*), yaitu pengetahuan praktis yang didapat dari pengalaman, maka dikembangkan aplikasi forum berbasis online untuk mendukung tujuan tersebut. Melalui panduan penggunaan forum komunitas berbasis *web*, diharapkan agar mampu memberikan kemudahan bagi para pengguna, khususnya bagi pegawai di BPPT, untuk mengakses dan mengelaborasi aplikasi komunitas praktisi dalam kegiatan kerja sehari-hari sebagai salah satu tools dalam mengelola pengetahuan.

Manajemen pengetahuan terkait dengan 'Layanan Infrastruktur Informasi', secara khusus terkoneksi ke *service desk* dalam rangka mengumpulkan informasi terutama adanya insiden serta penyelesaiannya serta resolusi dalam 'Manajemen Masalah'. KMS di BII dikembangkan berhubungan langsung dengan *service desk*, sehingga sebelum dilakukan penanganan perbaikan, bisa jadi telah ada jenis masalah yang sama yang telah ditangani sebelumnya, sehingga penyelesaiannya bisa lebih cepat mendapatkan resolusinya. Oleh karena itu, pencatatan terus menerus pengalaman yang ada dengan catatan yang rapi itu dapat dipakai sebagai KMS yang bermanfaat.

### C. Manajemen Keamanan Informasi

Manajemen keamanan Informasi sangat penting dan sangat berpengaruh dalam lingkungan Infrastruktur Informasi, maka BII harus memperhatikan dan melaksanakan berbagai arahan yang ada di Buku Kebijakan Keamanan Informasi BPPT (BKKI), dimana di dalamnya terdapat arahan yang spesifik dalam pengelolaan Infrastruktur juga.

Sebagai petunjuk teknis, maka BKKI dipakai sebagai acuan yang bisa diterjemahkan dalam SOP yang mendukung keamanan informasi kemudian pelaksanaan tata kelolanya menyatu dengan apa yang dilakukan di BII. Karena dokumen BKKI itu sudah mengacu pada arahan dan framework yaitu ISO 27000, maka dalam hal ini dapat dipakai dengan langsung, karena sudah teruji. Dengan demikian Manajemen Keamanan Informasi yang digunakan BII telah mempunyai arahan yang baku dan tinggal disempurnakan serta dilaksanakan secara praktis. Dengan menambah beberapa SOP dan SIK lebih detailnya.

### D. *Business Continuity Plan (BCP)*

Kegiatan layanan tidak dapat terhindar dari adanya gangguan/kerusakan yang disebabkan oleh alam maupun manusia misalnya terjadinya gempa bumi, bom, kebakaran, banjir, *power failure*, kesalahan teknis, kelalaian manusia, demo buruh, huru-hara dan sebagainya. Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi, tetapi juga berdampak pada kegiatan operasional layanan terutama pelayanan kepada pengguna. Bila tidak ditangani secara khusus, selain PMI akan menghadapi risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan pengguna kepada PMI.

Untuk meminimalisasi risiko tersebut, PMI memiliki *Business Continuity Management (BCM)* yaitu proses manajemen terpadu dan menyeluruh untuk menjamin kegiatan operasional PMI tetap dapat berfungsi walaupun terdapat gangguan/bencana guna melindungi kepentingan para *stakeholder*. BCM merupakan bagian yang terintegrasi dengan kebijakan manajemen risiko secara keseluruhan. BCM PMI didukung dengan hal-hal sebagai berikut:

- a. adanya pengawasan aktif manajemen;
- b. pelaksanaan *Business Impact Analysis* dan *Risk Assessment*;
- c. penyusunan *Business Continuity Plan (BCP)* yang memadai;
- d. pengujian terhadap BCP; dan
- e. dilakukan pemeriksaan oleh Auditor Internal.

---

Dokumen *Business Continuity Plan (BCP)* PMI adalah dokumen tertulis yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pengurangan risiko, penanganan dampak gangguan/bencana dan proses pemulihan agar kegiatan operasional organisasi dan pelayanan kepada pengguna tetap dapat berjalan. Rencana tindak tertulis tersebut melibatkan seluruh sumber daya termasuk sumber daya manusia yang mendukung fungsi layanan dan kegiatan operasional yang kritis. Komponen prosedur BCP meliputi *Disaster Recovery Plan (DRP)* dan *Contingency Plan (CP)*.

*Disaster Recovery Plan (DRP)* lebih menekankan pada aspek teknologi dengan fokus pada *data recovery/restoration plan* dan berfungsinya sistem aplikasi dan infrastruktur TI yang kritikal. Sedangkan, *Contingency Plan (CP)* menekankan pada rencana tindak untuk menjaga kelangsungan layanannya apabila terjadi gangguan atau bencana termasuk tindakan antisipatif menghadapi kondisi terburuk misalnya bila peralatan yang digunakan sama sekali tidak dapat dipulihkan untuk waktu yang cukup lama. *Contingency Plan (CP)* meliputi pula rencana untuk memastikan kelangsungan seluruh layanan PMI.

### **Business Impact Analysis**

Efektifitas dari suatu BCP sangat bergantung pada kemampuan manajemen untuk secara tepat mengidentifikasi kritis tidaknya berbagai proses kerja atau aktivitas yang ada di PMI. Dengan demikian *Business Impact Analysis (BIA)* merupakan dasar dari penyusunan keseluruhan BCP. Hal-hal yang harus dianalisis dalam BIA meliputi:

- a. tingkat kepentingan (*criticality*) masing-masing proses bisnis dan ketergantungan antar proses bisnis serta prioritisasi yang diperlukan;
- b. tingkat ketergantungan terhadap pihak penyedia jasa;
- c. tingkat *Maximum Tolerable Outage/Recovery Time Objective* (berapa lama BII dapat bekerja tanpa sistem atau fasilitas yang mengalami gangguan dan atau berapa cepat sistem atau fasilitas tersebut harus berfungsi kembali);
- d. tingkat *Minimum Resources Requirement* (personil, data dan kelengkapan sistem serta fasilitas yang diperlukan secara minimal agar bisnis bisa pulih dan berjalan);
- e. dampak potensial dari kejadian yang bersifat tidak spesifik dan tidak dapat dikontrol terhadap proses bisnis dan pelayanan kepada pengguna;
- f. dampak disaster terhadap seluruh bagian dan fungsi layanan, bukan hanya terhadap data processing;
- g. estimasi *downtime* maksimum yang dapat ditoleransi dan tingkat toleransi atas kehilangan data dan terhentinya proses bisnis serta dampak *downtime* terhadap kerugian finansial;
- h. jalur komunikasi yang dibutuhkan untuk berjalannya pemulihan;
- i. kemampuan dan pengetahuan petugas mengenai *contingency plan* dan ketersediaan petugas pengganti di tempat pemulihan;
- j. dampak hukum dan pemenuhan ketentuan yang terkait, seperti ketentuan mengenai kerahasiaan data pengguna.

### **Business Continuity Plan PMI**

Penyusunan BCP dilakukan setelah proses BIA dan *risk assessment*. BCP terdiri dari kebijakan, strategi, skenario dan prosedur yang diperlukan untuk dapat memastikan kelangsungan proses bisnis pada saat terjadinya gangguan atau bencana. BCP memuat beberapa alternatif strategi yang dapat diambil untuk mengatasi masing-masing jenis dan ukuran gangguan atau bencana. Strategi pemulihan tersebut disesuaikan dengan hasil BIA, analisis risiko, sumber daya yang dimiliki serta kapasitas dan tingkat teknologi organisasi.

Contoh strategi yang dapat dipilih antara lain, penggunaan jasa pihak lain (*outsourcing*), *Disaster Recovery Center (hot site, warm site atau cold site)* dan atau *Business Recovery Center*.

Setiap strategi yang dipilih hendaknya disertai analisis/alasan yang melatarbelakangi dan harus didukung dengan sistem dan prosedur yang sesuai.

Adapun jenis-jenis prosedur dalam BCP antara lain mencakup:

- a. prosedur tanggap darurat (*emergency response - immediate steps*) untuk mengendalikan krisis pada saat terjadi gangguan/bencana, membatasi dampak kerugian, serta menentukan perlu tidaknya mendeklarasikan keadaan *disaster*;
- b. prosedur pemulihan sistem yang memungkinkan kegiatan operasional organisasi dapat kembali ke kondisi normal;
- c. prosedur pemulihan bisnis (*business recovery*) yang menjabarkan tugas dan tanggung jawab di masing-masing proses bisnis agar dapat segera memulihkan kegiatan operasional organisasi. Termasuk dalam hal ini *contingency plan* untuk pelayanan pengguna secara manual apabila dibutuhkan;
- d. prosedur sinkronisasi data digunakan untuk memastikan kesamaan antara data mesin produksi dengan data yang ada di *backup site*, serta untuk memastikan semua data hasil pemrosesan bisnis selama masa pemulihan telah masuk ke dalam sistem.

Setiap prosedur BCP di atas sekurang-kurangnya mencakup komponen sebagai berikut:

a. Personil

Apabila diperlukan, dalam organisasi tim kerja BCP dapat dibentuk sub-sub tim untuk koordinasi, pelaksanaan prosedur tanggap darurat, pelaksanaan pemulihan sistem, pelaksanaan pemulihan proses bisnis dan evaluasi atau umpan balik. BCP harus secara jelas mengemukakan komposisi, wewenang dan tanggung jawab setiap tim kerja tim kerja BCP dan memiliki alur komunikasi yang terintegrasi.

b. Teknologi

Prosedur yang disusun harus memperhatikan komponen teknologi yang dimiliki organisasi seperti perangkat keras, perangkat lunak, fasilitas komunikasi, sampai dengan peralatan pemrosesan kegiatan operasional di masing-masing fungsi layanan. Selain itu, hal-hal yang berkaitan dengan *data files* dan *vital records* juga perlu diperhatikan seperti keberadaan DRC dan dokumentasi sistem dan data backup.

c. *Disaster Recovery Center* ( DRC)

BII harus memastikan ketersediaan DRC sebagai backup DC yang dapat dioperasikan apabila DC tidak dapat beroperasi atau dalam kondisi disaster. Sesuai dengan alternatif strategi yang dipilih organisasi, DRC dapat dikelola sendiri maupun oleh pihak penyedia jasa. BII memperhatikan hal-hal sebagai berikut:

- (1) DRC ditempatkan pada lokasi yang terpisah dari lokasi *Data Center*, dengan memperhatikan faktor geografi:
  - a) jangkauan geografi atas suatu gangguan/bencana dan dampaknya terhadap kota atau wilayah tempat lokasi DRC berada;
  - b) analisis risiko yang berkaitan dengan lokasi DRC (apakah wilayah gempa atau petir) dan terhubung dengan infrastruktur komunikasi dan listrik yang berbeda dengan DC, serta fasilitas lain yang diperlukan untuk tetap berjalannya suatu sistem;

- (2) kondisi rentannya lokasi yang dipilih dengan kemungkinan huru-hara dan kerusakan;
- (3) DRC memiliki pasokan listrik dan sarana telekomunikasi yang dapat menjamin beroperasinya DRC;
- (4) sistem di DRC harus kompatibel dengan sistem yang digunakan pada DC dan harus disesuaikan jika terjadi perubahan pada DC;
- (5) merupakan *restricted area*; dan
- (6) memperhitungkan waktu tempuh untuk terjaminnya proses *recovery*.

d. *Backup* Dokumentasi, Sistem dan Data

BII menjamin ketersediaan backup yang efektif dari informasi bisnis yang penting, perangkat lunak dan dokumentasi terkait sistem dan user untuk setiap proses fungsi layanan yang penting (*critical*). Hal-hal yang harus diperhatikan dalam dokumentasi, sistem dan data *backup* antara lain:

- (1) *backup* dimaksud harus disimpan di lokasi lain dari DC (*off site*). Setiap perubahan dan modifikasi harus didokumentasikan dan salinannya juga harus diperbaharui;
- (2) media backup harus disimpan di lingkungan yang aman di lokasi *off site* dengan standar sistem pengamanan yang memadai;
- (3) *full system backup* harus dilakukan secara periodik. Jika terjadi perubahan sistem yang mendasar maka *full system backup* harus dilakukan sesegera mungkin;
- (4) seluruh media *backup* menggunakan standar *labelling*/penamaan untuk dapat mengidentifikasi penggunaan, tanggal dan jadwal retensi;
- (5) media *backup* harus diuji secara regular untuk meyakini bahwa dapat digunakan pada saat diperlukan (keadaan *emergency*);
- (6) memiliki prosedur untuk disposal media *backup*.

e. *Business Recovery Center* (BRC) / *Crisis Center* / *Business Resumption Center*

BCP memiliki skenario mengenai lokasi kegiatan dari masing-masing fungsi bisnis untuk berbagai tingkat *disaster*. Untuk tingkat bencana total *disaster* atau *catastrophic*, PMI menyiapkan lokasi alternatif agar tetap dapat menjalankan kegiatan fungsi bisnis.

f. Fasilitas Komunikasi

BII memastikan bahwa alternatif jalur komunikasi yang terdapat di wilayah operasional dapat digunakan pada saat gangguan/bencana, baik di lingkungan intern maupun dengan pihak eksternal.



## BAB IX MONITORING DAN EVALUASI

Lingkup monitoring dan evaluasi ini secara luas melingkupi dan memonitor mulai dari hal terkecil dari peralatan hingga berfungsinya layanan yang menjadi inti dari pelaksanaan pekerjaan yang ada di BII.

### Monitoring

Monitoring adalah proses melihat keadaan dari objek yang diawasi. Dalam proses monitoring infrastruktur ini, tidak hanya tentang fungsi peralatan saja yang diawasi tetapi juga proses pelaksanaan layanan sehingga layanan yang diberikan memuaskan pengguna.

Daftar Peralatan monitoring yang ada di BII antara lain:

Tabel 9.16 Daftar Peralatan Monitoring

No.	Nama Peralatan Monitor	Fungsi monitoring untuk
1	MRTG	Monitoring Trafik perangkat dan sebagian server
2	PRTG	Monitoring Sensor Perangkat
3	NMS (OPEN NMS)	Monitoring status perangkat
4	Nagios	Monitoring status perangkat
5	Wireles Controller	Memonitor perangkat AccessPoint enterprise
6	PHP Server Monitor	Memonitor link Access dari eksternal
7	Device base Monitoring	Monitoring langsung Merangkat, (UTM,Switch)
8	End Point Security (Kaspersky)	Monitoring Antivirus End Client
9	Mail Gateway	Monitoring Aktivitas Mail
10	VMWare	Monitoring Infrastruktur Cloud

Peralatan monitoring tersebut sangat penting untuk digunakan, baik untuk merekam kejadian serta untuk menganalisis berbagai keadaan yang ada dalam infrastruktur informasi maupun layanan yang diberikan oleh BII.

Untuk memperbaiki sistem monitoring di masa mendatang beberapa peralatan monitoring perlu ditingkatkan serta sistem dalam melaksanakan monitoring dan pemberian *alert* kepada petugas lebih dipercepat dan komunikatif.

Pelaksanaan monitoring ini adalah untuk membantu Kepala Bidang Infrastruktur Informasi dalam mendapatkan informasi secara cepat serta mempunyai konten yang jelas dan spesifik. Kepala BII dan Kepala Sub Bidang di bawahnya, perlu merencanakan serta mengembangkan

peralatan monitoring untuk mempercepat deteksi serta memudahkan dalam melakukan kontrol terhadap Infrastruktur. Untuk mendapatkan kemudahan atas gambaran kemampuan monitoring ini supaya dibuat dan diperbaiki suatu daftar peralatan monitoring, yang berisi nama, tempat monitoring, ruang lingkup monitoring, serta kemampuan atau parameter monitoring yang bisa dilakukan.

### Evaluasi

Evaluasi merupakan proses perbandingan hasil dari monitoring, pada waktu yang berbeda, adalah proses melihat keadaan dari objek yang diawasi, kemudian dianalisis perbedaan tersebut. Dalam proses evaluasi ini pertama tentang layanan yang diberikan kemudian masuk pada evaluasi peralatan yang menyusun layanan tersebut.

Evaluasi yang dilakukan disesuaikan dengan tujuan atau sasaran kegiatan yang secara spesifik seperti apa yang ada pada indikator kinerja kegiatan. Sehingga diharapkan ukuran yang digunakan merupakan hal yang mudah dimengerti.

Tabel 9.17 Tabel Evaluasi Layanan BII

No	Bahan evaluasi	Proses/indikator evaluasi	Waktu evaluasi	Pelaksana
1	Layanan Mail & Internet	Availability, capacity,	Bulanan	SubBid Optimasi
2	Services Desk	Respons time, kepuasan	Triwulan	Kabid BII
3	Cloud system	Capacity, Security	Triwulan	Kabid BII
4	IP Based Communication	Availability	Triwulan	Kabid Pengembangan
5	BandWidth ISP	Reliability, respons time,	Bulanan	Kabid BII

Evaluasi ini dapat ditambahkan jenis atau bahan evaluasi, sesuai kebutuhan manajemen serta kebutuhan peningkatan kualitas layanan. Hasilnya direkam dalam *file* tertentu dibahas dalam rangka proses peningkatan berbagai parameter termasuk layanan yang diselenggarakan BII.

### Audit Internal

Audit internal adalah audit yang dilaksanakan oleh staf Pusat Manajemen Informasi (PMI) sebagai auditor (pihak yang melakukan audit) terhadap bidang-bidang dan sub bagian TU sebagai *auditee* (pihak yang diaudit.) di lingkungan PMI berkaitan dengan sistem, prosedur dan kegiatan-kegiatan yang dilaksanakan. Dimana yang di audit adalah layanan adalah kegiatan layanan yang dilakukan oleh bidang atau sub bagian TU di lingkungan PMI sesuai dengan tugas pokok dan fungsinya kepada *stakeholder* baik internal maupun eksternal BPPT. Dimana hasil akhirnya adalah rekomendasi untuk dilakukan tindakan perbaikan yang dilakukan untuk memperbaiki berdasarkan temuan-temuan dari audit internal.

Temuan-temuan tersebut dibagi menjadi 3 tiga:

1. Temuan klasifikasi *major* adalah temuan diklasifikasikan *major* bilamana tercantum dalam kriteria audit dan berpengaruh secara langsung terhadap mutu layanan sehingga sasaran mutu yang ditetapkan tidak tercapai.
2. Temuan klasifikasi *minor* adalah temuan diklasifikasikan *minor* bilamana tercantum dalam kriteria audit dan tidak berpengaruh secara langsung terhadap mutu layanan sehingga sasaran mutu yang ditetapkan masih dapat tercapai.
3. Temuan klasifikasi observasi adalah temuan diklasifikasikan observasi bilamana tidak dicantumkan pada kriteria audit tapi menjadi masukan yang penting bagi perbaikan berkelanjutan.

### **Kaji Ulang Manajemen**

Kaji ulang manajemen adalah kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi sehingga pemenuhan kesesuaian secara efektif dan efisien dapat tercapai berdasarkan sumber daya yang ada untuk memenuhi persyaratan sistem manajemen mutu, pengguna maupun metode dan peraturan yang berlaku.

Periode yang umum untuk menyelenggarakan suatu kaji ulang manajemen adalah setiap dua belas bulan. Periode lainnya adalah sesuai kebutuhan misalnya jika ditemukan suatu isu yang serius dan berisiko pada bisnis maupun operasional, pengaduan pengguna yang mempengaruhi penerapan sistem manajemen mutu dan ketidaksesuaian yang terjadi dan berdampak pada kinerja layanan.

Kaji ulang manajemen bertujuan untuk evaluasi efektivitas dan efisiensi penerapan sistem manajemen mutu, yaitu:

- Membantu mencapai kebijakan dan sasaran mutu
- Membantu mengendalikan operasional layanan TI
- Meningkatkan efektivitas dan efisiensi kinerja dengan mengurangi ketidaksesuaian yang terjadi
- Menentukan perubahan yang diperlukan untuk dokumentasi dan kegiatan operasional
- Menentukan kebutuhan sumber daya termasuk pelatihan personil
- Menentukan tindakan perbaikan dan pencegahan
- Menentukan jumlah ketidaksesuaian yang direduksi sejalan dengan waktu

Materi sebagai bahan pembahasan dalam kaji ulang manajemen antara lain:

1. Kecocokan kebijakan dan prosedur;
2. Laporan dari personil manajerial dan perekayasa;
3. Hasil audit internal yang terakhir;
4. Tindakan perbaikan dan pencegahan;
5. Umpan balik pengguna, pengaduan, rekomendasi tentang peningkatan dan
6. Faktor-faktor relevan lainnya seperti kegiatan pengendalian mutu, sumber daya, dan pelatihan staf.



## **BAB X PENUTUP**

Demikian petunjuk teknis sistem tata kelola infrastruktur informasi ini disusun sebagai pendetailan untuk terselenggaranya tugas dan fungsi Bidang Infrastruktur Informasi. Penyusunan berdasarkan atas arahan dan aturan kerja yang ada dan dilaksanakan di BPPT, serta pedoman pelaksanaan yang ada di Bidang Infrastruktur Informasi. Penanganan tata kelola ini kemudian dilaksanakan oleh SDM yang profesional, diorganisasikan secara benar disertai sistem yang mampu untuk mudah dilakukan audit dalam berbagai seginya.

## REFERENSI

- Admin, & Admin. (2018, November 27). Service level management. Retrieved from <http://tierrasalto.com/service-level-management/>.
- CIO BPPT. *Rencana Tindak BPPT 2015-2019*. (2016). Jakarta: BPPT.
- ISACA. (2012). *Cobit® 5: a business framework for the governance and management of enterprise It*. Rolling Meadows, IL.
- ISACA. (2012). *In COBIT 5: enabling processes*. Rolling Meadows, IL.
- ISACA. (2014). *Vendor management using Cobit 5*. Rolling Meadows, IL.
- ITIL v3 Process Maps. (2019, October 23). Retrieved from <http://www.itskeptic.org/node/1995>.
- Materi Presentasi Training Pengembangan Tata Kelola Infrastruktur TIK BPPT*. (2017). Jakarta: IT Consultant & Training KNK.
- Kajian Pengembangan Tata Kelola Infrastruktur TIK BPPT berdasarkan COBIT 5*. (2017). Jakarta: BPPT.
- Tim CIO BPPT. (2016). *Rencana Induk Teknologi Informasi 2015-2019*. Jakarta: BPPT.
- Yanuar, Ahmad Ismed, Rochmadi, Taslim dan Setyawan, S. Imam. *Kebijakan Keamanan Informasi: mengamankan keamanan informasi di era digital*. (2017). Jakarta: BPPT Press.
- Yanuar, Ahmad Ismed. *Panduan Manajemen Risiko PMI*. (2015). Jakarta: BPPT.

## INDEKS

### A

*Access Management*, vii, 82, 88  
administrator, 56, 64, 73  
aksesabilitas, 24  
*alert*, 91, 106  
*Align, Plan, and Organize (APO)*, 26, 39  
analisis proses, 7  
*auditee*, 107  
auditor, 2, 25, 31, 107  
availabilitas, 24, 60, 92  
*Availability Management*, 58

### B

*Backbone*, 18, 21  
Badan Pengkajian dan Penerapan  
Teknologi, iv, 4  
*bandwith*, 70  
Bidang Infrastruktur Informasi, v, 5, 8, 9,  
10, 14, 15, 40, 51, 53, 56, 57, 78, 110  
BPPT, iv, v, vi, viii, 1, 2, 3, 4, 5, 6, 7, 8, 9,  
10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21,  
22, 24, 25, 29, 30, 32, 33, 34, 35, 40, 42,  
43, 48, 51, 52, 53, 54, 55, 56, 60, 61, 64,  
65, 66, 70, 77, 91, 93, 100, 101, 108,  
110, 111  
*Build, Acquire, and Implement (BAI)*, 26  
*Business Continuity Plan (BCP)*, vii, 10, 93,  
101  
*Business Continuity Planning*, 6  
*Business Impact Analysis (BIA)*, 102  
*Business Process Management*, 7  
*business process owners*, 25  
*Business Service Continuity*, 7

### C

*Capacity Management*, 38, 58, 69  
catatan insiden, 86

Catatan Konfigurasi, 81  
CERT, 16  
*chair person*, 26, 27  
*Change Advisory Board (CAB)*, 77  
*Change Management*, vi, 38, 74, 76, 78  
*Chief Information Officer*, 6, 40  
*Cloud*, 19, 20, 41, 43, 48, 53, 54, 70, 106,  
107  
COBIT, vi, viii, x, 1, 3, 4, 12, 16, 25, 26, 27,  
28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 39,  
40, 48, 51, 57, 111  
*Computer Emergency Response Team*, 16  
*Configuration Management System (CMS)*,  
80  
*console management*, 90  
*consolidation*, 90  
***Continual Service Improvement (CSI)***, 31  
*control access*, 21  
*Control Objective for Information &  
Related Technology (COBIT)*, 1  
*control objectives*, 25, 31  
*Crisis Center*, 104  
CSIRT, vi, viii, 16, 17, 60

### D

*data center*, 53, 90, 92  
*Data Center*, viii, 18, 19, 20, 21, 54, 91,  
104  
Data Kepakaran, 100  
*decision sheet*, 76  
*Definitive Media Library (DML)*, 81  
*Deliver, Service and Support (DSS)*, 26, 43  
*Deming Quality Cycle*, 31  
*desain proses*, 7  
*detail plan*, 5  
*diagnosa kematangan*, 6

Digital Library, 100

Disaster Recovery site, 21

dokumen kontrak, 66

DRC, viii, 21, 91, 103, 104

## E

e-government, v, 1, 3, 8, 12, 14, 24, 40, 41

e-mail, 24, 53, 70

enabler, 33

engineer, 42, 92

Enterprise Architecture, 6

Evaluasi, vii, x, 6, 16, 26, 65, 67, 86, 88, 89, 97, 107

Evaluate, Direct, dan Monitor (EDM), 26

Evaluation, 74

event management, 83, 84

Event Management, vii, 82, 84

## F

facility management, 90

fase desain, 6

fase evaluasi, 6

fase implementasi, 6

fase kontrol, 6

fiber optic, 18

framework, v, 3, 4, 5, 11, 12, 15, 16, 24, 25, 32, 36, 40, 57, 82, 101, 111

## G

Good Corporate Governance (GCG), 94

good governance, 12

GovCSIRT, 16

governance, 12, 24, 27, 39, 111

Government Computer Security Incident Respon Team, 17

## H

Help Desk, 92

high availability, 21

High Level Design, 20

Hyperconverged solution, 21

## I

Implisit Knowledge, 100

Incident Management, vii, 39, 51, 82, 85

Information Security Management, 58, 60

Information Technology Infrastructure Library (ITIL), 2, 28

infrastruktur informasi, v, 1, 2, 3, 5, 6, 8, 9, 11, 12, 14, 16, 17, 25, 39, 51, 53, 59, 91, 93, 106, 110

Infrastruktur informasi, v, viii, 4, 11, 12, 13, 14, 24, 56, 57, 73, 106

instruction sheet, 76

Interface, 51

Internet, 11, 42, 54, 107

Intranet, 11, 42, 54

Inventory Service Catalogue, 60

ISACA, 2, 25, 36, 111

ISO 9001, 11

IT Operation Management, vii, ix, 82, 90

IT Portofolio, 6

IT Service Continuity Management, 58

IT Service Management, viii, 2, 3, 28, 31, 32, 63

IT Strategic Plan, 6

IT Tactical Plan, 6

Item konfigurasi (CI), 81

ITIL, vi, viii, x, 2, 3, 12, 16, 25, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 39, 48, 51, 53, 57, 59, 63, 64, 70, 75, 78, 80, 82, 83, 89, 111

ITSM, 2, 3, 12, 28, 31, 32, 58

## J

job scheduling, 90

## K

kapasitas, 9, 14, 15, 16, 24, 25, 55, 60, 66, 68, 69, 70, 72, 103

Keamanan informasi, 17

Keamanan sistem, 6

Keberlanjutan sistem, 6

Kehandalan sistem, 6

Ketersediaan sistem, 6

*Knowledge Management*, vi, 74, 81, 99

komunitas praktisi, 100

## L

LAN (*Local Area Network*), 18, 21

Layanan Cloud, 11, 64

Layanan email, 11

layanan IaaS, 64

layanan infrastruktur, 5, 9, 13, 14, 15, 17, 39, 40, 53, 58, 60

Layanan streaming, 11

level operasional, 5, 70, 92

level strategis, 3, 5, 6

level taktis, 3, 4, 5, 6

*life cycle*, 7, 14

## M

*maintenance*, 58, 62

*Major Issues Review*, 87

Manajemen Akses, vii, 88

Manajemen Aset dan Konfigurasi, vi, 78, 79, 81

Manajemen Even, vii, 84, 85, 88

Manajemen Insiden, vii, 85, 86, 87, 88, 89

Manajemen Masalah, vii, 56, 57, 85, 86, 87, 88, 100

manajemen pengetahuan, v, 1, 53, 67, 93

Manajemen Rilis, 77, 78, 79, 80

manajemen risiko, v, 3, 6, 9, 93, 94, 95, 96, 101, 111

*Monitor, Evaluate, and Assess (MEA)*, 26

monitoring, 14, 15, 39, 44, 56, 60, 70, 73, 78, 85, 92, 106, 107

## N

*Network*, 18, 21, 22, 70

## O

*Open Journal System*, 100

*operating level agreement (OLA)*, 62

*Operational Execution*, 5

optimasi layanan, 14, 61

optimasi sistem, 56

Otorisasi, 77

*output*, 1, 45, 46, 49, 50, 68, 73

## P

pemasok, 60, 65, 66, 67, 77, 81, 86

pemodelan, 7

pengolahan data, v

penyimpanan data, v, 46

perencanaan infrastruktur, 5, 6, 17

pertukaran informasi, v

*Plan, Build, Run and Monitor (PBRM)*, 26

*Plan-Do-Check-Act (PDCA)*, 31

*Problem Management*, vii, 39, 82, 87

proses bisnis, 8, 12, 13, 14, 15, 51, 93, 102, 103

Pusat Manajemen Informasi, iv, v, vi, 1, 2, 3, 4, 8, 11, 107

## R

*RACI Matrix*, 96

*Recovery*, 10, 21, 41, 91, 92, 102, 103, 104

*recovery sites*, 90

*Release & Deployment Management*, 74

*Release Closure*, 79

Rencana Induk Teknologi Informasi, v, vi, 3, 4, 9, 40, 111

Rencana Pembangunan Jangka Menengah Nasional, 7  
Rencana Strategis, v, 3  
repositori *online*, 100  
*Request Fulfillment*, vii, 82, 88, 89  
*Risk Assessment*, 101  
*Risk IT*, 2, 26, 28  
*Risk Treatment Plan (RTP)*, 97  
RITI, v, vi, 3, 4, 5, 9, 40, 66  
RPJMN, 7

## S

SAC (*Service Acceptance Criteria*), 60  
sensor, 12  
server, 21, 24, 47, 53, 54, 55, 58, 69, 70, 72, 106  
*Service Asset & Configuration Management*, 74  
*Service Catalogue*, vi, 58, 60  
*Service Catalogue Management*, 58  
*Service Delivery*, 28, 31  
*Service design*, 58  
*service desk*, 51, 53, 73, 81, 82, 83, 85, 87, 90, 91, 100  
*service level agreement*, 62  
*Service Level Management*, vi, viii, 38, 58, 60, 61, 62  
*service operation*, 51, 53, 74, 81, 91  
*service strategy*, 24, 38, 39, 74  
*service transition*, 61, 74  
*Service Validation*, 74  
sharing informasi, 12  
*single point of contact*, 53  
sistem *Backup*, 20  
Sistem *Cluster*, viii, 18, 19

Sistem Gedung Bertingkat, 18  
sistem infrastruktur, 42  
sistem manajemen, v, 3, 9, 30, 32, 67, 93, 94, 96, 108  
sistem *switch*, 18, 21  
SLR (*Service Level Requirement*), 60  
*stakeholder*, 7, 8, 26, 27, 33, 101, 108  
standar operasional prosedur (SOP), 40  
*storage*, 24, 58, 69, 70, 72  
sumber daya TI, 6, 68, 72  
*Supplier Management*, vi, 38, 58, 60, 65, 66  
*system backup*, 104

## T

tata kelola, v, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 24, 25, 26, 27, 28, 31, 32, 36, 40, 43, 51, 53, 57, 83, 93, 95, 110  
*Technical Management*, 82  
teknologi informasi, v, 1, 2, 3, 6, 7, 8, 11, 17, 24, 25, 28, 29, 31  
Teknologi Informasi dan Komunikasi, v, 1  
*testing*, 14, 58, 61, 62, 70, 72, 73, 76, 78  
TIK, 5, 14, 29, 30, 32, 33, 34, 35, 42, 52, 111  
tingkat kepuasan, 6  
*Transition Planning and Support*, 74  
*troubleshooting*, 42

## U

*Underpinning Contracts*, 67

## V

Val IT, 2, 26, 28

## W

WLAN (*Wireless Local Area Network*), 18, 22