TUGAS AKHIR – KS091336

PEMBUATAN INDEKS PENILAIAN KESIAPAN MANAJEMEN KEAMANAN LAYANAN TEKNOLOGI INFORMASI BERBASIS ISO 27000, ITIL V3 DAN COBIT 4.1
(STUDI KASUS : BTSI ITS SURABAYA)

FARROH SAKINAH
NRP 5210 100 060

Supervisor I
Bambang Setiawan, S.Kom, M.T

DEPARTMENT OF INFORMATION SYSTEM
Faculty od of Information Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2014

FINAL PROJECT – KS091336

APPLICATION FOR MAKING INDEX OF READINESS ASSESSMENT OF SECURITY MANAGEMENT OF INFORMATION TECHNOLOGY SERVICES BASED ON ISO 27000, ITIL V3 AND COBIT 4.1 (CASE STUDY: BTSI ITS SURABAYA)

FARROH SAKINAH
NRP 5210 100 060

Supervisor I
Bambang Setiawan, S.Kom, M.T

DEPARTMENT OF INFORMATION SYSTEMS
Faculty of Information Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2014

PEMBUATAN INDEKS PENILAIAN KESIAPAN MANAJEMEN KEAMANAN LAYANAN TEKNOLOGI INFORMASI BERBASIS ISO 27000, ITIL V3 DAN COBIT 4.1
(STUDI KASUS : BTSI ITS SURABAYA)

Nama Mahasiswa	:	Farroh Sakinah
NRP	:	5210100060
Jurusan	:	Sistem Informasi FTIf – ITS
Dosen Pembimbing I	:	Bambang Setiawan, S.Kom, M.T

Abstrak

Pemanfaatan Teknologi Informasi (TI) dalam mendukung terselenggaranya pelayanan yang optimal menjadi kebutuhan utama organisasi saat ini. Akan tetapi, jaminan pengelolaan layanan yang baik dirasa belum maksimal tanpa adanya penggunaan sebuah standar. Penggunaan sebuah standard dirasa belum maksimal terlihat dari cakupan yang disediakannya kurang luas sehingga organisasi merasa perlu untuk menggabungkan beberapa standar dengan harapan standar-standar tersebut dapat saling melengkapi. Pengimplementasian beberapa standar ini dapat dimonitoring pencapaiannya oleh organisasi dengan menggunakan alat ukur penilaian kesiapan. Pembuatan alat ukur penilaian kesiapan pengimplementasian manajemen keamanan layanan dalam tugas akhir ini dimulai dengan melihat control objective dari service delivery and support berdasarkan COBIT 4.1 yang dipetakan kebutuhan pengimplementasiannya dalam operasional manajemen layanan sesuai dengan Service Management di dalam ITIL v3 (Information Technology Infrastructure Library). Selanjutnya kebutuhan manajemen layanan ini diukur tingkat kesiapannya dengan maturity model COBIT 4.1 dan disesuaikan dengan framework ISO 27000 untuk memaksimalkan manajemen keamanan informasi.

Kata Kunci : ***Indeks Penilaian, Keamanan Teknologi Informasi, ISO 27000, COBIT 4.1, ITIL v3, Manajemen Layanan.***.

APPLICATION FOR MAKING INDEX OF READINESS ASSESSMENT OF SECURITY MANAGEMENT OF INFORMATION TECHNOLOGY SERVICES BASED ON ISO 27000, ITIL V3 AND COBIT 4.1 (CASE STUDY: BTSI ITS SURABAYA)

Name	: Farroh Sakinah
NRP	: 5210100060
Department	: Sistem Informasi FTIf – ITS
Supervisor	: Bambang Setiawan, S.Kom, M.T

Abstract

The use of Information Technology in supporting the well being of optimized service become necessary mean for any organization in this era. But, the insurance for a good service management cannot be optimized without the use of any standard. But, the use of a standard is not good enough when its range is not wide enough. Thus, there will be a need to join some standards so that they will be able to complete each others. Implementation of these standards can be monitored with a properness measurement tool. The creation of a measurement tool to score the properness of service security management implementation within this final project is started by finding control objective on service delivery and support in COBIT 4.1 with mapping service management needs according to ITIL v3. Then, these service management needs are measured with maturity model COBIT 4.1 standard and be complied with ISO 27000 framework to maximized Information Security Management.

Key Word : Assessment Index, Information Security, ISO 27000, COBIT 4.1, ITIL v3, Service Management.

Halaman ini sengaja dikosongkan.

PEMBUATAN INDEKS PENILAIAN KESIAPAN MANAJEMEN KEAMANAN LAYANAN TEKNOLOGI INFORMASI BERBASIS ISO 27000, ITIL V3 DAN COBIT 4.1
(STUDI KASUS : BTSI ITS SURABAYA)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:
FARROH SAKINAH
5210 100 060

Surabaya, Juli 2014

KETUA
JURUSAN SISTEM INFORMASI

Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
NIP. 19730219 199802 1 001

PEMBUATAN INDEKS PENILAIAN KESIAPAN MANAJEMEN KEAMANAN LAYANAN TEKNOLOGI INFORMASI BERBASIS ISO 27000, ITIL V3 DAN COBIT 4.1
(STUDI KASUS : BTSI ITS SURABAYA)

TUGAS AKHIR
Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:
FARROH SAKINAH
5210 100 060

Disetujui Tim Penguji: Tanggal Ujian : 25 Juni 2014
Periode Wisuda : September 2014

Bambang Setiawan, S.Kom, M.T **(Pembimbing I)**

Edwin Riksakomara, S.Kom, M.T **(Penguji I)**

Arif Wibisono S.Kom, M.Sc **(Penguji II)**

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa karena atas rahmat dan hidayah-Nya, tugas akhir yang berjudul "**PEMBUATAN INDEKS PENILAIAN KESIAPAN MANAJEMEN KEAMANAN LAYANAN TEKNOLOGI INFORMASI BERBASIS ISO 27000, ITIL V3 DAN COBIT 4.1 (STUDI KASUS : BTSI ITS SURABAYA)**" ini telah selesai.

Tugas akhir ini disusun untuk memenuhi sebagian oesyaratan untuk memperoleh gelar Sarjana Komputer, Fakultas Teknologi Informasi, Insititut Teknologi Sepuluh Nopember Surabaya.

Pada kesempatan kali ini penulis mengucapkan teirma kasih dan penghargaan yang sebesar-besarnya kepada :

1. Ibu dan Ayah tercinta yang telah membimbing, mengajarkan, mendidik dan mengayomi penulis sejak kecil, serta doa-doa dan dukungannya selama ini. Semoga Allah menyayangi keduanya sebagaimana beliau berdua menyayangi penulis yang tanpa akhir.
2. Bapak Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom_selaku ketua jurusan Sistem Informasi ITS.
3. Bapak Bambang Setiawan, S.Kom, M.T selaku pembimbing yang telah membimbing penulis tanpa kenal waktu membatu penulis mempersiapkan tugas akhir ini.
4. Pihak BTSI ITS Surabaya, Pihak manajemen dan segenap tim infrastruktur dan keamanan BTSI yang telah membantu dan membimbing dalam pengerjaan tugas akhir ini.
5. Bapak Bambang Widjanarko selaku laboran E-bisnis Sistem Informasi Jurusan Sistem Informasi yang telah memfasilitasi laboratorium dengan segala keperluan administrasi nya untuk mendukung penyelesaian tugas akhir ini.
6. Rekan-rekan seperjuangan semenjak mahasiswa baru, Aldioctavia Vicka, Ayunda Puspa, Eka Jatiningsih, Farah Dita, Regina Bestrya, Mutia Ratih, M Harindra, Tissa

Rifanti, Adhika Pratomo, Muhammad AB, M. Zainnurromadhoni dan Desy Gitapratama yang telah mendukung dan menyemangati penulis selama mengerjakan tugas akhir. *I love you all*.

7. Tim Fasilitator Patriot dan Tim Pemandu Merah Putih yang telah sangat bersabar mendukung dan menyemangati penulis.
8. Tim Kementrian PSDM BEM ITS Ragam Warna 2013/2014 yang telah mendukung dan menyemangati penulis.
9. Rekan – rekan mahasiswa Sistem Informasi angkatan 2010 yang telah memotivasi dan mendukung dengan semangat angkatan yang luar biasa.

Semoga tugas akhir ini memberikan manfaat terhadap penulis, pihak BTSI ITS Surabaya dan pembaca lainnya, serta dapat memberikan kontribusi pada ilmu pengetahuan dan teknologi informasi dan komunikasi.

Surabaya, Juli 2014

Penulis

DAFTAR ISI

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Halaman ini sengaja dikosongkan.

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

Pada bab ini, akan dijelaskan tentang Latar Belakang Masalah, Perumusan Masalah, Batasan Masalah, Tujuan Tugas Akhir, dan Relevansi atau Manfaat Kegiatan Tugas Akhir.

1.1 Latar Belakang Masalah

Organisasi dan perusahaan saat ini melakukan transformasi dan peningkatan pelayanan dengan pemanfaatan teknologi informasi (TI) dalam proses bisnisnya. Akan tetapi, upaya tersebut dirasa belum maksimal tanpa adanya pengimplementasian manajemen layanan dan keamanan yang terencana dan terarah berdasarkan standar. Penggunaan standar ini bertujuan untuk membantu manajemen mengetahui sejauh mana fungsi dan kinerja layanan mendukung proses bisnis dan strategi organisasi [1].

Penggunaan satu buah standar saat ini pun dirasa kurang luas cakupannya untuk memenuhi seluruh kebutuhan manajemen TI terutama untuk memastikan layanan dapat berjalan dengan baik dan aman [2]. Berdasarkan hal tersebut, maka tugas akhir ini bertujuan menggabungkan beberapa standar pengelolaan dan keamanan layanan dalam sebuah indeks penilaian.

Pembuatan indeks penilaian ini menggunakan standar ISO 27000 terutama ISO 27002 sebagai *information security management*. Kerangka ITIL digunakan untuk konsep dan teknik pengelola serta operasi teknologi informasi (TI) yang berdasarkan *control objective* penyampaian dan dukungan (*delivery and support*) yang baik dan *maturity model* dari COBIT 4.1. Dengan mengkombinasikan keempat standar ini, diharapkan mampu menghasilkan sebuah standar penilaian akan manajemen keamanan layanan Tl [2] untuk membantu organisasi me-*monitoring* dan membuat rencana keberlanjutan pengembangan TI-nya.

1.2 Rumusan Permasalahan

Sesuai latar belakang yang telah dipaparkan di atas, maka permasalahan yang akan diselesaikan dalam tugas akhir ini adalah bagaimana menghasilkan sebuah indeks untuk penilaian kesiapan manajemen keamanan layanan SI/TI pada sebuah organisasi yang sesuai dengan standar COBIT 4.1, ITIL V3 dan ISO 27000 berbasis *Microsoft excel worksheet.*

1.3 Batasan Masalah/Ruang Lingkup

Dari perumusan masalah di atas, batasan tugas akhir ini adalah sebagai berikut :

a. Pembuatan indeks penilaian kesiapan manajemen keamanan layanan SI/TI mengacu pada standar COBIT 4.1 terfokus pada bagian *Delivery and Support*, ISO 27000 terutama ISO 27002 yang dipetakan dengan standar ITIL v3 dan diukur dengan standar dari COBIT 4.1.
b. Pemilihan komponen dari indeks penilaian kesiapan manajemen keamanan layanan SI/TI dilakukan dengan konsep hibridasi.
c. Perancangan indeks penilaian kesiapan manajemen keamanan layanan SI/TI ini difokuskan pada pembuatan standar nilai, form isian nilai dan dashboard berbasis *Microsoft excel worksheet.*
d. Organisasi penelitian pembuatan indeks penilaian kesiapan manajemen layanan SI/TI ini menggunakan Badan Teknologi dan Sistem Informasi (BTSI) ITS Surabaya.

1.4 Tujuan

Tujuan tugas akhir ini adalah untuk menghasilkan indeks penilaian pengimplementasian standar (berupa standar nilai, form isian nilai dan dashboard hasil penilaian kesiapan pengimplementasian ISO 27000, ITIL v3 dan COBIT 4.1) berbasis *Microsoft excel worksheet* untuk memandu manajemen keamanan layanan SI/TI pada sebuah perusahaan/organisasi.

1.5 Manfaat

Manfaat yang dapat diambil dari tugas akhir ini adalah sebagai berikut:

a. Dapat memberikan luaran berupa indeks dan form isian penilaian berbasis *Microsoft excel worksheet*, yang diharapkan dapat membantu organisasi mempersiapkan tata kelola keamanan layanan SI/TI yang sesuai dengan standar ISO 27000, ITIL V3 dan COBIT 4.1.
b. Dapat memberikan luaran berupa sumbangan pemikiran dan sebagai referensi kepada peneliti lain yang melakukan penelitian serupa.

1.6 Sistematika Penulisan

Dalam pengerjaan buku tugas akhir ini, akan dijelaskan menjadi 5 bab dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang menjelaskan latar belakang, tujuan tugas akhir, manfaat tugas akhir dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan istilah-istilah serta dasar teori yang digunakan pada tugas akhir. Informasi tersebut berasal dari buku, jurnal, atau artikel terkait.

BAB III METODOLOGI

Bab ini membahas alur dan tata pengerjaan tugas akhir dari awal hingga selesai. Metodologi tersebut digambarkan pada sebuah *flowchart* dan diberikan penjelasan di tiap tahapannya.

BAB IV PEMBUATAN INDEKS PENILAIAN

Bab ini menjelaskan rancangan desain indeks yang dibuat berdasarkan kebutuhan, yaitu berbasis *Microsoft Excel Worksheet.*

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang dapat diambil dari tugas akhir dan saran untuk kelanjutan pengembangan indeks.

.

BAB II
TINJAUAN PUSTAKA

Terdapat beberapa standar yang digunakan dalam pembuatan tugas akhir ini. Untuk mempermudah pemahaman mengenai konsep dan standar penilaian yang akan digunakan, berikut merupakan penjelasan literatur yang digunakan.

2.1 Tata Kelola Teknologi Informasi

Tata Kelola Teknologi Informasi didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis dapat tercapai melalui penambahan nilai sekaligus terkait dengan pengelolaan proses TI. Tidak hanya pengelolaan proses, tetapi juga memastikan bahwa proses tersebut telah dipenuhi oleh sumber daya TI yang memberikan dukungan secara optimal terhadap pemenuhan tujuan bisnis [3].

Committee of Sponsoring Organizations of the Treadway Commission, atau disingkat COSO, telah menyusun suatu definisi umum untuk pengendalian, standar, dan kriteria internal yang dapat digunakan perusahaan menilai sistem pengendalian mereka. Sedangkan, di dunia informatika dan informasi, dibangunlah sebuah *framework* untuk mengontrol kegiatan internal dalam pengelolaannya bernama *Control Objective for Information and related Technology*, disingkat COBIT yang di turunkan dari COSO.

Dalam praktik penggunaannya di dalam *IT Operation*, terdapat beberapa tiang penyangga atau rujukan agar terciptanya bangunan TI yang kokoh yaitu, *Service Management*, *App. Development (SDLC)*, *IT Security*, *Project Management*, *IT Planning* dan *Quality System* [3]. Adapun fokus utama pengerjaan tugas akhir ini adalah tata kelola teknologi informasi pada *IT Security.*

2.2 COBIT 4.1

Control Objectives for Information and related Technology (COBIT) adalah sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, manajemen dan pengguna *(user)* untuk menjembatani *gap* antara risiko bisnis, melaksanakan kontrol serta permasalahan-permasalahan teknis [4].

Gambar 2.1 IT Governance dalam COBIT 4.1

IT governance merupakan satu kesatuan dengan *enterprise governance* guna meningkatkan efektivitas dan efisiensi proses bisnis perusahaan yang saling berhubungan. *IT governance* menyediakan struktur yang menghubungkan proses TI, sumber daya TI dan informasi bagi pembuatan strategi dengan tujuan organisasi.

Tujuan dari pengimplementasian COBIT terbagi dalam tiga tingkatan [3], yaitu :

1. Tujuan dan langkah pengukuran TI terdefinisikan sesuai dengan harapan bisnis terhadap TI.
2. Tujuan dan langkah pengukuran TI yang ada telah mendefinisikan bagaimana proses TI menyampaikan dan mendukung objektif TI.
3. Menetapkan setiap tujuan dari aktivitas yang harus terjadi di dalam proses untuk mncapai performa yang diharapkan lengkap dengan langkah pengukurannya.

Untuk memenuhi kebutuhan bisnis, sebuah informasi harus memenuhi beberapa kriteria kontrol yang mengacu pada COBIT sebagai persyaratan bisnis untuk informasi. Berdasarkan kualitas yang lebih luas, persyaratan keamanan, terdapat tujuh kriteria informasi, yaitu :

1. Efektivitas (*Effectiveness*), berkaitan dengan informasi yang relevan dan berkaitan dengan proses bisnis serta disampaikan pada waktu yang tepat, benar, konsisten dan tepat guna.
2. Efisiensi (*Efficiency*), penyediaan informasi melalui proses yang optimal (paling produktif dan ekonomis) dalam penggunaan sumber dayanya.
3. Kerahasiaan (*Confidentiality*), berfokus pada proses menjaga informasi sensitive dari akses yang tidak sah.
4. Integritas (*Integrity*), berkaitan dengan keakuratan dan kelengkapan informasi serta validitas informasi yang sesuai dengan nilai-nilai dan harapan bisnis.
5. Ketersediaan (*Availability*), berkaitan dengan informasi tetap tersedia ketika diperlukan oleh proses bisnis saat ini dan di masa depan. Hal ini juga menyangkut memastikan tersedianya sumber daya pengamanan yang diperlukan.
6. Pemenuhan persyaratan (*Compliance*), proses penyediaan informasi yang ada telah mematuhi undang-undang, peraturan dan pengaturan kontrak yang telah disetujui dalam

proses bisnis baik kriteria eksternal maupun kebijakan internal bisnis.

7. Kehandalan (*Reliability*), berkaitan dengan penyediaan informasi yang tepat bagi manajemen untuk mengoperasikan dan menjalankan tanggung jawab tata kelolanya.

Untuk mengatur TI yang efektif, penting bagi organisasi menghargai setiap proses dan risiko dalam TI yang dikelola. Biasanya organisasi membagi proses tersebut dalam proses bidang merencanakan, membangun, menjalankan dan memonitor.

Dalam kerangka COBIT, keempat *domain/* proses bidang tersebut adalah :

1. *Plan and Organise* (PO) - Menyediakan arahan perencanaan dan pengorganisasian untuk solusi proses penyampaian (AI) dan pelayanan (DS)
2. *Acquire and Implement* (AI) - Menyediakan solusi bagi organisasi melewati fase perubahan arahan menjadi layanan
3. *Deliver and Support* (DS) - Solusi yag telah dibuat sebelumnya, digunakan oleh *end user*.
4. *Monitor and Evaluate* (ME) – Memonitoring dan mengevaluasi semua proses untuk memastikan bahwa seluruh arahan telah diikuti.

Dalam pengerjaan tugas akhir ini, penulis berfokus pada *domain Delivery and Support* (DS). Hal ini berdasarkan pada studi kasus pelaksanaan tugas akhir yaitu organisasi yang bergerak di bidang penyediaan layanan publik, dimana ruang lingkup TI dalam proses bisnisnya lebih menekankan dalam proses menyampaikan dan mendukung layanan.

2.2.1 *Domain Delivery and Support* dalam COBIT 4.1

Domain ini berkaitan dengan pengiriman dari layanan yang terjadi dan yang dibutuhkan, meliputi penyampaian layanan, pengelolaan keamanan secara kontinu, penyediaan dukungan layanan bagi pengguna, serta manajemen data dan fasilitas operasional.

Domain ini harus mampu menjawab :

1. Apakah layanan TI yang disampaikan sesuai dengan prioritas bisnis?
2. Apakah biaya TI yang dianggarkan organisasi telah digunakan dengan optimal?
3. Apakah tenaga kerja dapat menggunakan sistem TI secara produktif dan aman?
4. Apakah kerahasiaan, integritas dan ketersediaan informasi yang aman telah terpenuhi?

2.2.1.1 **DS1** ***Define and Manage Service Levels***

DS1.1 *Service Level Management Framework*

Menentukan kerangka kerja yang menyediakan proses manajemen formal tingkatan layanan antara pelanggan dengan penyedia layanan. Kerangka ini menjaga keselarasan kebutuhan bisnis dengan prioritas dan fasilitias yang dipahami oleh pelanggan dan penyedia layanan.

Kerangka *Service Level Management* mencangkup proses menciptakanan persyaratan layanan, definisi layanan, OLAs dan sumber pendanaan. Kerangka ini juga mendefinisikan struktur organisisasi untuk menentukan manajemen tingkat layanan yang meliputi peran, tugas dan tanggung jawab pelanggan dan penyedia layanan internal dan eksternal.

DS1.2 *Definition of Service*

Dasaran untuk mendefinisikan layanan TI sesuai karakteristik layanan dan kebutuhan bisnis. Proses ini harus memastikan bahwa layanan diatur dan disimpan secara terpusat melalui pendekatan *Service Catalogue Portfolio*.

DS1.3 *Service Level Agreement*

Proses untuk menentukan dan menyetujui SLA bagi seluruh layanan TI yang kritis berdasarkan kebutuhan pelanggan dan kemampuan TI.

Proses ini harus mencakup komitmen pelanggan; persyaratan dukungan layanan; metrik kuantitatif dan kualitatif

untuk mengukur layanan yang ditandatangani oleh para *stakeholder*; pendanaan dan pengaturan komersial, jika ada; dan pembagian peran dan tanggung jawab, termasuk pengawasan dari SLA.

Ketersediaan, keandalan, kinerja, kapasitas, tingkat dukungan, perencanaan keberlanjutan layanan, keamanan dan permintaan untuk menyelesaikan kendala layanan menjadi faktor pertimbangan dalam pembuatan *Service Level Agreement* (SLA).

DS1.4 *Operating Level Agreement*

Proses untuk menentukan OLA yang digunakan untuk menjelaskan bagaimana layanan akan dikirimkan secara teknis untuk mendukung SLA secara optimal.

DS1.5 *Monitoring and Reporting of Service Level Achievement*

Proses memantau kinerja berdasarkan beberapa kriteria tingkat layanan tertentu. Laporan pencapaian tingkat pelayanan harus disediakan dalam format yang mudah dimengerti oleh *stakeholder*.

Hasil pemantauan dianalisis dan ditindaklanjuti untuk mengidentifikasi *tren* negatif dan positif, baik penilaian layanan secara individu maupun layanan secara keseluruhan.

DS1.6 *Review of Service Level Agreement and Contracts*

Secara teratur SLA dan kontrak dasar (*Underpinning Contracts*) ditinjau oleh penyedia layanan internal dan eksternal untuk memastikan bahwa mereka telah menyampaikan layanan secara efektif, *up to date* dan setiap perubahan dalam persyaratan telah diperhitungkan.

2.2.1.2 DS2 *Manage Performance and Capacity*

DS2.1 *Identification of All Supplier Relationships*

Identifikasi untuk semua pemasok layanan, dan mengkategorikan mereka sesuai dengan jenis, signifikansi dan tingkat kekritisannya. Hal ini dilakukan untuk membangun hubungan dalam penyampaian teknis dan pembagian peran,

pembagian tanggung jawab, penjelasan tujuan, luaran yang diharapkan, dan dokumen resmi yang menunjukkan adanya persetujuan dari masing-masing wakil pemasok.

DS2.2 *Supplier Relationship Management*

Proses formal untuk memanajemen hubungan dengan setiap pemasok. Penanggung jawab hubungan harus bekerjasama dengan mempertimbangkan isu-isu dari sisi pelanggan dan pemasok serta memastikan hubungan yang terjalin berkualitas berdasarkan kepercayaan dan transparansi (misalnya, melalui SLA).

DS2.3 *Supplier Risk Management*

Mengidentifikasi dan mengurangi risiko yang berkaitan dengan kinerja pemasok dalam menyampaikan layanan yang efektif dengan cara yang aman dan efisien secara terus menerus. Proses ini harus memastikan bahwa kontrak sesuai dengan standar bisnis secara *universal* dan memenuhi persyaratan hukum dan peraturan.

Manajemen risiko sendiri harus lebih mempertimbangkan perjanjian *non-disclosure* (NDAs), *escrow contracts*, *continued supplier viability*, kesesuaian dengan persyaratan keamanan, daftar pemasok alternatif, hukuman dan penghargaan, dll dalam pembuatannya.

DS2.4 *Supplier Performance Monitoring*

Menetapkan proses untuk memantau layanan yang diberikan oleh supplier guna memastikan bahwa pemasok telah memenuhi kebutuhan bisnis saat ini dan terus mematuhi perjanjian kontrak dan SLA, dan kinerja yang diberikan kompetitif dengan pemasok alternatif.

2.2.1.3 DS3-*Manage Performance and Capacity*

DS3.1 *Performance and Capacity Planning*

Proses untuk menetapkan perencanaan peninjauan kinerja dan kapasitas sumber daya TI guna memastikan bahwa kapasitas

biaya yang dikeluarkan dan kinerja yang tersedia untuk melakukan proses sesuai sebagaimana yang telah ditentukan dalam SLA.

Perencanaan kapasitas dan kinerja harus menggunakan teknik pemodelan yang tepat untuk menghasilkan model terbaik yang telah memperkirakan kinerja, kapasitas dan *throughput* dari sumber daya TI saat ini.

DS3.2 *Current Performance and Capacity*

Proses menilai kinerja dan kapasitas sumber daya TI saat ini untuk menentukan apakah kapasitas dan kinerja yang ada cukup untuk memberikan hasil yang disepakati di beberapa tingkat layanan.

DS3.3 *Future Performance and Capacity*

Proses melakukan peramalan kinerja dan kapasitas sumber daya TI secara berkala untuk meminimalkan risiko kemungkinan gangguan layanan karena kapasitas yang tidak memadai atau penurunan kinerja, dan mengidentifikasi kelebihan kapasitas untuk kemungkinan pemindahan pengalokasian, Mengidentifikasi tren beban kerja dan menentukan perkiraan yang tepat sebagai masukan untuk perencanaan kinerja dan kapasitas selanjutnya.

DS3.4 *IT Resources Availability*

Proses menyediakan kapasitas dan kualitas kinerja yang diperlukan, memperhitungkan aspek seperti beban kerja normal, persyaratan penyimpanan dan *lifecycle* sumber daya TI.

Ketentuan seperti membuat prioritas tugas, mekanisme toleransi kesalahan dan praktik alokasi sumber daya harus disusun. Manajemen harus memastikan bahwa rencana berkelanjutan telah sesuai dengan rencana ketersediaan, kapasitas dan kinerja sumber daya individu TI.

DS3.5 *Monitoring and Reporting*

Proses pemantauan kinerja dan kapasitas sumber daya TI yang berkelanjutan. Data yang dikumpulkan harus memiliki dua tujuan:

1. Untuk mempertahankan dan menyempurnakan kinerja TI saat ini dan mengatasi masalah seperti ketahanan, *continuity*, proyeksi beban kerja, rencana penyimpanan, dan akuisisi sumber daya.
2. Untuk melaporkan ketersediaan layanan yang telah disampaikan dalam proses bisnis, seperti yang dipersyaratkan dalam SLA bersamaan dengan semua laporan dan rekomendasi untuk tindakan korektif.

2.2.1.4 **DS4-*Ensure Continuous Service***

DS4.1 *IT Continuity Framework*

Proses mengembangkan kerangka dasar yang telah dimiliki sebelumnya untuk menjamin kelangsungan TI dalam mendukung manajemen bisnis organisasi menggunakan proses yang konsisten. Tujuan dari kerangka ini harus membantu dalam menentukan tingkat ketahanan yang diperlukan infrastruktur dan untuk mendorong pengembangan pemulihan bencana dan rencana keberlanjutan TI.

Kerangka ini harus membahas struktur organisasi dalam melaksanakan manajemen kontinuitas, yang meliputi peran, tugas dan tanggung jawab penyedia layanan internal dan eksternal, dan proses perencanaan yang membuat aturan dan struktur untuk mendokumentasikan, pengujian dan melaksanakan pemulihan bencana dan rencana keberlanjutan TI.

Rencana ini juga membahas beberapa *item* penting, seperti identifikasi sumber daya utama, mencatat kunci dependensi, pemantauan dan pelaporan ketersediaan sumber daya kritis, alternatif pengolahan, dan prinsip-prinsip *backup* dan *recovery.*

DS4.2 *IT Continuity Plans*

Proses mengembangkan *IT Continuity Plan* berdasarkan kerangka yang dirancang untuk mengurangi dampak dari gangguan besar pada fungsi dan proses bisnis utama.

Perencanaan harus didasarkan pada pemahaman dampak risiko terhadap proses bisnis utama, dan tingkat pemenuhan persyaratan untuk menjamin ketahanan, alternatif pengolahan dan kemampuan pemulihan dari semua layanan kritis TI.

Proses perencanaan ini juga harus mencakup penyediaan pedoman penggunaan, pembagian peran dan tanggung jawab, pembuatan prosedur, perencanaan proses komunikasi, dan pendekatan dalam proses pengujian *IT Continuity Plan.*

DS4.3 *Critical IT Resources*

Proses menfokuskan perhatian pada *item* tertentu yang dianggap paling penting dalam rencana berkesinambungan TI untuk membangun ketahanan dan menetapkan prioritas dalam situasi pemulihan.

Proses ini juga harus mampu merencanakan langkah untuk menghindari pemulihan gangguan pada *item* yang kurang-kritis dan memastikan respon dan pemulihan sesuai dengan prioritas kebutuhan bisnis, dengan memastikan bahwa biaya yang dialokasikan masih dalam tingkatan yang dapat diterima dan memenuhi persyaratan peraturan dan kontrak.

DS4.4 *Maintenance of the IT Continuity Plan*

Proses yang mendorong manajemen TI untuk mendefinisikan dan melaksanakan prosedur perubahan kontrol untuk memastikan bahwa rencana berkesinambungan TI terus *up to date* dan tetap mencerminkan kebutuhan bisnis yang sebenarnya.

DS4.5 *Testing of the IT Continuity Plan*

Pengujian *IT Continuty Plan* secara teratur untuk memastikan bahwa sistem TI dapat pulih secara efektif, setiap kekurangan dapat ditangani dan rencana tetap relevan.

Hal ini memerlukan persiapan yang cermat, dokumentasi, dan pelaporan hasil pengetesan yang baik. Berdasarkan hasil pengetesan, dibuatlah rencana pelaksanaan aksi sesuai dengan hasil yang didapatkan.

DS4.6 *IT Continuity Plan Training*

Menyediakan kepada semua pihak yang berkepentingan/ memerlukan sesi pelatihan rutin tentang prosedur, peran dan tanggung jawab dalam menghadapi kasus insiden atau bencana.

Pelaksanaan pelatihan berdasarkan dengan strategi dari masing-masing organisasi.

DS4.7 *Distribution of the IT Continuity Plan*

Proses menentukan strategi distribusi pelaksanaan seluruh *item* yang ada di dalam *IT Continuity Plan* yang dikelola organisasi.

Penentuan strategi ini dilakukan untuk memastikan bahwa rencana bejalan dengan benar dan aman, layanan hanya tersedia bagi pihak yang memiliki ijin, pihak yang berkepentingan, beserta waktu dan lokasi yang ditentukan.

DS4.8 *IT Services Recovery and Resumption*

Pembuatan rencana tindakan yang akan diambil dalam periode tertentu ketika TI sudah mulai pulih dalam *IT Continuity Plan*. Proses ini termasuk menentukan aktivasi penyediaan cadangan, inisiasi alternatif pengolahan, proses komunikasi dengan pelanggan dan *stakeholder* lengkap dengan prosedur pengembaliannya.

Proses ini diharapkan mampu memastikan bahwa bisnis memahami proses pemulihan TI dan menyediakan investasi teknologi yang diperlukan untuk mendukung pemulihan bisnis.

DS4.9 *Offsite Backup Storage*

Penyimpanan media *backup offsite* untuk semua dokumentasi dan sumber daya TI kritis lainnya yang diperlukan untuk pemulihan dan kesinambungan rencana TI.

Proses ini harus telah menentukan isi informasi apa saja yang dimasukkan dalam penyimpanan informasi cadangan bekerjasama dengan pemilik proses bisnis dan personil TI.

Pihak pengelola fasilitas *backup offsite* harus mampu merespon kebijakan klasifikasi data dan praktek penyimpanan media organisasi. Manajemen TI sendiri harus memastikan bahwa pengaturan *backup offsite* dinilai secara berkala, setidaknya setiap tahun, untuk konten, perlindungan lingkungan dan keamanan, kompatibilitas *hardware* dan *software*.

DS4.10 *Post-resumption Review*

Proses pengecekan apakah manajemen TI telah menetepkan prosedur penilaian ketersediaan dalam perencanaan yang mencukupi dan sesuai dengan kebutuhan proses bisnis saat ini.

2.2.1.5 DS5-Ensure Systems Security

DS5.1 *Management of IT Security*

Proses pengelolaan keamanan TI sesuai tingkatan organisasi, mulai dari tingkat tertinggi agar manajemen tindakan pengelolaan keamanan sejalan dengan kebutuhan bisnis.

DS5.2 *Security Plan*

Proses menerjemahkan risiko bisnis dan persyaratan kepatuhan dalam rencana keamanan TI secara keseluruhan dengan mempertimbangkan infrastruktur TI dan budaya keamanan organisasi.

Perencanaan ini juga harus memastikan bahwa rencana diimplementasikan dalam kebijakan dan prosedur keamanan bersama dengan investasi yang tepat di bidang jasa, personil, perangkat lunak dan perangkat keras. Mengkomunikasikan

kebijakan dan prosedur keamanan kepada seluruh *stakeholder* dan pengguna.

DS5.3 *Identity Management*

Proses memastikan bahwa semua pengguna (internal, eksternal dan sementara) dan aktivitas mereka pada sistem TI (aplikasi bisnis, lingkungan TI, sistem operasi, pengembangan dan pemeliharaan) mendapat identifikasi (ID) unik.

Proses pengaktifan identitas pengguna melalui mekanisme otentikasi yang mampu mengkonfirmasikan hak akses pengguna ke sistem dan data sesuai dengan kebutuhan bisnis yang didefinisikan dan didokumentasikan dengan persyaratan kerja yang melekat pada identitas pengguna.

DS5.4 *User Account Management*

Proses permintaan, pengembangan, penutupan, penanggunahan, dan modifikasi *account* pengguna dan hak pengguna terkait dalam sebuah prosedur manajemen akun pengguna.

Proses ini menyertakan prosedur persetujuan bahwa manajemen berhak menguraikan data atau sistem yang diberikan hak akses. Prosedur ini harus berlaku untuk semua pengguna, termasuk administrator (pengguna khusus) dan pengguna internal dan eksternal, untuk keadaan normal maupun kasus darurat.

Hak dan kewajiban relatif terhadap akses dan informasi ke dalam sistem perusahaan harus diatur dalam kontrak untuk semua jenis pengguna. Selain itu, pihak manajemen wajib melakukan tinjauan manajemen rutin dari semua akun terkait.

DS5.5 *Security Testing, Surveillance and Monitoring*

Proses pengujian dan *monitoring* pelaksanaan keamanan TI secara proaktif. Keamanan TI harus dire-akreditasi pada waktu yang tepat untuk memastikan bahwa dasar keamanan informasi perusahaan yang disetujui tetao dipertahankan.

Proses pemantauan *logging* memungkinkan pencegahan dini dan/atau deteksi dan pelaporan yang tepat waktu pada kejadian berikutnya dan/atau kegiatan yang tidak normal yang mungkin perlu ditangani.

DS5.6 *Security Incident Definition*

Proses mendefinisikan dan mengkomunikasikan karakteristik insiden keamanan potensial dengan jelas sehingga mereka dapat diklasifikasikan dan dirawat oleh proses pengelolaan insiden dan *problem* dengan baik.

DS5.7 *Protection of Security Technology*

Memastikan teknologi yang berhubungan dengan keamanan, tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi keamanan yang tidak perlu.

DS5.8 *Chryptographic Key Management*

Menentukan kebijakan dan prosedur yang ada dalam mengatur generasi, perubahan, pencabutan, perusakan, distribusi, sertifikasi, penyimpanan, penggunaan dan pengarsipan kunci kriptografi untuk menjamin perlindungan terhadap modifikasi dan pengungkapan informasi yang tidak sah.

DS5.9 *Malicious Software Prevention, Detection and Correction*
Network Security

Proses pencegahan, deteksi dan langkah-langkah perbaikan di tempat (terutama *up-to-date patch* keamanan dan pengendalian virus) di seluruh organisasi untuk melindungi sistem informasi dan teknologi dari *malware* (misalnya, virus, *worm, spyware, spam*).

DS5.10 *Network Security*

Mengunakan teknik keamanan dan prosedur manajemen terkait (misalnya, *firewall*, penyediaan kelengkapan peralatan keamanan, segmentasi jaringan, deteksi intrusi) untuk

mengotorisasi akses dan kontrol informasi mengalir dari dan ke dalam jaringan.

DS5.11 *Exchange of Sensitive Data*

Memastikan proses pertukaran data transaksi sensitif hanya melalui jalur jaringan yang dipercaya atau media yang terkontrol untuk menyediakan keaslian konten, bukti pengiriman, dan bukti penerimaan.

2.2.1.6 DS6-Identify and Allocate Costs

DS6.1 *Definition of Services*

Proses identifikasi semua biaya TI, dan pemetaannya dalam layanan TI guna mendukung model biaya yang transparan. Layanan TI harus dikaitkan dengan proses bisnis sehingga bisnis dapat mengidentifikasi tingkat penagihan biaya layanan terkait.

DS6.2 *IT Accounting*

Proses menemukan dan mengalokasikan biaya yang sebenarnya sesuai dengan pemodelan biaya yang dimiliki organisasi. *Varians* antara perkiraan dan biaya yang sebenarnya harus dianalisis dan dilaporkan, sesuai dengan sistem pengukuran keuangan perusahaan.

DS6.3 *Cost Modeling and Charging*

Membangun dan menggunakan pemodelan biaya TI berdasarkan definisi layanan yang mendukung perhitungan biaya masing-masing layanan. Pemodelan biaya TI ini harus memastikan bahwa penyediaan layanan dapat diidentifikasi, diukur dan diprediksi oleh pengguna untuk mendorong penggunaan sumber daya secara optimal.

DS6.4 *Cost Model Maintenance*

Secara teratur organisasi meninjau dan menetapkan patokan kelayakan model biaya untuk mempertahankan relevansi dan kesesuaiannya dengan kegiatan bisnis dan TI yang berkembang.

2.2.1.7 DS7-Educate and Train Users

DS7.1 *Identification of Education and Training Needs*

Menetapkan dan secara teratur memperbarui kurikulum untuk setiap kelompok sasaran karyawan dengan mempertimbangkan:

1. kebutuhan bisnis saat ini dan masa depan sesuai dengan strategi organisasi
2. Penilaian informasi sebagai aset
3. Nilai-nilai organisasi (nilai-nilai etika, kontrol dan keamanan budaya, dll)
4. Implementasi infrastruktur TI dan perangkat lunak baru (yaitu paket, aplikasi)
5. Keterampilan saat ini dan masa depan, profil kompetensi, dan sertifikasi dan / atau reakreditasi yang diperlukan
6. Metode Pengiriman (misalnya, kelas, berbasis web atau langsung), ukuran kelompok sasaran, aksesibilitas dan waktu pelaksanaan pelatihan.

DS7.2 *Delivery of Training and Education*

Berdasarkan kebutuhan pendidikan dan pelatihan yang diidentifikasi, dilaksanakan pelatihan terhadap sekelompok sasaran dan anggotanya dengan mekanisme pengiriman yang efisien dari sisi guru, pelatih, dan mentor.

Proses ini harus mampu menunjuk pelatih dan mengatur sesi pelatihan tepat waktu, pendataan pendaftaran (termasuk persyaratan), kehadiran dan evaluasi kinerja sesi latihan.

DS7.3 *Evaluation of Training Received*

Evaluasi pelatihan dan isi pelatihan yang telah selesai dilaksanakan untuk relevansi, kualitas, efektivitas, retensi pengetahuan, biaya dan nilai.

Hasil evaluasi ini harus dijadikan sebagai masukan untuk mendefinisikan kurikulum dan metode pengiriman sesi pelatihan selanjutnya.

2.2.1.8 DS8-Manage Service Desk and Incidents

DS8.1 *Service Desk*

Menetapkan fungsi *service desk*, yang merupakan perantara antarmuka pengguna dengan TI, untuk melakukan pendaftaran, berkomunikasi, pengiriman dan menganalisa semua panggilan, melaporkan insiden, memenuhi permintaan layanan dan memberikan tuntutan informasi.

Organisasi harus menyediakan proses monitoring dan eskalasi berdasarkan tingkat pelayanan yang disepakati sesuai SLA yang memungkinkan klasifikasi dan prioritas dari setiap masalah yang dilaporkan sebagai insiden, permintaan layanan atau permintaan informasi. Mengukur kepuasan pengguna akhir dengan kualitas *sevice desk* dan layanan TI.

DS8.2 *Registration of Customer Queries*

Menetapkan fungsi dan sistem untuk mengizinkan penebangan dan pelacakan panggilan, insiden, permintaan layanan dan kebutuhan informasi. Proses ini bekerja sama dengan banyak proses, seperti manajemen insiden, manajemen masalah, manajemen perubahan, manajemen kapasitas dan manajemen ketersediaan.

Insiden harus diklasifikasikan menurut prioritas bisnis dan layanan yang diteruskan ke tim manajemen masalah (*problem management*) yang tepat. Bila diperlukan, organisasi harus menyimpan informasi tentang status permintaan pelanggan dalam jangka waktu tertentu.

DS8.3 *Incident Escalation*

Menetapkan prosedur untuk *service desk* sehingga insiden yang dapat diselesaikan secara cepat dan tepat meningkat sesuai dengan batasan yang telah ditentukan dalam SLA. Proses ini diharapkan mampu memastikan bahwa kepemilikan insiden dan *incident lifecycle* yang dilaporkan ke *service desk* berbasis pada pemenuhan kebutuhan pengguna.

DS8.4 *Insident Closure*

Menetapkan prosedur untuk pemantauan penetapan waktu yang tepat melakukan *clearance* permintaan pelanggan. Saat kejadian telah diselesaikan, pastikan bahwa *service desk* telah mencatat langkah-langkah resolusi, dan memastikan setiap tindakan yang diambil telah disetujui oleh pelanggan.

Proses ini juga berkewajiban untuk mencatat dan melaporkan insiden yang belum terselesaikan (kesalahan yang diketahui) untuk memberikan informasi kepada manajemen masalah yang tepat.

DS8.5 *Reporting and Trend Analysis*

Proses pelaporan kegiatan oleh *service desk* memungkinkan manajemen untuk mengukur kinerja pelayanan, waktu respon layanan dan mengidentifikasi tren atau masalah yang terjadi berulang, sehingga kualitas layanan dapat terus ditingkatkan.

2.2.1.9 DS9-Manage the Configuration

DS9.1 *Configuration Repository and Baseline*

Menetapkan alat pendukung dan sebuah repositori terpusat untuk menampung semua informasi yang relevan tentang *item* konfigurasi. Proses ini termasuk prose memantau dan mencatat semua aset dan perubahan aset. Menjaga dasar *item* konfigurasi untuk setiap sistem dan pelayanan sebagai pos pemeriksaan kembali setelah perubahan.

DS9.2 *Identification and Maintenance of Configuration Items*

Menetapkan prosedur konfigurasi untuk mendukung manajemen dan perubahan ke dalam repositori konfigurasi. Mengintegrasikan prosedur ini dengan prosedur manajemen perubahan, manajemen insiden dan manajemen masalah.

DS9.3 *Configuration Integrity Review*

Secara berkala meninjau data konfigurasi untuk memverifikasi dan mengkonfirmasi integritas dari konfigurasi

saat ini dan sebelumnya. Secara berkala meninjau perangkat lunak yang diinstal terhadap kebijakan penggunaan perangkat lunak untuk mengidentifikasi perangkat lunak pribadi atau kemungkinan perangkat lunak tidak berlisensi atau contoh perangkat lunak yang telah melebihi perjanjian lisensi saat ini. Laporan dari proses ini akan memberikan masukan untuk tindak memperbaiki kesalahan dan penyimpangan yang ditemukan.

2.2.1.10 DS10-Manage Problem

DS10.1 *Identification and Classification of Problems*

Melaksanakan proses untuk melaporkan dan mengklasifikasikan masalah yang telah diidentifikasi sebagai bagian dari manajemen insiden.

Langkah-langkah yang terlibat dalam klasifikasi masalah serupa dengan langkah-langkah dalam mengklasifikasikan insiden; manajemen menentukan kategori, dampak, urgensi dan prioritas.

Kategorisasi masalah sesuai dengan grup terkait atau *domain* (misalnya, perangkat keras, perangkat lunak, perangkat lunak pendukung). Pengelompokan ini cocok dengan tanggung jawab organisasi yang berbasis pada pemenuhan kebutuhan pelanggan.

DS10.2 *Problem Tracking and Resolution*

Proses untuk memastikan bahwa sistem manajemen masalah menyediakan fasilitas *audit trail* yang memadai untuk memungkinkan pelacakan, menganalisis dan menentukan penyebab akar dari semua masalah yang dilaporkan dengan mempertimbangkan:

1. Semua item konfigurasi yang terkait
2. Permasalahan dan insiden
3. kesalahan yang disebut dan diduga
4. Pelacakan tren masalah.

Mengidentifikasi dan mencari solusi berkelanjutan untuk menangani akar penyebab, meningkatkan permintaan perubahan melalui proses manajemen perubahan yang ditetapkan.

Selama proses penyelesaian, manajemen masalah (*problem management*) harus memperoleh laporan berkala dari manajemen perubahan sesuai kemajuan dalam menyelesaikan masalah dan kesalahan yang ditemukan.

DS10.3 *Problem Closure*

Menyediakan prosedur untuk menutup catatan masalah baik setelah konfirmasi penghapusan sukses dari kesalahan yang diketahui atau setelah kesepakatan dengan bisnis tentang bagaimana alternatif menangani masalah tersebut.

DS10.4 *Integration of Configuration, Incident and Problem Management*

Mengintegrasikan proses yang terkait konfigurasi, insiden dan manajemen masalah untuk memastikan terlaksananya manajemen yang efektif dan perbaikan masalah dapat dilakukan.

2.2.1.11 DS11-Manage Data

DS11.1 *Business Requirements for Data Management*

Proses untuk memastikan semua data yang digunakan untuk pemrosesan diterima dan diproses secara lengkap, akurat dan tepat waktu, dan semua *output* disampaikan sesuai dengan kebutuhan bisnis, dukungan melakukan *restart* dan kebutuhan pengolahan.

DS11.2 *Storage and Retention Arrangements*

Menentukan dan menerapkan prosedur untuk penyimpanan data yang efektif dan efisien, melakukan retensi dan pengarsipan untuk memenuhi tujuan bisnis, kebijakan keamanan organisasi dan persyaratan peraturan.

DS11.3 *Media Library Management System Disposal*

Menentukan dan menerapkan prosedur untuk menjaga inventarisasi media yang tersimpan dan diarsipkan untuk memastikan kegunaan dan integritasnya.

DS11.4 *Disposal*

Menentukan dan menerapkan prosedur untuk memastikan bahwa kebutuhan bisnis akan perlindungan data sensitif dan perangkat lunak terpenuhi ketika data dan perangkat keras akan dibuang, dimusnahkan atau di *transfer*.

DS11.5 *Backup and Restoration*

Menentukan dan menerapkan prosedur untuk *backup* dan pemulihan sistem, aplikasi, data dan dokumentasi sesuai dengan kebutuhan bisnis dan rencana berkelanjutan organisasi.

DS11.6*Security Requirements for Data Management*

Mendefinisikan dan menerapkan kebijakan dan prosedur untuk mengidentifikasi dan menerapkan persyaratan keamanan yang berlaku untuk melaksanakan proses penerimaan, pengolahan, penyimpanan *output data* untuk memenuhi tujuan bisnis, kebijakan keamanan organisasi dan persyaratan peraturan.

2.2.1.12 DS12-Manage the Physical Environment

DS12.1 *Site Selection and Layout*

Mentukan dan memilih situs penempatan fisik bagi peralatan TI untuk mendukung strategi teknologi terkait dengan strategi bisnis.

Pemilihan dan desain tata letak situs harus memperhitungkan risiko yang terkait dengan bencana alam dan kemungkinan pengerusakan oleh perbuatan manusia, disisi lain juga harus mempertimbangkan hukum dan peraturan, seperti peraturan kesehatan dan keselamatan kerja.

DS12.2 *Physical Security Measures*

Menentukan dan menerapkan langkah-langkah keamanan fisik sesuai dengan kebutuhan bisnis untuk mengamankan lokasi dan aset fisik.

Langkah-langkah keamanan fisik harus mampu secara efektif mencegah, mendeteksi dan mengurangi risiko yang berkaitan dengan pencurian, suhu, api, asap, air, getaran, teror, *vandalisme*, listrik padam, bahan kimia atau bahan peledak.

DS12.3 *Physical Access*

Menentukan dan menerapkan prosedur memberikan, batas dan mencabut akses ke lokasi, bangunan dan daerah sesuai dengan kebutuhan bisnis, termasuk dalam keadaan darurat, akses ke tempat, atau bangunan dan daerah harus mendapat persetujuan yang disahkan, dicatat dan dimonitor.

Aturan ini harus berlaku untuk semua orang yang memasuki tempat, termasuk staf, staf temporer, klien, *vendor*, pengunjung atau pihak ketiga lainnya.

DS12.4 *Protection Against Environmental Factors*

Mendesain dan menerapkan langkah-langkah untuk perlindungan terhadap faktor lingkungan baik dengan meng-*install* peralatan khusus dan perangkat untuk me-*monitoring* dan mengontrol lingkungan.

DS12.5 *Physical Facilities Management*

Pengelolaan fasilitas, termasuk tenaga dan peralatan komunikasi, sesuai dengan peraturan perundang-undangan, persyaratan teknis dan bisnis, spesifikasi *vendor*, dan pedoman kesehatan dan keselamatan.

2.2.1.13 DS13-Manage Operations

DS13.1 *Operations Procedures and Instructions*

Proses menentukan, menerapkan dan memelihara prosedur untuk operasi TI, memastikan bahwa anggota staf

operasi akrab dengan semua tugas operasi yang relevan bagi mereka.

Prosedur operasional harus mencakup pergeseran serah terima (serah terima resmi dari aktivitas, *update status*, masalah operasional, prosedur eskalasi dan laporan tanggung jawab terkini) untuk mendukung disepakatinya tingkat layanan dan memastikan keberlangsungan operasi berkelanjutan.

DS13.2 *Job Scheduling*

Mengatur penjadwalan pekerjaan, proses dan tugas ke urutan paling efisien, memaksimalkan *throughput* dan pemanfaatan untuk memenuhi kebutuhan bisnis.

DS13.3 *IT Infrastructure Monitoring*

Menentukan dan menerapkan prosedur untuk memantau infrastruktur TI dan kegiatan yang terkait. Memastikan bahwa informasi kronologis yang memadai disimpan dalam *log* operasi untuk memungkinkan rekonstruksi, ulasan dan pemeriksaan urutan waktu operasi dan kegiatan lain di sekitarnya atau operasi yang mendukung.

DS13.4 *Sensitive Documents and Output Devices*

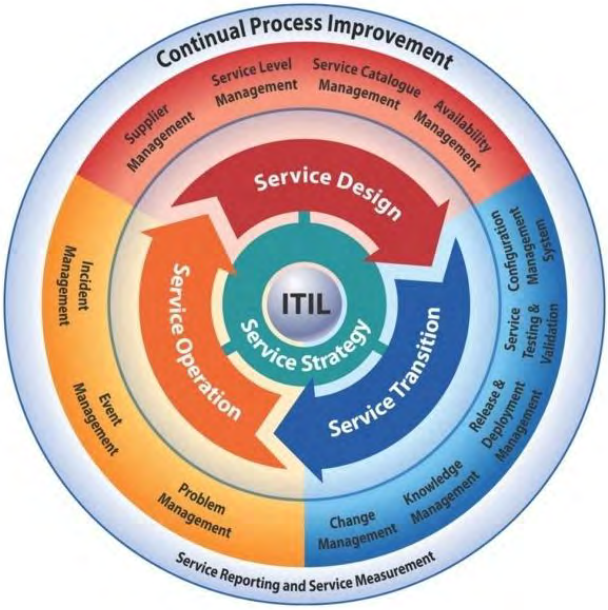
Menetapkan pengaman yang tepat, baik secara fisik, praktik akuntansi dan manajemen persediaan lebih kepada aset TI yang sensitif, seperti bentuk khusus, surat berharga, *printer* bagi tujuan khusus atau token keamanan.

DS13.5 *Preventive Maintenance for Hardware*

Menentukan dan menerapkan prosedur untuk memastikan perawatan dan waktu melakukan perawatan infrastruktur untuk mengurangi frekuensi dan dampak dari kegagalan atau penurunan kinerja ketika proses bisnis sedang berjalan.

2.3 ITIL V3

Information Technology Infrastructure Library (ITIL) adalah standar praktik yang terkait dengan layanan teknologi informasi. ITIL menyediakan *framework* / kerangka praktik yang baik dalam memandu pengelolaan manajemen layanan TI [2].



Gambar 2.2 Service Lifecycle dalam ITIL

Tujuan ITIL dapat dilihat dari dua buah prespektif. Prespektif pertama adalah dari sisi pelanggan dan prespektif kedua dilihat dari sisi manajemen TI.

Tujuan dan keuntungan penggunaan ITIL dari prespektif pelanggan :

1. Tujuan penyampaian layanan TI lebih berfokus kepada pelanggan dan persetujuan untuk meningkatkan kualitas pelayanan akan meningkatkan hubungan antara pelanggan dengan pihak manajemen.

2. Organisasi mampu mendeskripsikan layanan dengan lebih baik, menggunakan bahasa yang dimengerti oleh pelanggan, dan dengan detail yang lebih terperinci.
3. Manajemen kualitas, ketersediaan, kehandalan, dan biaya layanan yang lebih baik.
4. Komunikasi dengan pihak organisasi TI meningkat dengan poin-poin yang disetujui dalam kontrak.

Sedangkan tujuan atau keuntungan yang didapatkan dari prespektif manajemen TI adalah:

1. Organisasi TI membangun struktur yang lebih jelas, lebih efisien dan terfokus pada tujuan organisasi.
2. Organisasi TI lebih dapat mengontrol infrastruktur dan layanan yang ditangguhkan kepadanya, dan perubahan dapat lebih mudah untuk dilaksanakan.
3. Struktru proses yang efisien dan mendukung kerangka pelaksanaan *outsourcing* yang efektif dalam elemen layanan TI.
4. Mengikuti *best practice* untuk perubahan kultur dalam menyediakan layanan, dukungan untuk mengenali kualitas manajemen sistem berdasarkan ISO 9000 *series* atau ISO/IEC 20000.
5. Kerangka dapat mendukung pelaksanaan komunikasi internal yang baik dengan *supplier* dan untuk men-standarkan prosedur identifikasi layanan.

Service atau layanan adalah tentang menyampaikan *value* (nilai) kepada konsumen. ITIL mendefinisikan layanan sebagai sarana penyampaian *value* kepada pelanggan guna menfasilitasi hasil yang pelanggan inginkan tanpa adanya status kepemilikan terhadap biaya atau risiko yang spesifik [5].

Service atau layanan diharapkan mampu meningkatkan kinerja dan mengurangi tekanan yang datang dari kendala-kendala penyampaian *value* terhadap konsumen. Selanjutnya,

peningkatan kinerja ini diiringi juga dengan meningkatkan kemungkinan hasil yang semakin mendekati harapan konsumen.

Value atau nilai sendiri adalah inti dari konsep sebuah layanan. Dari prespektif konsumen, layanan terdiri dari dua buah komponen yaitu kegunaan dan jaminan. Kegunaan adalah apa yang didapatkan oleh pelanggan dan jaminan adalah bagaimana jaminan akan kegunaan ini tersedia.

ITIL mendefinisikan *service management* adalah sebuah seperangkat kemampuan organisasi yang terspesialisasi untuk memberikan nilai kepada pelanggan dalam bentuk jasa atau layanan.

Tedapat lima buah tahap di dalam ITIL yaitu, *Service Strategy, Service Design, Service Transition, Service Operation* dan *Continual Service Improvement* [5].

1 ***Service Strategy*** – Tahap merancang, mengembangkan dan menerapkan *service management* dari sisi proses, perencanaan sumber daya dan teknologi beserta rekomendasi peningkatannya.
2 ***Service Design*** – Tahap desain pemilihan untuk layanan TI yang sesuai di organisasinya, termasuk di dalamnya arsitektur, proses, kebijakan dan dokumentasi dari sisi teknologi yang digunakan, sumber daya manusia yang dibutuhkan dan pemilihan *partner*. Tujuan tahap desain ini adalah untuk memenuhi kebutuhan bisnis di saat ini dan masa depan.
3 ***Service Transition*** – Tahap mengembangkan dan meningkatkan kemampuan untuk melakukan transisi layanan kepada layanan yang baru baik dari sisi teknologi, sumber daya dan kerjasama dengan *partner*.
4 ***Service Operation*** – Tahap memastikan efektivitas dan efisiensi dapat tercapai dalam penyediaan jasa pendukung yang telah di rencanakan sehingga *value* dari layanan terpenuhi bagi pelanggan dan *service provider*.
5 ***Continual Service Improvement*** – Tahap menciptakan dan memelihara *value* bagi pelanggan dengan merencanakan pengembangan desain dan proses pengoperasian layanan.

2.3.1 *Service Strategy*

Di dalam *service strategy* terdapat tiga buah proses utama, yaitu :

1. *Financial Management*
2. *Service Portfolio Management*
3. *Demand Management*

2.3.1.1 Financial Management

Financial Management merupakan komponen yang saling berintegrasi dalam manajemen layanan. Proses ini mendukung informasi penting bahwa manajemen harus mampu mengjamin penyampaian layanan yang efisien dan efektif (secara biaya) tetap dapat berjalan [5]. *Financial management* memungkinkan organisasi untuk melakukan justifikasi penuh terhadap penggunaan biaya yang di alokasikan ke dalam layanan.

Financial management memastikan bahwa seluruh biaya yang digunakan dapat dilaporkan secara transparan (contoh : melalui *service catalogue*) dan pihak manajemen bisnis dapat memahami penggunaannya dengan mudah.

2.3.1.2 Service Portfolio Management (SPM)

Service portfolio mendeskripsikan pendukung layanan (*service provider*) seperti apakah yang dibutuhkan sesuai persyaratan *value*/nilai bisnis organisasi [5].

Service portfolio menformulasikan kebutuhan bisnis dan reaksi yang diharapkan dari *service provider* terhadap kebutuhan tersebut. *Service portfolio* memastikan bahwa persaingan antar *service provider* dapat diukur dengan melihat masing-masing keunggulannya.

Dengan SPM, manajemen dapat mengukur kualitas yang diinginkan bersamaan dengan biaya yang dibutuhkan. SPM dapat melihat poin penghematan biaya dengan tetap membangun kualitas dari layanan tersebut dengan lebih mudah.

Tujuan utama dari SPM adalah organisasi mampu membangun nilai maksimal yang diinginkan dengan secara

bersamaan menutup risiko dan penghematan biaya yang tidak dibutuhkan.

2.3.1.3 Demand Management

Demand management (DM) merupakan aspek penting dalam *service management*. DM harus mampu menjadikan antara pemasukan dengan permintaan dalam proses bisnis seimbang. Selain itu, manajemen harus mampu menprediksi produk atau layanan apakah yang diinginkan paling mendekati dengan ekspektasi pasar, bahkan apabila dimungkinkan, lebih dari yang diprediksikan [5].

Akan tetapi, apabila organisasi mengikuti *demand* maka akan memberikan risiko yang lebih tinggi terhadap *service provider*, contoh, ketika kapasitas berlebih akan mempengaruhi biaya yang mana peningkatan biaya bertentangan dengan *value* organisasi.

Penggunaan *Service level agreement*, peramalan permintaan, perencanaan dan koordinasi ketat dengan konsumen akan mampu mengurangi permintaan berlebih yang tidak terserap, akan tetapi kesemua ini tidak dapat dilakukan secara bersamaan. Oleh karena itu pihak manajemen harus mampu menghadapi permasalahan tambahan dalam proses mensinkronisasikan data produksi dan konsumsi organisasi.

2.3.2 Service Design

Di dalam *service design* terdapat tujuh buah proses utama, yaitu :

1. *Service catalogue management*
2. *Service level management*
3. *Capacity management*
4. *Availability management*
5. *IT service continuity management*
6. *Information security management*
7. *Supplier management*

2.3.2.1 Service Catalogue Management

Tujuan pembuatan *service catalogue management* (SCM) adalah untuk membangun sebuah katalog layanan yang berisikan informasi lengkap, status, interaksi yang dimungkinkan dan hubungan yang saling berhubungan untuk seluruh layanan yang akan dibangun [5].

Service catalogue akan digunakan sebagai informasi utama layanan. Dengan menggunakan katalog, setiap orang dalam organisasi dapat melihat apakah layanan yang akan disampaikan kepada pelanggan, bagaimana layanan tersebut diberikan, bagaimana layanan tersebut digunakan, untuk tujuan apa, dan bagaimanakah tingkat kualitas yang diprediksikan pelanggan.

Berbeda dengan *service portfolio*, SCM merupakan bagian dari *service portfolio* yang menampilkan hanya layanan yang aktif dan disetujui saja dalam *service operation*. SCM membagi layanan menjadi beberapa komponen yang berisikan kebijakan, panduan dan pertanggungjawaban, rencana *service level* dan perencanaan penyampaiannya kepada pelanggan.

2.3.2.2 Service Level Management

Tujuan dari proses *Service Level Management* (SLM) adalah untuk melihat bahwa *level* yang disetujui dalam persyaratan layanan TI tercapai baik disaat ini maupun dimasa mendatang [5].

SLM memastikan bahwa komunikasi dan hubungan yang baik mungkin untuk dilakukan terhadap seluruh bagian yang berkepentingan (internal maupun eksternal). Dengan terjalinnya komunikasi yang baik, apabila terjadi gangguan, SLM mampu memberikan umpan balik sehubungan dengan penyebab dan informasi pendukung yang digunakan untuk tindakan pencegahan yang dapat diambil.

2.3.2.3 Capacity Management

Tujuan dari penggunaan *capacity management* adalah untuk mendukung prediksi kapasitas TI sesuai dengan kebutuhan saat ini dan dimasa mendatang guna menghindari kemungkinan penambahan biaya [5].

Capacity manangement menjadi gambaran inti dari performa TI dan permasalahan kapasitas. Sebagai contoh, jaringan dan *server* mengambil bagian penting yang menopang tugas harian kegiatan operasional dapat berjalan. *Capacity management* berfokus pada ruang kapasitas dan lingkungan sistem mencukupi.

Capacity management bertanggung jawab dalam merencanakan sumber daya TI guna menyampaikan *level* kualitas layanan yang konsisten sesuai dengan kebutuhan pelanggan saat ini dan masa mendatang.

Perencanaan *capacity management* ditentuan berdasarkan konsultasi dengan seluruh pelanggan. Perencanaan ini kemudian dispesifikasikan lagi berdasarkan biaya yang dimiliki organisasi.

2.3.2.4 Availability Management

Tujuan dari penggunaan *availability management* adalah untuk memastikan bahwa tingkat ketersediaan layanan yang disampaikan sesuai atau melebihi persetujuan yang ada dengan biaya se-efektif mungkin [5].

Proses di dalam *availability management* termasuk proses mendesain, mengimplementasikan, mengukur, mengatur dan meningkatkan layanan TI dan komponen pendukungnya. Hal ini didasari pada ketersediaan layanan akan memberikan dampak langsung kepada kepuasan pelanggan dan reputasi organisasi, oleh karena itu, *availability management* menjadi kebutuhan penting organisasi seperti *capacity management* sehingga proses ini harus tersedia dalam tingkatan pertama pembuatan layanan.

2.3.2.5 IT Service Continuity Management

Tujuan dari *IT service continuity management* (ITSCM) adalah untuk mendukung keberlangsungan bisnis yang memerlukan fasilitas TI (sistem komputer, jaringan, dll) berkelanjutan [5].

ITSCM lebih berfokus pada dukungan TI terhadap proses bisnis yang mungkin memiliki risiko bencana lebih besar. Proses ini juga meliputi seluruh area kantor dan sistem akomodasi personal.

ITSCM tidak berfokus pada risiko jangka panjang, hasil dari perubahan proses bisnis dan organisasi. Ketika suatu ancaman memiliki dampak yang cukup besar, organisasi memiliki waktu yang cukup lama untuk mengidentifikasi dan mengambil tindakan pencegahan. Masalah teknis kecil, seperti kesalahan yang tidak utama tidak termasuk ke dalam proses ini, tetapi di *handle* dalam *incident management.*

ITSCM memiliki daya dukung kepada perencanaan keberlangsungan bisnis. Organisasi biasanya menggunakan ini untuk membangun kesadaran akan keberlangsungan dan kebutuhan perbaikan dan memberikan keputusan yang diimplementasikannya dalam proses BCP (*business continuity plan)*.

2.3.2.6 Information Security Management

Tujuan dari *Information Security Management* adalah untuk menghubungkan antara TI dengan keamanan bisnis. Selain itu untuk memastikan bahwa *information security* dilakukan secara efektif di seluruh operasi manajemen layanan [5].

Information security management harus memiliki wawasan yang baik terhadap seluruh arena TI dan keamanan bisnis, seperti perencanaan dan kebijakan *business security* saat ini dan masa depan, kebutuhan keamanan, kebutuhan hukum yang harus dipenuhi dan risiko bisnis dan TI (dan bagaimana langkah pengaturannya).

Information security management memastikan bahwa seluruh kebijakan *information security* sesuai dengan peraturan dan kebijakan yang berlaku. Hal ini direalisasikan dengan berupaya meningkatkan kesadaran internal akan isu keamanan layanan.

Pihak manajemen bertanggung jawab terhadap informasi bisnis dan harus mampu menyelesaikannya ketika terjadi bahaya. Pihak manajemen teratas organisasi harus menyadari bahwa *information security* adalah bagian yang terintegrasi dengan peraturan organisasi. Dengan prespektif inilah, setiap *IT Service provider* harus memiliki kesadaran kebijakan yang baik sesuai dengan *service management* dan kontrolnya.

2.3.2.7 Supplier Management

Tujuan dari *supplier management* adalah mengatur setiap *supplier* untuk memberikan layanan yang terarah dalam kualitas yang konsisten dan penggunaan yang tepat [5].

Proses dalam *supplier management* berfokus pada seluruh *supplier* dan kontrak yang dibuat dalam mendukung hasil layanan sesuai dengan ekspektasi pelanggan. Semakin besar kontribusi yang diberikan oleh *supplier*, semakin besar upaya yang harus diberikan dalam membangun hubungan dengan *supplier* dan semakin tinggi juga dampak *supplier* terhadap pembuatan strategi organisasi.

Supplier management membantu organisasi memastikan bahwa biaya yang dikeluarkan oleh organisasi tepat guna. Sebagai tambahan, hal ini akan dimasukkan ke dalam tujuan kontrak dengan *supplier* yang kemudian di tuangkan dalam dokumen SLA.

Tujuan akhir yang diharapkan adalah kualitas layanan TI sesuai dengan ekspetasi. *Supplier management* akan di sesuaikan dengan kebutuhan organisasi dan kebutuhan manajemen keamanan informasi dalam ITSCM.

2.3.3 Service Transition

Di dalam *service transition* terdapat tujuh buah proses utama, yaitu :

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

2.3.3.1 Transition Planning and Support

Tujuan dari proses *transition planning and support* adalah untuk merencanakan dan mengkoordinasikan sumber daya guna memastikan bahwa spesifikasi dalam *service design* mampu terealisasi. Selain itu, untuk memulai fase transisi, identifikasi, pengaturan dan pembatasan risiko dapat mengganggu proses layanan sehingga membutuhkan pengawalan dalam pengimplementasiannya [5].

Manfaat yang diberikan oleh proses ini adalah organisasi mampu melakukan pendekatan penuh akan perencanaan peningkatan yang terhubung dengan perencanaan proses transisi sehingga memungkinkan *project plans client*, *supplier* dan bisnis dapat diubah ditengah prosesnya.

2.3.3.2 Change Management

Setiap perubahan memiliki alasan proaktif dan reaktif. Sebagai contoh, tindakan proaktif adalah meningkatnya biaya atau dibutuhkannya peningkatan layanan. Contoh tindakan reaktif adalah organisasi berubah untuk menghadapi sebuah gangguan atau beradaptasi dengan perubahan lingkungan.

Proses perubahan sendiri merupakan kemungkinan penambahan, modifikasi atau pengurangan dari sebuah otorisasi, rencana, atau komponen pendukung layanan dan seluruh dokumen yang berhubungan [5].

Perubahan yang didasari dari gangguan layanan kemungkinan akan memberikan dampak yang merugikan terhadap hasil bisnis organisasi. Akan tetapi manajemen perubahan yang baik akan memberikan hasil yang baik juga terhadap proses bisnis organisasi.

2.3.3.3 Service Asset and Configuration Management

Tujuan dari proses *service asset and configuration management* (SACM) adalah untuk mendukung model dalam *IT infrastructure*. Di dalam model ini layanan yang berhubungan dengan komponen TI yang berbeda antara satu dengan yang lainnya membutuhkan perantara. Fokusan dari proses ini adalah untuk mendefinisikan layanan dan komponen infrastruktur serta proses pemeliharaan dengan catatan konfigurasi yang akurat [5].

Aset yang digunakan di seluruh fase layanan masuk ke dalam ruang lingkup *asset management*. Proses ini menawarkan ulasang lengkap seluruh aset, dan menunjukkan pihak yang bertanggung jawab melakukan kontrol dan perawatan aset tersebut.

Manfaat dari proses SACM ini adalah kemampuan organisasi dalam meyelidiki, merencanakan dan melakukan perubahan dan rilis meningkat, insiden dan masalah dapat diselesaikan dengan lebih mudah, meningkatkan koordinasi antar standar, meningkatkan pemenuhan persyaratan hukum dan lebih memahami pengeluaran biaya yang berhubungan dengan layanan.

2.3.3.4 Release and Deployment Management

Release and deployment management sebuah proses untuk mengarahkan pembangunan, pengetesan dan penyediaan layanan yang spesifik dalam *service design*, sehingga dengan melewati proses ini kebutuhan dan objektivitas organisasi dapat bertemu dengan masing-masing kebutuhan dan objektivitas *stakeholder* [5].

Dengan menjalankan proses *release and deployment management* yang efektif dapat membantu organisasi memahami

perubahan dengan lebih baik, murah dan risiko yang relatif lebih sedikit dan objektivitas operasional dapat didukung dengan baik. Selain itu pendekatan pengimplementasiannya akan lebih konsisten dengan proses penelusuran audit yang lebih mudah.

2.3.3.5 Service Validation and Testing

Pengetesan sebuah sistem adalah sebuah proses yang penting guna memastikan kualitas yang ditetapkan tercapai. Testing dapat memastikan bahwa setiap layanan yang baru (atau baru saja mengalami perubahan) '*fit for purpose´* dan '*fit to use*' [5].

Fit to purpose memiliki artian bahwa layanan berjalan sesuai dengan ekspetasi pelanggan sedangkan *fit to use* adalah seluruh aspek *availability*, *continuity*, *capacity* dan *security* layanan terpenuhi.

Hal ini penting dilakukan karena setiap gangguan layanan akan memberikan dampak terhadap operasi bisnis bagi *service provider* dan *client* yang menggunakan layanan. Hal ini akan mempengaruhi reputasi organisasi, kehilangan pelanggan dan mungkin kecelakaan fatal.

2.3.3.6 Evaluation

Evaluasi adalah proses umum untuk menverifikasi performa yang dapat diterima baik dari sisi harga, kualitas hingga manfaatnya [5]. Evaluasi memberikan inputan penting bagi peningkatan masa depan *service development* dan *change management*.

2.3.3.7 Knowledge Management

Tujuan dari *knowledge management* adalah untuk meningkatkan kualitas pengambilan keputusan sebuah proses (manajemen) dengan memastikan bahwa informasi yang dapat terpercaya tersedia di seluruh proses *service lifecycle* [5].

Knowledge management terutama sekali digunakan dalam proses *transition*. Sebuah proses transisi dapat dikatakan berhasil

bergantung pada luasnya informasi dan pengetahuan pengguna, *service desk, tim support* dan *supplier*. Contoh spesifik dari proses *knowledge management* adalah :

1. Pelatihan dan transfer ilmu, *intellectual property,* pemenuhan informasi dan standar
2. Dokumentasi *error*, informasi temuan lingkungan dan pengetesan.

2.3.4 Service Operation

Di dalam *service operation* terdapat delapan buah proses utama, yaitu :

1. *Event Management*
2. *Incident Management*
3. *Request Fulfillment*
4. *Problem Management*
5. *Access Management*
6. *Monitoring and Control*
7. *IT Operations*
8. *Service Desk*

2.3.4.1 Event Management

Event atau kejadian merupakan sebuah kegiatan acak atau kegiatan yang tampak dan memiliki maksud untuk *management infrastructure IT* atau untuk menyampaikan layanan, atau proses evaluasi dampak penyimpangan layanan [5].

Event biasanya dipantau menggunakan alat/*tools* untuk memastikan tingkat ke-efektifitasan operasinya. Sebuah organisasi harus sadar akan status infrastrukturnya dan mampu mendeteksi penyimpangan dari eksekusi proses operasional *regular*. Fokusan dalam proses *event management* adalah untuk mendeteksi kejadian, menganalisa dan menetapkan tindakan yang diambil oleh pihak manajemen.

Event management mendukung mekanisme deteksi insiden dini dan mampu melakukan aktivitas pemantauan secara otomatis secara bersamaan tanpa jeda. Jika *event management*

terhubung dengan proses *service management* lainnya, maka organisasi dimungkinkan mampu mendeteksi perubahan status atau gangguan layanan; mampu menentukan orang atau tim tertentu untuk memberikan respon secepat mungkin sehingga mampu meningkatkan performa proses bisnis. Selain itu, *event management* adalah dasaran dalam pelaksanaan pengoperasian proses bisnis secara otomatis sehingga mampu meningkatkan efektivitas dan mengurangi biaya dengan proses kerja yang inovatif.

2.3.4.2 Incident Management

Proses *incident management* adalah proses untuk menangani insiden. Insiden ini dapat berbentuk kesalahan, pertanyaan atau pernyataan yang diajukan pengguna (biasanya melewati telepon atau *service desk*) kepada staf teknis, atau secara otomatis dapat dideteksi dan dilaporkan melalui alat pemantau kejadian [5].

Insiden sendiri merupakan sebuah gangguan yang tidak terencana terhadap layanan atau penurunan kualitas layaann TI. Manajemen insiden melingkupi seluruh kejadian yang mengganggu atau mungkin akan mengganggu layanan.

Manfaat yang diberikan oleh manajemen insiden adalah organisasi dimungkinkan mampu melacak dan menyelesaikan insiden dengan mengurangi waktu *downtime* sehingga layanan dapat tersedia dalam jangka waktu yang relatif lebih panjang. Selain itu, organisasi akan mampu menjalankan operasional TI berdasarkan prioritas bisnis; hal ini dikarenakan insiden manajemen mampu mengidentifikasikan prioritas bisnis dan mendistribusikan sumber daya dengan dinamis.

2.3.4.3 Request Fulfillment

Service request adalah permintaan dari pengguna akan informasi, saran, perubahan atau akses layanan. Dikarenakan setiap permintaan mempengaruhi proses bisnis tetap organisasi

yang memungkinkan menambahkan risiko, sehingga lebih baik proses ini ditangani oleh proses yang terpisah.

Proses penanganan permintaan bergantung dengan sifat dari permintaan. Dalam banyak kasus proses dapat dibagi berdasarkan aktivitas yang dipenuhi. Beberapa organisasi memasukkan *service fulfillment* ke dalam bentuk insiden, sedangkan insiden dan permintaan memiliki perbedaan. Insiden biasanya adalah kejadian yang terjadi di luar rencana, sedangkan *service request* seharusnya adalah sesuatu yang bisa dan harus direncanakan.

Manfaat yang diberikan oleh proses *request fulfillment* adalah organisasi dapat dengan cepat dan efektif mengakses layanan standar yang tersedia sehingga hal ini dapat meningkatkan produktivitas atau kualitas dari layanan dan produk bisnis [5].

2.3.4.4 Problem Management

Problem adalah penyebab utama satu atau lebih insiden [5]. Fokus utama dari *problem management* adalah untuk mencegah masalah dan insiden terjadi, mengeliminasi insiden yang berulang, dan meminimalisir dampak insiden yang tidak dapat dicegah.

Problem management terdiri dari aktivitas diagnosa dan fokus pada penyebab mendasar insiden dan mencari solusi dari permasalahan. Selain itu, proses ini harus memastikan bahwa solusi yang diajukan terimplementasi dengan baik dengan prosedur kontrol yang tepat, atau kata lain *problem management* terhubung dengan *change management* dan *release management*.

2.3.4.5 Access Management

Access management menjamin hanya pengguna layanan yang disetujui saja yang memiliki hak akses, dan menolak seluruh pengguna yang tidak memiliki hak akses. *Access management* memang menggaransi pengguna dapat mengakses layanan, akan tetapi hal ini tidak serta merta menggaransi akses akan selalu

tersedia di waktu yang telah disetujui, hal ini menjadi tanggung jawab *availability management.*

Dengan menggunakan *access management*, organisasi akan mampu untuk mengontrol akses layanan untuk membangun nilai keamanan informasi yang lebih efektif, karyawan mendapatkan hak akses sesuai dengan *level* pekerjaan, kesalahan penggunaan selama akses data menjadi lebih sedikit, dan penggunaan standar akses akan lebih mudah diimplementasikan [5].

2.3.4.6 Monitoring and Control

Proses pengukuran dan kontrol layanan didasari pada siklus monitoring, pelaporan dan aksi inisiasinya, sedangkan pada proses *monitoring and control* akan berfokus pada tiga buah tindakan yaitu *monitoring, reporting* dan *control*.

Monitoring menuju pada proses observasi situasi dan mencari perubahan yang diperlukan di sepanjang waktu. *Reporting* menuju pada proses menganalisa, menproduksi dan mendistribusikan *output* aktivitas yang di monitoring. *Control* sendiri menuju kepada proses manajemen kegunaan dan tingkah laku alat [5].

2.3.4.7 IT Operations

Untuk menyampaikan layanan sesuai dengan yang disetujui oleh pelanggan, *service provider* pada awalnya harus mengatur infrastruktur teknis yang digunakan dalam menyampaikan layanan. Meskipun layanan tidak memiliki permintaan pengguna baru, pengimplementasian layanan baru, terjadinya insiden dan tidak adanya perubahan yang diperlukan sebenarnya *service operation* sudah sibuk untuk berfokus memastikan layanan yang berjalan sesuai dengan standar layanan yang disetujui.

Service operations biasanya memiliki *central point* tempat seluruh operasi diatur berdasarkan berbagai macam kegiatan dan

rutinitias operasional dan melaporkan status atau performa komponen teknologinya [5].

Pusat pelaksana operasional organisasi melakukan kegiatan observasi utama dalam infrastruktur TI sehingga setiap kegiatan dapat dimonitoring dan diatur dengan usaha seminimal mungkin.

Di dalam pusat pelaksana operasional terdapat banyak aktivitas, seperti pusat manajemen, penanganan kejadian, kontak utama diluar jam aktif operasional. Di dalam beberapa organisasi, *service desk* masuk ke dalam pusat pelaksana operasional.

2.3.4.8 Service Desk

Service desk merupakan unit fungsional yang berasosiasi untuk menguasai beberapa kejadian layanan [5]. Layanan ini dapat berupa telepon, infrastruktur internet atau pelaporan secara otomatis.

Service desk merupakan komponen utama dari departemen TI di organisasi. *Service desk* menjadi satu-satunya kontak bagi pengguna TI ketika terjadi insiden atau adanya permintaan layanan.

Tujuan utama dari *service desk* adalah menyediakan *normal service* secepat mungkin bagi pengguna TI. Hal ini dapat berarti memperbaiki kesalahan teknis, atau memenuhi permintaan layanan atau menjawab pertanyaan yang diajukan.

2.3.5 Service Improvement

Di dalam *service improvement* terdapat dua buah proses utama, yaitu :

1. *CSI Improvement Process*
2. *Service Reporting*

2.3.5.1 CSI Improvement Process

Continual service improvement process (CSI) atau tujuh langkah proses pengembangan mendeskripsikan bagaimana langkah untuk mengukur dan melaporkan [5]. Pengembangan

menggunakan siklus P-D-C-A. Hasil dari siklus perencanaan CSI adalah *service improvement plan* (SIP).

Apabila *service level management* menemukan bahwa sebuah layanan perlu ditingkatkan, maka siklus peningkatan dapat menggunakan CSI karena CSI memiliki daftar aktivitas untuk mencapai peningkatan layanan. CSI akan membuat SIP untuk kebutuhan ekseskusinya dalam bentuk proses TI dengan *input*, aktivitas, *output*, aturan dan pelaporan.

Tujuh langkah pengukuran peningkatan layanan :

1. *What should you measure ?*
2. *What can you measure ?*
3. *Gather data (measure)*
4. *Process data*
5. *Analyze data*
6. *Present and use information*
7. *Implement corrective action*

2.3.5.2 Service Reporting

Service reporting process merupakan proses yang bertanggung jawab dalam menurunkan dan menyalurkan hasil laporan yang didapatkan dalam fase *development service*. Pelaporan ini harus sesuai dengan *lay-out* yang dimiliki organisasi, baik secara konten maupun frekuensi pelaksanaan laporan [5].

Prose dalam *service reporting* adalah pertama melakukan pengumpulan data, kemudian data tersebut di proses kedalam informasi untuk dilaporkan kepada organisasi, menerbitkan hasil laporan dengan memberikan sajian laporan sesuai *level* keperluan dan kelengkapan informasi oleh masing-masing pihak yang mendapatkan laporan.

2.4 ITIL dan Komitmen Manajemen

Komitmen merupakan sebuah tindakan melakukan instruksi atau mempercayakan sesuatu. Komitmen juga dapat diartikan sebagai sebuah persetujuan atau perjanjian untuk

menggunakan siklus P-D-C-A. Hasil dari siklus perencanaan CSI adalah *service improvement plan* (SIP).

Apabila *service level management* menemukan bahwa sebuah layanan perlu ditingkatkan, maka siklus peningkatan dapat menggunakan CSI karena CSI memiliki daftar aktivitas untuk mencapai peningkatan layanan. CSI akan membuat SIP untuk kebutuhan ekseskusinya dalam bentuk proses TI dengan *input*, aktivitas, *output*, aturan dan pelaporan.

Tujuh langkah pengukuran peningkatan layanan :

1. *What should you measure ?*
2. *What can you measure ?*
3. *Gather data (measure)*
4. *Process data*
5. *Analyze data*
6. *Present and use information*
7. *Implement corrective action*

2.3.5.2 Service Reporting

Service reporting process merupakan proses yang bertanggung jawab dalam menurunkan dan menyalurkan hasil laporan yang didapatkan dalam fase *development service*. Pelaporan ini harus sesuai dengan *lay-out* yang dimiliki organisasi, baik secara konten maupun frekuensi pelaksanaan laporan [5].

Prose dalam *service reporting* adalah pertama melakukan pengumpulan data, kemudian data tersebut di proses kedalam informasi untuk dilaporkan kepada organisasi, menerbitkan hasil laporan dengan memberikan sajian laporan sesuai *level* keperluan dan kelengkapan informasi oleh masing-masing pihak yang mendapatkan laporan.

2.4 ITIL dan Komitmen Manajemen

Komitmen merupakan sebuah tindakan melakukan instruksi atau mempercayakan sesuatu. Komitmen juga dapat diartikan sebagai sebuah persetujuan atau perjanjian untuk

melakukan sesuatu di masa mendatang. Komitmen individu dalam sebuah tim adalah yang membuat tim atau sebuah organisasi tersebut dapat bekerja [6].

Sebuah organisasi yang telah berkomitmen untuk memperbaiki manajemen layanannya dengan menggunakan ITIL senantiasa telah berkomitmen untuk menjalankan setiap aktivitas agar proses implementasi dapat berjalan sepenuhnya.

2.4.1 *Service Strategy*

Service Strategy memberikan panduan untuk mendesain ruang lingkup, pengembangan dan implementasi manajemen layanan berdasarkan kapasitas dan prespektif strategi organisasi [2].

Pengimplementasian *Service Strategy* dalam sebuah perusahaan / organisasi, harus mampu menjawab kebutuhan sebagai berikut [6] :

1. Penilaian terhadap proses, sumber daya manusia dan teknologi terkini
2. Rekomendasi peningkatan area.

2.4.2 Service Design

Service Design atau *Service Project* berisikan panduan untuk mendesain dan mengembangkan layanan dan proses bisnis berdasarkan manajemen TI. Fase ini termasuk penjabaran/ pengembangan dari strategi perusahaan yang sudah didefinisikan di dalam *portfolio* layanan [2].

Pengimplementasian *Service Design* dalam sebuah perusahaan / organisasi, harus mampu menjawab kebutuhan sebagai berikut [6] :

1. Proses desain layanan
2. Mencangkup *high level process guide* yang berisikan *executive summary*, tujuan proses, aktivitas proses, aturan dan tanggung jawab, RACI matriks, Penilaian kualitas dan kriteria audit.
3. Persetujuan perjanjian

Ketiga aktivitas ini bertujuan untuk memastikan bahwa organisasi mampu memilih teknologi, sumber daya, dan *partner* sesuai dengan nilai yang dimiliki organisasi sejak awal proses pembangunan layanan.

2.4.3 Service Transition

Service transition menawarkan bimbingan untuk seluruh proses *development* dan *improvement* dari transisi sebuah proses menjadi layanan yang baru ataupun transformasi dari sebuah proses menjadi operasi. Bagian ini menggabungkan beberapa bagian dalam manajemen, mulai dari manajemen operasi, manajemen program dan manajemen risiko [2].

Pengimplementasian *Service Transition* dalam sebuah perusahaan/organisasi, harus mampu menjawab kebutuhan sebagai berikut [6] :

1. Membangun prosedur dan instruksi kerja
2. Dokumentasi pendukung yang lengkap

Kedua aktivitas ini bertujuan untuk memastikan bahwa teknologi, sumber daya, dan *partner* yang telah di pilih dalam proses sebelumnya dapat digunakan sesuai dengan nilai yang dimiliki organisasi dan kontrak kerja yang telah disepakati.

2.4.4 *Service Operation*

Service Operation merupakan praktek dari layanan yang efektif dan efisien dalam penyampaian dan proses dukungan layanan untuk memastikan nilai (*value*) tersampaikan kepada *customer* dan *service provider* [2].

Pengimplementasian *Service Operation* dalam sebuah perusahaan / organisasi, harus mampu menjawab kebutuhan sebagai berikut [6] :

1. Perencanaan Pelatihan
2. Pelatihan staff dalam aktivitas proses layanan, aturan dan pertanggungjawaban, dan mampu menjalankan TI

3. Skenario dalam training sesuai dengan gambaran utama proses.

Ketiga aktivitas ini bertujuan untuk memastikan bahwa seluruh stategi dan perencanaan yang telah dibuat dapat terus berjalan dalam proses bisnis keadaan normal/*regular*.

2.4.5 *Continual Service Improvement*

Continuous Improvement of Services atau yang biasa dikenal dengan *Service Review* merupakan proses untuk mengkreasikan dan *maintain value* yang diberikan kepada pengguna dan pelanggan dengan konsep, implementasi dan operasi yang lebih baik [2].

Pengimplementasian *Service Continous Improvement of Service* dalam sebuah perusahaan/organisasi, harus mampu menjawab kebutuhan untuk meninjau keefektifan dan keefisienan dari proses, teknologi, sumber daya manusia dan *partner* perusahaan/organisasi yang akan menjadi rekomendasi bagi perencanaan peningkatan layanan lanjutan [6].

2.5 ISO/IEC 27000:2005

Tujuan dari keamanan informasi adalah untuk melindungi aset guna memastikan kelangsungan bisnis tetap berjalan, meminimalkan risiko bisnis dan memaksimalkan keuntungan perusahaan [4].

ISO/IEC 27000:2005 *series* adalah sebuah standar untuk manajemen keamanan informasi yang diakui secara internasional. ISO 27000:2005 *series* terdiri dari banyak standar dan dokumen mulai dari standar yang sebelumnya telah lebih dahulu dikenal dan diterbitkan juga standar yang masih menunggu penomoran untuk dipublikasikan. ISO yang akan digunakan pada pengerjaan tugas akhir ini adalah ISO 27001:2005 dan 27002:2005.

3. Skenario dalam training sesuai dengan gambaran utama proses.

Ketiga aktivitas ini bertujuan untuk memastikan bahwa seluruh stategi dan perencanaan yang telah dibuat dapat terus berjalan dalam proses bisnis keadaan normal/*regular*.

2.4.5 *Continual Service Improvement*

Continuous Improvement of Services atau yang biasa dikenal dengan *Service Review* merupakan proses untuk mengkreasikan dan *maintain value* yang diberikan kepada pengguna dan pelanggan dengan konsep, implementasi dan operasi yang lebih baik [2].

Pengimplementasian *Service Continous Improvement of Service* dalam sebuah perusahaan/organisasi, harus mampu menjawab kebutuhan untuk meninjau keefektifan dan keefisienan dari proses, teknologi, sumber daya manusia dan *partner* perusahaan/organisasi yang akan menjadi rekomendasi bagi perencanaan peningkatan layanan lanjutan [6].

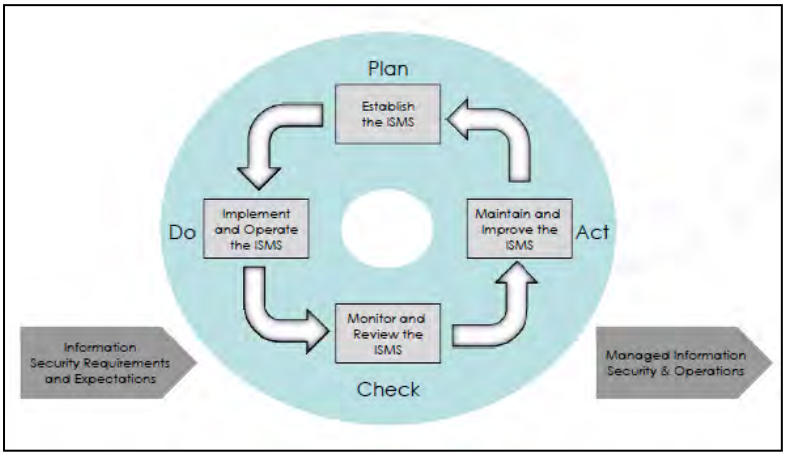
2.5 ISO/IEC 27000:2005

Tujuan dari keamanan informasi adalah untuk melindungi aset guna memastikan kelangsungan bisnis tetap berjalan, meminimalkan risiko bisnis dan memaksimalkan keuntungan perusahaan [4].

ISO/IEC 27000:2005 *series* adalah sebuah standar untuk manajemen keamanan informasi yang diakui secara internasional. ISO 27000:2005 *series* terdiri dari banyak standar dan dokumen mulai dari standar yang sebelumnya telah lebih dahulu dikenal dan diterbitkan juga standar yang masih menunggu penomoran untuk dipublikasikan. ISO yang akan digunakan pada pengerjaan tugas akhir ini adalah ISO 27001:2005 dan 27002:2005.

2.5.1 ISO/IEC 27001

ISO/IEC 27001 merupakan sebuah standar untuk membangun sistem manajemen keamanan informasi (ISMS). Di dalamnya terdapat empat buah langkah proses untuk menerapkan ISO/IEC 17799 dan bagaimanakah cara untuk menetapkan, menerapkan, memantau dan memelihara ISMS [7].



Gambar 2.3 ISMS Proses berdasarkan ISO 27001:2005

Tabel 2.1Definisi Proses ISMS Model

Fase	Tindakan	Deskripsi
Plan	Menetapkan	Menetapkan kebijakan ISMS, objektivitas, proses dan prosedur yang relevan berdasarkan manajemen risiko dan rencana peningkatan keamanan informasi dalam peyampaian layanan.
Do	Implementasi dan Pengoperasian	Mengimplementasikan dan mengoperasikan kebijakan ISMS, kontrol proses dan prosedur yang telah ditentukan.

Check	Peninjauan dan Ulasan	Menilai dan mengukur kinerja proses berdasarkan kebijakan ISMS, objektif dan laporan hasil kepada pihak manajemen.
Act	Perbaikan dan Peningkatan	Mengambil tindakan perbaikan dan pencegahan berdasarkan hasil audit internal, *management review*, atau informasi lainnya yang mendukung peningkatan berkelanjutan ISMS.

2.5.2 ISO/IEC 27002:2005

ISO/IEC 27002 pada awalnya diterbitkan untuk mengganti standar sebelumnya yaitu ISO 17799:2005 yang digunakan sebagai *best practice* manajemen keamanan informasi. Pada dasarnya, ISO 27002 menguraikan ratusan kontrol potensial dan mekanisme kontrolnya, yang akan di implementasikan, dan mengikuti teori yang di pandukan dalam ISO 27001 [8].

Di dalam ISO/IEC 27002 ditetapkan pedoman yang digunakan sebagai prinsip umum untuk memulai, melaksanakan, memelihara dan meningkatkan keamanan informasi dalam sebuah organisasi. ISO/IEC 27002 memiliki 14 rincian area yang sebelumnya hanya dijelaskan dalam 11 area dalam ISO/IEC 17799.

Area dalam ISO/IEC 27002 :

1. *Framework - Acceptable Use of Information Technology Resources*
2. *Information Security Definition & Terms*
3. *Risk Assessment*
4. *Security Policy*
5. *Organization of Information Security*
6. *Asset Management*
7. *Human Resources Security*
8. *Physical and Environmental Security*
9. *Communication and Operations Management*
10. *Access Control*

11. *Information System Acquisition, Development and Maintenance*
12. *Information Security Incident Management*
13. *Business Continuity Management*
14. *Compliance*

2.5.2.1 Security Policy

Security Policy merupakan kontrol pertama dalam ISO 17799:2005 *checklist*. Didalamnya berisikan dukungan, komitmen, dan tujuan yang ingin di capai dalam hal keamanan informasi oleh manajemen organisasi, termasuk di dalamnya :

1. *Information Security Policy Document*

Sebuah dokumen yang berisikan langkah dan konsep dari pengimplementasian kebijakan keamanan informasi yang mengatur tujuan keamanan organisasi. Dokumen ini biasanya dilengkapi dengan hirarki standar, panduan dan prosedur untuk membantu menjalankan operasi sesuai dengan kebijakan.

2. *Ownership and review*

Guna memastikan bahwa komitmen manajemen dalam keamanan informasi tetap berjalan, ditetapkan penanggung jawab dan jadwal *review* terhadap dokumen kebijakan keamanan informasi.

2.5.2.2 Organizational Security

Organizational security merupakan kontrol untuk memenuhi kebutuhan manajemen dalam membangun kerangka penopang dan mengatur infrastruktur keamanan, termasuk di dalamnya :

1. *Management information security forum*

Sebuah forum yang mendukung berbagai komite dari berbagai macam disiplin ilmu berdiskusi dan menyebarkan isu keamanan informasi kepada seluruh bagian organisasi.

2. Information system security officer (ISSO)

Pusat aksi, sebagai poin inti kontak, pemberi arahan dan pengambilan keputusan untuk setiap isu keamanan informasi.

3. Information security responsibilities

Tanggung jawab keamanan informasi individu sudah dengan jelas dialokasikan lengkap dengan masing-masing deskripsi tugasnya.

4. Authorization processes

Memastikan bahwa setiap pertimbangan keamanan dievaluasi dan mendapatkan persetujuan untuk setiap proses *information systems* yang baru ataupun mengalami modifikasi.

5. Specialist information

Memelihara hubungan baik dengan *specialist* bidang tertentu yang memiliki akses tertentu ke dalam sistem yang tidak dikuasai oleh organisasi.

6. Organizational cooperation

Memelihara hubungan *information-sharing partners* dan petugas hukum yang berwenang.

7. Independent review

Mekanisme untuk mengijinkan adanya ulasan mandiri akan ke-efektivitasan keamanan organisasi.

8. Third-party access

Mekanisme untuk menentukan interaksi pihak ketiga dengan organisasi berdasarkan kebutuhan bisnis.

9. Outsourcing

Perencanaan *outsourcing* organisasi harus memiliki kesepakatan kontrak dengan kebutuhan keamanan yang jelas.

2.5.2.3 Asset Classification and Control

Klasifikasi dan kontrol aset merupakan kontrol organisasi akan kemampuan infrastruktur keamanan yang ada dalam menjaga aset organisasi, termasuk di dalamnya :

1. *Accountability and inventory*

Mekanisme untuk memelihara inventori aset yang akurat dan menetapkan penanggung jawab dan tanggung jawabnya terhadap semua aset.

2. *Classification*

Mekanisme mengklasifikasikan aset berdasarkan analisa dampak bisnis.

3. *Labeling*

Standar pelabelan yang jelas berdasarkan klasifikasi aset.

4. *Handling*

Standar pengendalian; termasuk di dalamnya pengenalan, *transfer*, pelepasan, dan pembuangan aset; semua berdasarkan klasifikasi aset.

2.5.2.4 Personal Security

Personal security merupakan kontrol keamanan yang bertujuan agar organisasi mampu mencegah risiko yang datang dari interaksi manusia, termasuk di dalamnya :

1. *Term and condition of employment*

Setiap karyawan berhak mendapatkan informasi yang jelas akan tanggung jawab keamanan mereka masing-masing sebagai seorang karyawan.

2. *Training*

Program pelatihan kesadaran keamanan informasi diwajibkan untuk diberikan kepada seluruh karyawan, termasuk karyawan baru.

3. *Recourse*

Proses formal untuk karyawan yang melanggar kebijakan keamanan informasi.

2.5.2.5 Physical and Environmental Security

Physical and environmental security merupakan kontrol keamanan terhadap risiko yang ada di lingkungan organisasi, termasuk di dalamnya :

1. *Location*

   Lingkungan organisasi harus mendapatkan analisa risiko lingkungan.

2. *Physical security perimeter*

   Parameter keamanan lingkungan harus diidefinisikan secara jelas dan terlihat fisiknya. Beberapa lingkungan mungkin memiliki beberapa zona berdasarkan klasifikasi *level* atau kebutuhan organisasinya.

3. *Access control*

   Setiap pelanggaran terhadap parameter keamanan harus di kontrol keluar dan masuknya dengan baik sesuai dengan klasifikasi *level*-nya.

4. *Equipment*

   Peralatan harus secara jelas diletakkan di dalam lingkungan untuk memastikan kesigapan keamanan fisik dan lingkungan organisasi.

5. *Asset transfer*

   Mekanisme aset keluar masuk berdasarkan parameter keamanan.

6. *General*

   Kebijakan dan standar, seperti penggunaan peralatan, *secure storage*, dan prinsip "*clean desk*", harus ditentukan sesuai dengan wilayan keamanan operasional.

2.5.2.6 Communications and Operations Management

Communications and operations management merupakan kontrol terhadap kemampuan organisasi untuk memastikan operasi asetnya berjalan dengan benar dan aman, termasuk di dalamnya :

1. *Operational procedures*

Kumpulan prosedur umum untuk mendukung organisasi dapat menjalankan operasinya berdasarkan standar dan kebijakan yang ada.

2. *Change control*

Proses untuk mengatur/kontrol perubahan dan konfigurasi, termasuk di dalamnya manajemen perubahan dalam *information security management system*.

3. *Segregation of duties*

Pemisahan dan perputaran jabatan dapat meminimalisir terjadinya kolusi dan korupsi.

4. *Capacity planning*

Mekanisme untuk mengontrol kapasitas organisasi untuk menghindari ketidaktersediaan layanan.

5. *System acceptance*

Metodologi untuk mengevaluasi perubahan sistem guna memastikan *confidentiality, integrity* dan *availability* tetap tersedia.

6. *Malicious code*

Kontrol akan adanya perencanaan mitigasi risiko yang datang dari *malicious code*.

7. *Housekeeping*

Kebijakan, standar, panduan, dan prosedur untuk proses *housekeeping* rutin seperti jadwal *backup* dan pencatatan *logging*.

8. *Network management*

Kontrol untuk mengatur operasi yang aman dalam infrastruktur jaringan.

9. *Media handling*

Kontrol untuk memastikan penanganan dan pembuangan *information* storage *media* berjalan dengan baik dan terdokumentasi.

10. *Information exchange*

Kontrol untuk mengatur pertukaran informasi termasuk di dalamnya persetujuan *end user*, *user* dan mekanisme *transfer* informasi.

2.5.2.7 Access Control

Access control merupakan sebuah kontrol akan kemampuan organisasi dalam mengontrol akses asetnya berdasarkan standar kebutuhan bisnis dan keamanan, termasuk di dalamnya :

1. *Business requirements*

   Kontrol kebijakan akses aset organisasi berdasarkan standar kebutuhan keamanan dan bisnis dan 'peraturan tidak tertulis' yang ada di dalam organisasi.

2. *User management*

   Mekanisme untuk pemberian, memilih, mengotrol, dan mengeluarkan karyawan beserta seluruh aset yang melekat di dalam dirinya.

3. *User responsibilities*

   Menginformasikan pengguna akan tanggung jawab masing-masing, termasuk penggunaan *password* dan peralatan kantor.

4. *Network access control*

   Kebijakan penggunaan layanan jaringan.

5. *Host access control*

   Mekanisme kontrol terhadap penggunaan terminal jaringan.

6. *Application access control*

   Pembatasan akses terhadap aplikasi berdasarkan analisa tingkatan keamanan pengguna yang dibutuhkan.

7. *Access monitoring*

   Mekanisme kontrol akses sistem untuk mendeteksi aktivitas yang tidak diijinkan.

8. *Mobile computing*

   Kebijakan dan standar penjagaan aset, akses aman, dan tanggung jawab pengguna.

2.5.2.8 System Development and Maintenance

System development and maintenance merupakan sebuah kontrol akan kemampuan organisasi dalam mengontrol keamanan

information systems telah tersambung dan terpelihara, termasuk di dalamnya :

1. *System and application security requirements*

   Menggabungkan pertimbangan keamanan informasi dalam spesifikasi kebutuhan *application development.*

2. *Cryptography*

   Kebijakan, standar, dan prosedur pengaturan penggunaan dan pemeliharaan kriptografi.

3. *System integrity*

   Mekanisme kontrol akses, dan verifikasi ketangguhan pengoperasioan *software* dan data, termasuk di dalamnya proses melacak, mengevaluasi, dan menggabungkan *asset upgrades* dan *patches*.

4. *Development security*

   Mengintegrasikan kontrol perubahan dan *technical review* ke dalam proses *development*.

2.5.2.9 Information Security Incident Management

Information security incident management merupakan sebuah kontrol untuk kemampuan organisasi menghadapi dan menyelesaikan insiden yang terjadi di dalam keamanan informasi organisasi, termasuk di dalamnya :

1. *Reporting information security events and weaknesses*

   Prosedur pelaporan kejadian formal harus tersedia dan disadari oleh setiap karyawan dan pihak ketiga lengkap dengan analisa risiko dan proses mitigasinya

2. *Management of information security incidents and improvement*

   Tindakan harus segera diberikan secepat mungkin ketika terdapat pelaporan sesuai dengan prosedur yang telah ditentukan. Proses berkelanjutan untuk monitoring dan evaluasi pun diperlukan.

2.5.2.10 Business Continuity Management

Business continuity management merupakan kontrol kemampuan organisasi menghilangkan gangguan dalam proses operasional, termasuk di dalamnya :

1. *Business continuity planning*

   Strategi perencanaan keberlanjutan proses bisnis berdasarkan analisa dampak terhadap organisasi.

2. *Business continuity testing*

   Pengetesan dan dokumentasi strategi keberlanjutan proses bisnis.

3. *Business continuity maintenance*

   Identifikasi tanggung jawab strategi keberlanjutan proses bisnis yang baik untuk memastikan proses penilaian dan perbaikan dapat dilakukan secara berkelanjutan.

2.5.2.11 Compliance

Compliance merupakan kemampuan organisasi dalam memenuhi standar kebutuhan keamanan regional, nasional maupun kontrak yang ada, termasuk di dalamnya :

1. *Legal requirement*

   Kesadaran akan peraturan regulator, *intellecetual property rights* (IPR), penjagaan data organisasi, penggunaan kriptografi dan semua kebutuhan berdasarkan peraturan yang disetujui.

2. *Technical requirement*

   Mekanisme untuk menverifikasi eksekusi penggunaan kebijakan.

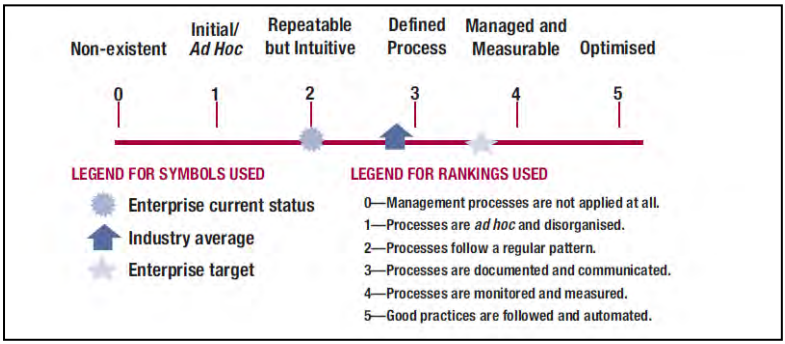
3. *System audits*

   Kontrol audit untuk memaksimalkan efektivitas, meminimalisir gangguan dan menjaga peralatan audit.

2.6 *Maturity Model* COBIT 4.1

COBIT menyediakan parameter untuk penilaian pengelolaan TI pada suatu organisasi dengan menggunakan *maturity models* yang bisa digunakan untuk penilaian kesadaran pihak pengelola (*management awareness*) dan tingkat kematangan (*maturity level*) menggunakan metode penilaian (*scoring*).

Model kematangan (*maturity models*) tersebut seperti terlihat dalam Gambar berikut:



Gambar 2.4 Contoh Grafik Penggunaan Maturity Model

1. ***Maturity level 1 – Initialized***
   Pada *maturity level* 1, proses biasanya masih berbentuk *ad hoc* (tanpa pengawasan dan arahan yang jelas).
2. ***Maturity level 2 – Managed***
   Pada *maturity level* 2, sebuah organisasi telah mencapai seluruh tujuan spesifik dan utama proses untuk berjalan.
3. ***Maturity level 3 – Defined***
   Pada *maturity level* 3, sebuah organisasi telah mencapai seluruh tujuan spesifik dan utama proses dengan komunikasi dan dokumentasi yang baik.
4. ***Maturity level 4 – Quantitatively Managed***
   Pada *maturiy level* 4, sebuah organisasi telah mencapai seluruh tujuan utama proses dengan komunikasi dan

dokumentasi yang baik ditambah dengan adanya proses pengawasan dan pengukuran capaian kinerja yang baik.

5. Maturity level 5 – Optimizing

Pada *maturity level* 5, seluruh proses dari tingkatan 1 sampai 4 telah dilaksanakan dalam organisasi dan dapat berjalan otomatis sesuai dengan *best practice* yang ada.

2.7 Indeks KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi.

Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005 [9].

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya tugas pokok dan fungsi yang ada.

Data yang digunakan dalam evaluasi ini nantinya akan memberikan *snapshot* indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan yang dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

2.8 ITIL dengan ISO 27001 dan ISO 27002

The Information Technology Infrastructure Library (ITIL) v3 memiliki presprektif utama untuk dijadikan *best practice* dalam seluruh siklus manajemen layanan. ITIL terdiri dari lima publikasi, dimana di setiap tahapannya memiliki panduan yang spesifik bagi manajemen layanan.

dokumentasi yang baik ditambah dengan adanya proses pengawasan dan pengukuran capaian kinerja yang baik.

5. Maturity level 5 – Optimizing

Pada *maturity level* 5, seluruh proses dari tingkatan 1 sampai 4 telah dilaksanakan dalam organisasi dan dapat berjalan otomatis sesuai dengan *best practice* yang ada.

2.7 Indeks KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi.

Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005 [9].

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya tugas pokok dan fungsi yang ada.

Data yang digunakan dalam evaluasi ini nantinya akan memberikan *snapshot* indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan yang dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

2.8 ITIL dengan ISO 27001 dan ISO 27002

The Information Technology Infrastructure Library (ITIL) v3 memiliki presprektif utama untuk dijadikan *best practice* dalam seluruh siklus manajemen layanan. ITIL terdiri dari lima publikasi, dimana di setiap tahapannya memiliki panduan yang spesifik bagi manajemen layanan.

ISO 27001 dan ISO 27002 dengan ITIL v3 adalah dua buah standar yang saling melengkapi. Kedua standar ini merupakan *best practice*, dimana ITIL lebih berfokus dalam manajemen layanan dan ISO 27001 berfokus pada keamanan informasi. Keduanya berdasarkan pada model *Plan-Do-Check-Act* (PDCA).

Di dalam prespektif ITIL, kebanyakan dari kontrol yang ada di ISO 27001 dan ISO 27002 telah menjadi bagian dari manajemen layanan. ISO 27002 mendefinisikan kontrol untuk manajemen risiko guna memenuhi spesifikasi keamanan organisasi.

ITIL mendefinisikan kontrol untuk manajemen risiko, memastikan bahwa nilai bisnis tercapai dan proses dapat berjalan sesuai rencana. Kedua standar ini sama-sama mengidentifkasikan keamanan diseluruh aspek layanan untuk memanajemen risiko secara efektif di seluruh bagian infrastruktur layanan.

2.8.1 Service Strategy

Service strategy berfokus untuk mendefinisikan tujuan bisnis untuk layanan yang baru ataupun yang sudah berjalan sebelumnya [10].

Terdapat beberapa faktor untuk menentukan sebuah strategi layanan dikatakan sukses atau gagal. Faktor ini mendefiniskan aset layanan apakah yang harus dieksekusi berhasil di dalam strategi layanan .

Beberapa faktor yang harus dipertimbangkan dalam *service strategy* :

1. *Availability requirements*
2. *Capacity requirements*
3. *Business and IT service continuity requirements*
4. Pemenuhan persyaratan dalam kontrak dan hukum yang berlaku
5. Penjagaan layanan dan aset layanan dengan berbagai *level* risiko

6. Memastikan akses seluruh layanan dan aset layanan telah melalui persetujuan pihak berwenang (yang bertanggung jawab)
7. Penjagaan aset dari akses yang tidak disetujui dan berbahaya.

Tabel 2.2 Referensi Manajemen Keamanan dalam Service Strategy ITIL

Standard	***Section***
ITIL v3	*Service Strategy: 6 Strategy and organization*
	Service Design: 6.4 Roles and Responsibilities
	Service Transition: 6 Organizing for Service Transition
	Service Operation: 6 Organizing for Service Transition
	Continual Service Improvement: Organization for Continual Service Improvement
ISO 27001	5.1 *Management commitment*
ISO 27002	*8.1.1 Roles and responsibilities*

2.8.2 Service Design

Service design berfokus pada proses desain layanan untuk menghubungkan antara objektif bisnis dengan fase strategi layanan. *Service design* juga berfokus dalam mengidentifikasi manajemen risiko untuk memastikan *level* risiko yang mungkin terjadi selama proses bisnis berlangsung [10].

2.8.2.1 Information Security Management

ITIL mendefinisikan kebutuhan dalam manajemen keamanan informasi adalah bagian dari *service design*.

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

ISMS digunakan untuk mengidentifikasikan kebutuhan pelaksanaan desain, implementasi , manajemen dan *maintenance* keamanan organisasi.

Di dalam prespektif ITIL, ISMS memiliki faktor :

1. Kebijakan keamanan dan kebijakan pendukung
2. *Security plan* – berisikan strategi layanan terhubung dengan objektif bisnis, hukum yang berlaku dan kebutuhan sesuai kontrak; termasuk deskripsi seluruh kontrol keamanan layanan.
3. struktur keamanan organisasi – aturan dan tanggung jawab
4. manajemen risiko keamanan
5. proses *monitoring* untuk memastikan pemenuhan aturan dan mendukung proses *feedback* yang efektif
6. strategi komunikasi dan perencanaan keamanan
7. strategi dan perencanaan pelatihan dan kesadaran keamanan bagi karyawan
8. identifikasi dan dokumentasi pengoperasian dan pemeliharaan kontrol keamanan.
9. Pertimbangan keamanan dalam kontrak dengan pihak ketiga
10. Menetapkan peningkatan *security control*, *security risk management* berkelanjutan dan meminimalisir kemungkinan risiko.

Tabel 2.3 Referensi Manajemen Keamanan dalam ISMS *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)*
ISO 27001	*4.2.1 Establish the ISMS*
ISO 27002	*6.1.1 Management commitment to information security*
	6.1.2 Information security co-ordination
	6.1.3 Allocation of information security responsibilities
	6.1.4 Authorization process for information processing facilities
	6.1.5 Confidentiality agreements

	6.1.6 Contact with authorities
	6.1.7 Contact with special interest groups

2.8.2.1.2 Authorized Services/Ports/Protocols

Meskipun ITIL dengan ISO 27001 dan ISO 27002 sama-sama tidak membahas akan pembatasan layanan, tetapi *ports* dan *protocols* hanya diijinkan untuk diakses oleh jaringan yang memiliki hubungan bisnis untuk mengefektifkan kontrol dan meminimalisir risiko infrastruktur layanan.

Aktivitas untuk menentukan *services, ports* dan *protocols* yang tepat termasuk di dalam ISMS. Pihak manajemen atas organisasi melakukan penerimaan dan memberikan rekomendasi yang digunakan pihak manajemen. Dengan membatasi penggunaan *service, ports* dan *protocols* berdasarkan dokumen persetujuan ini akan memperkecil kemungkinan risiko dan serangan terhadap layanan yang tidak diinginkan.

Setiap layanan harus dikelola sesuai dengan area keamanan yang telah ditentukan. Selain itu, infrastruktur layanan harus dilacak dengan terjadwal guna memastikan tidak adanya akses layanan yang tidak diijinkan.

Tabel 2.4 Referensi Manajemen Keamanan dalam *Authorized Services/Ports/Protocols* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)*
ISO 27001	*4.2.1 Establish the ISMS*

2.8.2.1.3 Risk Management Methodology and Guidelines

Manajemen risiko berfokus pada kemampuan mengukur dan melakukan mitigasi risiko layanan. Fokusan dari manajemen risiko adalah untuk menganalisa risiko keamanan dan kelemahan yang ada di dalam infrastruktur yang mungkin terjadi.

Risk assessment berfokus pada proses analisa ancaman dan kelemahan yang akhirnya menjadi inputan bagi *service change. Risk mitigation* merupakan proses yang berfokus untuk meminimalisir risiko yang hadir bersamaan dalam *service change* berdasarkan *level* penerimaannya.

Tabel 2.5 Referensi Manajemen Keamanan Risk *Management* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Transition: 4.6.5.9 Risk Management*
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*4.1 Assessing security risks*
	6.2.1 Identification of risks related to external parties
	10.1.2 Change management
	12.5.1 Change control procedures
	12.5.3 Restrictions on changes to software packages

2.8.2.1.4 Security Policies

Kebijakan keamanan merupakan kontrol keamanan yang mengidentifikasikan objektifitas organisasi dan bagaiman langkah pelaksanaannya untuk mendukung komitmen keamanan informasi organisasi.

Beberapa bagian dari kebijakan keamanan (tetapi tidak terbatas hanya dalam *list* ini, dimungkinkan untuk dikembangkan) :

1. *Acceptable use policy* (penggunaan aset, email dan internet)
2. *Access control policy*
3. *Password management policy*
4. *Log management policy*
5. *Asset disposal policy*

Tabel 2.6 Referensi Manajemen Keamanan *Security Policies* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.4.1 Security framework*
	Service Design: Information Security Mgmt: 4.6.4.2 The Information Security Policy
ISO 27001	*4.2.1 Establish the ISMS*
ISO 27002	*5.1.1 Information security policy document*
	5.1.2 Review of the information security policy
	7.1.3 Acceptable use of assets
	11.1.1 Access control policy
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services

2.8.2.1.5 Data Classification & Information Handling

Untuk memastikan informasi terjaga dengan baik, seluruh aset informasi harus diklasifikasikan dan aturan penggunaannya dijabarkan. Organisasi harus mendefinisikan dan mengklasifikasikan skema dan kriteria masing-masing klasifikasi.

Faktor yang harus didefinisikan :

1. *Access controls/restrictions*
2. *Copying procedures/restrictions*
3. *Storage procedures/restrictions*
4. *Encryption requirements*
5. *Data retention requirements*
6. *Restrictions on the transmission of the information*

7. *Restrictions on communication of the information*
8. *Procedures for the destruction of the information*

Tabel 2.7 Referensi Manajemen Keamanan *Data Classification* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.4.2 The Information Security Policy*
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
ISO 27001	*4.3 Documentation requirements*
ISO 27002	*7.2.1 Classification guidelines*
	7.2.2 Information labeling and handling

2.8.2.1.6 Security Plan

Rencana keamanan berisikan identifikasi yang dalam mengukur keamanan manajemen risiko keamanan informasi. Rencana keamanan dibangun sebagai bagian ISMS.

Langkah pembuatan *security plan* :

1. Identifikasi risiko
2. Analisa dan evaluasi risiko
3. Identifikasi dan evaluasi pilihan dalam penyelesaian risiko
4. Memiki kontrol penyelesaian risiko

Faktor yang harus ada di dalam *security plan* :

1. Struktur organisasi dan peraturan keamanan yang berhubungan
2. Kebijakan keamanan
3. *Software* yang digunakan
4. layanan, *port* dan *protocols* yang digunakan
5. Parameter pertahanan
6. Zona keamanan
7. Batasan pertahanan
8. Kontrol hubungan antar zona keamanan
9. Kontrol akses

10. Mekanisme ketersediaan/redundansi
11. Monitoring kejadian, kondisi dan kapasitas layanan
12. Audit catatan dan sinyal kejadian
13. Proses dan prosedur
14. Kontrol audit

Tabel 2.8 Referensi Manajemen Keamanan *Security Plan* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.4.1 Security framework*
	Service Design: Information Security Mgmt: 4.6.5.1 Security controls
	Service Design: Information Security Mgmt: 4.6.6.2 Outputs
ISO 27001	*4.2.1 Establish the ISMS*
ISO 27002	*4 Risk assessment and treatment*
	6.1.2 Information security co-ordination
	11.4.4 Remote diagnostic and configuration port protection
	11.4.5 Segregation in networks
	11.4.6 Network connection control
	11.4.7 Network routing control
	12.1.1 Security requirements analysis and specification

2.8.2.2 Capacity Management

2.8.2.2.1 Capacity Monitoring

Dengan organisasi melakukan *capacity monitoring*, akan meminimalisir risiko penurunan kualitas layanan dan ketidaktersediaan kapasitas.

Penggunaan sumber daya layanan harus dimotoring dan tindakan yang tepat harus ditentukan ketika penggunaan layanan

melebihi batasan yang telah ditentukan. Sumber daya pun harus dimonitoring untuk memastikan performanya tetap sesuai dengan yang diharapkan.

Tabel 2.9 Referensi Manajemen Keamanan *Capacity Monitoring* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Capacity Management: 4.3.5.4 The underpinning activities of Capacity Management*
	Service Design : Capacity Management: 4.3.5.5 Threshold management and control
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*10.3.1 Capacity management*

2.8.2.2.2 Capacity Review

Kapasitas dari seluruh komponen layanan harus di *review* secara rutin untuk meminimalisir risiko dari penurunan kualitas layanan dan kemungkinan kekurangan kapasitas dalam pola perubahan penggunaan.

Tabel 2.10 Referensi Manajemen Keamanan *Capacity Review* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Capacity Management: 4.3.5.7 Modelling and trending*
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*10.3.1 Capacity management*

2.8.2.3 Availability Management

2.8.2.3.1 Assessment of Risks Related to Availability

Risiko yang berhubungan dengan *availability* harus diukur secara rutin untuk memastikan layanan yang tersedia saat ini sesuai atau melebihi target yang telah ditentukan sebelumnya.

Terdapat beberapa cara untuk melakukan pendekatan penilaian risiko yang berhubungan dengan *availability*. *Information security management* berkewajiban untuk menetapkan metodologi yang tepat digunakan oleh organisasi.

Tabel 2.11 Referensi Manajemen Keamanan *Assessment Risk Related to Availability* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - page 108 Service Failure Analysis*
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - page 117 Single Point of Failure analysis
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - page 117 Fault Tree Analysis
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - page 118 Risk Analysis and Management
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*4.1 Assessing security risks*
	13.2.2 Learning from information security incidents

2.8.2.3.2 Availability Monitoring

Untuk memastikan ketersediaan layanan tidak terganggu dengan kegagalan sistem atau terjadinya insiden keamanan, dibutuhkan pengimplementasian monitoring *availability*.

ISO 27001/2 berfokus pada *confidentiality, integrity* dan *availability* aset informasi. *Availability management* dan *information security management* berbagi kebutuhan untuk

melakukan monitoring *availability*. Kategori dalam pengukuran *monitoring* adalah performa layanan, kesehatan (*health*) layanan, kapasitas layanan dan kemampuan mengidentifikasi tindakan ganjil dalam layanan.

Tabel 2.12 Referensi Manajemen Keamanan *Availability Monitoring* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces*
	Service Design: Information Security Mgmt: 4.6.6.2 Outputs
	Service Design: Information Security Mgmt: 4.6.9 Challenges, Critical Success Factors and risks
	Service Design: 4.4 Availability Management
ISO 27001	*4.2.4 Maintain and improve the ISMS*
ISO 27002	*10.10.5 Fault Logging*
	13.1.1 Reporting information security events
	13.2.1 Responsibilities and procedures
	13.2.2 Learning from information security incidents

2.8.2.4 Service Level Management

2.8.2.4.1 Security Related Service Level Targets

Kebutuhan bisnis harus mampu menjamin *Service Level RequirementI* (SLR) dan *Service Level Agreement* (SLA) tercapai. Ketika insiden terjadi, dampak yang di berikan terhadap pengoperasian sistem akan lebih besar daripada yang tertera dalam SLA. Oleh Karena itu, untuk mengukur keamanan insiden harus di definisikan dan disediakan mekanisme untuk menetapkan tipe, *volume*, dan biaya dari insiden yang terukur dan ter-*monitoring*.

Tabel 2.13 Referensi Manajemen Keamanan *Security Related Service Level Targets* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces*
	Service Design: Information Security Mgmt: 4.6.6.2 Outputs
	Service Design: 4.2 Service Level Management
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*13.2.2 Learning from information security incidents*

2.8.2.5 IT Service Continuity Management

2.8.2.5.1 Service Continuity Management Process

ITIL dan ISO 27002 keduanya mengidentifikasikan kebutuhan untuk meminimalisir dampak kegagalan atau bencana dalam komponen layanan kritis dan memastikan keberlanjutan layanan.

Kebutuhan keamanan informasi harus teridentfikasi di dalam proses *service continuity management*. Di dalam prespektif *service continuity management* proses harus terdiri dari :

1. Pengukuran risiko keberlanjutan layanan
2. Identifikasi seluruh aset dalam proses kritis bisnis
3. Identifikasi dan pertimbangan pengimplementasian kontrol pencegahan dan mitigasi risiko
4. Memastikan keamanan setiap individu dan fasilitas pemroses informasi organisasi terjaga dengan baik
5. Pembuatan dan dokumentasi dari *business continuity plan* telah membahas kebutuhan keamanan informasi
6. Adanya pengetesan dan *update regular* rencana SCM.
7. Memastikan bahwa rencana keberlanjutan manajemen bisnis tergabung dalam proses dan struktur organisasi
8. Memastikan bahwa tanggung jawab untuk proses *business continuity management* telah mencapai tingkatan yang baik di organisasi.

Tabel 2.14 Referensi Manajemen Keamanan *Service Continuity Management Process* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: 4.5 IT Service Continuity Management*
ISO 27001	*4.2.1 Establish the ISMS*
ISO 27002	*14.1.1 Including information security in the business continuity management process*

2.8.2.5.2 Service Continuity Risk Assessment

Service continuity risk harus diikuti dengan pertimbangan keamanan untuk memastikan tingkat keamanan yang dapat diterima dipertahankan ketika terjadi kesalahan.

Pengukuran *service continuity risk* berfokus dalam proses identifikasi dan pengukutan kejadian yang dapat menyebabkan gangguan proses bisnis. Skenario kejadian kesalahan harus mendefinisikan apakah kesalahan berasal dari peralatan, manusia (*human error*), pencurian, kebakaran, bencana alam dan kemungkinan terorisme.

Tabel 2.15 Referensi Manajemen Keamanan *Service Continuity Risk Assessment* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: IT Service Continuity Management: 4.5.5.2 Stage 2 - Requirements and strategy*
ISO 27001	*4.2.1 Establish the ISMS*
ISO 27002	*14.1.2 Business continuity and risk assessment*

2.8.2.5.3 Service Continuity Plan

ITIL dan ISO 27002 sama-sama mengidentifikasikan kebutuhan *service continuity plan* untuk memastikan layanan dapat dilanjutkan dalam jangka waktu yang dapat diterima.

Service continuity plan harus memuat :

1. Identifikasi setiap aturan dan tanggung jawab

2. Identifikasi prosedur *service continuity*
3. Implementasi prosedur *service continuity*
4. Prosedur operasional bersamaan dengan proses *recovery* dan *restoration* layanan
5. Dokumentasi proses dan prosedur
6. Pelatihan proses dan prosedur kepada karyawan *service continuity*
7. memastikan *testing* dan *updating service continuity plans* berjalan

Tabel 2.16 Referensi Manajemen Keamanan *Service Continuity Plan* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: IT Service Continuity Management: 4.5.5.2 Stage 3 - Implementation*
ISO 27001	*4.2.1 Establish the ISMS*
ISO 27002	*14.1.3. Developing and implementing continuity plans including information security*
	14.1.4 Business continuity planning framework

2.8.2.5.4 Testing of Service Continuity Plan

ITIL dan ISO 27002 sama-sama mendefiniskan kebutuhan untuk melakuan pengetesan *service continuity plan* secara terjadwal untuk memastikan rencana *up to date* dan berjalan efektif.

Terdapat beberapa teknis dalam melakukan testing :

1. Identifikasi desktop–dengan mengidentifikasi jalannya skenario dan *recovery and resolution plans*
2. Pengetesan proses *recovery*
3. *Recovery* alternatif
4. Pengetesan fasilitas dan layanan dari pihak ketiga
5. Percobaan pengetesan keseluruhan

Tabel 2.17 Referensi Manajemen Keamanan *Testing of Service Continuity Planning* dalam *Service Design* ITIL

Standard	***Section***
ITIL v3	*Service Design: IT Service Continuity Management: 4.5.5.2 Stage 3 - Implementation*
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*14.1.5 Testing, maintaining and re-assessing business continuity plans*

2.8.2.6 Supplier Management

2.8.2.6.1 Security Requirement Identified in Third Party Agreements

Untuk membangun keamanan informasi layanan yang di akses, proses, komunikasikan atau diurus oleh pihak eksternal, kebutuhan keamanan informasi harus diidenfikasikan dalam kontrak dengan pihak ketiga. Kontrak ini harus sesuai dengan objektivitas bisnis dan kebijakan keamanan organisasi.

Tabel 2.18 Referensi Manajemen Keamanan *Security Requirement Identified in Third Party Agreement* dalam Service Design ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputsand interfaces*
ISO 27001	*Service Design: 4.7 Supplier Management*
ISO 27002	*4.2.1 Establish the ISMS*
	6.2.1 Identification of risks related to external parties
	6.2.2 Addressing security when dealing with customers
	6.2.3 Addressing security in third party agreements
	10.2.1 Service delivery
	10.2.2 Monitoring and review of third party

	services
	10.2.3 Managing changes to third party services

2.8.3 Service Transition

Service transition berfokus dalam memastikan bahwa perubahan yang dilakukan berjalan dengan konsisten dan dengan cara yang efektif. Siklus ini juga berfokus dalam memastikan tidak ada risiko yang tidak diprediksi dalam proses perubahan.

Untuk memastikan konsistensi dan tingkat risiko dalam tingkat yang dapat diterima, informasi aset dan konfigurasi perubahan terbaru harus terjaga dan akurat sehingga keputusan tindakan perubahan dapat dilakukan secara efektif.

2.8.3.1 Release and Deployment Management

2.8.3.1.1 Risk Assessment of Proposed Released

Melakukan pengukuran risiko keamanan yang berhubungan dengan pengajuan rilis membantu organisasi untuk mengidentifikasi dan menyiapkan mitigasi risiko yang mungkin terjadi sebelum proses pengenalan sistem.

Pengukuran risiko harus dilakukan sebelum fase rilis sehingga langkah mitigasi dapat di masukkan ke dalam dokumen rencana rilis. Apabila proses rilis juga melibatkan pihak ketiga, maka analisa risiko pihak ketiga juga harus dilakukan.

Tabel 2.19 Referensi Manajemen Keamanan *Release and Deployment Management* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Transition: Evaluation: 4.6.5.9 Risk Management*
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management

ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*4.1 Assessing security risks*
	6.2.1 Identification of risks related to external parties
	12.1.1 Security requirements analysis and specification
	12.4.2 Protection of system test data
	12.5.5 Outsourced software development

2.8.3.2 Asset & Configuration

2.8.3.2.1 Asset Inventory

Identifikasi yang akurat akan data inventaris organisasi terkini sangat penting untuk memastikan penjagaan yang tepat bagi aset telah terimplementasi. ISO 27001 mendefinisikan aset adalah segala sesuatu yang memiliki nilai bagi organisasi. ITIL mendefinisikan tipe aset terdiri dari :

1. Manajemen
2. Organisasi
3. Proses
4. *Knowledge*
5. Manusia / karyawan
6. Informasi
7. Aplikasi
8. Infrastruktur
9. Kekayaan organisasi

Sedangkan ISO 27002 mendefinisikan aset tambahan seperti reputasi organisasi. Keduanya, ITIL dan ISO 27002 menyatakan identifikasi aset harus didefinisikan dengan jelas.

Tabel 2.20 Referensi Manajemen Keamanan *Asset Inventory* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)*
	Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective
	Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business
	Service Transition: Service Asset and Configuration Management: 4.3.4.2 Basic concepts
	Service Transition: Service Asset and Configuration Management: 4.3.4.3 Configuration Management System
	Service Transition: Service Asset and Configuration Management: 4.3.5.3 Configuration identification
ISO 27001	*4.2.1 Establish the ISMS*
ISO 27002	*7.1.1 Inventory of assets*
	7.1.2 Ownership of assets

2.8.3.2.2 Asset Review

Fokus dalam proses *asset review* adalah untuk memastikan informasi aset (konfigurasi, kepemilikan, status, lokasi, dll) telah lengkap dan sesuai dengan keadaan asli/*real* aset di lingkungan orgamisasi.

Tabel 2.21 Referensi Manajemen Keamanan *Asset Review* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)*
	Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective
	Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business
	Service Transition: Service Asset and Configuration Management: 4.3.5.6 Verification and audit
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*7.1.1 Inventory of assets*
	7.1.2 Ownership of assets

2.8.3.2.3 Secure Baseline

Dengan menentukan batasan aman organisasi, risiko peralatan aplikasi dapat berkurang sesuai dengan keadaan jaringan dan parameter pertahanan kebijakan keamanan organisasi.

Batas aman konfigutasi harus dibangun untuk setiap tipe komponen dalam proses pembangunannya. Pengukuran risiko untuk setiap tipe komponen sangat direkomendasikan untuk mengetahui risiko aktual layanan.

Tabel 2.22 Referensi Manajemen Keamanan *Secure Baseline* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Transition: Configuration Management 4.3.5.3 Configuration identification - page 77 Identification of configuration baselines*
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.6.1 Network controls*
	10.10.1 Audit logging
	11.3.1 Password use
	11.4.1 Policy on use of network services
	11.5.1 Secure log-on procedures
	11.5.5 Session time-out
	11.5.6 Limitation of connection time
	12.1.1 Security requirements analysis and specification
	12.4.1 Control of operational software
	12.6.1 Control of technical vulnerabilities

2.8.3.2.4 Clock Syncronization

ITIL dan ISO 27002 keduanya menyarankan untuk seluruh peralatan dan aplikasi yang terhubung memiliki sinkronisasi waktu yang sama. Sinkronisasi waktu ini akan berguna dalam proses investigasi kejadian yang melewati multi-sistem aplikasi.

Clock syncrinization adalah bagian penting dalam *audit log data* baik dalam proses perbaikan atau mengidentfikasi korelasi kejadian kasus penyalahgunaan dan pendisiplinan.

Tabel 2.23 Referensi Manajemen Keamanan *Clock Syncronization* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Transition: Service Asset and Configuration*

	Management: 4.3.5.3 Configuration identification
	Service Operation : Event Management : 4.1.5.6 Event correlation
ISO 27001	*ISO 27001 4.2.2 Implement and operate the ISMS*
ISO 27002	*ISO 27002 10.10.6 Clock synchronization*

2.8.3.2.5 Configuration Control

ITIL dan ISO 27002 keduanya menyatakan kebutuhan untuk mencatat konfigurasi setiap waktu sangatlah penting karena beberapa proses dalam ITIL berdasarkan pada catatan *historical configuration data*.

Incident management menggunakan *configuration back-up* untuk mengembalikan sistem setelah terjadinya kesalahan. *Problem management* menggunakan *historical configurations* untuk mencari tahu akar asal terjadinya masalah. *Release and deployment management* menggunakan *current configurations* untuk menrencanakan rilis versi terbaru. *Information security management* menggunakan data konfigurasi untuk mengukur risiko infrastruktur.

Ketika sebuah konfigurasi dilakukan, salinan dari konfigurasi harus disimpan dan mendapatkan label berdasarkan tanggal pelaksanaan konfigurasi.

Tabel 2.24 Referensi Manajemen Keamanan *Configuratin Control* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*ITIL v3 Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)*
	Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective
	Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business

	Service Transition: Service Asset and Configuration Management: 4.3.4.3 Configuration Management System
	Service Transition: Service Asset and Configuration Management: 4.3.5.4 Configuration control
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.1.2 Change management*
	13.2.1 (Management of information security incidents and improvements) Responsibilities and Procedures
	12.5.1 Change control procedures

2.8.3.2.6 Verification of Actual Configuration

Sebelumnya telah diketahui bahwa konfigurasi yang baik adalah konfigurasi yang mampu menampilkan gambaran konfigurasi sesuai seperti ketika di lakukan pengetesan dan sesuai dengan persyaratan konfigurasi, sebagai contoh sebelum proses konfigurasi, akan dijelaskan bagaimana kondisi ideal saat proses *deploy* dilakukan. Konfigurasi dari pengetesan keamanan terakhir akan mempengaruhi standar konfigurasi atau batasan aman dari penilaian pelaksanaan konfigurasi.

Tidak boleh adanya risiko yang tidak terduga dalam infrastruktur membuat konfigurasi harus dipastikan sesuai dengan kebijakan keamanan organisasi dan kebijakan manajemen perubahan. Pengecekan mandiri akan konfigurasi juga disarankan untuk dilakukan.

Pelaksanaan konfigurasi yang sebenarnya harus sesuai dengan standar konfiguasi, ketika diperlukan perubahan, harus mendapatkan persetujuan terlebih dahulu.

Tabel 2.25 Referensi Manajemen Keamanan *Verification of Actual Configuration* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*ITIL v3 Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)*
	Service Transition: Service Asset and Configuration Management: 4.3.5.4 Configuration control
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.1.2 Change management*
	12.5.1 Change control procedures

2.8.3.3 Service Validation And Testing

2.8.3.3.1 Security Acceptance Testing

ITIL dan ISO 27002 mengidentifikasikan kebutuhan pelaksanaan perubahan berdasarkan kebutuhan implementasi telah sesuai dengan persyaratan dan kebutuhan organisasi. Proses ini termasuk proses verifikasi bahwa perubahan tidak akan terganggu oleh risiko yang tidak teranalisa sebelumnya.

Information security management bertanggung jawab dalam menentukan bentuk pengetesan apakah yang cocok digunakan berdasarkan lingkungan dan ruang lingkup sistemnya.

Security acceptance tests untuk aplikasi, *operating systems* dan *network operating systems* harus termasuk dari *penetration testing, vulnerability scan* dan atau *port scan.* Hal ini penting untuk dilakukan guna memastikan informasi/aset yang dimiliki oleh organisasi tidak bocor.

Tabel 2.26 Referensi Manajemen Keamanan *Security Acceptance Testing* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*ITIL v3 Service Transition: Service Validation and Testing: 4.5.4.10 Types of testing - Table 4.2 Examples of Service Management manageability tests*

ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.3.2 System acceptance*
	12.2.1 Input data validation
	12.2.2 Control of internal processing
	12.2.3 Message Integrity
	12.2.4 Output data validation
	12.5.4 Information leakage

2.8.3.4 Change Management

Fokusan dari *change management* baik dalam ITIL maupun ISO 27002 adalah untuk meminimalisir risiko (bisnis dan keamanan) berdasarkan perubahan yang dilakukan.

2.8.3.4.1 Change Approval

Dalam ITIL maupun ISO 27002, *change approval* merupakan hal kritis dalam pelaksanaan kontrol audit untuk memastikan bahwa perubahan yang dilakukan tidak memberikan dampak risiko terhadap infrastruktur.

Dari prespektif keamanan, setiap pengajuan perubahan memerlukan evaluasi untuk menentukan apakah pengukuran keamanan diperlukan dalam perubahan tersebut atau tidak.

Tabel 2.27 Referensi Manajemen Keamanan *Change Approval* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*ITIL v3 Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces*
	Service Transition: 4.2 Change Management
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.1.2 Change management*
	12.5.1 Change control procedures

	12.5.2 Technical review of applications after operating system changes
	12.5.3 Restrictions on changes to software packages

2.8.3.4.2 Risk Assessment of Proposed Change

Penilaian risiko dalam ketersediaan dan atau keamanan layanan harus dilakukan dalam RFC yang disetujui. Perubahan penting yang dilakukan setelah terjadinya *problem* akan memberikan risiko yang besar, sebaliknya perubahaan sebelum pelaksanaan pembangunan infrastruktur relatif lebih kecil.

Information security management memiliki kewajiban penting dalam mengukur setiap perubahan. Secara khusus *Information security management* berfokus pada proses memastikan bahwa penilaian risiko yang tepat telah dilakukan sebelum persetujuan perubahan diusulkan.

Tabel 2.28 Referensi Manajemen Keamanan *Risk Assessment of Proposed Change* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Transition: 4.2 Change Management*
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*4.1 Assessing security risks*
	6.2.1 Identification of risks related to external parties
	10.1.2 Change management
	12.5.1 Change control procedures
	12.5.3 Restrictions on changes to software packages

2.8.3.4.3 Update Log Management System

Log data merupakan *input* penting dalam ITIL *event management* dan menyimpan *log data* merupakan kewajiban dalam ISO 27002. Kebijakan *log management* organisasi menentukan *logging requirement* dan jarak waktu/periode pelaksanaan *back-up log data.*

Pengimplementasian rencana pelaksanaan perubahan harus mengikuti aturan dalam *configure collection data log* semaksimal mungkin. Hal ini akan mengurangi risiko kehilangan *log data* atau kegagalan konfigurasi data.

Tabel 2.29 Referensi Manajemen Keamanan *Update Log Management System* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*ITIL v3 Service Transition: Change Management: 4.2.6 Process activities, methods and techniques*
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.10.1 Audit logging*
	10.10.3 Protection of log information
	10.10.4 Administrator and operator logs
	10.10.5 Fault logging

2.8.3.4.4 Update Configuration Management Database **(CMDB)**

Setiap pengimplementasian rencana perubahan harus memasukkan juga langkah *update configuration management database* (CMDB) untuk merefleksikan perubahan apa sajakah yang telah berhasil dalam sistem.

CMDB berisikan *configuration items* (CI) yang digunakan dalam prosedur dam proses. Aset informasi yang memiliki CMDB pendukung proses lainnya, perlu dipastikan konfigurasi asetnya tetap aktual dan akurat.

Tabel 2.30 Referensi Manajemen Keamanan *Update* CMDB dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Transition: 4.2 Change Management*
	Service Transition: Service Asset and Configuration Mgmt: 4.3.1 Purpose, goal and objectives
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*7.1.1 Inventory of assets*
	7.1.2 Ownership of assets
	12.6.1 Control of technical vulnerabilities

2.8.3.4.5 Post-Change Security Verification

Post-change security verification merupakan kontrol audit untuk memastikan bahwa tidak ada risiko tambahan yang muncul dari hasil pelaksanaan perubahan.

Tabel 2.31 Referensi Manajemen Keamanan *Post-Change Security Verification* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Transition: Service Validation and Testing: 4.5.4.10 Types of testing -Table 4.2 Examples of Service Management manageability tests*
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.3.2 System acceptance*
	12.2.1 Input data validation
	12.2.2 Control of internal processing
	12.2.3 Message Integrity
	12.2.4 Output data validation
	12.5.4 Information leakage

2.8.3.4.6 Change Reconciliation

ITIL dan ISO 27002 mengidentifikasikan kebutuhkan pengukuran kesesuaian perubahan dengan kebijakan dan proses perubahan. *Change reconciliation* merupakan sebuah kontrol audit untuk memastikan bahwa seluruh perubahan terimplementasi dalam infrastruktur sistem sesuai yang telah disepakati.

Dalam rangka memastikan *change reconciliation* yang aktual, semua catatan perubahan konfigurasi dari perangkat dan *log* aplikasi harus di-ekstrak dan di petakan setiap perubahan/permintaan yang disetujui untuk melakukan perubahan. Jika perubahan tidak sesuai dengan RFC, maka pihak yang berwenang harus membuat laporan insiden.

Tabel 2.32 Referensi Manajemen Keamanan *Change Reconciliation* dalam *Service Transition* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces*
	Service Transition: 4.2 Change Management
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*10.1.2 Change management*
	10.10.3 Protection of log information
	12.5.1 Change control procedures

2.8.3.5 Knowledge Management

2.8.3.5.1 Security Awareness Education & Training

Kesadaran keamanan merupakan bagian kritis dari kontrol keamanan. Jika karyawan, kontraktor dan pengguna pihak ketiga tidak menpraktekkan kewajiban sesuai kebijakan keamanan maka risiko yang belum dianalisa sebelumnya akan muncul di dalam infrastruktur.

ITIL dan ISO 27002 mengidentifikasikan kebutuhan akan pendidikan dan pelatihan kesadaran keamanan. Pelatihan

kesadaran keamanan organisasi seharusnya dilaksanakan secara berkala (biasanya per tahun) untuk memastikan pencapaian persyaratan hukum/kebijakan keamanan.

Tujuan dari pendidikan dan pelatihan kesadaran keamanan adalah untuk meminimalisir risiko yang mungkin terjadi dalam interaksi atau kesalahan manusia (*human error*) dengan meningkatkan kesadaran karyawan, kontraktor dan pengguna pihak ketiga akan ancaman yang ada sesuai dengan kewajiban masing-masing. Selain itu, pelatihan juga bertujuan untuk memastikan pengguna menyadari penggunaan alat-alat pendukung kebijakan keamanan organisasi.

Pelatihan dan pendidikan ini diharapkan mampu membuat pengguna sadar apa yang harus dilakukan atau bagaimana cara mengerjakan tugas mereka dengan aman dan mereka sadar akan kewajiban mereka melaporkan setiap kesalahan dan insiden berdasarkan prosedur yang sudah ditentukan.

Tabel 2.33 Referensi Manajemen Keamanan *Knowledge Management* dalam *Service Transition* ITIL

Standar	***Section***
ITIL v3	*Service Transition: 4.7 Knowledge Management*
ISO 27001	*5.2.2 Training, awareness and competence*
ISO 27002	*8.2.1 Management responsibilities*
	8.2.2 Information security awareness, education, and training
	2.8.4 Disciplinary process

2.8.4 Service Operation

Service operation berfokus pada bagaimana cara mengatur dan mendukung pelaksanaan layanan berdasarkan setiap *service level* yang telah disetujui.

2.8.4.1 Event Management

2.8.4.1.1 Event Logging

Peralatan dan aplikasi harus dikonfigurasikan ke dalam catatan kegiatan/*event logging* untuk mempermudah deteksi masalah dan aktivitas yang tidak diijinkan di dalam infrastruktur layanan.

Log data harus dijaga untuk melawan akses yang tidak diinginkan. *System administrators* tidak boleh melakukan penghapusan catatan aktivitasnya. Jika tidak dimungkinkan, *log data* harus dirujuk dengan *remote log repository*.

Wewenang *Log data repository* tidak boleh berada di bawah orang yang menjalankan sistem tersebut secara langsung (harus adanya pembedaan antara tugas dan kewajiban).

Tabel 2.34 Referensi Manajemen Keamanan *Event Logging* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Event Management: 4.1.5.2 Event notification*
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.10.1 Audit Logging*
	10.10.2 Monitoring system use
	10.10.3 Protection of log information
	10.10.4 Administrator and operator logs
	10.10.5 Fault logging
	10.10.6 Clock synchronization

2.8.4.1.2 Health and Performance Monitoring

Information security management dan *availability management* keduanya sama-sama berkonsentrasi dalam ketersediaan layanan dan informasi di organisasi sehingga *monitoring* kesiapan dan performa layanan termasuk ke dalam *security control*.

Availability management berkonsentrasi untuk mendefinisikan langkah *monitoring* spesifik yang sesuai dengan kebutuhan layanan. *Monitoring* ketersediaan dan perfoma harus terhubung dalam pengukuran *availability management* dan secara otomatis berubah menjadi laporan insiden ketika batasan atau kesalahan telah dilewati.

Tabel 2.35 Referensi Manajemen Keamanan *Health and performance monitoring* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Event Management: 4.1.5.2 Event notification*
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.6.1 Network controls*

2.8.4.1.3 Event Correlation & Alerting

Network monitoring systems dapat dilihat dari tingkat *volume* data secara signifikan. Dalam satu waktu, sebuah sistem dimungkinkan mengubah banyak *log message*.

Menghubungkan *event monitoring correlation* secara otomatis akan membantu dalam menyaring data untuk mengidentifikasikan *event* dalam organisasi secara signifikan.

Penggunaan penanda/*alert* dalam *event correlation* sangat membantu. Biasanya, ketika sebuah *event* terjadi, maka *alert* akan langsung berkolerasi. Pilihan *alert* yang digunakan dapat berupa pencatatan *logging*, mengirimkan *alert* ke dalam *ticketing system*, mngirim *email* atau mengeksekusi program langsung ketika kejadian terjadi.

Tabel 2.36 Referensi Manajemen Keamanan *Event Correlation & Alerting* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Event Management: 4.1.5.4 Event filtering*
	Service Operation: Event Management: 4.1.5.5 Significance of events
	Service Operation: Event Management: 4.1.5.6 Event correlation
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.6.1 Network controls*

2.8.4.1.4 Periodic Review of Security Events

Security event correlation systems yag rumit seperti pendeteksian gangguan dan sistem *security information and event management* (SIEM) harus mampu menproses beberapa kejadian keamanan untuk mendeteksi kejanggalan.

Sistem ini sebenarnya mampu untuk merubah *alert* secara langsung, akan tetapi beberapa *security events* harus melalui pantauan langsung dari manusia. Direkomendasikan bila dimungkinkan dilakukan *review* harian pelaksanaan keamanan.

Tabel 2.37 Referensi Manajemen Keamanan *Periodic Review of Security Events* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Event Management: 4.1.5.5 Significance of events*
	Service Operation: Event Management: 4.1.5.6 Event correlation
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.4.1 Controls against malicious code*
	13.1.1 Reporting information security events

	13.1..2 Reporting security weaknesses
	10.10.2 Monitoring system use

2.8.4.2 Incident Management

2.8.4.2.1 Incident Response Procedures

Prosedur respon insiden formal sangat penting untuk merespon masalah keamanan yang berhubungan dengan insiden. Selain untuk mengurangi waktu perbaikan, penggunaan prosedur respon insiden formal juga mengurangi dampak potensial insiden terhadap organisasi.

Dalam dokumen analisa insiden biasanya terdiri dari macam insiden dan tingkat insiden, kemudian bagaimana langkah responnya dan keterangan keutamaan atau keuntungan dari masing-masing aktivitas responnya.

Tabel 2.38 Referensi Manajemen Keamanan *Incident Response Procedures* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Incident Management: 4.2.5.3 Incident categorization*
	Service Operation: Incident Management: 4.2.5.7 Investigation and Diagnosis
	Service Operation: Incident Management: 4.2.5.8 Resolution and Recovery
ISO 27001	*4.2.2 Implement and operate the ISMS*
ISO 27002	*10.1.1 Documented operating procedures*
	13.2.1 Management of information security incidents and improvements Responsibilities and procedures

2.8.4.3 Problem Management

2.8.4.3.1 Post Incident Management (PIR)

Tujuan dari pelaksanaan *review* setelah terjadinya insiden adalah untuk mengukur ke-efektivitasan proses deteksi, respon,

dan analisa seluruh kegiatan manajemen keamanan insiden dan identifikasi tindakan yang cocok apabila insiden terjadi atau kejadian insiden terjadi kembali, untuk meminimalisir dampak bagi kejadian insiden kedepannya.

Meskipun pelaksanaan *review* setelah terjadinya insiden (PIR) tidak dijelaskan secara eksplisit dalam ITIL dan ISO 27002, tetapi keduanya mengkritisi untuk mengadakan kegiatan yang dapat memastikan keamanan informasi.

Organisasi dimungkinkan menemui sebuah insiden yang membutuhkan proses investigasi lanjutan atau kemungkinan insiden terulang lebih besar. PIR membantu organisasi dalam meningkatkan hubungan komunikasi antara pengguna dengan mendemonstrasikan fungsi pengguna terhadap bisnis.

PIR insiden minimal terdiri dari faktor berikut :

1. Layanan dan pengguna yang melapor
2. Waktu terjadi insiden
3. Waktu insiden berhasil diselesaikan
4. Deskpripsi tanda terjadinya insiden
5. Apa yang harus dilakukan; siapa yang melaksanakan
6. *Post incident analysis*
7. Tindakan untuk mencari akar permasalahan insiden
8. Identifikasi lingkungan; bila diperlukan
9. Identifikasi tindakan perbaikan; bila diperlukan

Tim keamanan memegang tanggung jawab penuh dalam pengimplementasian PIR. Tindakan perbaikan bisa meliputi tindakan perubahan konfigurasi, implementasi, tambahan monitoring, hingga perubahan kebijakan/prosedur.

Tabel 2.39 Referensi Manajemen Keamanan PIR dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Problem Management: 4.4.5 Process activities, methods and techniques*
ISO 27001	*4.2.3 Monitor and review the ISMS*

ISO 27002	*13.2.2 Learning from information security incidents*

2.8.4.3.2 Security Advisories and Vendor Patch Review

Melakukan perbaikan terhadap kelemahan-kelemahan keamanan yang ditemukan dapat mengurang risiko terjadinya insiden dengan menemukan beberapa kelemahan yang belum diketahui sebelumnya.

Pelaksanaan *regular review* berdasarkan rekomendasi keamanan dan *vendor patch review* dapat membantu keamanan organisasi lebih cepat .

Terdapat dua pendekatan dalam pelaksanaan *security advisories and vendor patch review* yatu *centralized patch management* dan *distributed patch management*.

Tabel 2.40 Referensi Manajemen Keamanan *Security Advisories and Vendor Patch Review* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Problem Management: 4.4.5.1 Problem detection*
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*6.1.7 Contact with special interest groups*
	10.4.1 Controls against malicious code
	12.1.1 Security requirements analysis and specification
	12.6.1 Control of technical vulnerabilities

2.8.4.4 Request Fulfillment Management

2.8.4.4.1 Verification of Requester's Credentials

Pengguna mengajukan *service request* untuk meminta layana *service catalog* atau informasi akan layanan tersebut. Sebelum proses permintaan layanan, permintaan yang diidentifikasikan harus diverifikasi dengan dasaran yang telah disepakati.

Proses verifikasi permintaan ini dapat mengurangi risiko kehilangan atau bahaya organisasi yang muncul dalam proses pemenuhan layanan atau informasi berdasarkan kewenangan tiap individu.

Tabel 2.41 Referensi Manajemen Keamanan *Request Fulfillment Management* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Request Fulfillment: 4.3.5.3 Other approval*
	Service Operation: Access Management: 4.5.5.1 Requesting access
	Service Operation: Access Management: 4.5.5.2 Verification
ISO 27001	*4.2.2 Establish and operate the ISMS*
ISO 27002	*7.1.3 Acceptable use of assets*
	11.1.1 Access control policy
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services

2.8.4.5 Access Management

2.8.4.5.1 Request for Access

ITIL dan ISO 27002 mengidentifikasikan kebutuhan untuk adanya prosedur yang menjamin akses ke dalam aset informasi. Seluruh permintaan akses aset informasi harus melewati proses persetujuan terlebih dahulu dan percobaan *audit* untuk menghindari adanya akses aset informasi yang tidak diijinkan.

Prosedur permintan akses harus berisikan proses verifikasi identitas yang mengajukan permintaan dan ketetapan bisnis dalam akses aset seperti mekanisme formal penerimaan permintaan.

Informasi audit yang harus termuat dalam *request for access*:

1. Nama pengaju permintaan akses
2. Waktu pengajuan
3. Status (*waiting for approval/approved/denied*)
4. *Approver*
5. Waktu penerimaan
6. Penilaian terhadap pengajuan permintaan
7. Kurun waktu akses
8. Orang yang memenuhi permintaan

Tabel 2.42 Referensi Manajemen Keamanan *Request for Access* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Request Fulfillment: 4.3.5.3 Other approval*
	Service Operation: Access Management: 4.5.5.1 Requesting access
	Service Operation: Access Management: 4.5.5.2 Verification
ISO 27001	*4.2.2 Establish and operate the ISMS*
ISO 27002	*7.1.3 Acceptable use of assets*
	11.1.1 Access control policy
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services

2.8.4.5.2 Revocation of Access Rights

Untuk menghindari akses aset informasi yang tidak diijinkan, perlu untuk dibuatkan prosedur formal mengembalikan hak akses aset informasi terutama ketika sudah tidak lagi digunakan. Prosedur ini juga harus memuat langkah percobaan audit serangan terhadap seluruh aturan akses.

Prosedur pengembalian aturan akses harus memuat percobaan audit, identifikasi dampak penggunaan, waktu pengajuan permintaan akses, permintaan akses, daftar akses yang diijinkan, waktu pengembalian akses dan pengguna yang mengaplikasikan aturan perubahan akses.

Tabel 2.43 Referensi Manajemen Keamanan *Revocation of Access Rights* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Access Management: 4.5.5.2 Verification*
	Service Operation: Access Management: 4.5.5.6 Removing or restricting rights
ISO 27001	*4.2.2 Establish and operate the ISMS*
ISO 27002	*11.1.1 Access control policy*
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services

2.8.4.5.3 Periodic Review of Access Right

Untuk menverifikasi aturan dalam kebijakan akses kontrol organisasi, kebijakan akses pengguna harus diulas secara berkala. Proses ulasan aturan akses harus meliputi verifikasi akses apakah akses tidak digunakan lagi, pengguna sedang keluar area kantor untuk jangka waktu tertentu atau pengguna sedang keluar dari area organisasi.

Tabel 2.44 Referensi Manajemen Keamanan *Periodic Review of Access Right* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Access Management: 4.5.5.5 Logging and tracking access*
ISO 27001	*4.2.3 Monitor and review the ISMS*

ISO 27002	*11.1.1 Access control policy*
	11.2.4 Review of user access rights
	11.2.2 Privilege Management
	15.2.1 Compliance with security policies and standards
	15.2.2 Technical compliance checking

2.8.4.5.4 Periodic Review of Access Attempts

Dalam jangka waktu tertentu, *review* proses percobaan (berhasil dan gagal) dalam mengakses aset informasi harus dilakukan untuk meminimalisir potensi kehilangan dan atau bahaya dari aktivitas yang tidak diijinkan. Percobaan akses yang tidak biasa akan menjadi indikator persetujuan sistem lanjutan.

Ketika aktivitas anomali terdeteksi, dibuatlah laporan insiden. *Review* dari proses percobaan ini terdiri dari aktivitas percobaan beserta kejadian dari hasil percobaan tersebut (*events of interest*).

Tabel 2.45 Referensi Manajemen Keamanan *Periodic Review of Access Attempts* dalam *Service Operation* ITIL

Standar	***Section***
ITIL v3	*Service Operation: Access Management: 4.5.5.5 Logging and tracking access*
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*11.1.1 Access control policy*
	15.2.1 Compliance with security policies and standards
	15.2.2 Technical compliance checking

2.8.5 Continual Service Improvement

Continual Service Improvement berfokus pada bagaimana cara memastikan bahwa layanan dapat berlanjut penggunaan dan perkembangannya dengan tetap memenuhi kebutuhan organisasi di seluruh fase layanan.

2.8.5.1 Review Effectiveness of Process

Pelaksanaan *review* di seluruh proses layanan dilakukan untuk memastikan bahwa keberlanjutan layanan dapat berjalan secara efektif dan efisien dengan tetap melakukan peningkatan mengikuti perubahan kebutuhan bisnis dari waktu ke waktu.

Fokusan dalam periode pelaksanaan *review* adalah mencari tahu opsi peningkatan yang ada, termasuk di dalamnya, proses yang dianggap tidak efektif akan dihapuskan. Hal ini dilakukan karena ketidaksesuaian proses akan mengakibatkan pengurangan performa proses atau kekurangan dalam penguasaan proses.

Proses *review* menggunakan inputan utama data langsung dari pengguna layanan karena mereka adalah pengguna yang langsung terkena dampak dari ketidak efentifitasan layanan.

Tabel 2.46 Referensi Manajemen Keamanan *Review Effectiveness of Process* dalam *Continual Service Improvement* ITIL

Standar	***Section***
ITIL v3	*All ITIL v3 processes*
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*6.1.1 Management commitment to information security*
	15.2.1 Compliance with security policies and standards

2.8.5.2 Review of Security Policies

Untuk memastikan kesesuaian kebutuhan organisasi dengan hukum dan regulasi yang berlaku, ITIL dan ISO 27002

merekomendasikan kebijakan keamanan organisasi diulas secara berkala untuk memperbarui kemungkinan kebutuhannya.

ITIL merekomendasikan bahwa kebijakan keamanan minimal di-*review* satu tahun satu kali, atau ketika :

1. Adanya pembaharuan atau perubahan kebutuhan keamanan
2. Insiden keamanan yang mengindikasikan adanya celah dalam kebijakan keamanan
3. Adanya ancaman dan serangan baru
4. Hasil dari *security review* atau *audit*

Tabel 2.47 Referensi Manajemen Keamanan *Review of Security Policies* dalam *Continual Service Improvement* ITIL

Standar	***Section***
ITIL v3	*Service Design: Information Security Management: 4.6.4.2 The Information Security Policy*
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*5.1.1 Information security policy document*
	5.1.2 Review of the information security policy
	15.1.1 Identification of applicable legislation
	15.1.4 Data protection and privacy of personal information

2.8.5.3 Preventive/Corrective Action Management

Aksi perbaikan dan pencegahan harus diidentifikasikan dalam kebanyakan proses penjaminan layanan. Aktivitas dalam proses perbaikan dan pecegahanan lebih efektif dikembangkan dan diaplikasikan dalam infrastruktur sistem. Biasanya tim operasional telah menyediakan masing-masing daftar tindakan yang dapat dilakukan untuk perbaikan dan pencegahan.

Pihak auditor menginginkan bukti pelaksanaan tindakan perbaikan/pencegahan yang teridentifikasi, memiliki daftar prioritas yang jelas, terarah dan lengkap dengan garis hubungan yang jelas antar nilai bisnis dan kebijakan kemanan yang objektif.

Tabel 2.48 Referensi Manajemen Keamanan *Preventive/Corrective Action Management* dalam *Continual Service Improvement* ITIL

Standar	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques*
	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
ISO 27001	*4.2.3 Monitor and review the ISMS*
	4.2.4 Maintain and improve the ISMS
	8 ISMS improvement
ISO 27002	*13.2.2 Learing from information security incident*

2.8.5.4 Non-Conformance Management

Kebijakan organisasi telah mengidentifikasikan bagaimana risiko dapat ditolerir dengan efektif. Kebijakan biasanya terarah, berisi beberapa larangan, kewajban memenuhi persyaratan hukum, serta langkah me-minimalisir risiko dan biaya. Hal ini dilakukan karena kesalahan dalam kebijakan akan meningkatkan risiko bagi organisasi.

Untuk mempertemukan kebutuhan, antara ITIL dan ISO 27001 dengan 27002 seluruh ketidak sesuaian kebijakan, standar, proses atau prosedur harus di laporkan. Ketidak sesuaian dapat dilaporkan oleh *end user*, *IT support and administrators*, *process manager* atau siapapun yang berinteraksi dengan sistem. Kesalahan pengguan atau tindakan yang tidak sesuai kebijakan termasuk ke dalam laporan ketidaksesuaian.

ITIL dan ISO 27001/2 keduanya menyatakan bahwa *review* dan *monitoring* merupakan kunci untuk meningkatkan performa. Informasi dalam laporan aan membantu organisasi mengidentifikasikan titik/sistem yang membutuhkan peningkatan.

Auditor harus memastikan sebelumnya organisasi telah memiliki kebijakan dan prosedur pelaporan dan pengaturan

ketidaksesuaian. Kesalahan untuk mengikuti kebijakan/ proses/prosedur mengindikasikan bahwa revisi harus dilakukan oleh organisasi.

Tabel 2.49 Referensi Manajemen Keamanan *Non-Conformance Management* dalam *Continual Service Improvement* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques*
	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
ISO 27001	*4.2.3 Monitor and review the ISMS*
	4.2.4 Maintain and improve the ISMS
ISO 27002	*15.2.1 Compliance with security policies and standards*
	15.2.2 Technical compliance checking

2.8.5.5 Security Risk Assessments

.Penilaian risiko secara berkala dapat membantu organisasi mengidentifikasikan dan mencari tahu langkah mitigasi yang cocok dan dibutuhkan untuk mengurangi risiko hingga ke tingkat/*level* yang dapat diterima oleh organisasi.

Aktivitas dalam penilaian risiko keamanan termasuk identifikasi tingkat penerimaan risiko, menghitung dan membuat daftar prioritas risiko, serta menentukan langkah mitigasi risiko.

Tabel 2.50 Referensi Manajemen Keamanan *Security Risk Assessment* dalam *Continual Service Improvement* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques*
ISO 27001	*4.2.1 Establish the ISMS*
	4.2.3 Monitor and review the ISMS

ISO 27002	*4.1 Assessing security risks*
	4.2 Treating security risks
	9.1.1 Physical security perimeter
	10.6.2 Security of network services
	14.1.2 Business continuity and risk assessment
	15.2.2 Technical compliance checking

2.8.5.6 Technical Infrastructure Review

Untuk memastikan sistem telah memenuhi seluruh persyaratan hukum berdasarkan kebijakan dan standar, ISO 27001 mengidentifikasikan kebutuhan untuk melakukan *technical infrastructure review* secara berkala.

Penyampaian hasil *technical infrastructure review* termasuk laporan hasil temuan, rekomendasi aksi perbaikan dan pencegahan untuk ssetiap ketidaksesuaian yang terdeteksi akan dilaporkan dan dijadikan dasaran untuk pengembangan layanan selanjutnya.

Tabel 2.51 Referensi Manajemen Keamanan *Technical Infrastucture Review* dalam *Continual Service Improvement* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques*
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*10.10.2 Monitoring system use*
	15.2.2 Technical compliance checking

2.8.5.7 Independent Security Review

Untuk memastikan manajemen keamanan di dalam infrastruktur layanan berjalan efektif, *independent review* harus dilakukan secara berkala ketika perubahan yang signifikan diperlukan dalam sistem yang telah dijalankan.

Pelaksana *review* harus dilakukan di bawah tanggung jawab bagian/orang yang memiliki tanggung jawab di area tersebut (tim tertentu, internal maupun eksternal).

Review dapat dilakukan untuk seluruh proses sistem maupun hanya berfokus pada satu komponen spesifik. Ruang lingkup dari tiap *independent review* tergantung pada kebijakan manajemen.

Tabel 2.52 Referensi Manajemen Keamanan *Independent Security Review* dalam *Continual Service Improvement* ITIL

Standard	***Section***
ITIL v3	*Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques*
ISO 27001	*4.2.3 Monitor and review the ISMS*
ISO 27002	*6.1.8 Independent review of information security*
	15.3.1 Information systems audit controls

2.9 ITIL dan COBIT Terkait dengan ISO 27000

Saint-Jerman [2] menyoroti bahwa pelaksanaan keamanan dan kontrol ISO/IEC 27000 yang dikombinasikan dengan standar ITIL atau COBIT mampu mengurangi ancaman kritis yang dapat mengganggu hasil proyek.

ISO/IEC 27000 memiliki struktur utama untuk diterapkan dalam menjamin keamanan organisasi secara keseluruhan di semua tingkat. Masalah administrasi dan manajemen yang tidak dibahas dalam standar ISO/IEC 27000 ditangani oleh ITIL dan COBIT. Hal ini dimungkinkan karena ISO/IEC 27000 memiliki fitur untuk menjaga kerahasiaan, integritas dan ketersediaan informasi dalam organisasi. Ketersediaan informasi ini ditangani dalam ITIL dan COBIT dengan aspek kualitas, kehandalan dan pemeliharaan TI .

Metode yang akan digunakan adalah, ITIL digunakan untuk menentukan strategi, konsep, dan proses yang terkait dengan manajemen TI. COBIT digunakan untuk mengevaluasi

faktor penentu keberhasilan, metrik, indikator dan audit, standar ISO/IEC 27000 untuk memandu pengelolaan TI dalam kaitannya dengan masalah keamanan.

2.10 Konsep Hibridasi

Hibridasi merupakan sebuah konsep persilangan antara dua atau lebih bagian yang saling bergabung untuk mendapatkan sifat-sifat baru yang diinginkan dapat bervariasi jenisnya dengan mengambil beberapa sifat dari kedua bagian indukan asalnya. Konsep hibridasi biasanya digunakan dalam dunia kimia atau biologi untuk menyilangkan dua buah atom atau spesies untuk mendapatkan atom/spesies baru [11].

Dalam pembuatan indeks penilaian kesiapan manajemen keamanan layanan SI/TI ini, digunakan konsep hibridasi *introgresive*, yaitu tipe persilangan yang salah satu standar seolah-olah sifatnya mendominir sifat-sifat standar lain sehingga populasi *hybrid* yang terbentuk seolah-olah hanya terdiri atas satu jenis standar yang mendominir tersebut .

Uji nyata untuk mengetahui apakah data atau hasil yang diperoleh sesuai atau menyimpang dari nisbah yang diharapkan atau tidak, dapat dievaluasi dengan melakukan perbandingan validitas hasil dengan standar indukannya.

faktor penentu keberhasilan, metrik, indikator dan audit, standar ISO/IEC 27000 untuk memandu pengelolaan TI dalam kaitannya dengan masalah keamanan.

2.10 Konsep Hibridasi

Hibridasi merupakan sebuah konsep persilangan antara dua atau lebih bagian yang saling bergabung untuk mendapatkan sifat-sifat baru yang diinginkan dapat bervariasi jenisnya dengan mengambil beberapa sifat dari kedua bagian indukan asalnya. Konsep hibridasi biasanya digunakan dalam dunia kimia atau biologi untuk menyilangkan dua buah atom atau spesies untuk mendapatkan atom/spesies baru [11].

Dalam pembuatan indeks penilaian kesiapan manajemen keamanan layanan SI/TI ini, digunakan konsep hibridasi *introgresive*, yaitu tipe persilangan yang salah satu standar seolah-olah sifatnya mendominir sifat-sifat standar lain sehingga populasi *hybrid* yang terbentuk seolah-olah hanya terdiri atas satu jenis standar yang mendominir tersebut .

Uji nyata untuk mengetahui apakah data atau hasil yang diperoleh sesuai atau menyimpang dari nisbah yang diharapkan atau tidak, dapat dievaluasi dengan melakukan perbandingan validitas hasil dengan standar indukannya.

BAB III
METODOLOGI

Pada bab ini akan di jelaskan metodologi yang di gunakan dalam pengerjaan tugas akhir. Metodologi diperlukan sebagai panduan setiap tahapan pengerjaan untuk dapat berjalan terarah dan sistematis. Secara garis besar, metodologi penelitian terdiri dari beberapa tahapan seperti pada gambar berikut:

Gambar 3.1 Metodologi Pengerjaan

3.1 INPUT

Tahap ini dilakukan untuk memahami dan meninjau kebutuhan apa saja yang dibutuhkan untuk membuat indeks penilaian kesiapan manajemen keamanan layanan teknologi informasi dari sisi *best practice*. Tahap ini dimulai dengan

melakukan *review* studi literatur lalu melakukan wawancara dan verifikasi data awal dengan melakukan tinjauan langsung terhadap organisasi.

3.2 PROSES

Setelah seluruh kebutuhan pembuatan indeks keamanan layanan informasi terpenuhi, langkah selanjutnya adalah pembuatan indeks. Pembuatan indeks pada tahap ini akan menggunakan *Microsoft Office Excel Worksheet*.

3.2.1. Pemetaan Variabel Evaluasi

Berdasarkan karakteristik dari masing-masing standar, kekuatan dan kelemahan masing-masing struktur dievaluasi dan digabungkan untuk saling melengkapi.

Standar pertama yang digunakan menjadi struktur indeks adalah COBIT 4.1. Penggunaan COBIT sebagai dasaran pemetaan dikarenakan COBIT telah memiliki *control objective* yang mendasari dalam pengembangan strategi TI di organisasi.

Domain COBIT yang digunakan adalah domain *Delivery and Support* seperti yang telah di jelaskan dalam sub bab **2.2.1 *Delivery and Support* COBIT 4.1 Bab II**.

Setelah mendapatkan *control objective* dari COBIT 4.1, kemudian dibuatkan pemetaannya dengan ITIL v3. Hal ini didasari pada metodologi ITIL yang dapat digunakan untuk penentuan langkah menyediakan dan menjalankan strategi, konsep dan proses yang terkait dengan pengelolaan teknologi informasi [2].

Adapun Struktur indeks difokuskan pada lima klasifikasi, yaitu :

1. *Service Strategy* → Strategi Layanan
2. *Service Design* → Desain Layanan
3. *Service Transition* → Proses Peralihan Layanan
4. *Service Operation* → Pelaksanaan Layanan
5. *Continual Service Improvement* → Proses Peningkatan Layanan

Langkah selanjutnya adalah pemilihan atribut data yang dapat dijadikan parameter indeks yang disebut dengan area. *Area* yang dipakai adalah ISO 27002:2005. Dengan metode hibridasi, area dipilih dan diuraikan sesuai dengan kebutuhan dan kondisi lapangan yang berhubungan langsung dengan keamanan organisasi, yaitu :

1. *Security Policy*
2. *Organization Security*
3. *Asset Classification and Control*
4. *Personal Security*
5. *Physical and Environmental Security*
6. *Communication and Operations Management*
7. *Access Control*
8. *System Development and Maintenance*
9. *Information Security Incident Management*
10. *Business Continuity Management*
11. *Compliance*

3.2.2. Penetapan Skoring dan Status Penilaian

Penetapan skoring dan status penilaian menggunakan parameter penilaian COBIT 4.1, yaitu model kematangan (*maturity models*) berdasarkan tingkat kematangan manajemen keamanan layanan dari tiap atribut keamanannya. Atribut yang diukur adalah area evaluasi yang telah ditentukan sebelumnya.

Adapun status dan nilai yang digunakan adalah :

Tabel 3.1 Skoring Indeks Penilaian berdasarkan *Maturity Model* Cobit 4.1

Skor	Status	Keterangan
0	*Non-existient*	*Management Processes are not applied at all*
1	*Initial*	*Processes are ad hoc and disorganized*
2	*Repeatable*	*Processes follow a regular pattern*
3	*Defined*	*Processes are documented and communicated*
4	*Managed*	*Processes are monitored and measured*
5	*Optimized*	*Good practices are followed and automated*

3.2.3. Pembuatan Indeks Penilaian

Tahapan berikutnya adalah pembuatan indeks penilaian kesiapan manajemen keamanan dari penggabungan proses/konsep dengan area dan penetapan skoring dan status penilaian yang telah dilakukan sebelumnya. Indeks penilaian yang akan dibuat merupakan indeks berbasis *Microsoft excel worksheet*.

3.2.4. Verifikasi

Pada tahap ini dilakukan verifikasi terhadap indeks penilaian yang telah dibuat. Verifikasi dilakukan dengan cara membandingkan apakah semua bagian dalam indeks penilaian telah sesuai dengan kebutuhan penilaian dan standar yang digunakan. Jika masih terdapat ketidaksesuaian, maka dilakukan perbaikan kembali terhadap isi indeks penilaian.

3.3 OUTPUT

Tahap ini dilakukan untuk memastikan setiap kebutuhan dalam menilai kesiapan manajemen keamanan layanan teknologi informasi sebuah organisasi yang telah dilakukan dalam dua proses sebelumnya telah sesuai. Tahap ini merupakan tahap *review* pembuatan dengan melakukan pengujian penggunaan.

Pengujian pertama penggunaan indeks penilaian kesiapan manajemen keamanan akan dilakukan di Badan Teknologi dan Sistem Informasi (BTSI) Institut Teknologi Sepuluh Nopember untuk melihat hasil tinjauan dan pendapat dari pihak manajemen untuk menjadi bahan masukan dan evaluasi akan pengembangan indeks.

3.3.1 Dokumen Panduan Penggunaan Indeks Penilaian Kesiapan Manajemen Layanan Teknologi Informasi

Langkah berikutnya adalah penyusunan dokumen panduan yang meliputi pendahuluan, tujuan, ruang lingkup, penggunaan indeks penilaian kesiapan manajemen keamanan layanan, manajemen keamanan layanan, dokumentasi manajemen keamanan layanan dan rekomendasi pelaksanaan *assessment*

manajemen keamanan layanan yang akan memudahkan dan memandu auditor internal dalam menggunakan indeks.

3.3.2 Indeks Penilaian Kesiapan Manajemen Layanan Teknologi Informasi

Setelah seluruh kebutuhan dan proses pembuatan indeks keamanan layanan informasi terpenuhi, langkah selanjutnya adalah melakukan perbaikan berdasarkan hasil uji dan verifikasi indeks yang menghasilkan dokumen evaluasi.

Halaman ini sengaja di kosongkan.

BAB IV
PEMBUATAN INDEKS PENILAIAN

Pada bab ini akan dijelaskan mengenai rancangan indeks yang akan dibangun pada tugas akhir ini. Rancangan tersebut merupakan penggabungan dari beberapa standar yang telah dijabarkan pada bab sebelumnya.

4.1 Inputan

4.1.1 Badan Teknologi Sistem Informasi (BTSI)

Badan Teknologi Sistem Informasi (BTSI) atau Lembaga Pengembangan Sistem Informasi (LPTSI) adalah badan di Institut Teknologi Sepuluh Nopember (ITS) yang berfungsi sebagai unit pelaksana teknis di bidang pengelolahan data yang berada di bawah dan bertanggung jawab langsung kepada Rektor.

Dalam proses bisnis keseharian pembinaannya dilakukan oleh Pembantu Rektor I, dengan tugas mengumpulkan, mengolah, menyajikan, dan menyimpan data dan informasi serta memberikan layanan untuk program-program pendidikan, penelitian, dan pengabdian kepada masyarakat.

Untuk menyelenggarakan tugas tersebut UPT Pusat Komputer mempunyai fungsi :

- Mengumpulkan dan mengolah data dan informsi
- Menyajikan dan menyimpan data dan informasi
- Melakukan urusan tata usaha Pusat Komputer

Adapun daftar *Standard Operasional Procedure* (SOP) yang telah dimiliki oleh BTSI adalah sebagai berikut :

Tabel 4.1 Daftar SOP BTSI

No.	PROSEDUR OPERASIONAL BAKU
1.	Proses Pembuatan Sistem Informasi Baru
2.	Pengembangan Sistem Informasi oleh Unit
3.	Proses Pengujian Sistem Informasi
4.	Proses Instalasi Sistem Informasi
5.	Pemutakhiran / Perbaikan Sistem Informasi

6.	Layanan Perbaikan Sistem Informasi (intern)
7.	Layanan Pembuatan Sistem Informasi (intern)
8.	Layanan Pembuatan Domain dan Hosting
9.	Layanan e-mail: Pembuatan Akun
10.	Layanan Penyediaan Legal Software
11.	Keluhan Pelanggan
12.	Layanan Sosialisasi Sistem Informasi (intern)
13.	Penyusunan Laporan Tahunan Rektor
14.	Penyusunan Buku Data 5 Tahunan
15.	Pengukuran Tingkat Kepuasan Stakeholder ITS
16.	Pembuatan Surat Pertanggungjawaban (SPJ)
17.	Pencairan Uang Muka Kegiatan (UMK)
18.	Pengadaan Barang dan Jasa
19.	Rekrutmen Personil Magang dan Kontrak
20.	Pemusnahan Dokumen

Dengan Rincian Fasilitas Sebagai Berikut :

Tabel 4.2 Daftar Infrastruktur BTSI

No.	Infrastruktur
1.	Gedung Y yang merupakan pusat dari pengolahan data, divisi komputing, pelayanan perangkat lunak dan pusat administrasi Badan Teknologi dan Sistem Informasi.
2.	Tiga ruang pada gedung Perpustakaan pada lantai 6 yaitu sebagai pusat ITS-net dan pada bagian ini terletak semua fasilitas server, router dan lain-lain.
3.	Dua ruang di gedung Q yaitu sebagai ruang pusat layanan, pusat sisietm informasi dan pusat data dan pelaporan.

Tabel 4.3 Daftar Perangkat Lunak BTSI

No.	Perangkat Lunak
1.	MATLAB lengkap dengan Toolbox-nya
2.	Oracle
3.	Borland Delphi

4.	Ms. Visual Studio
5.	Borland C++ Builder
6.	Ms Back Office Server
7.	Novell Netware
8.	Unigraphics
9.	Ansys
10.	Arc/Info
11.	Erdas Image Pro
12.	Mentor Graphics
13.	Rebis

Tabel 4.4 Daftar Perangkat Keras BTSI

No.	Perangkat Keras
1.	Infrastruktur jaringan serat optik seluruh ITS
2.	Router CB3500 (sembilan unit)
3.	Switch SS3300
4.	Switch SS1100
5.	Switch SMC 6724AL2 (dua unit)
6.	Omnidirectional Wireless Antenna (satu unit)
7.	Sectoral Wireless Antenna (satu unit)
8.	Grid Wireless Antenna (satu unit)
9.	Access Point (empat belas unit)
10.	HP Server LH3 (tiga unit)
11.	HP Desktop High-end
12.	HP Desktop Low-end
13.	HP UX
14.	HP Compaq Proliant (dua unit)
15.	HP Proliant (tiga unit)

Tabel 4.5 Daftar Alat Cetak / presentasi BTSI

No.	Alat Cetak/Presentasi
1.	Plotter A0
2.	DeskJet Printer A0
3.	Printer Color Laser

4.	Scanner A0
5.	Scanner high precession
6.	Mimio
7.	LCD
8.	Digitizer

Secara implisit, daftar layanan yang diberikan oleh BTSI adalah sebagai berikut :

Tabel 4.6 Daftar Layanan BTSI

No.	Layanan
1.	Email
2.	Pembuatan Sistem Informasi
3.	Data dan Pelaporan
4.	Desain Jaringan Komputer
5.	Instalasi Jaringan Komputer
6.	Website dan webhosting
7.	Data Processing
8.	Webblog

4.1.2 Wawancara dan Pengambilan Data

Pada tahapan ini dilakukan analisa manajemen keamanan layanan TI di organisasi studi kasus, yaitu LPTSI. Proses pengambilan data dengan menganalisa komponen-komponennya dilakukan sebagai langkah pencarian kelemahan untuk perbaikan kedepannya sesuai dengan definisi kebutuhan di awal.

Pengambilan data ditunjukkan pada **Lampiran A – Kuisioner Penggalian Kebutuhan Indeks.** Ringkasan Hasil dan Pembahasan Verifikasi

Dari proses penggalian data sebelumnya, didapatkan bahwa kondisi *existing* manajemen keamanan layanan LPTSI masih belum sesuai dengan kondisi ideal berdasarkan standar keamanan layanan, karena masih terdapat beberapa ketidaksesuaian ketersediaan tata kelola TI.

Keamanan dalam pelaksanaan layanannya belum menjadi fokusan, LPTSI masih membutuhkan sebuah pola yang cocok digunakan dalam pengukuran tingkat *maturity* dari manajemen keamanan layanan TI. Dengan menggabungkan beberapa *framework* dan beberapa *best practice* ini, diharapkan mampu menjawab kebutuhan tersebut.

Dengan adanya penggalian data langsung ke LPTSI ITS Surabaya maka dasaran untuk pembuatan indeks penilaian kesiapan manajemen keamanan layanan berbasis kerangka layanan ITIL V3 dan standar keamanan ISO 27002:2005 telah terpenuhi.

4.2 Proses

Struktur yang dijadikan sebagai pondasi indeks adalah ITIL v3 dengan lima buah fokusan. Di dalam sub bab ini akan dijabarkan penjelasan dari masing-masing fokusan.

4.2.1 Pemetaan Indeks Penilaian

Pemetaan indeks penilaian kesiapan manajemen keamanan layanan didasarkan kepada konsep proses manajemen layanan yang baik dengan di dalamnya di petakan area manajemen keamanan.

Pemetaan ini menggunakan konsep hibridasi yang didasari pada kebutuhan organisasi, yaitu tidak hanya memastikan layanannya dapat berjalan dengan baik sesuai dengan kualitas yang direncanakan, tetapi juga mampu memastikan bahwa layanan berjalan dengan aman.

Keamanan dalam pelaksanaan layanannya belum menjadi fokusan, LPTSI masih membutuhkan sebuah pola yang cocok digunakan dalam pengukuran tingkat *maturity* dari manajemen keamanan layanan TI. Dengan menggabungkan beberapa *framework* dan beberapa *best practice* ini, diharapkan mampu menjawab kebutuhan tersebut.

Dengan adanya penggalian data langsung ke LPTSI ITS Surabaya maka dasaran untuk pembuatan indeks penilaian kesiapan manajemen keamanan layanan berbasis kerangka layanan ITIL V3 dan standar keamanan ISO 27002:2005 telah terpenuhi.

4.2 Proses

Struktur yang dijadikan sebagai pondasi indeks adalah ITIL v3 dengan lima buah fokusan. Di dalam sub bab ini akan dijabarkan penjelasan dari masing-masing fokusan.

4.2.1 Pemetaan Indeks Penilaian

Pemetaan indeks penilaian kesiapan manajemen keamanan layanan didasarkan kepada konsep proses manajemen layanan yang baik dengan di dalamnya di petakan area manajemen keamanan.

Pemetaan ini menggunakan konsep hibridasi yang didasari pada kebutuhan organisasi, yaitu tidak hanya memastikan layanannya dapat berjalan dengan baik sesuai dengan kualitas yang direncanakan, tetapi juga mampu memastikan bahwa layanan berjalan dengan aman.

	Strategy				Service						Transition						Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 1 - Define and Manage Service Levels																									
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N

Gambar 4.1 Pemetaan Indeks Penilaian

Proses hibridasi ini menghasilkan pemetaan indeks yang lebih terarah dengan mencocokkan fase manajemen keamanan layanan dengan manajemen keamanan yang dibutuhkan di masing-masing fase dengan *control objective* strategi TI yang kesemuanya menggunakan *best practice*.

Pemetaan indeks penilaian ditunjukkan pada **Gambar 4.1 Pemetaan Indeks Penilaian** merupakan proses untuk melihat hubungan antara satu standar dengan standar lainnya. Rincian dari aktivitas ini di lampirkan dalam **LAMPIRAN D Pemetaan Indeks Penilaian.**

Pemetaan ini melihat prespektif dari masing-masing *control objective* dalam COBIT 4.1 terutama dalam proses *Delivery and Support* dengan melihat hubungan keterikatan antara ISO 270002 dengan ITIL V3.

Dari hasil pemetaan ini, didapati kesimpulan :

1. Seluruh *Control Objective* dalam ***Delivery and Support*** **COBIT terimplementasi** kecuali *COBIT DS 6- Identify and Allocate Costs* yang diharapkan mampu diimplentasikan menggunakan manajemen terpisah dalam *Financial Management* dalam ITIL.
2. Seluruh ***Lifecycle*** **ITIL V3 terimplementasi** kecuali *Continous Service Improvement* yang hanya mampu diimplementasikan oleh ISO 27002 dalam sisi Reporting,

tetapi tidak dalam sisi *Service Measurement & Control* dan *Return on Investment on CSI.*

3. Proses manajemen keamanan layanan dapat **dimaksimalkan pada saat *Service Design***, terbukti dengan mampu terpenuhinya kebutuhan keamanan manajemen layanan di seluruh proses *Service Design* baik oleh ISO 27002 maupun COBIT 4.1
4. Meskipun secara eksplisit ***DS7-Educate and Train Users, DS11-Manage Data, DS12-Manage Physical Environment*** terlihat seperti tidak memiliki hubungan dengan metodologi lainnya dalam indeks, akan tetapi tujuan dari ketiga *control objective* tersebut dapat terjawab dalam **checklist ISO 27000** (*ISO7-Human Resources Security, ISO9-Communication and Operations Management, ISO8-Physical and Environmental Security*).
5. Seluruh proses dari manajemen keamanan layanan memiliki korelasi yang baik antara standar dengan standar lainnya kecuali tentang penekanan akan kewajiban bagi organisasi dalam memenuhi seluruh kebutuhan persyaratan keamanan yang dapat di *cover* dalam **ISO 27002– *Compliance***.
6. Dalam menetapkan manajemen keamanan layanan di fase ***Service Strategy***, organisasi berfokus pada ***COBIT DS 1-Define and Manage Service Levels*** dengan mempertimbangkan *Services Security Policy* and Organization of Information dalam *Demand Management*, serta ***COBIT DS 2 - Manage Third-Party Services*** dalam menentukan *positioning* pihak ketiga di dalam *Organization of Information and Business Continuity Management* dalam *Service Generation*.
7. Dalam menetapkan manajemen keamanan layanan di fase ***Service Design***, organisasi berfokus pada ***COBIT DS 1-Define and Manage Service Levels*** dengan memastikan bahwa *Service Catalogue Management* organisasi telah mencangkup :
    - *Security Policy*

- *Organization of Information Security*
- *Human Resources Security*
- *Physical and Environmental Security*
- *Information System Acquisition, Development*

Service Level Management yang mempertimbangkan *level* kemungkinan terjadi dan pengelompokan dari macam-macam insiden dalam *Information Security Incident Management Information*.

Pada ***COBIT DS2 - Manage Third-Party Services*** dengan melakukan manajemen di *Supplier Management* yang mempertimbangkan *positioning supplier* di dalam *Organization of Information Security*.
Pada COBIT ***DS3 - Manage Performance and Capacity*** dan ***COBIT DS11- Manage Data*** dengan memastikan *Availability Management* telah tercangkup dalam :

- *Communication and Operations Management*
- *Access Control*

dan pada ***COBIT DS3 - Manage Performance and Capacity*** dan ***COBIT DS12- Manage Physical Environment Capacity Management*** dengan memastikan *Availability Management* telah tercangkup dalam telah tercangkup dalam :

- *Security Policy*
- *Asset Management*
- *Physical and Environmental Security*

Pada ***COBIT DS4-Ensure Continous Service*** dengan memastikan *IT Service Continuity Management* telah tercangkup dalam:

- *Security Policy*
- *Asset Management*
- *Human Resources Security*
- *Communication and Operations Management*

- *Access Control*
- *Information Security Incident Management*
- *Business Continuity Management*

Pada ***COBIT DS5 - Ensure System Securities*** dengan memastikan *Information Security Management* telah tercangkup dalam :

- *Security Policy*
- *Organization of Information Security*
- *Physical and Environmental Security*
- *Communication and Operations Management*

8. Dalam menjalakan manajemen keamanan layanan di fase ***Service Transition***, organisasi berfokus pada ***DS7-Educate and Train Users*** dalam proses *Release & Deployment Management* yang mempertimbangkan keamanan dalam sisi :
   - *Communication and Operations Management*
   - *Information System Acquisition, Development and Maintenance*

   Pada ***DS 9-Manage the Configuration dalam Service Asset & Configuration Management*** yang mempertimbangkan keamanan dalam proses *Information System Acquisition, Development and Maintenance.*
   Pada ***DS12-Manage Physical Environment*** dan ***DS 13-Manage Operations*** di dalam proses *Change Management* yang mempertimbangkan keamanan dalam sisi :
   - *Communication and Operations Management Service Asset & Configuration Management*
   - *Information System Acquisition, Development and Maintenance.*

9. Dalam menjalakan manajemen keamanan layanan di fase ***Service Operation***, organisasi berfokus pada ***DS8- Manage***

Service Desk and Incident dalam proses *Incident Management* yang mencangkup keamanan dalam:

- *Human Resources Security*
- *Communication and Operations Management*
- *Access Control*
- *Business Continuity Management*
- *Request Fulfillment dalam Organization of Information Security*

Pada ***DS10-Manage Problems*** dalam proses *Problem Management* yang mencangkup :

- *Physical and Environmental Security*
- *Communication and Operations Management*
- *Information System Acquisition, Development and Maintenance*

Pada ***DS13-Manage Operation*** dalam proses *Event Management* yang memperhatikan keamanan dalam *Communication and Operations Management* serta proses *Access Management* yang aman berdasarkan :

- *Organization of Information Security*
- *Business Continuity Management*

Dari ke-sembilang kesimpulan di atas, dibuatlah struktur pembuatan Indeks Penilaian Kesiapan Manajemen Keamanan yang ditunjukkan dalam **Tabel 4.7 Struktur Pemetaan Indeks Penilaian Kesiapan Manajemen Keamanan**.

Tabel 4.7 Struktur Pemetaan Indeks Penilaian Kesiapan Manajemen Keamanan

ITIL	ISO	COBIT	
Service Strategy	Kebijakan Keamanan	**DS1 DS2**	***Maturity Model***
	Struktur Organisasi		
Service Design	Manajemen Aset	**DS1 DS2 DS3 DS4 DS5 DS11**	
	Keamanan Sumber Daya Manusia		
	Keamanan Fisik dan Lingkungan		
Service Transition	Penambahan, Pengembangan dan Pemeliharaan Sistem Informasi	**DS7 DS9 DS12 DS13**	
Service Operation	Manajemen Komunikasi dan Operasional	**DS8 DS10 DS13**	
	Kontrol Akses		
	Manajemen Insiden Keamanan		
Continual Service Improvement	*Business Continuity Management*	-	
	Pemenuhan Persyaratan		

Fokusan utama dalam pemetaan ini adalah dapat dibuatnya sebuah formula yang komprehensif dalam pembuatan indeks bagi organisasi agar mampu memanajemen layanan yang aman. Sehingga panduan teknis untuk memanajemen keamanan berdasarkan ITIL menjadi landasan konsep/ prosesnya.

Di dalam masing-masing konsep/proses dimasukkan area keamanan dari ISO 27002:2005 yang tepat untuk dipenuhi pada fase tersebut guna menyiapkan manajemen keamanan.

Keamanan manajemen layanan dalam indeks ini tidaklah dipandang sebagai sebuah layanan yang berdiri sendiri, akan tetapi sebagai kesatuan manajemen layanan yang dilakukan oleh organisasi. Pengukuran *maturity level* nantinya akan memberikan gambaran menyeluruh akan kesiapan manajemen keamanan layanan organisasi.

4.2.1.1 *Service Strategy*

Service Strategy dalam manajemen layanan informasi yang telah dijabarkan dalam **Sub-bab 2.8.1 tentang ITIL dengan ISO 270001 dan ISO 270002 – *Service Strategy*, BAB II** memiliki 7 buah fokusan keamanan. Ketujuh fokusan keamanan ini dapat dipenuhi dengan memaksimalkan persiapan area keamanan *Security Policy* dan *Organizational Security* yang telah dijabarkan dalam Bab II, tentang ISO 27002 dengan terperinci dalam **sub-bab 2.5.2.1 *Security Policy*** dan **2.5.2.2 *Organizational Security***.

Tabel 4.8 Pemetaan fokusan *Service Strategy*

Service Strategy	**Area ISO 27002**	
Menilai Kesiapan Organisasi dari sisi Proses, Sumber Daya dan Teknologi	**Kebijakan Keamanan**	komitmen dan arahan organisasi dijabarkan dan disempurnakan menjadi tujuan pelaksanaan manajemen keamanan informasi organisasi.
Rekomendasi untuk *Improvement*	**Struktur Organisasi**	Pengelolaan kerangka manajemen keamanan yang telah disetujui baik dari sisi internal maupun eksternal organisasi

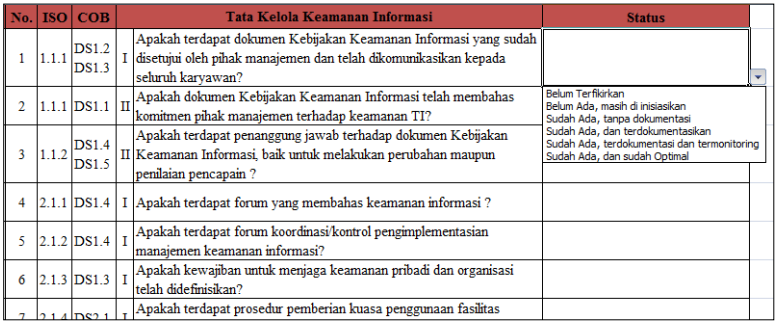
Kesiapan organisasi dalam indeks penilaian kesiapan keamanan manajemen layanan memiliki 15 uraian pertanyaan dengan status penilaian dalam enam buah tingkatan (*maturity model*). Pertanyaan antar fokusan memiliki keterkaitan satu sama lainnya.

Tabel 4.9 Implementasi Struktur *Service Strategy dalam Indeks Kesiapan Manajemen Keamanan Layanan SI/TI*

ISO 27002		Fokusan	No.	ISO	COB
Kebijakan Keamanan		Dokumen Kebijakan Keamanan Informasi	1	1.1.1	DS1.2 DS1.3
			2	1.1.1	DS1.1
		Review Dokumen Kebijakan Informasi	3	1.1.2	DS1.4 DS1.5
Struktur Organisasi	**internal**	Komitmen Manajemen Organisasi	4	2.1.1	DS1.4
		Koordinasi Keamanan	5	2.1.2	DS1.4
		Alokasi Tanggung Jawab	6	2.1.3	DS1.3
		Pemberian Kuasa Penggunaan Fasilitas	7	2.1.4	DS2.1
		Pusat Informasi	8	2.1.5	DS1.4
		Kontak Institusi Penting	9	2.1.6	DS2.2
		Independent Review	10	2.1.7	DS1.5
	eksternal	Identifikasi Risiko Pihak Ketiga	11	2.2.1	DS2.1
		Kontrak Kerjasama	12	2.2.2	DS2.2
		Outsourcing	13	2.3.1	DS2.3
			14	2.3.1	DS2.1
			15	2.3.1	DS2.4

Setiap dari masing-masing pertanyaan memiliki daya dukung tersendiri terhadap manajemen keamanan dan manajemen layanan di tiap fokusan areanya. Dengan menggunakan konsep

hibridasi ini, tujuh tujuan dari manajemen keamanan layanan *service strategy*-ITIL terpenuhi meskipun masih belum menyentuh pada *Financial Management-Service Strategy* seperti pada proses utama ITIL-*Service Strategy* yang dijabarkan dalam **sub-bab 2.3.1.1 tentang ITIL - *Service Strategy*, BAB II**.



No.	ISO	COB		Tata Kelola Keamanan Informasi	Status
1	1.1.1	DS1.2 DS1.3	I	Apakah terdapat dokumen Kebijakan Keamanan Informasi yang sudah disetujui oleh pihak manajemen dan telah dikomunikasikan kepada seluruh karyawan?	
2	1.1.1	DS1.1	II	Apakah dokumen Kebijakan Keamanan Informasi telah membahas komitmen pihak manajemen terhadap keamanan TI?	
3	1.1.2	DS1.4 DS1.5	II	Apakah terdapat penanggung jawab terhadap dokumen Kebijakan Keamanan Informasi, baik untuk melakukan perubahan maupun penilaian pencapain ?	
4	2.1.1	DS1.4	I	Apakah terdapat forum yang membahas keamanan informasi ?	
5	2.1.2	DS1.4	I	Apakah terdapat forum koordinasi/kontrol pengimplementasian manajemen keamanan informasi?	
6	2.1.3	DS1.3	I	Apakah kewajiban untuk menjaga keamanan pribadi dan organisasi telah didefinisikan?	
7	2.1.4	DS2.1	I	Apakah terdapat prosedur pemberian kuasa penggunaan fasilitas	

Gambar 4.2 Screenshot *Service Strategy* dalam Indeks Kesiapan Manajemen Keamanan Layanan TI

Gambar 4.2 merupakan *Screenshot* dari tampilan Indeks Kesiapan Keamanan dalam kesiapan organisasi. Diharapkan pihak manajemen organisasi dapat memandu atribut persiapan manajemen keamanan layanan dan keamanan organisasinya dari sisi kesiapan mendasar melalui indeks ini.

Pengguna nantinya dapat memberikan penilaian berdasarkan hasil temuan sebenarnya di dalam organisasi yang tentunya dilengkapi dengan bukti dokumentasi berdasarkan buku panduan pengguna.

4.2.1.2 *Service Design*

Service Design dalam manajemen layanan informasi yang telah dijabarkan dalam Bab II, **sub-bab 2.8.2 tentang ITIL dengan ISO 27001 dan ISO 27002 – *Service Design*** memiliki 6 buah fokusan keamanan. Ke-enam fokusan keamanan ini dapat dipenuhi dengan memaksimalkan persiapan area keamanan *Asset Classification and Control, Personal Security* dan *Physical and Environmental Security* yang telah dijabarkan dalam Bab II,

tentang ISO 27002 dengan terperinci dalam **sub-bab 2.5.2.3** ***Asset Classification and Control*****, 2.5.2.4** ***Personal Security*** dan **2.5.2.5** ***Physical and Environmental Security***.

Tabel 4.10 Pemetaan fokusan *Service Design*

Service Design	Area ISO 27002	
Pemilihan Teknologi	**Manajemen Aset - Keamanan fisik dan lingkungan organisasi**	mampu mengklasifikasikan dan melakukan kontrol terhadap infrastruktur keamanan guna menjaga aset organisasi.
Pemilihan *partner* kerja		mampu menganalisa dan mempersiapkan keamanan organisasi dari sisi lingkungan organisasi
Pemilihan Sumber daya manusia	**Keamanan sumber daya manusia**	mampu mencegah risiko yang melekat dalam interaksi manusia

Pemilihan penggunaan konsep dari *Service Design* menjadi Manajemen aset adalah bahwa pada fase ini, sebuah organisasi harus memandang teknologi yang dimilikinya sebagai sebuah aset, baik dari sisi sumber daya manusia, teknologi hingga lingkungan sekitarnya .

Service Design dalam indeks penilaian kesiapan keamanan manajemen layanan memiliki 30 uraian pertanyaan dengan status penilaian dalam enam buah tingkatan (*maturity model*). Pertanyaan antar fokusan memiliki keterkaitan satu sama lainnya.

Tabel 4.11 Penjabaran Pemetaan masing-masing Atribut Pertanyaan Struktur Indeks Kesiapan *Service Design*

ISO 27002		Fokusan	No.	ISO	COB
Manajemen Aset	**Tanggung Jawab Aset**	Inventaris Aset	**1**	3.1.1	DS4.1
		Penerimaan Penggunaan Aset	**2**	3.1.1	DS5.3
	Klasifikasi Informasi	Pedoman Klasifikasi	**3**	3.2.1	DS5.1
		Prosedur *Labeling* dan *Handling* Informasi	**4**	3.2.2	DS4.4
Keamanan Sumber Daya Manusia	**Pemilihan Karyawan**	Proses Penerimaan Karyawan	**5**	4.1.2	DS5.3
			6	4.1.2	DS5.3
		Aturan dan Tanggung Jawab	**7**	4.1.1	DS4.7
			8	4.1.1	DS3.2
		Term and Conditions Karyawan	**9**	4.1.4	DS5.3
		Perjanjian Penjagaan Rahasia Organisasi	**10**	4.1.3	DS5.4
	Pengembangan Sumber Daya	Kesadaran, Pendidikan dan Pelatihan Keamanan Informasi	**11**	4.2.1	DS4.2
		Proses Pendisiplinan Karyawan	**12**	4.3.5	DS5.4
	Pemberhentian atau Pengganti an Karyawan	Proses Pemberhentian	**13**	-	DS5.4
		Pengembalian Aset	**14**	-	DS3.4
		Pemberhentian Hak Akses	**15**	-	DS5.4

Keamanan Fisik dan Lingkungan	**Pengamanan Area**	Bekerja di Area yang Aman	**16**	5.1.4	DS4.4
		Pengamanan Kantor, Ruangan dan Fasilitas	**17**	5.1.3	DS12/5
			18	5.1.3	DS5.6
		Penjagaan dari Ancaman Lingkungan Luar Organisasi	**19**	5.1.3	DS12.1
		Akses Area Pemrosesan	**20**	5.1.5	DS5.10
	Keamanan Peralatan	Peletakan dan Penjagaan Keamanan Peralatan	**21**	5.2.1	DS12.1
		Peralatan Pendukung	**22**	5.2.2	DS4.3
		Keamanan Kabel	**23**	5.2.3	DS5.9
		Pemeliharaan Peralatan	**24**	5.2.4	DS4.4
			25	5.2.4	DS4.4
			26	5.2.4	DS4.4
		Keamanan Peralatan dengan Pengecualian	**27**	5.2.5	DS11.5
		Keamanan Pembuangan Peralatan	**28**	5.2.6	DS11.3
		Clear Desk and Clear Screen	**29**	5.3.1	DS12.3
			30	5.3.1	DS12.4

Setiap dari masing-masing pertanyaan memiliki daya dukung tersendiri terhadap manajemen keamanan dan manajemen layanan di tiap fokusan areanya.

Dengan menggunakan konsep hibridasi ini, tujuan dari manajemen aset dalam *service design*-ITIL terpenuhi seperti pada

proses utama ITIL-*Service Design* yang dijabarkan dalam Bab II, **sub-bab 2.3.2 tentang ITIL – *Service Design***.

No.	ISO	COB		Pengelolaan Aset Informasi	Status
1	3.1.1	DS4.1	I	Apakah terdapat catatan inventaris aset penting yang berhubungan dengan sistem informasi?	
2	3.1.1	DS5.3	II	Apakah klasifikasi keamanan dan identifikasi keamanan lokasi aset telah didefinisikan?	Belum Terfikirkan Belum Ada, masih di inisiasikan Sudah Ada, tanpa dokumentasi Sudah Ada, dan terdokumentasikan Sudah Ada, terdokumentasi dan termonitoring Sudah Ada, dan sudah Optimal
3	3.2.1	DS5.1	I	Apakah terdapat skema atau pedoman klasifikasi yang membantu dalam menentukan penanganan dan penjagaan informasi?	
4	3.2.2	DS4.4	II	Apakah terdapat prosedur *labelling* dan *handling* informasi berdasarkan skema klasifikasi informasi organisasi?	
5	4.1.2	DS5.3	I	apakah terdapat pengecekan verifikasi karyawan tetap saat pendaftaran ?	
6	4.1.2	DS5.3	II	apakah dalam pengecekan verifikasi karyawan meliputi : - Referensi Karakteristik - Pengecekan Akademik - Kualitifikasi Profesi - Pengecekan Identitas Diri	

Gambar 4.3 Screenshot *Service Design* dalam Indeks Kesiapan Manajemen Keamanan Layanan TI

Gambar 4.3 merupakan *Screenshot* dari tampilan Indeks Kesiapan Keamanan dalam *service design*. Diharapkan pihak manajemen organisasi dapat memandu atribut persiapan manajemen keamanan layanan dan keamanan organisasinya dari sisi kesiapan keamanan aset yang dimilikinya melalui indeks ini.

Pengguna nantinya dapat memberikan penilaian berdasarkan hasil temuan sebenarnya di dalam organisasi yang tentunya dilengkapi dengan bukti dokumentasi berdasarkan buku panduan pengguna.

4.2.1.3 Service Transition

Service Transition dalam manajemen layanan informasi yang telah dijabarkan dalam Bab II, **sub-bab 2.8.3 tentang ITIL dengan ISO 27001 dan ISO 27002 – *Service Transition*** memiliki tujuh buah fokusan keamanan. Ketujuh Fokusan keamanan ini dapat dipenuhi dengan memaksimalkan persiapan area keamanan *System Development and Maintenance* yang telah dijabarkan dalam Bab II, tentang ISO 27002 dengan terperinci dalam **sub-bab 2.5.2.8 *System Development and Maintenance***.

Tabel 4.12 Pemetaan fokusan *Service Transition*

Service Transition	**Area ISO 27002**	
Pembangunan Teknologi	**Proses Penambahan, Pengembangan, dan Pemeliharaan Sistem Informasi**	Proses pengawasan terhadap pengembangan dan pemeliharaan sistem mampu memastikan bahwa kontrol keamanan yang tepat telah dibuat dan dijalankan diseluruh bagian organisasi.
Pembangunan Sumber Daya Manusia		
Pembangunan Kerjasama dengan *partner*		

Penyusunan keamanan TI dalam indeks penilaian kesiapan keamanan manajemen layanan memiliki 20 uraian pertanyaan dengan status penilaian dalam enam buah tingkatan (*maturity model*). Pertanyaan antar fokusan memiliki keterkaitan satu sama lainnya.

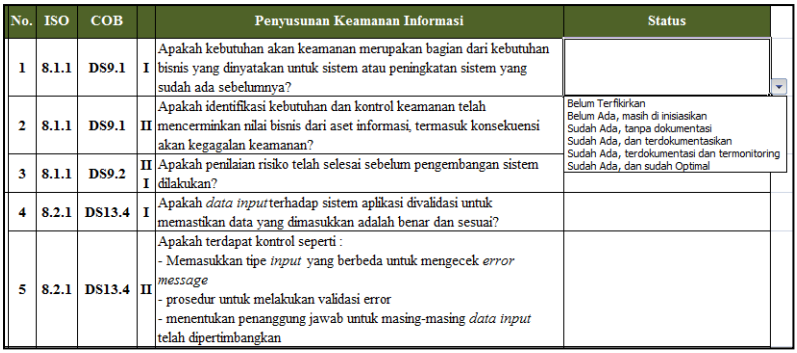
Tabel 4.13 Penjabaran Pemetaan masing-masing Atribut Pertanyaan Struktur Indeks Kesiapan *Service Transition*

ISO 27002	Fokusan	No.	ISO	COB
Tingkat Kebutuhan	Analisa Kebutuhan dan Spesifikasi Keamanan	**1**	**8.1.1**	**DS9.1**
		2	**8.1.1**	**DS9.1**
		3	**8.1.1**	**DS9.2**
Memastikan Proses yang Tepat	Validasi *Data Input*	**4**	**8.2.1**	**DS13.4**
		5	**8.2.1**	**DS13.4**
	Pengaturan Proses *Internal*	**6**	**8.2.2**	**DS12.2**
		7	**8.2.2**	**DS9.3**
	Pesan Keamanan	**8**	**8.2.3**	**DS13.5**
chryptographic controls	Kebijakan	**9**	**8.3.1**	**DS5.8**
	Key Management	**10**	**8.3.2**	**DS5.8**

		11	**8.3.5**	**DS5.8**
Keamanan *system files*	kontrol *operational software*	**12**	**8.4.1**	**DS9.3**
	Menjaga data pengetesan sistem	**13**	**8.4.2**	**DS13.4**
	Kontrol akses terhadap *program source code*	**14**	**8.4.3**	**DS12.5**
Kontrol Akses *program source code*	Prosedur Pengontrolan Perubahan	**15**	**8.5.1**	**DS9.3**
	Pemantauan setelah perubahan Sistem	**16**	**8.5.2**	**DS9.1**
	Larangan dalam Perubahan *software packages*	**17**	**8.5.3**	**DS9.2**
		18	**8.5.3**	**DS9.1**
	Kebocoran Informasi	**19**	**8.5.4**	**DS12.4**
	outsourced software development	**20**	**8.5.5**	**DS12.2**

Setiap dari masing-masing pertanyaan memiliki daya dukung tersendiri terhadap manajemen keamanan dan manajemen layanan di tiap fokusan areanya.

Dengan menggunakan konsep hibridasi ini, tujuan dari manajemen aset dalam *service design*-ITIL terpenuhi seperti pada proses utama ITIL-*Service Transition* yang dijabarkan dalam **sub-bab 2.3.3 tentang ITIL – *Service Transition,* BAB II**.



No.	ISO	COB		Penyusunan Keamanan Informasi	Status
1	8.1.1	DS9.1	I	Apakah kebutuhan akan keamanan merupakan bagian dari kebutuhan bisnis yang dinyatakan untuk sistem atau peningkatan sistem yang sudah ada sebelumnya?	
2	8.1.1	DS9.1	II	Apakah identifikasi kebutuhan dan kontrol keamanan telah mencerminkan nilai bisnis dari aset informasi, termasuk konsekuensi akan kegagalan keamanan?	
3	8.1.1	DS9.2	II I	Apakah penilaian risiko telah selesai sebelum pengembangan sistem dilakukan?	
4	8.2.1	DS13.4	I	Apakah *data input* terhadap sistem aplikasi divalidasi untuk memastikan data yang dimasukkan adalah benar dan sesuai?	
5	8.2.1	DS13.4	II	Apakah terdapat kontrol seperti : - Memasukkan tipe *input* yang berbeda untuk mengecek *error message* - prosedur untuk melakukan validasi error - menentukan penanggung jawab untuk masing-masing *data input* telah dipertimbangkan	

Belum Terfikirkan
Belum Ada, masih di inisiasikan
Sudah Ada, tanpa dokumentasi
Sudah Ada, dan terdokumentasikan
Sudah Ada, terdokumentasi dan termonitoring
Sudah Ada, dan sudah Optimal

Gambar 4.4 Screenshot *Service Transition* dalam Indeks Kesiapan Manajemen Keamanan Layanan TI

Gambar 4.4 merupakan *Screenshot* dari tampilan Indeks Kesiapan Keamanan dalam *service transition*. Diharapkan pihak manajemen organisasi dapat memandu atribut persiapan manajemen keamanan layanan dan keamanan organisasinya dari sisi kesiapan keamanan aset yang dimilikinya melalui indeks ini.

Pengguna nantinya dapat memberikan penilaian berdasarkan hasil temuan sebenarnya di dalam organisasi yang tentunya dilengkapi dengan bukti dokumentasi berdasarkan buku panduan pengguna.

4.2.1.4 Service Operation

Service Operation dalam manajemen layanan informasi yang telah dijabarkan dalam **Sub-bab 2.8.5 tentang ITIL dengan ISO 270001 dan ISO 270002 – *Service Operation*, BAB II** memiliki 5 buah fokusan keamanan. Kelima fokusan keamanan ini dapat dipenuhi dengan memaksimalkan persiapan area keamanan *Physical Environment Security, Communication and Operations Manangement* dan *Access Control* yang telah dijabarkan dalam Bab II, tentang ISO 27002 dengan terperinci dalam **sub-bab 2.5.2.5 *Physical Environment Security*, 2.5.2.6 *Communication and Operations Manangement*** dan ***2.5.2.7 Access Control.***

Tabel 4.14 Pemetaan fokusan *Service Operation*

Service Operation	**Area ISO 27002**	
Aktivitas Operasional Langsung	**Manajemen Komunikasi dan Operasional**	organisasi telah menjalankan proses operasional dan komunikasi yang aman bagi asetnya
	Kontrol Akses	aset organisasi telah digunakan sesuai dengan persyaratan akses bisnis organisasi
	Manajemen Insiden Layanan	mampu mencegah risiko masalah keamanana TI terulang

Pelaksanaan manajemen keamanan layanan TI dalam indeks penilaian kesiapan keamanan manajemen layanan memiliki 68 uraian pertanyaan dengan status penilaian dalam enam buah tingkatan (*maturity model*). Pertanyaan antar fokusan memiliki keterkaitan satu sama lainnya.

Tabel 4.15 Penjabaran Pemetaan masing-masing Atribut Pertanyaan Struktur Indeks Kesiapan *Service Operation*

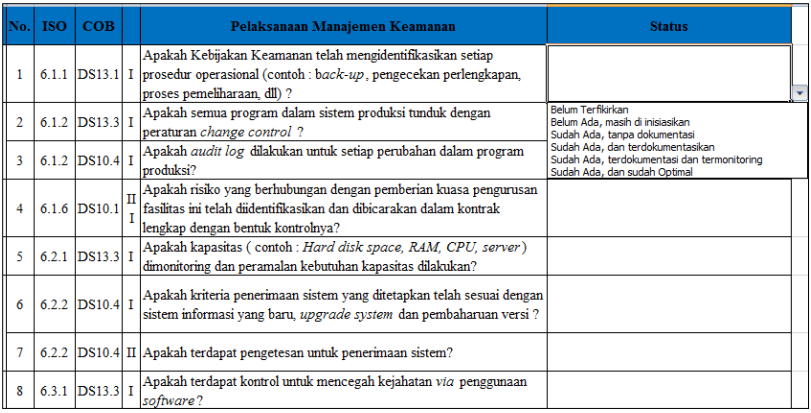
ISO 27002:2015		**Fokusan**	**No.**	**ISO**	**COB**
Manajemen Komunikasi dan Operasional	Prosedur dan Pertanggung jawaban Operasional	Dokumentasi Kebijakan Operasional	1	6.1.1	DS13.1
		Manajemen Perubaahan	2	6.1.2	DS13.3
			3	6.1.2	DS10.4
			4	6.1.6	DS10.1
	Perencanaan	Perencanaan	5	6.2.1	DS13.3

	dan Penerimaan Sistem	Kapasitas			
		Penerimaan Sistem	6	6.2.2	DS10.4
			7	6.2.2	DS10.4
	Penjagaan	Kontrol Kejahatan	8	6.3.1	DS13.3
			9	6.3.1	DS13.3
			10	6.3.1	DS13.5
			11	6.3.1	DS13.2
			12	6.3.1	DS13.3
	Back-up	Informasi *Back-up*	13	6.4.1	DS13.2
			14	6.4.1	DS13.2
		Penjagaan *log*	15	6.4.2	DS8.2
			16	6.4.2	DS13.2
		Catatan Kesalahan	17	6.4.3	DS10.2
			18	6.4.3	DS10.2
	Kontrol Akses Jaringan	Kontrol Jaringan	19	6.5.1	DS13.3
	Pengelolaan Media	Manajemen *Removable Media*	20	6.6.1	DS13.4
		Keamanan Sistem Dokumentasi	21	6.6.4	DS13.5
			22	6.6.4	DS8.5

		Pengangkutan Media Fisik	23	6.7.2	DS13.5
		electronic commerce	24	6.7.3	DS10.1
			25	6.7.3	DS10.2
		Pesan Elektronik	26	6.7.4	DS10.1
	Layanan *electronic commerce*	Sistem Informasi Bisnis	27	6.7.5	DS10.1
			28	6.7.5	DS10.2
		Penyediaan Informasi Umum	29	6.7.6	DS13.4
			30	6.7.6	DS13.3
	Monitoring	Pemeriksaan *log*	31	7.7.1	DS8.5
		Pemantauan Penggunaan Sistem	32	7.7.2	DS8.5
		Sinkronisasi Waktu	33	7.7.3	DS13.1

Setiap dari masing-masing pertanyaan memiliki daya dukung tersendiri terhadap manajemen keamanan dan manajemen layanan di tiap fokusan areanya.

Dengan menggunakan konsep hibridasi ini, tujuan dari manajemen aset dalam *service operation*-ITIL terpenuhi seperti pada proses utama ITIL-*Service Operation* yang dijabarkan dalam Bab II, **sub-bab 2.3.4 tentang ITIL – *Service Operation***.



No.	ISO	COB		Pelaksanaan Manajemen Keamanan	Status
1	6.1.1	DS13.1	I	Apakah Kebijakan Keamanan telah mengidentifikasikan setiap prosedur operasional (contoh : *back-up*, pengecekan perlengkapan, proses pemeliharaan, dll) ?	
2	6.1.2	DS13.3	I	Apakah semua program dalam sistem produksi tunduk dengan peraturan *change control* ?	
3	6.1.2	DS10.4	I	Apakah *audit log* dilakukan untuk setiap perubahan dalam program produksi?	
4	6.1.6	DS10.1	II I	Apakah risiko yang berhubungan dengan pemberian kuasa pengurusan fasilitas ini telah diidentifikasikan dan dibicarakan dalam kontrak lengkap dengan bentuk kontrolnya?	
5	6.2.1	DS13.3	I	Apakah kapasitas (contoh : *Hard disk space, RAM, CPU, server*) dimonitoring dan peramalan kebutuhan kapasitas dilakukan?	
6	6.2.2	DS10.4	I	Apakah kriteria penerimaan sistem yang ditetapkan telah sesuai dengan sistem informasi yang baru, *upgrade system* dan pembaharuan versi ?	
7	6.2.2	DS10.4	II	Apakah terdapat pengetesan untuk penerimaan sistem?	
8	6.3.1	DS13.3	I	Apakah terdapat kontrol untuk mencegah kejahatan *via* penggunaan *software*?	

Belum Terfikirkan
Belum Ada, masih di inisiasikan
Sudah Ada, tanpa dokumentasi
Sudah Ada, dan terdokumentasikan
Sudah Ada, terdokumentasi dan termonitoring
Sudah Ada, dan sudah Optimal

Gambar 4.5 Screenshot *Service Operation* dalam Indeks Kesiapan Manajemen Keamanan Layanan TI

Gambar 4.2 merupakan *Screenshot* dari tampilan Indeks Kesiapan Keamanan dalam *service operation*. Diharapkan pihak manajemen organisasi dapat memandu atribut persiapan manajemen keamanan layanan dan keamanan organisasinya dari sisi pelaksanaan manajemen keamanan layanan yang dimilikinya melalui indeks ini.

Pengguna nantinya dapat memberikan penilaian berdasarkan hasil temuan sebenarnya di dalam organisasi yang tentunya dilengkapi dengan bukti dokumentasi berdasarkan buku panduan pengguna.

4.2.1.5 *Continous Service Improvement*

Continous Service Improvement dalam manajemen layanan informasi yang telah dijabarkan dalam **Sub-bab 2.8.5 tentang ITIL dengan ISO 270001 dan ISO 270002 – *Continual Service Improvement*, BAB II** memiliki 2 buah fokusan keamanan. Kedua fokusan keamanan ini dapat dipenuhi dengan memaksimalkan perencanaan pengembangan layanan dengan *Continual Service Improvement Process* dan *Service* yang telah dijabarkan dalam Bab II, tentang ISO 27002 dengan terperinci

dalam **sub-bab 2.3.5.1 *CSI Improvement Process***, dan ***2.3.5.1 Service Reporting.***

Tabel 4.16 Pemetaan fokusan *Continual Service Improvement*

Continous Service Improvement	**Area ISO 27002**	
Perencanaan Pengembangan	***Business Contiuity Management***	organisasi mampu merencanakan pengembangan strategi guna menetralkan setiap gangguan di masa depan
	Pemenuhan Persyaratan	organisasi mampu memenuhi setiap persyaratan yang dibutuhkan mulai dari peraturan nasional hingga internasional akan manajemen keamanan yang baik.

Pelaksanaan perencanaan pengembangan manajemen keamanan layanan TI dalam indeks penilaian kesiapan keamanan manajemen layanan memiliki 18 uraian pertanyaan dengan status penilaian dalam enam buah tingkatan (*maturity model*). Pertanyaan antar fokusan memiliki keterkaitan satu sama lainnya.

Tabel 4.17 Penjabaran Pemetaan masing-masing Atribut Pertanyaan Struktur Indeks Kesiapan *Continual Service Improvement*

ISO 27002: 2015		**Fokusan**	**No**	**ISO**	**COB**
Continuity Manageme	Aspek *Informatio n Security* dalam BCP	*Business Continuity Planning Framework(BCP)*	1	9.1.4	DS4.1
			2	9.1.4	DS4.4

			3	9.1.4	DS4.2
		Pengetesan *BCP*	4	9.1.5	DS4.5
		Information Security dalam manajemen BCP	5	9.1.2	DS4.8
			6	9.1.2	DS4.2
		Mengembangkan dan Mengimplementasikan BCP + *Information Security*	7	9.1.1	DS4.4
Pemenuhan Persyaratan	Memenuhi Persyaratan Hukum	Identifikasi dan Pengaplikasian Peraturan	8	10.1.1	-
			9	10.1.1	-
		intellectual property rights (IPR)	10	10.1.2	-
			11	10.1.2	-
		Pengamanan Data dan Informasi Pribadi	12	10.1.4	-
		Pencegahan Penyalahgunaan Informasi dan Fasilitas	13	10.1.5	-
		Kontrol Penggunaan *Chryptograpic*	14	10.1.6	-

	Pemenuhan Standar *Security Policies* dan Teknis Pengecekan	Memenuhi standar *security policies*	15	10.2.1	-
			16	10.2.2 .	-
	Pertimbangan Audit Sistem Informasi	Kontrol Audit Sistem Informasi	17	10.3.1	-
		Penjagaan pada *tools* Audit	18	10.3.2	-

Setiap dari masing-masing pertanyaan memiliki daya dukung tersendiri terhadap manajemen keamanan dan manajemen layanan di tiap fokusan areanya.

Dengan menggunakan konsep hibridasi ini, tujuan dari manajemen aset dalam *continous service improvement*-ITIL terpenuhi seperti pada proses utama ITIL-*Continual Service Improvement* yang dijabarkan dalam Bab II, **sub-bab 2.3.5 tentang ITIL– *Continual Service Improvement***.

No.	ISO	COB		Perencanaan Pengembangan	Status
1	9.1.4	DS4.1	I	Apakah organisasi memiliki *framework Business Continuity Plan*?	
2	9.1.4	DS4.4	II	Apakah *framework* ini di-*maintained* untuk memastikan setiap perencanaan konsisten dan mampu mengidentifikasikan prioritas pengetesan dan *maintenance* ?	
3	9.1.4	DS4.2	II	Apakah *framework* ini juga mengidentifikasi kondisi aktivasi dan individu yang bertanggung jawab mengeksekusi setiap komponen dari *Business Continuity Plan* ?	
4	9.1.5	DS4.5	I	Apakah *Business Continuity Plans* di-tes secara rutin untuk memastikan rencananya *up to date* dan berjalan efektif?	
5	9.1.2	DS4.8	I	Apakah kejadian yang mungkin mengganggu proses bisnis telah diidentifikasi (contoh : kebakaran, banjir, gempa, dll)?	
6	9.1.2	DS4.2	III	Apakah *Strategy Plan* dikembangkan berdasarkan hasil penilaian risiko ini untuk menentukan pendekatan menyeluruh dalam *Business*	

Belum Terfikirkan
Belum Ada, masih di inisiasikan
Sudah Ada, tanpa dokumentasi
Sudah Ada, dan terdokumentasikan
Sudah Ada, terdokumentasi dan termonitoring
Sudah Ada, dan sudah Optimal

Gambar 4.6 *Screenshot Continual Service Improvement* dalam Indeks Kesiapan Manajemen Keamanan Layanan TI

4.2.2 Penetapan Skoring dan Status Penilaian

Penetapan skoring dan status penilaian menggunakan parameter penilaian COBIT 4.1, yaitu model kematangan (*maturity models*) berdasarkan tingkat kematangan manajemen keamanan layanan di organisasi yang dijabarkan dalam **sub-bab 2.6 tentang *Maturity Model* COBIT 4.1, BAB II.**

4.2.3 Verifikasi

Pada tahapan ini dilakukan verifikasi akan isi dari indeks penilaian kesiapan manajemen keamann layanan TI yang telah dibuat. Verifikasi ini dilakukan dengan pengecekan kembali masing-masing atribut / *item* pertanyaan dari penilaiana akan hubungan dan keterikatan dukungannya antara satu standar dengan standar lainnya sebagai langkah memastikan bahwa seluruh kebutuhan yang telah dijabarkan diawal telah terpenuhi.

Pelaksanaan Verifikasi ditunjukkan pada **Lampiran E – Verifikasi Komponen Penyusunan Indeks.** Ringkasan kesimpulan dari pelaksanaan verifikasi ini adalah :

1. Seluruh bagian dari *Service Lifecycle* dari ITIL V3 terimplementasi kecuali *Continual Service Improvement*.
2. Seluruh bagian dari ISO 27002 dapat terimplementasi tanpa terkecuali, terutama bagian *Compliance*, untuk memastikan bahwa organisasi sadar untuk melakukan pemenuhan persyaratan hukum yang menjadi penekanan khusus dalam ISO 27002.
3. Terdapat 4 buah *control objectives* dari *Delivery and Support* COBIT 4.1 secara eksplisit tidak terimplementasi, tetapi dapat didukung oleh ITIL dan ISO 27002, yaitu DS7-*Educate and Train Users*, DS11-*Manage Data*, DS12-*Manage Physical Environment* yang tujuan dari ketiga *control objective* tersebut dapat terjawab dalam ISO 27002 (ISO7-*Human Resources Security*, ISO9-*Communication and Operations Management*, ISO8-*Physical and Environmental Security*) dan DS6 – *Identify and Allocate Costs* yang dapat dipenuhi oleh *Financial Management-Service Strategy– ITIL.*

4.2.2 Penetapan Skoring dan Status Penilaian

Penetapan skoring dan status penilaian menggunakan parameter penilaian COBIT 4.1, yaitu model kematangan (*maturity models*) berdasarkan tingkat kematangan manajemen keamanan layanan di organisasi yang dijabarkan dalam **sub-bab 2.6 tentang *Maturity Model* COBIT 4.1, BAB II.**

4.2.3 Verifikasi

Pada tahapan ini dilakukan verifikasi akan isi dari indeks penilaian kesiapan manajemen keamann layanan TI yang telah dibuat. Verifikasi ini dilakukan dengan pengecekan kembali masing-masing atribut / *item* pertanyaan dari penilaiana akan hubungan dan keterikatan dukungannya antara satu standar dengan standar lainnya sebagai langkah memastikan bahwa seluruh kebutuhan yang telah dijabarkan diawal telah terpenuhi.

Pelaksanaan Verifikasi ditunjukkan pada **Lampiran E – Verifikasi Komponen Penyusunan Indeks.** Ringkasan kesimpulan dari pelaksanaan verifikasi ini adalah :

1. Seluruh bagian dari *Service Lifecycle* dari ITIL V3 terimplementasi kecuali *Continual Service Improvement*.
2. Seluruh bagian dari ISO 27002 dapat terimplementasi tanpa terkecuali, terutama bagian *Compliance*, untuk memastikan bahwa organisasi sadar untuk melakukan pemenuhan persyaratan hukum yang menjadi penekanan khusus dalam ISO 27002.
3. Terdapat 4 buah *control objectives* dari *Delivery and Support* COBIT 4.1 secara eksplisit tidak terimplementasi, tetapi dapat didukung oleh ITIL dan ISO 27002, yaitu DS7-*Educate and Train Users*, DS11-*Manage Data*, DS12-*Manage Physical Environment* yang tujuan dari ketiga *control objective* tersebut dapat terjawab dalam ISO 27002 (ISO7-*Human Resources Security*, ISO9-*Communication and Operations Management*, ISO8-*Physical and Environmental Security*) dan DS6 – *Identify and Allocate Costs* yang dapat dipenuhi oleh *Financial Management-Service Strategy– ITIL.*

4.2.4 Dashboard

Dashboard menawarkan sebuah solusi yang unik dan canggih kepada sebuah organisasi yang memerlukan informasi, akan tetapi mereka biasanya 'tersandung' di potensi yang mereka miliki. *Dashboard* harus dapat dilihat di dalam konteks yang historikal agar bentuk dashboard yang ditampilkan dapat dimengerti [12]

Business Intelligence (BIS) *Dashboard* adalah sebuah alat visualisasi data yang menampilkan status terkini dari sebuah metrik dan *Key Performance Indicator* (KPI) untuk sebuah organisasi. *Dashboard* mengkonsolidasikan dan menyusun angka-angka, metrik dan juga performa *scorecard* dalam satu layar.*Dashboard* dapat disesuaikan untuk peran tertentu dan metrik tampilan ditargetkan untuk satu titik pandang atau fokusan. Fitur penting dari produk *dashboard* termasuk antarmuka yang dapat disesuaikan dan kemampuan untuk menarik data secara *real-time* dari berbagai sumber.

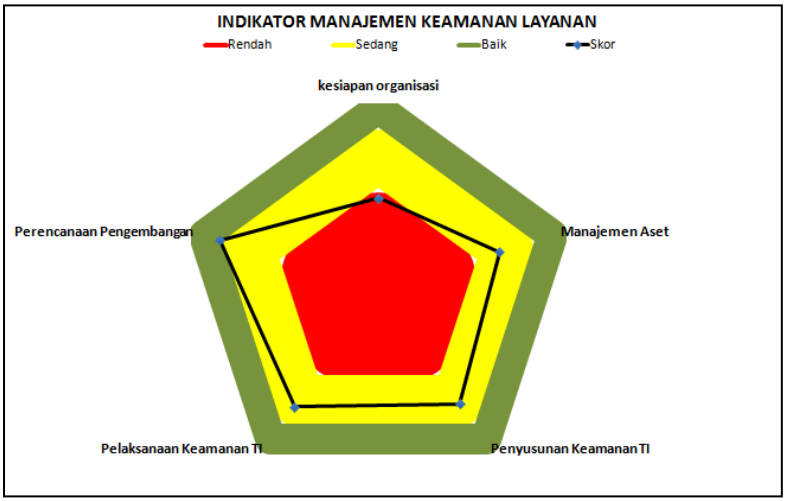
4.2.4.1 Dashboard Indikator Kinerja

Sumber data yang digunakan dalam pembuatan *dashboard* indikator kinerja adalah rata-rata capaian dari masing-masing proses manajemen keamanan teknologi informasi.

Terdapat tiga indikator capaian, yaitu :

1. **Merah :** Pelaksanaan manajemen keamanan informasi masih dalam proses inisiasi atau belum menjadi fokusan utama dari organisasi. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 1 dan 2 dari 6 tingkatan pengukuran dengan *maturity model*.
2. **Kuning :** Pelaksanaan manajemen keamanan informasi sudah menjadi fokusan utama dari organisasi akan tetapi pelaksanaannya belum optimal. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 3 dan 4 dari 6 tingkatan pengukuran dengan *maturity model*.

3. **Hijau** : Pelaksanaan manajemen keamanan informasi sudah optimal baik dari sisi manajemen hingga pelaksanaannya di tingkat operasional. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 5 dan 6, dari 6 tingkatan pengukuran dengan *maturity model*.



Gambar 4.1 Dashboard Indikator Kinerja

Gambar di atas merupakan gambar *dashboard* indikator manajemen keamanan layanan. Sebagai contoh penghitungan capaian, kesiapan organisasi masuk ke dalam indikator merah yaitu manajemen keamanan informasi dari sisi kesiapan organisasi rendah kurang meskipun sudah berada di garis terluar dari area merah.

Di dalam proses manajemen aset, penyusunan keamanan TI dan pelaksanaan keamanan TI sudah berada di sisi sedang. Hal ini bias didasari dari kesiapan organisasinya yang belum optimal dalam menopang pelaksanaan operasional keamanan layanan TI.

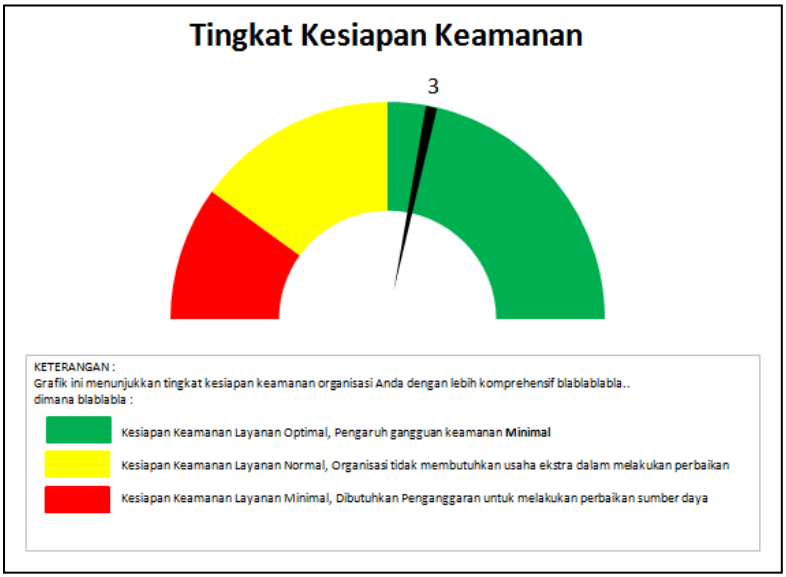
Terakhir dapat di lihat dari perencanaan pengembangan yang sudah memasuki area hijau, area baik atau optimal. Dengan

melihat dashboard ini, diharapkan organisasi dapat melihat dengan lebih menyeluruh akan proses manakah yang harus mendapatkan fokusan lebih dan perbaikan.

4.2.4.2 Dashboard Kesiapan Keamanan

Sumber data yang digunakan dalam pembuatan *dashboard* kesiapan keamanan adalah rata-rata capaian dari seluruh proses manajemen keamanan teknologi informasi.

Terdapat tiga indikator capaian yang sama dengan dashboard indikator kinerja, hanya saja pada dashboard ini, nilai yang didapatkan adalah rata-rata dari keseluruhan kesiapan keamanan organisasi.



Gambar 4.2 Tingkat Kesiapan Keamanan

Gambar di atas merupakan gambar *dashboard* tingkat kesiapan keamanan layanan. Sebagai contoh penghitungan capaian, kesiapan organisasi masuk ke dalam indikator hijau

dimana secara keseluruhan kesiapanan manajemen keamanan sudah optimal.

4.3 Output / Luaran

4.3.1 Dokumen Panduan Penggunaan Indeks Penilaian Kesiapan Manajemen Keamanan Layanan

Dokumen panduan ini berisikan langkah-langkah penggunaan indeks penilaian kesiapan manajemen keamanan layanan TI. Panduan tersebut ditunjukkan pada **Lampiran B**. di dalam bagian ini, akan dibahas komponen apa saja yang menjadi referensi dalam pembuatan panduan.

4.3.1.1 Bizmanual dan Indeks Penilaian

Bizmanualz merupakan perusahaan yang bergerak di bidang pembuatan *template* kebijakan perusahaan sejak tahun 1995, yang telah melayani lebih dari 24.000 pelanggan di seluruh dunia, dengan kebijakan dan prosedur perusahaan lengkap dalam bentuk *template* untuk proses bisnis utama: Akuntansi, Keuangan, IT, SDM, Sales & pemasaran, Keamanan, *Disaster*, ISO *Quality*. Semua *template* SOP dari Bizmanualz telah diteliti dan telah mengikuti *bestpractice* [13].

Di dalam bidang TI, Bizmanualz telah mendeskripsikan kelengkapan SOP organisasi dengan rincian dalam lima buah bidang. Dengan menggunakan standar ini, akan dilakukan pengecekan kelengkapan akan panduan indeks yang akan dibuat dengan lima bidang *template* yang telah disediakan oleh Bizmanualz.

dimana secara keseluruhan kesiapanan manajemen keamanan sudah optimal.

4.3 Output / Luaran

4.3.1 Dokumen Panduan Penggunaan Indeks Penilaian Kesiapan Manajemen Keamanan Layanan

Dokumen panduan ini berisikan langkah-langkah penggunaan indeks penilaian kesiapan manajemen keamanan layanan TI. Panduan tersebut ditunjukkan pada **Lampiran B**. di dalam bagian ini, akan dibahas komponen apa saja yang menjadi referensi dalam pembuatan panduan.

4.3.1.1 Bizmanual dan Indeks Penilaian

Bizmanualz merupakan perusahaan yang bergerak di bidang pembuatan *template* kebijakan perusahaan sejak tahun 1995, yang telah melayani lebih dari 24.000 pelanggan di seluruh dunia, dengan kebijakan dan prosedur perusahaan lengkap dalam bentuk *template* untuk proses bisnis utama: Akuntansi, Keuangan, IT, SDM, Sales & pemasaran, Keamanan, *Disaster*, ISO *Quality*. Semua *template* SOP dari Bizmanualz telah diteliti dan telah mengikuti *bestpractice* [13].

Di dalam bidang TI, Bizmanualz telah mendeskripsikan kelengkapan SOP organisasi dengan rincian dalam lima buah bidang. Dengan menggunakan standar ini, akan dilakukan pengecekan kelengkapan akan panduan indeks yang akan dibuat dengan lima bidang *template* yang telah disediakan oleh Bizmanualz.

Tabel 4.18 SOP IT oleh Bizmanualz

	ID	Keterangan	√ / -	Ref
IT Administration	ITAD101	*Information Technology Management*	√	SS-1
	ITAD102	*IT Records Management*	√	SO-17
	ITAD103	*IT Document Management*	√	SD-1
	ITAD104	*IT Device Naming Conventions*	√	SD-5
	ITAD105	*TCP/IP Implementation Standards*	√	SO-25
	ITAD106	*Network Infrastructure Standards*	√	SO-61
	ITAD107	*Computer and Internet Usage Policy*	√	SS-9
	ITAD108	*E-Mail Policy*	√	SO-39
	ITAD109	*IT Outsourcing*	√	ST-21
	ITAD110	*Department Satisfaction*	√	SS-10
IT Asset Management	ITAM101	*IT Asset Standards*	√	SD-1
	ITAM102	*IT Asset Management*	√	SD-3
	ITAM103	*IT Vendor Selection*	√	SS-13
	ITAM104	*IT Asset Assessment*	√	SD-2
	ITAM105	*IT Asset Installation Satisfaction*	√	SS-10
IT Training and Support	ITTS101	*IT System Administration*	√	SO-16
	ITTS102	*IT Support Center*	√	SS-10
	ITTS103	*IT Server / Network Support*	√	SO-25
	ITTS104	*IT Troubleshooting*	√	SO-64
	ITTS105	*IT User-Staff Training Plan*	√	SD-12
Security and Disaster	ITSD101	*IT Threat And Risk Assessment*	√	CSI-6
	ITSD102	*IT Security Plan*	√	SS-1
	ITSD103	*IT Media Storage*	√	SO-27

	ITSD104	*IT Disaster Recovery*	√	SD-19
	ITSD105	*Computer Malware*	√	ST-10
	ITSD106	*IT Access Control*	√	SO-51
	ITSD107	*IT Security Audits*	√	CSI-24
	ITSD108	*IT Incident Handling*	√	SO-85
Software Development	ITSW101	*IT Project Definition*	√	ST-1
	ITSW102	*IT Project Management*	√	ST-1
	ITSW103	*Systems Analysis*	√	ST-13
	ITSW104	*Software Design*	√	SD-1
	ITSW105	*Software Programming*	√	SO-15
	ITSW106	*Software Documentation*	√	SO-29
	ITSW107	*Software Testing*	√	SO-9
	ITSW108	*Design Changes During Development*	√	ST-17
	ITSW109	*Software Releases and Updates*	√	CSI-2
	ITSW110	*Software Support*	√	SD-24
	ITSW111	*Software Consulting Services*	√	SS-10
	ITSW112	Software Training	√	SD-12

Keterangan :
SS : *Service Strategy*
SD : *Service Design*
ST : *Service Transition*
SO : *Service Operational*
CSI : *Continual Service Improvement*

Dengan melakukan peninjauan kelengkapan SOP antara bizmanualz dan indeks penilaian, dapat dilihat bahwa indeks penilaian telah memenuhi standar minimal untuk kebijakan di bidang teknologi informasi.

4.3.1.2 TeSCA Smart Campus Award

TESCA (Telkom *Smart Campus Award*) merupakan penghargaan yang diberikan Telkom kepada Perguruan Tinggi Negeri dan Swasta di Indonesia. Khususnya dalam aspek implementasi teknologi informasi dan komunikasi.

TESCA merupakan begian dari komitmen Telkom untuk mendorong perguruan tinggi di Indonesia melakukan berbagai percepatan untuk meningkatkan kualitasnya melalui pemanfaatan teknologi informasi dan komunikasi dalam praktek belajar mengajar di kampus.

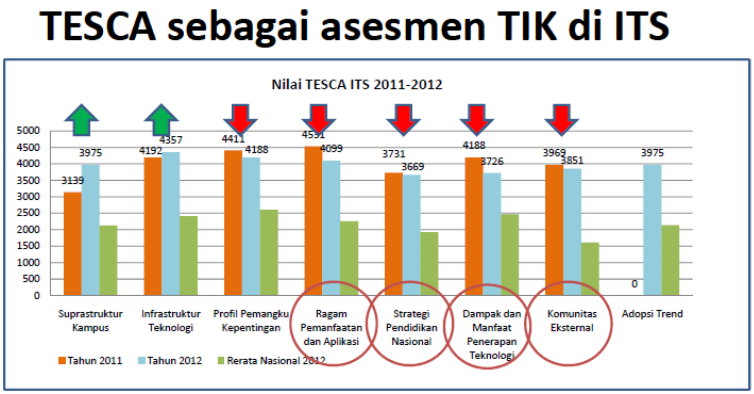
Dari 119 list pertanyaan, dapat dikelompokkan fokusan pertanyaan sebagai berikut :

1. Suprastruktur Kampus
2. Infrastruktur Teknologi
3. Profil Pemangku Kepentingan
4. Ragam Pemanfaatan dan Aplikasi
5. Strategi Pendidikan Nasional
6. Dampak dan Manfaat Penerapan Teknologi
7. Komunikasi Eksternal
8. Adopsi Tren

Adapun salah satu yang menjadi fokusan utama dalam pembuatan indeks penilaian manajemen keamanan layanan teknologi informasi ini adalah membantu organisasi studi kasus mampu menjawab pertanyaan yang berhubungan dengan keamanan di TeSCA *Award.*

LPTSI sebagai badan pengelola teknologi informasi di ITS, senantiasa berusaha memberikan fasilitas dan layanan yang prima dengan salah satunya berusaha untuk semakin mendekati ekspetasi pelanggan dengan tata kelola teknologi informasi berdasarkan Tesca Award sebagai salah satu standar pelaksanaan teknologi informasi di organisasi bidang institute pendidikan.

Hasil dari evaluasi pelaksanaan TI di ITS berdasarkan *Tesca Award* dapat dilihat dalam gambar berikut :



Gambar 4.3 TESCA award di ITS

Dari delapan fokusan pelaksanaan TI di institusi pendidikan berdasarkan TESCA, terdapat empat fokusan utama yang bernilai dibawah rata-rata, yaitu :

1. Ragam Pemanfaatan dan Aplikasi
2. Strategi Pendidikan Nasional
3. Dampak dan Manfaat Penerapan Teknologi
4. Komunikasi Eksternal

Fokusan utama dalam perbaikan tata kelola LPTSI ke depannya yang dituangkan dalam masterplan LPTSI 2013-2017 mulai dari bidang pusat pengelolaan dan pelayanan TIK, pusat pengembangan SI, pusat data dan pelaporan hingga pusat infrastruktur dan keamanan informasi.

4.3.1.3 Standardisasi SLA dan OLA

Service Level Agreement (SLA) merupakan sebuah kerangka untuk memastikan bahwa seluruh kebutuhan layanan dan *customer* telah terpenuhi sesuai dengan kebutuhan organisasi.

Terdapat beberapa macam dalam pembuatan SLA, yaitu layanan berbasis SLA dan *customer* berbasis SLA.

Selain itu, terdapat OLA (*Operational Level Agreement*) yang merupakan sebuah kerangka persetujuan yang menjadi

dasaran organisasi untuk menyampaikan kualitas layanan yang telah disepakati sesuai dengan SLA dalam proses bisnisnya.

Menurut [14], prinsip dari pembuatan sebuah layanan (*service design*) harus mempertimbangkan faktor penyusunnya,termasuk kebutuhan fungsionalitas, nilai bisnis dan seluruh batasan pembangunannya. Dan kesemua pertimbangan ini akan dijabarkan secara rinci dalam dokumen SLA/OLA.

LPTSI sendiri hingga bulan Juni 2014 masih menggunakan POB (Pelaksanaan Operasional Baku) dalam menjalankan layanannya yang masih dirasa kurang untuk melingkupi seluruh kebutuhan pelaksanaan manajemen layanan yang baik. Panduan dalam pembuatan SLA dan OLA yang baik akan dijabarkan dalam **Lampiran B – Panduan Penggunaan Indeks**.

4.3.1.4 *Assessment* Manajemen Keamanan Layanan

Assessment adalah suatu proses sistematis, mandiri, dan terdokumentasi untuk mengevaluasinya secara objektif guna menentukan sejauh mana capaian telah dipenuhi. [15]

Di dalam **Lampiran B – panduan penggunaan indeks**, selain standar operasinal yang baik, dilengkapi juga dengan prosedur dan panduan pelaksanaan *assessment* agar manajemen keamanan layanan yang sudah direncanakan dapat dipantau dan adanya tindakan keberlanjutan.

4.3.2 Indeks Penilaian Kesiapan Manajemen Keamanan Layanan

Indeks penilaian kesiapan manajemen keamanan layanan SI/TI mengacu pada standar ISO 27000 terutama ISO 27002 yang dipetakan dengan standar ITIL v3 dan diukur dengan standar dari COBIT 4.1 dapat digunakan dengan berbasis *Microsoft excel worksheet.*

BAB V
PENUTUP

Berdasarkan hasil pengerjaan tugas akhir ini, terdapat beberapa kesimpulan dan saran sebagai berikut:

5.1 Kesimpulan

1. Pembuatan indeks penilaian manajemen keamanan layanan dengan menggabungkan standar berbasis *Service Delivery* COBIT 4.1, ITIL V3, ISO 27000 dan penilaian kesiapan berdasarkan *maturity model* COBIT 4.1, **relevan**. Hal tersebut ditunjukkan dengan dapat diperolehnya sebuah indeks penilaian yang saling mendukung antara satu standar dengan standar lainnya.
2. Kombinasi antara metodologi manajemen TI menggunakan ITIL, COBIT dan ISO / IEC 27002 akan memberikan hasil yang lebih komprehensif dan efisien baik dari sisi persiapan hingga pengimplementasian fitur-fitur yang sebelumnya tidak dipertimbangkan oleh organisasi yang hanya menggunakan satu buah metodologi.
3. Pembuatan indeks penilaian kesiapan manajemen keamanan layanan SI/TI yang dibuat adalah berupa *microsoft excel worksheet*. Verifikasi kelengkapan dan hubungan yang dilakukan terhadap indeks yang dibuat, yang terdapat di dalam point 4.2.3 Verifikasi BAB IV di dalam tugas akhir ini, memberikan bukti bahwa semua fitur/pertanyaan yang ada di dalam indeks berhubungan dan saling mendukung dengan baik dan sesuai dengan standar yang ada.
4. Indeks penilaian yang dibuat memiliki fitur yang dikhususkan untuk organisasi penyelenggara layanan publik, terutama di perguruan tinggi sehingga fitur/pertanyaan yang ada di dalam indeks lebih bersifat khusus. Adapun kekhususan indeks yang dibuat ini dibahas pada point 4.1.1 Badan Teknologi Sistem Informasi BAB IV di dalam tugas akhir ini.

5.2 Saran

Saran untuk pengembangan indeks penilaian kesiapan manajemen keamanan layanan selanjutnya adalah:

1. Perlunya pengembangan indeks ke dalam bentuk aplikasi, yang diharapkan aplikasi tersebut dapat terhubung langsung dengan dengan laporan kinerja proses bisnis organisasi secara otomatis.
2. Terkait dengan manajemen keamanan layanan, aplikasi belum meng-*cover* manajemen keamanan terkait proses *Transition Planning and Support* dan *Continual Service Improvement* ITIL, diharapkan terdapat pengembangan indeks lebih lanjut agar dapat meng-*cover* hal tersebut.
3. LPTSI masih menggunakan POB (Prosedur Operasional Baku) dalam melakukan manajemen layanannya. Untuk peningkatan manajemen, kami merekomendasikan LPTSI untuk mengimplementasikan dan pengontrolan pelaksanaan manajemen layanan menggunakan dokumen *Service Level Agreement* (SLA), sehingga nantinya manajemen layanan yang ada tidak bersifat statis dan dapat melakukan penambahan atau pengubahan SLA, jika suatu waktu terjadi perubahan proses bisnis maupun jenis layanan yang ada di LPTSI.
4. Untuk membantu pengimplementasian manajemen keamanan layanan yang baik di LPTSI, kami merekomendasikan untuk membangun sebuah tim auditor internal sehingga manajemen layanan yang ada dapat di *monitoring* pencapaian dan kinerjanya dengan baik.

DAFTAR PUSTAKA

[1] M. Kneller, "Best Management Practice," *Executive Briefing : The Benefits of ITIL,* p. 5, 2010.

[2] M. Gehrmann, *Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive Information Technology for Management in Organization,* p. 2, 2012.

[3] IT Governance Institute, COBIT 4.1, USA: IT Governance Institute, 2007.

[4] A. Calder and S. Watkins, IT Governance A Manager's Guide to Data Security and ISO 27001/27002, London: Kogan Page Limited, 2007.

[5] itSMF International, Foundation of IT Service Management based on ITIL V3, Van Haren, 2007.

[6] P. Lijnse, "Service Management Art," 2006. [Online].

[7] S. Architecture, Security Management Framework, Security Architecture, 2009.

[8] ISO/IEC, Information Technology - Security techniques - Code of Practice for Information Security Management, Switzerland: ISO/IEC 2005, 2005.

[9] Direktorat Keamanan Informasi Kementrian Komunikasi dan Informasi, INDEKS KAMI 2.3, Jakarta, 2007.

[10] K. V. Warren, InfoSec Reading Room, SANS Institute, 2010.

[11] Suryo, Keseimbangan Hibridasi dan Kastrasi, PT. Gramedia, 1984.

[12] S. Few, Information Dashboard Design; The effective Visual Communication of Data, California: O'Reilly, 2006.

[13] Bizmanualz. [Online]. Available: http://www.bizmanualz.com/product-category/sop-best-deals. [Accessed 14 5 2014].

[14] Office of Government Commerce, ITIL Version 3 Service Design, Buckinghamshire: OGC, 2011.

[15] R. A. Weber, Information Systems Control and Audit, Fremont, CA, USA: Prentice Hall Business Publishing, 1999.

[16] Office of Government Commerce, ITIL Version 3 Service Operation, Buckinghamshire: OGC, 2011.

[17] M. Rouse, "business intelligence dashboard," 16 November 2010. [Online]. Available: http://searchbusinessanalytics.techtarget.com/definition/business-intelligence-dashboard. [Accessed 14 Agustus 2013].

[18] T. Carlson, Information Security Management : Understanding ISO 17799, Lucent Technologies Worldwisw Services, 2001.

BIODATA PENULIS

Penulis bernama lengkap Farroh Sakinah dan dipanggil Farroh. Penulis lahir di Jakarta, 17 Januari 1991. Penulis memiliki semangat berkarya dan belajar yang tinggi. Dukungan terbesar baginya berasal dari kedua orang tua (Didi Mulyadi dan Ike Kania Dewi). Penulis telah menempuh pendidikan formal, yaitu di SDN 01 Pagi Meruya Selatan Jakarta, SMPN 75 Jakarta, SMAN 112 Jakarta. Selepas lulus dari SMA pada tahun 2009, penulis diterima di Jurusan Sistem Informasi FTIf-ITS pada tahun 2010 dan terdaftar dengan NRP 5210100060.

Penulis sangat menggemari dunia kepemanduan dan pelatihan. Penulis menjadi tim pemandu LKMM TD FTIf 2011, Ketua Badan Koordinasi Pemandu-PSDM Bem FTIf 2012-2013, tim Pemandu LKMM TM 2014 dan Dirjen Badan Koordinasi Pemandu-PSDM BEM ITS 2013-2014.

Di Jurusan Sistem Informasi ini, penulis mengambil Bidang Studi E-bisnis. Penulis juga pernah mengikuti pelatihan LKMM Pra-TD (Pra Tingkat Dasar) hingga LKMM TL (Tingkat Lanjut). Penulis melakukan kerja praktek di PT. Medco Energi Jakarta pada Juni-Juli 2013. Untuk kepentingan penelitian, penulis dapat dihubungi melalui *e-mail: farrohmulyadi@gmail.com.*

LAMPIRAN A
KUISIONER PENGGALIAN KEBUTUHAN INDEKS

Halaman ini sengaja di kosongkan

Keterangan kolom lampiran A :

a) **Proses Manajemen Layanan** merupakan penjelasan dari ruang lingkup manajemen layanan ITIL v3 yang digunakan sebagai kerangka utama dalam pembuatan tata kelola keamanan layanan TI.
b) **Keterangan** merupakan penjelas mengenai tiap-tiap ruang lingkup dan kaitannya dengan dokumen tata kelola keamanan layanan TI.
c) **Area Keamanan** merupakan penjelasan dari ruang lingkup manajemen keamanan ISO 27000 yang digunakan sebagai standar penilaian keamanan layanan TI.
d) **Sub Proses Aktivitas Standar Terkait** merupakan sub proses yang dimiliki oleh masing-masing ruang lingkup manajemen layanan yang digunakan dalam acuan tata kelola keamanan layanan TI.
e) **Ref (referensi) dan Indeks Penilaian** merupakan ID dari referensi sub proses aktivitas standar terkait.
f) **Nilai Verifikasi** merupakan persetujuan verifikasi atas kesesuaian ruang lingkup masing-masing proses dalam manajemen layanan dan manajemen keamanan dengan kondisi eksisting organisasi studi kasus.

Untuk melakukan penggalian data dengan lebih mudah akan kondisi eksisting LPTSI, penilaian menggunakan skala likert yang akan definisinya seperti dibawah ini:

1 : Sangat tidak sesuai

Apabila poin-poin yang ada pada kuisioner verifikasi penilaian kesiapan manajemen keamanan layanan TI yang ada tidak sesuai dengan sub-proses organisasi.

2 : Tidak sesuai

Apabila poin-poin yang ada pada kuisioner verifikasi penilaian kesiapan manajemen keamanan layanan TI yang ada tidak sesuai dengan sub-proses organisasi, hanya sebagian terkait standar dan tidak mencapai 50%.

3 : Cukup

Apabila poin-poin yang ada pada kuisioner verifikasi penilaian kesiapan manajemen keamanan layanan TI yang ada tidak sesuai dengan sub-proses organisasi, hanya sebagian terkait dan mencapai 50%-75%

4 : Sesuai

Apabila poin-poin yang ada pada kuisioner verifikasi penilaian kesiapan manajemen keamanan layanan TI yang ada telah sesuai dengan sub-proses organisasi dan mencapai lebih dari 75%

5 : Sangat sesuai

Apabila poin-poin yang ada pada kuisioner verifikasi penilaian kesiapan manajemen keamanan layanan TI yang ada telah sesuai dengan sub-proses organisasi secara keseluruhan.

Lampiran A
Hasil Wawancara Verifikasi kebutuhan Indeks

Biodata koresponden dari kuisioner verifikasi kebutuhan indeks :

Tempat	:	Badan Teknologi dan Sistem Informasi ITS Surabaya
Tanggal	:	19 Juni 2014
Jabatan	:	Sekertaris LPTSI ITS KASUB Pusat data & Pelaporan LPTSI Koordinator LPTSI
Tujuan	:	Mengetahui validitas indeks penilaian kesiapan manajemen keamanan layanan TI
Metode Pengisian	:	1. Pengisian langsung oleh Pihak yang bersangkutan 2. Diskusi dalam rapat Koordinasi LPTSI

Kuisioner penggalian data :

Proses Manajemen Layanan	Keterangan	Area Keamanan	Sub Proses Aktivitas Standar Terkait	Ref	Indeks Penilaian	Validasi				
						1	2	3	4	5
Kesiapan Organisasi *Service Strategy* - ITIL v3	Setiap proses yang berkaitan dengan kebijakan layanan dan struktur organisasi, harus di pastikan keamanannya dan di dukung dengan dokumentasi yang baik.	Dokumen Kebijakan Keamanan Layanan	Dokumen Kebijakan Keamanan Layanan	SLA	KO-1					
			Dokumentasi Persetujuan seluruh pihak	SLA	KO-2					
			Dokumentasi Penanggung jawab kebijakan	SLA	KO-3					
			Dokumentasi Ruang lingkup Persetujuan	SLA	KO-6					
		Keamanan Internal	Prosedur Forum Keamaan Internal	OLA	KO-4					
			Dokumentasi persetujuan jadwal forum	OLA	KO-5					
			Notulensi Forum	OLA	KO-7					
			Kebijakan Kesadaran Keamanan Pribadi	OLA	KO-8					
			Prosedur Pemberian Hak Akses	OLA	KO-9					
			Pusat Informasi	OLA	KO-10					
			Dokumentasi kontak institusi penting	OLA	KO-11					
			Auditor Internal	OLA	KO-12					
		Keamanan Eksternal	Dokumen Identifikasi dan penanggulangan Risiko pihak Ketiga	OLA	KO-13					
			Standar Keamanan Minimal Organisasi	OLA	KO-14					
			Standar Pemeliharaan Aset Organisasi	OLA	KO-15					

Proses Manajemen Layanan	Keterangan	Area Keamanan	Sub Proses Aktivitas Standar Terkait	Ref	Indeks Penilaian	Validasi				
						1	2	3	4	5
Manajemen Aset *Service Design* - ITIL v3	Setiap proses yang berkaitan dengan pemilihan teknologi, infrastruktur dan sumber daya yang menjalankan layanan baik dari sumber daya internal maupun eksternal, harus di pastikan keamanannya dan di dukung dengan dokumentasi yang baik.	Manajemen Aset	Dokumentasi Manajemen Inventaris Aset	SLA	MA-1					
			Dokumentasi Penanggung jawab Aset	SLA	MA2					
			Dokumentasi Klasifikasi Aset	SLA	MA-3					
			Prosedur Klasifikasi Aset	OLA	MA-4					
			Prosedur Labelling dan Handling Informasi	OLA	MA-5					
		Sumber Daya Manusia	Prosedur Pemilihan Karyawan	OLA	MA-6					
			Kontrak Karyawan	OLA	MA-10					
			Pelatihan dan Pengembangan Karyawan	SLA	MA-12					
			Prosedur Pendisiplinan Karyawan	OLA	MA-13					
			Prosedur Pemberhentian Karyawan	OLA	MA-14					
			Prosedur Pengembalian Aset	OLA	MA-15					
			Prosedur Pemberhentian Hak Akses	OLA	MA-16					
		Fisik dan Lingkungan	Kebijakan Pembatasan Informasi	SLA	MA-17					
			Prosedur Pengamanan Kantor, Ruangan dan Fasilitas	OLA	MA-18					
			Dokumen Penjagaan dari Bencana	SLA	MA-19					
			Dokumen Penjagaan Ancaman dari Tetangga	SLA	MA-20					
			Prosedur Keamanan Area	OLA	MA-21					
			Prosedur Peletakan Peralatan Penjagaan Keamanan	OLA	MA-24					

	Prosedur Pengadaan Peralatan Pendukung	OLA	MA-25					
	Prosedur Keamanan Kabel	OLA	MA-26					
	Prosedur Pemeliharaan Peralatan	OLA	MA-27					
	Prosedur Penggunaan Peralatan di luar Area	OLA	MA-30					
	Prosedur Pemusnahan Properti	OLA	MA-33					
	Prosedur *Clean Desk* dan C*lean Screen*	OLA	MA-34					

Proses Manajemen Layanan	Keterangan	Area Keamanan	Sub Proses Aktivitas Standar Terkait	Ref	Indeks Penilaian	Validasi				
						1	2	3	4	5
Penyusunan Keamanan TI *Service Transition - ITIL v3*	Setiap proses yang berkaitan dengan proses penambahan, pengembangan dan pemeliharaan TI, harus di pastikan keamanannya dan di dukung dengan dokumentasi yang baik.	Tingkat Kebutuhan	Dokumentasi Analisa Kebutuhan Keamanan	SLA	SK-1					
			Dokumentasi Analisa Kegagalam Keamanan	SLA	SK-2					
			Dokumentasi Analisa Risiko Keamanan	SLA	SK-3					
		Validitas Data	Prosedur Validasi *Input*	OLA	SK-4					
			Prosedur Kontrol *Input*	OLA	SK-5					
		Proses Internal	Prosedur Mitigasi Risiko	OLA	SK-7					
			Prosedur penggunaan Pesan Keamanan	OLA	SK-8					
			Prosedur Validasi *Output*	OLA	SK-9					
		Kriptografi	Kebijakan Kriptografi	SLA	SK-10					
			Prosedur penggunaan teknik kriptografi	OLA	SK-11					
		System File	Prosedur kotrol *operatonal system*	OLA	SK-13					
			Prosedur kotrol *source code*	OLA	SK-15					
		program source code	Prosedur perubahan sistem	OLA	SK-16					
			Prosedur Pemantauan Perubahan Sistem	OLA	SK-17					
			Prosedur Pencegahan Kebocoran Informasi	OLA	SK-20					
			Prosedur *Outsourced Software Development*	OLA	SK-21					

Proses Manajemen Layanan	Keterangan	Area Keamanan	Sub Proses Aktivitas Standar Terkait	Ref	Indeks Penilaian	Validasi				
						1	2	3	4	5
Pelaksanaan Keamanan TI *Service Operation - ITIL v3*	Setiap proses yang berkaitan dengan proses pelaksanaan layanan TI, harus di pastikan keamanannya dan di dukung dengan dokumentasi yang baik.	Manajemem Komunikasi dan Operasional	Dokumentasi Kebijakan Operasional	SLA	PK-1					
			Prosedur peninjauan *log*	OLA	PK-3					
			Pemisahan Tugas dan Wewenang	SLA	PK-4					
			Prosedur Pemisahan Fasilitas	OLA	PK-5					
			Prosedur Peninjauan dan Perencanan Kapasitas	OLA	PK-8					
			Prosedur Pengetesan Penerimaan Sistem	OLA	PK-9					
			Prosedur Penggunaan *Software* berlisensi	OLA	PK-12					
			Prosedur Penggunaan *Antivirus*	OLA	PK-14					
			Prosedur *Back-Up*	OLA	PK-17					
			Prosedur Pelaporan Kesalahan Sistem	OLA	PK-22					
			Prosedur Kontrol Jaringan	OLA	PK-25					
			Prosedur Penggunaan *removable media*	OLA	PK-27					
			Prosedur Penyimpanan Informasi	OLA	PK-29					
			Prosedur Pengecekan Akses	OLA	PK-31					
			Prosedur Pertukaran Informasi	OLA	PK-32					
			Prosedur Pengetesan Media *Back-up*	OLA	PK-48					
			Prosedur Pengangkutan Media Fisik	OLA	PK-34					
			Prosedur Pengontrolan *e-commerce*	OLA	PK-36					
			Prosedur Pengontrolan *e-mail*	OLA	PK-39					
			Kebijakan *electronic office system*	SLA	PK-41					
			Prosedur Pengontrolan *electronic office*	OLA	PK-42					

			system							
			Prosedur Penyebarluasan Informasi	OLA	PK-43					
			Prosedur Sinkronisasi Waktu	OLA	PK-50					
	Setiap proses yang berkaitan dengan proses pelaksanaan layanan TI, harus di pastikan keamanannya dan di dukung dengan dokumentasi yang baik.	Kontrol Akses	Kebijakan Akses	SLA	PK-51					
			Prosedur Manajemen Password	OLA	PK-56					
			Prosedur Pengawasan Akses	OLA	PK-58					
			Kebijakan Layanan Jaringan	SLA	PK-61					
			Prosedur Identifikasi Jaringan	OLA	PK-63					
			Prosedur Pengetesan Jaringan	OLA	PK-64					
			Prosedur *log-on* sistem	OLA	PK-70					
			Prosedur Pembatasan Koneksi	OLA	PK-76					
			Prosedur *Teleworking*	OLA	PK-82					
		Manajemen Insiden	Kebijakan Manajemen Insiden	SLA	PK-84					
			Prosedur Manajemen Insiden	OLA	PK-85					
			Prosedur *Audit Incident Log*	OLA	PK-88					
			Prosedur Pengumpulan Bukti Insiden	OLA	PK-89					
			Prosedur Pelaporan Insiden	OLA	PK-91					

Proses Manajemen Layanan	Keterangan	Area Keamanan	Sub Proses Aktivitas Standar Terkait	Ref	Indeks Penilaian	Validasi				
						1	2	3	4	5
Perencanaan Pengembangan Service Continuity - ITIL v3	Setiap proses yang berkaitan dengan proses pengembangan layanan TI, harus di pastikan keamanannya dan di dukung dengan dokumentasi yang baik.	*Business Continuity Management*	Kerangka *Business Continuity Plan* (OLA)	SLA	PP-1					
			Prosedur Pengembangan BCP dan Strategy Plan	OLA	PP-2					
			Prosedur Pengetesan BCP	OLA	PP-4					
			Prosedur Identifikasi Risiko dalam BCP	OLA	PP-6					
		Pemenuhan Persyaratan Hukum	Dokumentasi Hukum / Aturan	SLA	PP-11					
			Prosedur Pemenuhan Persyaratan Hukum	OLA	PP-12					
			Prosedur *Intellectual Property Rights* (IPR)	OLA	PP-13					
			Prosedur Pengamanan dan Penjagaan Penyalahgunaan Data dan Informasi	OLA	PP-15					
		Pemenuhan Standar	Operasional Pengecekan Kesesuaian Standar	OLA	PP-20					
		Audit Sistem	Prosedur Perencanaan Audit Sistem	OLA	PP-24					
			Prosedur Akses Audit Sistem	OLA	PP-25					

Rekomendasi hasil dari verifikasi kebutuhan indeks :

Proses Manajemen Layanan	ID	Sub Proses Aktivitas Standar Terkait	Responden 1	Responden 2	Responden 3	Responden 4	Kondisi Ideal	Perubahan/Penambahan	Keterangan
Kesiapan Organisasi *Service Strategy* - ITIL v3	S1	Dokumen Kebijakan Keamanan Layanan	5	4	4	3	4	1. Penambahan Dokumen Monitoring Pengimplementasian kebijakan keamanan layanan 2. Peninjauan kembali Persetujuan seluruh pihak dalam dokumen kebijakan 3. Peninjauan kembali penanggung jawab dalam dokumen kebijakan 4. Peninjauan kembali ruang lingkup dalam dokumen kebijakan	Rekomendasi sesuai panduan
	S2	Dokumentasi Persetujuan seluruh pihak	5	4	4	3	4		
	S3	Dokumentasi Penanggung jawab kebijakan	5	4	4	3	4		
	S4	Dokumentasi Ruang lingkup Persetujuan	5	4	4	3	4		
	S5	Prosedur Forum Keamaan Internal	4	3	3	3	4	Penambahan dokumen : 1. Prosedur Pelaksanaan Forum Jadwal Forum (terjadwal)& Penanggung jawab 2. Dokumen Notulensi Pelaksanaan Forum	Rekomendasi sesuai panduan
	S6	Dokumentasi persetujuan jadwal forum	4	2	2	3	4		
	S7	Notulensi Forum	4	2	3	2	4		

	S8	Kebijakan Kesadaran Keamanan Pribadi	4	3	3	2	4	1. Peninjauan kembali prosedur pelaksanaan kesadaran keamanan pribadi 2. Penambahan dokumen *monitoring* implementasi kebijakan kesadaran keamanan pribadi	Rekomendasi sesuai panduan
	S9	Prosedur Pemberian Hak Akses	5	3	3	3	4	Penambahan dokumen *monitoring hak akses*	Rekomendasi sesuai panduan
	S10	Pusat Informasi	5	4	3	3	4	Penambahan dokumen laporan aktivitas pusat informasi	Rekomendasi sesuai panduan
	S11	Dokumentasi kontak institusi penting	5	4	4	4	4	-	Sudah Baik
	S12	Auditor Internal	5	4	3	1	4	1. Peninjauan kembali, adakah kebijakan audit internal. 2. Apabila belum tersedia, susun kebijakan audit internalnya. Apabila sudah tersedia, tambahkan dokumen prosedur pelaksanaan audit internal. 3. Penambahan dokumen laporan (monitoring) pelaksanaan audit internal	Rekomendasi sesuai panduan

	S13	Dokumen Identifikasi dan penanggulangan Risiko pihak Ketiga	4	3	2	1	4	1. Peninjauan kembali, adakah kebijakan identifikasi risiko dari pihak ketiga 2. Apabila belum tersedia, susun kebijakan identifikasi risiko. Apabila sudah tersedia, tambahkan dokumen identifikasi penanggulangan risiko dari pihak ketiga. 3. Penambahan dokumen monitoring/*update* identifikasi risiko pihak ketiga	Rekomendasi sesuai panduan
	S14	Standar Keamanan Minimal Organisasi	4	3	2	3	4	1. Peninjauan kembali, adakah standar keamanan minimal organisasi 2. penambahan dokumen monitoring pelaksanaan standar keamanan minimal organisasi	Rekomendasi sesuai panduan
	S15	Standar Pemeliharaan Aset Organisasi	4	3	2	3	4	1. Peninjauan kembali, adakah standar pemeliharaan aset organisasi 2. Penambahan dokumen monitoring pelaksanaan standar pemeliharaan aset organisasi	Rekomendasi sesuai panduan

Proses Manajemen Layanan	ID	Sub Proses Aktivitas Standar Terkait	Responden 1	Responden 2	Responden 3	Responden 4	Kondisi Ideal	Perubahan/Penambahan	Keterangan
Manajemen Aset *Service Design* - ITIL v3	A1	Dokumentasi Manajemen Inventaris Aset	-	4	4	4	4	-	Sudah Baik
	A2	Dokumentasi Penanggung jawab Aset	-	4	4	4	4	-	Sudah Baik
	A3	Dokumentasi Klasifikasi Aset	-	4	3	3	4	1. Lihat Kesiapan Organisasi *Service Strategy* - ID S15 2. Peninjauan kembali prosedur klasifikasi aset dalam dokumen standar pemeliharaan aset 3. Peninjauan kembali dokumen klasifikasi aset dalam dokumen standar pemeliharaan aset	Rekomendasi sesuai panduan
	A4	Prosedur Klasifikasi Aset	-	4	3	3	4		
	A5	Prosedur Labelling dan Handling Informasi	-	3	3	4	4	1. Peninjauan kembali, adakah prosedur labeling dan handling informasi 2. penambahan dokumen *monitoring* pelaksanaan *labeling* dan *handling* informasi	Rekomendasi sesuai panduan
	A6	Prosedur Pemilihan Karyawan	-	4	4	4	4	-	Sudah Baik
	A7	Kontrak Karyawan	-	4	5	4	4	-	Sudah Baik
	A8	Pelatihan dan Pengembangan	-	4	5	4	4	-	Sudah Baik

		Karyawan							
	A9	Prosedur Pendisiplinan Karyawan	-	4	3	4	4	1. Peninjauan kembali, apakah organisasi telah memiliki prosedur pendisiplinan karyawan 2. penambahan dokumen monitoring pelaksanaan pendisiplinan karyawan	Rekomendasi sesuai panduan
	A10	Prosedur Pemberhentian Karyawan	-	3	3	3	4	1. Peninjauan kembali, adakah prosedur pemberhentian karyawan 2. penambahan dokumen monitoring pelaksanaan pemberhentian karyawan	Rekomendasi sesuai panduan
	A11	Prosedur Pengembalian Aset	-	3	4	4	4	1. Peninjauan kembali, adakah prosedur pengembalian aset 2. penambahan dokumen monitoring pelaksanaan prosedur pengembalian aset.	Rekomendasi sesuai panduan
	A12	Prosedur Pemberhentian Hak Akses	-	3	2	3	4	1. Lihat Kesiapan Organisasi *Service Strategy* - ID S9 2. Peninjauan kembali prosedur pemberhentian hak akses 3. peninjauan kembali dokumen laporan pelaksanaan prosedur pemberhentian hak akses	Rekomendasi sesuai panduan
	A13	Kebijakan Pembatasan Informasi		4	3	3	4	1. Peninjauan kembali, adakah kebijakan pembatasan informasi 2. penambahan dokumen monitoring pelaksanaan kebijakan pembatasan informasi	Rekomendasi sesuai panduan

	A14	Prosedur Pengamanan Kantor, Ruangan dan Fasilitas		3	3	4	4	1. Peninjauan dan pembuatan Prosedur pengamanan : a. Area (Kantor, ruangan, fasilitas) b. Bencana c. Ancaman tetangga (Lihat kesiapan organsasi *Service Strategy* - ID S13) 2. penambahan dokumen monitoring pelaksanaan prosedur pengamanan	Rekomendasi sesuai panduan
	A15	Dokumen Penjagaan dari Bencana		3	2	3	4		
	A16	Dokumen Penjagaan Ancaman dari Tetangga		3	2	3	4		
	A17	Prosedur Keamanan Area		4	2	2	4		
	A18	Prosedur Peletakan Peralatan Penjagaan Keamanan		4	2	2	4	1. Lihat Kesiapan Organisasi *Service Strategy* - ID S15 2. Peninjauan dan pembuatan Prosedur pengamanan peralatan: a. peletakan peralatan b. pengadaan peralatan pendukung c. keamanan kabel d. penggunaan diluar area 3. penambahan dokumen monitoring pengamanan peralatan dan pemeliharaannya.	Rekomendasi sesuai panduan
	A19	Prosedur Pengadaan Peralatan Pendukung		4	2	2	4		
	A20	Prosedur Keamanan Kabel		2	2	2	4		
	A21	Prosedur Pemeliharaan Peralatan		2	2	2	4		
	A22	Prosedur Penggunaan Peralatan di luar Area		3	2	2	4		
	A23	Prosedur Pemusnahan Properti		2	2	2	4	1. Peninjauan kembali, adakah prosedur pemusnahan *property* 2. Penambahan dokumen monitoring pelaksanaan pemusnahan *property*	Rekomendasi sesuai panduan

	A24	Prosedur *Clean Desk* dan C*lean Screen*		3	2	2	4	1. Lihat Kesiapan Organisasi *Service Strategy* - ID S8 2. Peninjauan kembali prosedur *clean desk* dan *clean screen* 3. Penambahan dokumen monitoring pelaksanaan *clean desk* and *clean screen*	Rekomendasi sesuai panduan

Proses Manajemen Layanan	ID	Sub Proses Aktivitas Standar Terkait	Responden 1	Responden 2	Responden 3	Responden 4	Kondisi Ideal	Perubahan/Penambahan	Keterangan
Penyusunan Keamanan TI *Service Transition - ITIL v3*	T1	Dokumentasi Analisa Kebutuhan Keamanan	5	3	2	2	4	1. Lihat Kesiapan Organisasi *Service Strategy* - ID S1 2. Peninjauan kembali Dokumen Kebijakan Keamanan, adakah analisa kebutuhan keamanan 3. Peninjauan kembali Dokumen Kebijakan Keamanan, adakah analisa kegagalan keamanan 4. Peninjauan kembali Dokumen Kebijakan Keamanan, adakah analisa risiko beserta prosedur mitigasinya 5. Penambahan dokumen *update* analisa kebutuhan keamanan, kegagalan keamanan dan risiko keamanan.	Rekomendasi sesuai panduan
	T2	Dokumentasi Analisa Kegagalan Keamanan	5	3	2	2	4		
	T3	Dokumentasi Analisa Risiko Keamanan	5	3	2	2	4		
	T4	Prosedur Mitigasi Risiko		3	2	2	4		
	T5	Prosedur Pencegahan Kebocoran Informasi		3	2	3	4	1. Lihat Manajemen Aset *Service Design*- ID A15-A17 2. Pembuatan dokumen prosedur pencegahan kebocoran informasi 3. Pembuatan dokumen monitoring pelaksanaan prosedur pencegahan kebocoran informasi	Rekomendasi sesuai panduan
	T6	Prosedur Validasi *Input*		3	2	2	4	1. Pembuatan dokumen prosedur kontrol	Rekomendasi

	T7	Prosedur Kontrol *Input*		3	2	2	4	dan validasi input output data 2. Pembuatan dokumen monitoring pelaksanaan kontrol input output data 3. Peninjauan kembali dokumen prosedur kontrol input output data, adapakah prosedur penggunaan pesan keamanan (untuk mengurangi kesalahan)	sesuai panduan
	T8	Prosedur Validasi *Output*		3	2	2	4		
	T9	Prosedur penggunaan Pesan Keamanan		3	2	2	4		
	T10	Kebijakan Kriptografi			2	2	4	1. Peninjauan kembali, adakah kebijakan penggunaan teknik kriptografi 2. Penambahan dokumen monitoring pelaksanaan penggunaan teknik kriptografi	Rekomendasi sesuai panduan
	T11	Prosedur penggunaan teknik kriptografi			3	2	4		
	T12	Prosedur kotrol *operational system*			3	3	4	1. Peninjauan kembali, adakah prosedur kontrol *operational system* 2. penambahan dokumen monitoring pelaksanaan kontrol *operational system*	Rekomendasi sesuai panduan
	T13	Prosedur kotrol *source code*			2	3	4	1. Peninjauan kembali, adakah prosedur kontrol *source code* 2. penambahan dokumen monitoring pelaksanaan kontrol *source code*	Rekomendasi sesuai panduan
	T14	Prosedur perubahan sistem			2	3	4	1. Peninjauan kembali, adakah prosedur perubahan sistem 2. penambahan dokumen monitoring pelaksanaan perubahan sistem	Rekomendasi sesuai panduan
	T15	Prosedur Pemantauan Perubahan Sistem			2	3	4		

	T16	Prosedur *Outsourced Software Development*			2	3	4	1. Lihat Kesiapan Organisasi *Service Strategy* - S13 2. Peninjauan kembali Dokumen analisa risiko pihak ketiga, adalah prosedur *outsourced software development*	Rekomendasi sesuai panduan

Proses Manajemen Layanan	ID	Sub Proses Aktivitas Standar Terkait	Responden 1	Responden 2	Responden 3	Responden 4	Kondisi Ideal	Perubahan/Penambahan	Keterangan
Pelaksanaan Keamanan TI *Service Operation - ITIL v3*	O1	Dokumentasi Kebijakan Operasional	4	-	2	3	4	1. Penambahan Dokumen kebijakan operasional layanan 2. Peninjauan kembali pemisahan tugas dan wewenang dalam dokumen kebijakan operasional 3. Peninjauan kembali pemisahan fasilitas (operasional dan *testing*) dalam dokumen kebijakan operasional 4. Pembuatan dokumen monitoring pelaksanaan dokumen kebijakan operasional layanan	Rekomendasi sesuai panduan
	O2	Pemisahan Tugas dan Wewenang	4	-	3	3	4		
	O3	Prosedur Pemisahan Fasilitas	4	-	2	2	4		
	O4	Prosedur peninjauan *log*	4	-	3	2	4	1. Pembuatan dokumen prosedur peninjauan *log* 2. Pembuatan dokumen monitoring pelaksanaan peninjauan *log*	Rekomendasi sesuai panduan
	O5	Prosedur Peninjauan dan Perencanan Kapasitas	4	-	2	2	4	1. Pembuatan dokumen prosedur peninjauan dan perencanaan kapasitas 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur peninjauan dan perencanaan kapasitas	Rekomendasi sesuai panduan

	O6	Prosedur Pengetesan Penerimaan Sistem	4	-	2	2	4	1. Pembuatan dokumen prosedur pengetesan penerimaan sistem 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur pengetesan penerimaan sistem	Rekomendasi sesuai panduan
	O7	Prosedur Penggunaan *Software* berlisensi	4	-	2	2	4	1. Pembuatan dokumen prosedur penggunaan *software* berlisensi 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur penggunaan *software* berlisensi	Rekomendasi sesuai panduan
	O8	Prosedur Penggunaan *Antivirus*	4	-	2	2	4	1. Pembuatan dokumen prosedur penggunaan *antivirus* 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur penggunaan *antivirus*	Rekomendasi sesuai panduan
	O9	Prosedur *Back-Up*	4	-	2	2	4	1. Pembuatan dokumen prosedur *back-up* 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur *back-up*	Rekomendasi sesuai panduan
	O10	Prosedur Pelaporan Kesalahan Sistem	4	-	2	2	4	1. Pembuatan dokumen prosedur pelaporan kesalahan 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur pelaporan kesalahan	Rekomendasi sesuai panduan
	O11	Prosedur Penggunaan *removable media*	4	-	2	2	4	1. Pembuatan dokumen prosedur penggunaan *removable media* 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur penggunaan *removable media*	Rekomendasi sesuai panduan

	O12	Prosedur Penyimpanan Informasi	4		2	2	4	1. Pembuatan dokumen prosedur penyimpanan informasi 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur penyimpanan informasi	Rekomendasi sesuai panduan
	O13	Prosedur Pengecekan Akses	4		2	2	4	1. Lihat Kesiapan Organisasi *Service Strategy* - ID S9 dan Manajemen Aset - *Service Design* - ID A12 2. Peninjauan kembali dokumen monitoring pelaksanaan akses	Rekomendasi sesuai panduan
	O14	Prosedur Pertukaran Informasi	4		2	2	4	1. Pembuatan dokumen prosedur pertukaran informasi 2. Pembuatan dokumen monitoring pelaksanaan prosedur pertukaran informasi	Rekomendasi sesuai panduan
	O15	Prosedur Pengetesan Media *Back-up*	4		2	2	4	1. Lihat Pelaksanaan Keamanan TI *Service Operation* - ID O9 2. Peninjauan kembali dokumen prosedur *back-up*, apakah memiliki prosedur pengetesan *media back-up* 3. Peninjauan kembali dokumen prosedur *back-up*, apakah memiliki dokumen *moniitoring* pengetesan *media back-up*	Rekomendasi sesuai panduan
	O16	Prosedur Pengangkutan Media Fisik	4		2	2	4	1. Pembuatan dokumen prosedur pengangkutan media 2. Pembuatan dokumen monitoring pelaksanaan prosedur pengangkutan media	Rekomendasi sesuai panduan

	O17	Prosedur Pengontrolan *e-commerce*	4		2	2	4	1. Pembuatan dokumen prosedur pengoperasian *e-commerce* 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur pengoperasian *e-commerce*	Rekomendasi sesuai panduan
	O18	Prosedur Pengontrolan *e-mail*	4		2	2	4	1. Pembuatan dokumen prosedur 2. pembuatan dokumen *monitoring* pelaksanaan prosedur pengontrolan *e-mail*	Rekomendasi sesuai panduan
	O19	Kebijakan *electronic office system*	4		2	2	4	1. Pembuatan dokumen kebijakan *e-office system* 2. Pembuatan dokumen *monitoring* pelaksanaan kebijakan *e-office system*	Rekomendasi sesuai panduan
	O20	Prosedur Pengontrolan *electronic office system*	4		2	2	4		
	O21	Prosedur Penyebarluasan Informasi	4		2	2	4	1. Lihat Manajemen Aset *Service Design* - A13 2. Peninjauan kembali Dokumen Pembatasan Informasi, adalah prosedur penyebarluasan informasi	Rekomendasi sesuai panduan
	O22	Prosedur Sinkronisasi Waktu	4		2	2	4	1. Lihat Kesiapan Organisasi *Service Strategy* - S14 2. Peninjauan kembali Dokumen Standar Minimal Keamanan Organisasi, apakah terdapat prosedur penyamaan sinkronisasi waktu	Rekomendasi sesuai panduan

	O23	Kebijakan Akses	5	4	3	3	4	1. Lihat Kesiapan Organisasi *Service Strategy* - S9 2. Lihat Manajemen Aset *Service Design* - A12 3. Lihat Pelaksanaan Keamanan TI *Service Operation* - O13 4. Peninjauan kembali ketiga dokumen menjadi kebijakan akses	Rekomendasi sesuai panduan
	O24	Prosedur Pengawasan Akses	5	4	3	3	4	1. Lihat Pelaksanaan Keamanan TI *Service Operation* - O23 2. Peninjauan kembali Dokumen kebijakan akses, apakah sudah memiliki prosedur pengawasan akses	Rekomendasi sesuai panduan
	O25	Prosedur Manajemen *Password*	5	4	3	3	4	1. Pembuatan dokumen prosedur manajemen *password* 2. Pembuatan dokumen *monitoring* pelaksanaan prosedur manajemen *password*	Rekomendasi sesuai panduan
	O26	Kebijakan Layanan Jaringan	5	3	3	3	4	1. Pembuatan dokumen kebijakan layanan jaringan 2. Peninjauan kembali dokumen kebijakan jaringan, apakah terdapat prosedur identifikasi jaringan. 3. Peninjauan kembali dokumen kebijakan jaringan, apakah terdapat prosedur pengetesan jaringan. 4. Peninjauan kembali dokumen kebijakan jaringan, apakah terdapat prosedur kontrol kebijakan jaringan	Rekomendasi sesuai panduan
	O27	Prosedur Identifikasi Jaringan	5	4	3	3	4		
	O28	Prosedur Pengetesan Jaringan	5	4	3	3	4		
	O29	Prosedur Kontrol Jaringan	5	4	2	2	4		

	O30	Prosedur *log-on* sistem	5	4	3	3	4	1. Lihat Manajemen Aset *Service Design* - A13 2. Peninjauan kembali Dokumen kebijakan pembatasan informasi, apakah memiliki prosedur *log-on* sistem	Rekomendasi sesuai panduan
	O31	Prosedur Pembatasan Koneksi	5	4	3	3	4	1. Lihat Manajemen *Aset Service Design* - A13 2. Peninjauan kembali dokumen kebijakan pembatasan informasi, apakah memiliki prosedur pembatasan akses sistem	Rekomendasi sesuai panduan
	O32	Prosedur *Teleworking*	5	4	3	3	4	pembuatan dokumen *monitoring* pelaksanaan prosedur *teleworking*	Rekomendasi sesuai panduan
	O33	Kebijakan Manajemen Insiden	5	3	3	2	4	1. Pembuatan dokumen kebijakan manajemen insiden 2. Peninjauan kembali dokumen kebijakan manajemen insiden, apakah terdapat prosedur manajemen insiden. 3. Peninjauan kembali dokumen kebijakan manajemen insiden, apakah terdapat prosedur *audit incident log.* 4. Peninjauan kembali dokumen kebijakan manajemen insiden, apakah terdapat prosedur pengumpulan bukti insiden 5. Peninjauan kembali dokumen	Rekomendasi sesuai panduan
	O34	Prosedur Manajemen Insiden	5	2	2	2	4		
	O35	Prosedur *Audit Incident Log*	5	2	2	2	4		
	O36	Prosedur Pengumpulan Bukti Insiden	5	2	2	2	4		
	O37	Prosedur Pelaporan Insiden	5	3	2	4	4		

								kebijakan manajemen insiden, apakah terdapat prosedur pelaporan insiden.	
Proses Manajemen Layanan	**ID**	**Sub Proses Aktivitas Standar Terkait**	**Responden 1**	**Responden 2**	**Responden 3**	**Responden 3**	**Kondisi Ideal**	**Perubahan/Penambahan**	**Keterangan**
Perencanaan Pengembangan *Service Continuity* - ITIL v3	PP1	Kerangka *Business Continuity Plan* (OLA)	4	3	2	2	4	1. Pembuatan dokumen kebijakan BCP Organisasi 2. Peninjauan kembali dokumen kebijakan BCP organisasi, apakah terdapat prosedur pengembangan BCP dan strategy plan 3. Peninjauan kembali dokumen kebijakan BCP organisasi, apakah terdapat prosedur pengetesan BCP 4. Peninjauan kembali dokumen kebijakan BCP organisasi, apakah terdapat prosedur identifikasi risiko BCP 5. Peninjauan kembali dokumen kebijakan BCP organisasi, apakah terdapat dokumen laporan monitoring kebijakan dan prosedur BCP	Rekomendasi sesuai panduan
	PP2	Prosedur Pengembangan BCP dan Strategy Plan	4	4	3	1	4		
	PP3	Prosedur Pengetesan BCP	5	3	2	1	4		
	PP4	Prosedur Identifikasi Risiko dalam BCP	5	3	2	1	4		

	PP5	Dokumentasi Hukum / Aturan	5	1	1	2	4	1. Pembuatan dokumen dokumetasi hukum/aturan yang harus dipenuhi 2. Pembuatan dokumen *update* peninjauan hukum/aturan yang telah terpenuhi	Rekomendasi sesuai panduan
	PP6	Prosedur Pemenuhan Persyaratan Hukum	4	1	1	1	4	1. Lihat Perencanaan Pengembangan *Service Continuity* - PP5 2. Peninjauan kembali Dokumen dokumentasi hukum/aturan yang harus dipenuhi, apakah sudah dilengkapi prosedur pelaporan pemenuhan persyaratan hukum	Rekomendasi sesuai panduan
	PP7	Prosedur *Intellectual Property Rights* (IPR)	4	1	1	1	4	1. Pembuatan dokumen prosedur IPR 2. Pembuatan dokumen *monitoring* prosedur IPR	Rekomendasi sesuai panduan
	PP8	Prosedur Pengamanan dan Penjagaan Penyalahgu-naan Data dan Informasi	4	2	1	1	4	1. Lihat Manajemen Aset *Service Design* -ID A13 dan Penyusunan Keamanan TI *Service Transition* ID T5 2. Peninjauan kembali Dokumen kebijakan pembatasan informasi, apakah memiliki prosedur pengamanan dan penjagaan penyalahgunaan data dan informasi	Rekomendasi sesuai panduan
	PP9	Operasional Pengecekan Kesesuaian Standar	5	4	2	2	4	1. Pembuatan dokumen prosedur pengecekan kesesuaian standar 2. Pembuatan dokumen *monitoring* prosedur pengecekan kesesuaian standar	Rekomendasi sesuai panduan

	PP10	Prosedur Perencanaan Audit Sistem	4	3	2	2	4	1. Lihat Kesiapan Organisasi *Service Strategy* - S12 2. Pembuatan dokumen prosedur perencanaan audit sistem 3. Pembuatan dokumen *monitoring* pelaksanaan prosedur perencanaan audit sistem 4. Peninjauan kembali, apakah prosedur perencanaan audit sistem telah membahsan pembatasan akses audit sistem.	Rekomendasi sesuai panduan
	PP11	Prosedur Akses Audit Sistem	4	3	2	2	4		

Halaman ini sengaja dikosongkan

LAMPIRAN B
PANDUAN PENGGUNAAN INDEKS

Halaman ini sengaja dikosongkan.

DISCLAIMER (KONDISI DOKUMEN PANDUAN)

Dokumen panduan ini berisikan tentang penjelasan dan langkah-langkah penggunaan indeks penilaian. Asumsi dalam pembuatan dokumen ini adalah Anda belum pernah menggunakan indeks penilaian kesiapan manajemen keamananan layanan sebelumnya dan Anda telah men-*download* indeks penilaian kesiapan manajemen keamanan layanan di dalam *personal computer* Anda.

Halaman ini sengaja di kosongkan.

1. Pendahuluan

Organisasi dan perusahaan saat ini melakukan transformasi dan peningkatan pelayanan dengan pemamfaatan teknologi informasi (TI) dalam proses bisnisnya. Akan tetapi, upaya tersebut dirasa belum optimal tanpa adanya pengimplementasian manajemen layanan dan keamanan yang terencana dan terarah dengan sebuah standar.

Penggunaan standar ini dimaksudkan untuk membantu manajemen mengetahui sejauh mana keamanan kinerja layanan yang mendukung proses bisnis dan strategi organisasi tersedia berdasarkan *bestpractice* yang sudah teruji.

Akan tetapi, penggunaan satu buah standar saja saat ini dirasa belum maksimal melihat cakupan yang disediakan kurang luas sehingga penggabungan beberapa standar dengan harapan standar-standar tersebut saling melengkapi dan mendukung. Pengimplementasiannya oleh organisasi mulai dilakukan. Penggabungan beberapa standar ini pun diharapkan mampu dimonitoring pencapaiannya dengan menggunakan alat ukur penilaian kesiapan berupa indeks.

Pembuatan indeks penilaian ini menggunakan standar ISO 27000 terutama ISO 27001:2005 dan 27002:2005 sebagai *information security management*. Kerangka ITIL digunakan untuk konsep dan teknik pengelolaan operasi teknologi informasi (TI) yang berasalkan dari *control objetive Delivery and Support* yang terukur berdasarkan *maturity model* dari COBIT 4.1.

Dengan penggunaan indeks penilaian ini, sebuah organisasi diharapkan mampu melakukan penilaian akan manajemen keamanan layanan Tl yang komprehensif dan mampu memberikan gambaran utuh kesiapan keamanan diorganisasinya saat ini.

2. Tujuan

Tujuan disusunnya Panduan Penilaian Kesiapan Manajemen Keamanan Teknologi Informasi ini adalah untuk :

2.1 Mampu memandu manajemen keamanan layanan SI/TI pada sebuah perusahaan/organisasi dengan memahami cara kerja dan menggunakan indeks penilaian.

2.2 Memungkinkan sebuah organisasi melakukan penilaian mandiri (*self-assesment*) secara objektif terhadap manajemen keamanan layanan SI/TI nya.

2.3 Memungkinkan sebuah organisasi melakukan penyusunan sistem dokumentasi minimum yang diperlukan untuk menerapkan tata kelola keamanan informasi

3. Ruang Lingkup Penerapan

3.1 Area Penerapan

Panduan ini direkomendasikan untuk diterapkan di lingkungan penyelenggara pelayanan publik yang meliputi:

a. Instansi pemerintah pusat dan daerah
b. Penyelenggara pelayanan publik lainnya

3.2 Area Penilaian Kesiapan

a. Kesiapan Organisasi / *Service Strategy*
b. Manajemen Aset / *Service Design*
c. Penyusunan Keamanan TI / *Service Transition*
d. Pelaksanaan Keamanan TI / *Service Operation*
e. Perencanaan Pengembangan / *Continual Service Improvement*

Lima area evaluasi ini merupakan rangkuman kontrol-kontrol keamanan sebagaimana dijelaskan dalam ISO/ISO 27002:2005 dengan mempertimbangkan komponen keamanan informasi apa saja yang harus dimiliki dan disiapkan dalam menyampaian dan menjalankan layanan oleh sebuah organisasi, khususnya instansi/lembaga penyelenggara pelayanan publik di

Indonesia. Area evaluasi ini didasari pada konsep dari penerapan manajemen layanan TI.

4. Penggunaan Indeks Penilaian Kesiapan Manajemen Keamanan Layana

Indeks penilaian merupakan indeks dengan basis ***Microsoft Excel Worksheet*** sehingga asumsi dari panduan ini adalah pengguna sudah terbiasa atau familiar dalam penggunannya sehari-hari. Di dalam indeks, pengguna dapat membaca masing-masing pertanyaan yang berhubungan dengan area dan memberikan penilaiannya berdasarkan keadaan eksistensi di organisasi dengan melampirkan dokumentasi pendukung.

Di dalam indeks penilaian, terdapat enam buah tingkatan penilaian, yaitu :

Tabel B.1 Tingkatan Nilai dalam Indeks

No	Penilaian	A	B	C	D	E
1	Belum Terfikirkan					
2	Belum Tersedia, Masih diinisiasi	√				
3	Sudah Ada, Tanpa Dokumentasi	√	√			
4	Suda Ada, dan Terdokumentasi	√	√	√		
5	Sudah Ada, Terdokumentasi dan Termonitoring	√	√	√	√	
6	Sudah Ada, dan sudah dapat berjalan otomatis	√	√	√	√	√

*Keterangan :

A : Terfikirkan

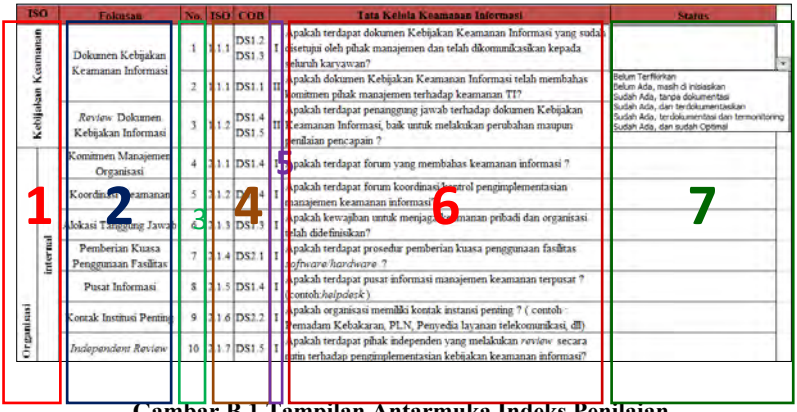
B : Sudah masuk ke dalam perencanaan bisnis

C : Sudah memiliki dokumentasi prosedur

D : Sudah memiliki system dan dokumentasi proses monitoring

E : Sudah memiliki Perencanaan Pengembangan

4.1 Komponen Indeks



Gambar B.1 Tampilan Antarmuka Indeks Penilaian

Gambar B.1 merupakan tampilan antarmuka salah satu *sheet* penilaian dalam indeks. Di dalamnya terdapat tujuh buah komponen penyusunan indeks, yaitu:

1. Proses utama dalam melakukan persiapan manajemen keamanan layanan
2. Sub proses, fokusan dari pengimplementasian proses persiapan manajemen keamanan layanan
3. Nomor, penomoran dari pertanyaan dalam indeks penilaian keamanan
4. Referensi merupakan ID dari referensi pertanyaan dari tata kelola keamanan, terdapat dua referensi, yaitu referensi berdasarkan ISO 17799 *checlist* dan *Delivery and Support* COBIT 4.1.
5. Tingkat dokumen, menunjukkan tingkat pengimplemetasian tata kelola dengan referensi (I) merupakan referensi untuk dokumen tingkat 1 tata kelola (Kebijakan), Dokumen dengan referensi (II) merupakan referensi untuk dokumen tingkat 2 tata kelola (Prosedur Operasional), Dokumen dengan referensi (III) merupakan

referensi untuk dokumen tingkat 3 tata kelola (Teknis Operasional).

6. Daftar pertanyaan tata kelola keamanan informasi
7. Status, tempat pengguna memberikan penilaian dengan memilih penilaian di dalam *dropdown list*.

4.2 Dashboard Indeks

Dalam sistem informasi, *dashboard* adalah sebuah alat yang mudah untuk dibaca, bersifat *real-time*, berguna untuk menunjukkan presentasi grafis dari status terkini (*snapshot*) dan tren historis indikator kinerja utama organisasi untuk memungkinkan pengambilan keputusan dengan meneliti informasi dengan hanya sekali pandang. Fitur penting dari produk dashboard BI termasuk *interface* yang dapat disesuaikan dengan kebutuhan dan kemampuan untuk menarik data *real-time* dari berbagai sumber.

Indeks penilaian kesiapan manajemen keamanan layanan SI/TI ini juga dilengkapi dengan *dashboard* untuk membantu organisasi memahami capaian kesiapannya dengan lebih mudah.

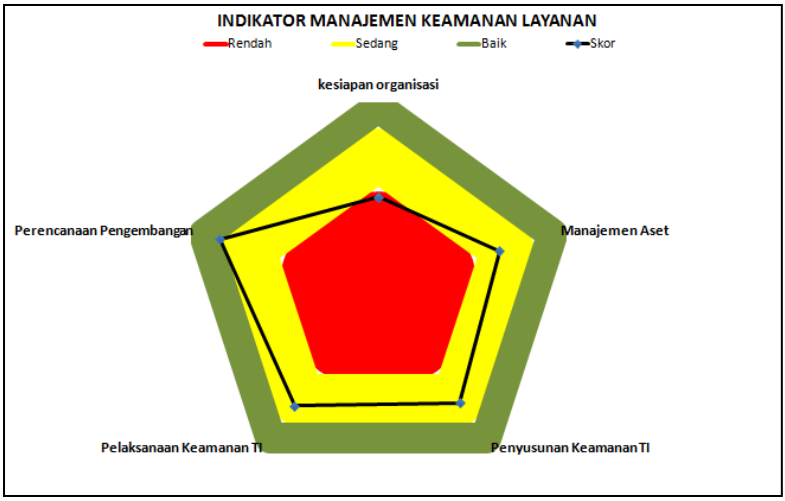
a. Dashboard Indikator Kinerja

Sumber data yang digunakan dalam pembuatan *dashboard* indikator kinerja adalah rata-rata capaian dari masing-masing proses manajemen keamanan teknologi informasi. *Dashboard* ditunjukkan dalam grafik berbentuk jaring dimana setiap satu jaringnya mewakili satu proses dengan tiga buah indikator menggunakan indikator warna, yaitu :

- Merah : Pelaksanaan manajemen keamanan informasi masih dalam proses inisiasi atau belum menjadi fokusan utama dari organisasi. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 1 dan 2 dari 6 tingkatan pengukuran dengan *maturity model*.
- Kuning : Pelaksanaan manajemen keamanan informasi sudah menjadi fokusan utama dari organisasi akan tetapi pelaksanaannya belum optimal. Hal ini didapatkan dari

rata-rata nilai persiapan yang masing memasuki tingkatan 3 dan 4 dari 6 tingkatan pengukuran dengan *maturity model*.

- Hijau : Pelaksanaan manajemen keamanan informasi sudah optimal baik dari sisi manajemen hingga pelaksanaannya di tingkat operasional. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 5 dan 6 dari 6 tingkatan pengukuran dengan *maturity model*.



Gambar B.2 Tampilan Dashboard Indikator Kerja

Gambar B.2 merupakan gambar *dashboard* indikator manajemen keamanan layanan. Sebagai contoh penghitungan capaian, kesiapan organisasi masuk ke dalam indikator merah yaitu manajemen keamanan informasi dari sisi kesiapan organisasi rendah kurang meskipun sudah berada di garis terluar dari area merah.

Di dalam proses manajemen aset, penyusunan keamanan TI dan pelaksanaan keamanan TI sudah berada di sisi sedang. Hal ini bias didasari dari kesiapan organisasinya yang belum optimal dalam menopang pelaksanaan operasional keamanan layanan TI.

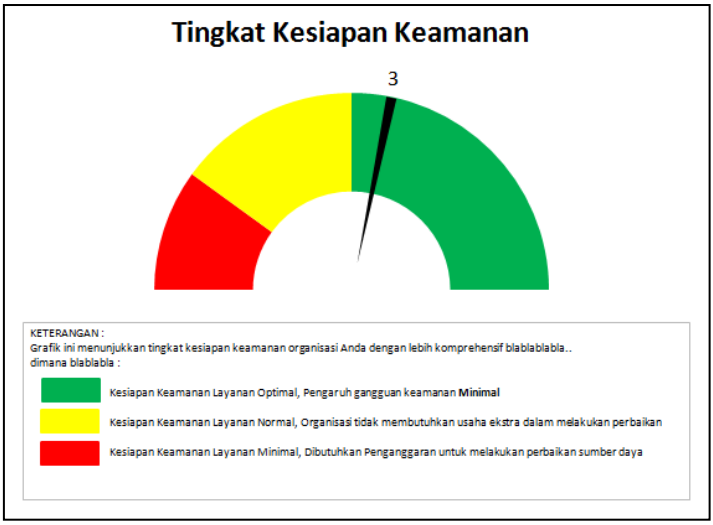
Terakhir dapat di lihat dari perencanaan pengembangan yang sudah memasuki area hijau, area baik atau optimal. Dengan melihat dashboard ini, diharapkan organisasi dapat melihat dengan lebih menyeluruh akan proses manakah yang harus mendapatkan fokusan lebih dan perbaikan.

b. Dashboard Kesiapan Keamanan

Sumber data yang digunakan dalam pembuatan *dashboard* kesiapan keamanan adalah rata-rata capaian dari seluruh proses manajemen keamanan teknologi informasi dengam menggunakan tipe grafik *gauge*.

Terdapat tiga indikator capaian, yaitu :

- Merah : Pelaksanaan manajemen keamanan informasi masih dalam proses inisiasi atau belum menjadi fokusan utama dari organisasi. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 1 dan 2 dari 6 tingkatan pengukuran dengan *maturity model*.
- Kuning : Pelaksanaan manajemen keamanan informasi sudah menjadi fokusan utama dari organisasi akan tetapi pelaksanaannya belum optimal. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 3 dan 4 dari 6 tingkatan pengukuran dengan *maturity model*.
- Hijau : Pelaksanaan manajemen keamanan informasi sudah optimal baik dari sisi manajemen hingga pelaksanaannya di tingkat operasional. Hal ini didapatkan dari rata-rata nilai persiapan yang masing memasuki tingkatan 5 dan 6 dari 6 tingkatan pengukuran dengan *maturity model*.



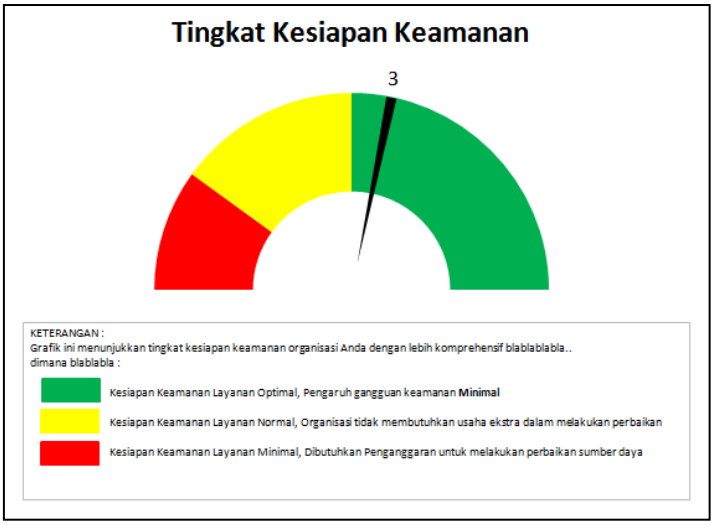
Gambar B.3 Tampilan Dashboard Tingkat Kesiapan

Gambar B.3 merupakan tampilan dari *dashboard* tingkat kesiapan keamanan layanan. Sebagai contoh penghitungan capaian yang ditampilkan dalam *dashboard*, pengguna dapat melihat bahwa kesiapan organisasi masuk ke dalam indikator hijau dimana secara keseluruhan kesiapanan manajemen keamanan sudah baik meskipun belum mencapai nilai paling maksimal, atau organisasi dapat melakukan peningkatan lagi apabila dimungkinkan.

5. Manajemen Keamanan Layanan

Berdasarkan pemetaan dari ketiga standar yaitu *Service & Delivery* COBIT 4.1 untuk proses manajemen penyampaian strategi TI organisasi, ITIL v3 sebagai *bestpractice* manajemen layanan dan ISO 270002 sebagai *bestpractice* penyediaan keamanan informasi, didapati kesimpulan sebagai berikut :

a. Dalam menetapkan manajemen keamanan layanan yang baik dalam fase ***Service Strategy***, organisasi harus berfokus pada COBIT DS *1-Define and Manage Service Levels* dengan



Gambar B.3 Tampilan Dashboard Tingkat Kesiapan

Gambar B.3 merupakan tampilan dari *dashboard* tingkat kesiapan keamanan layanan. Sebagai contoh penghitungan capaian yang ditampilkan dalam *dashboard*, pengguna dapat melihat bahwa kesiapan organisasi masuk ke dalam indikator hijau dimana secara keseluruhan kesiapanan manajemen keamanan sudah baik meskipun belum mencapai nilai paling maksimal, atau organisasi dapat melakukan peningkatan lagi apabila dimungkinkan.

5. Manajemen Keamanan Layanan

Berdasarkan pemetaan dari ketiga standar yaitu *Service & Delivery* COBIT 4.1 untuk proses manajemen penyampaian strategi TI organisasi, ITIL v3 sebagai *bestpractice* manajemen layanan dan ISO 270002 sebagai *bestpractice* penyediaan keamanan informasi, didapati kesimpulan sebagai berikut :

a. Dalam menetapkan manajemen keamanan layanan yang baik dalam fase ***Service Strategy***, organisasi harus berfokus pada COBIT DS *1-Define and Manage Service Levels* dengan

mempertimbangkan *Services Security Policy and Organization of Information* dalam ***Demand Management***, serta COBIT DS 2 -*Manage Third-Party Services* dalam menentukan *positioning* pihak ketiga di dalam *Organization of Information and Business Continuity Management* dalam proses ***Service Generation***.

b. Dalam menetapkan manajemen keamanan layanan yang baik dalam fase ***Service Design***, organisasi harus berfokus pada COBIT DS 1-*Define and Manage Service Levels* dengan memastikan bahwa Service Catalogue Management organisasi telah mencangkup :

- *Security Policy*
- *Organization of Information Security*
- *Human Resources Security*
- *Physical and Environmental Security*
- *Information System Acquisition, Development*

Service Level Management yang mempertimbangkan level kemungkinan terjadi dan pengelompokan insiden pada *Information Security Incident Management Information.*

COBIT DS 2-*Manage Third-Party Services* dengan melakukan *Supplier Management* yang mempertimbangkan *positioning* pihak *supplier* di dalam *Organization of Information Security*.

COBIT DS 3 -*Manage Performance and Capacity* dan COBIT DS 11-*Manage Data* dengan memastikan *Availability Management* telah tercangkup dalam :

- *Communication and Operations Management*
- *Access Control*

COBIT DS 3-*Manage Performance and Capacity* dan COBIT DS 12-*Manage Physical Environment Capacity Management* telah tercangkup dalam :

- *Security Policy*

- *Asset Management*
- *Physical and Environmental Security*

COBIT DS 4-*Ensure Continous Service* dengan memastikan *IT Service Continuity Management* telah tercangkup dalam:

- *Security Policy*
- *Asset Management*
- *Human Resources Security*
- *Communication and Operations Management*
- *Access Control*
- *Information Security Incident Management*
- *Business Continuity Management*

COBIT DS 5-*Ensure System Securities* dengan memastikan *Information Security Management* telah tercangkup dalam :

- Security Policy
- Organization of Information Security
- Physical and Environmental Security
- Communication and Operations Management

c. Dalam menetapkan manajemen keamanan layanan yang baik dalam fase ***Service Transition***, organisasi harus berfokus pada DS7-*Educate and Train Users* dalam proses *Release & Deployment Management* yang mempertimbangkan keamanan dalam sisi :

- *Communication and Operations Management*
- *Information System Acquisition, Development and Maintenance*

COBIT DS 9-*Manage the Configuration* dalam *Service Asset & Configuration Management* yang mempertimbangkan keamanan dalam proses *Information System Acquisition, Development and Maintenanc*e.

COBIT DS 12-*Manage Physical Environment* dan DS 13-*Manage Operations* di dalam proses *Change Management* yang mempertimbangkan keamanan dalam sisi :

- *Communication and Operations Management Service Asset & Configuration Mgmt*
- *Information System Acquisition, Development and Maintenance*

d. Dalam menjalankannmanajemen keamanan layanan yang baik dalam fase ***Service Operation***, organisasi harus berfokus pada COBIT DS 8-*Manage Service Desk and Incident* dalam proses *Incident Management* yang mencangkup keamanan dalam:

- *Human Resources Security*
- *Communication and Operations Management*
- *Access Control*
- *Business Continuity Management*
- dan *Request Fulfillment* dalam *Organization of Information Security*

COBIT DS 10-*Manage Problems* dalam proses *Problem Management* yang mencangkup :

- *Physical and Environmental Security*
- *Communication and Operations Management*
- *Information System Acquisition, Development and Maintenance*

COBIT DS 13-*Manage Operation* dalam proses *Event Management* yang memperhatikan keamanan dalam *Communication and Operations Management* serta proses *Access Management* yang aman berdasarkan :

- *Organization of Information Security*
- *Business Continuity Management*

e. Seluruh dari *lifecycle* ITIL v3 terimplementasi kecuali *Continous Service Improvement* yang hanya mampu diimplementasikan oleh ISO 27002 dalam sisi penekanan pentingnya pelaksanaan *Reporting*, tetapi tidak dalam sisi *Service Measurement & Control* dan *Return on Investment on CSI* yang hanya dapat dilakukan melalui *framework* ITIL v3 Sendiri.

Berdasarkan kesimpulan pemetaan diatas, dirancanglah standar tata kelola minimal yang harus dimiliki oleh organisasi lengkap dengan atribut masing-masing proses pengelolaannya.

1. Service Catalogue Management (SCM)

Untuk sebuah organisasi mampu memastikan manajemen keamanan layanan SI/TI yang dimilikinya berjalan dengan baik, informasi di dalam *Service Catalogue Management* minimal mencangkup seluruh informasi yang terdapat di dalam :

- *Security Policy*
- *Organization of Information Security*
- *Human Resources Security*
- *Physical and Environmental Security*
- *Information System Acquisition, Development and Maintenance*

2. Service Level Agreement (SLA)

Untuk sebuah organisasi mampu memastikan manajemen keamanan layanan SI/TI yang dimilikinya berjalan dengan baik, *Service Level Agreement* minimal mencangkup komponen-komponen penjelasan seperti yang dijabarkan dalam Tabel B.2 akan Komponen Minimal SLA .

Tabel B.2 Komponen Minimal SLA

Dokumen	Sub SLA	Komponen SLA
Service Security Policy		Definisi dan manajemen *Service Level*
		Bagaimana langkah *Manage Performance and Capacity*
		Information Security Management
		Bagaimana cara *Manage Physical Environment Capacity*
		Bagaimana organisasi mampu *Ensure Continous Service*
Organization of Information		Melakukan penggalian awal kebutuhan *Demand Management*.
		Mendefinisikan *positioning* pihak ketiga dalam organisasi (kontrak yang jelas)
		Information Security Management
		Manage Operation
		Communication and Operations Management
Information Security Incident		Mendefiniskan *Level Incident*
		Ensure Continous Service ketika insiden terjadi dalam organisasi
Communication and Operations Management		*Manage Performance and Capacity*
		Manage Data
		Ensure Continous Service
		Information Security Management
		Educate and Train Users
		Manage Service Desk and Incident
		Manage Problems
		Release & Deployment Management
	Change management	*Manage Physical Environment*
		Manage Operations

Access Control		*Manage Performance and Capacity*
		Manage Data
		Manage Service Desk and Incident
		Ensure Continous Service
Asset Management		*Manage Performance and Capacity*
		Manage Physical Environment Capacity
		Ensure Continous Service
Physical and Environmental Security		*Manage Performance and Capacity*
		Manage Physical Environment Capacity
		Manage Problems
		Information Security Management
Human Resource Security		*Ensure Continous Service*
		Manage Service Desk and Incident
Business Continuity Management		Ensure Continous Service
		Mendefinisikan keberlanjutan kerjasama pihak ketiga dalam organisasi (kontrak yang jelas)
		Manage Operation
		Manage Service Desk and Incident
		Communication and Operations Management
Information System Acquisition, Development and Maintenance		*Educate and Train Users*
		Release & Deployment Management
		Manage the Configuration
		Manage Problems
		Service Asset & Configuration Management
	Change management	*Manage Physical Environment*
		Manage Operations

6. Dokumentasi Manajemen Keamanan Layanan

6.1 Service Catalogue Management

Tujuan pembuatan *service catalogue management* (SCM) adalah untuk membangun sebuah katalog layanan yang berisikan informasi lengkap, status, interaksi yang dimungkinkan dan hubungan yang saling berhubungan untuk seluruh layanan yang akan dibangun.

Service catalogue akan digunakan sebagai informasi utama layanan. Dengan menggunakan katalog, setiap orang dalam organisasi dapat melihat apakah layanan yang harus disampaikan kepada pelanggan, bagaimana layanan tersebut diberikan, bagaimana layanan tersebut digunakan, untuk tujuan apa, dan bagaimanakah tingkat kualitas yang diprediksikan pelanggan.

Berbeda dengan *service portfolio*, SCM merupakan bagian dari *service portfolio* yang menampilkan hanya layanan yang aktif dan disetujui saja dalam *service operation*. SCM membagi layanan menjadi beberapa komponen yang berisikan kebijakan, panduan dan pertanggungjawaban, rencana *service level* dan perencanaan penyampaiannya kepada pelanggan.

Service Catalogue adalah dokumen kunci yang berisi informasi yang berharga berisi informasi lengkap layanan yang ditawarkan. Pembuatan dokumen ini sebaiknya disimpan sebagai satu set layanan *Configuration Items* (CIs) dalam *Configuratin Management* Systems (CMS), yang dipertahankan di bawah Manajemen Perubahan.

Tabel B.3 Contoh Tampilan *Service Catalogue*

Service Name	*Service Description*	*Service Type*	*Supporting Serices*	*Business Owners*	*Business Unit(s)*	*Service Manager(s)*	*Business Impact*	*Business Priority*	*SLA*	*Service Hours*	*Business Contacts*	*Escalation Contacts*	*Service Reports*	*Service Reviews*	*Security Rating*
Service 1															
Service 2															
Service 3															
Service 4															
Service 5															

Tabel B.2 merupakan contoh tampilan dari *Service Catalogue.* Satu set informasi berharga itu harus tersedia bagi siapa saja dalam organisasi. Setiap terdapat layanan baru, pihak manajemen perubahan harus segera memasukkannya ke dalam *Service Catalogue* sejak definisi awal persyaratan telah didokumentasikan dan disepakati, sehingga setiap informasi di bawahnya pun turut dicatat oleh pihak *service catalogue* mulai dari status setiap layanan hingga definisi tiap tahapan *lifecycle* yang dilewati.

6.2 *Service Level Agreement*

Service Level Agreement (SLA) merupakan sebuah kerangka untuk memastikan bahwa seluruh kebutuhan layanan dan *customer* telah terpenuhi sesuai dengan kebutuhan organisasi. Terdapat beberapa macam dalam pembuatan SLA, yaitu layanan berbasis SLA dan *customer* berbasis SLA.

Organisasi saat ini, telah mengembangkan manajemen layanan di organisasinya dengan menetapkan *multi-level SLA* dimana terdapat tiga buah tingkatan struktur SLA, yaitu :

1. **Tingkat Organisasi**
   Mencangkup seluruh kebutuhan manajemen layanan secara umum untuk dapat diaplikasikan kepada seluruh *customer*

organisasi. Kebutuhan manajemen layanan dalam tingkatan ini sangat minim kemungkinan pelanggaran sehingga kebutuhan untuk *update* atau pembaharuan sangat jarang dilakukan.

2. Tingkat *Customer*

Mencangkup seluruh kebutuhan berdasarkan *customer* atau masing-masing grup *business unit*, isi dari masing-masing SLA sangat bergantung dengan layanannya.

3. Tingkat Layanan

Mencangkup seluruh kebutuhan *service level management* yang relevan untuk sebuah layanan yang spesifik (satu buah layanan memiliki satu buah SLA).

a. Komponen SLA

Sebuah SLA minimal mampu mendeskripsikan beberapa komponen di bawah ini :

1. Pernyataan Persetujuan (Antara Pihak A dengan Pihak B)
2. Deskripsi Layanan Singkat
3. Jangka waktu berlaku
4. Persetujuan (tanda tangan)
5. Penjabaran Layanan
6. Ruang lingkup
7. Waktu Penyediaan Layanan
8. Ketersediaan Layanan
9. Kehandalan Layanan
10. Dukungan terhadap *customer*
11. Daftar Kontak yang dapat dihubungi
12. Performa Layanan
13. Waktu tenggat yang disetujui
14. *Functionality* (jika diperlukan)
15. Manajemen Perubahan
16. Pengembangan Layanan
17. Keamanan

18. Tanggung jawab
19. *Charging* (jika diperlukan)
20. *Service reporting and reviewing*
21. Daftar Pustaka
22. Dokumentasi Perubahan

b. Contoh SLA

Contoh SLA ini merupakan contoh gambaran kepada pengguna akan bentuk dan fungsi dari SLA. Akan tetapi SLA tidak harus selalu mengikuti *template* ini. Terdapat beberapa komponen yang hanya akan muncul ketika dibutuhkan oleh dokumen sehingga SLA ini lebih cocok untuk dijadikan referensi atau *checklist*, bukan sebagai acuan.

SERVICE LEVEL AGREEMENT (SLA – Contoh)

Persetujan ini dibuat antara …….. dan ……..

Persetujuan ini mencangku seluruh persyaratan yang mendukung layanan XYZ ….(deskripsi singkat layanan).

Persetujuan :

Nama……Posisi……Tanggal……

Nama……Posisi……Tanggal……

Deskripsi Layanan :

Layanan XYZ terdiri dari (deskripsi lengkap layanan termasuk nilai bisnis yang didukung oleh layanan, manfaat layanan dan seluruh informasi yang mendeskripsikan layanan seperti ruang lingkup, dampak dan prioritas layanan dalam proses bisnis).

Ruang Lingkup

Deskripsi batasan dari persetujuan.

Waktu Layanan
Deskripsi dari waktu layanan yang dapat di harapkan oleh pengguna bahwa layanan tersedia.

Termasuk juga di dalamnya :

a. Kondisi pengecualian (akhir pekan, hari libur nasional)
b. Prosedur permintaan khusus dan pelaporan kekurangan dari penyediaan layanan (Kontak yang dapat dihubungi – biasanya *service desk* – dan cara mengajukan permintaan / pelaporan khusus)
c. Persetujuan untuk kegiatan *maintenance* atau *housekeeping* bila hal tersebut dapat mengganggu waktu layanan.
d. Prosedur untuk mengajukan perubahan waktu layanan keseluruhan

Ketersediaan Layanan
Target dari ketersediaan layanan yang disediakan untuk mencapai waktu layanan yang telah disetujui, biasanya dalam presentase (contoh : 99.9%). Periode, metode dan penghitungan ketercapaian harus ditetapkan dan didokumentasikan.

Realibilitas
Jumlah maksimal dari kerentanan layanan yang dapat di toleransi (biasanya dengan jumlah toleransi per jangka waktu tertentu). Definisi dari kerentanan layanan ini ditinjau dan dicatat.

Customer Support
Rincian langkah untuk menghubungi *service desk*, waktu ketersediaannya dan bagaimana untuk mendapatkan *customer support* di luar waktu layanan harus di dokumentasikan. SLA pun dimungkinkan untuk memungkinkan pengguna melakukan pelaporan insiden. Pengukuran target juga harus dimasukkan (contoh : jumlah layanan per telepon, waktu tanggap laporan insiden (berdasarkan tingkat prioritas insiden)).

Tingkatan Kontak
Rincian dari tingkatan pelaporan dan pengerjaan layanan.

Performa Layanan
Rincian dari respon layanan yang direncanakan (contoh : rata-rata target respin, atau batas minimal pelaksanaan respon, kadang-kadang diungkapkan dalam presentase).

Batch Turnaround Times
Bila dimungkinkan, rincian dari waktu untuk pelaksanaan kumpulan perubahan, waktu penyelesaian dan kunci penyampaian layanan, termasuk waktu untuk menyampaikan input dan waktu untuk menghasilkan output yang dibutuhkan.

***Functionality* (jika di butuhkan):**
Rincian dari fungsionalitas minimal yang ditetapkan dan jumlah error yang dapat ditoleransi. Rincian ini termasuk tingkat kerumitan dan periode pelaporan.

Manajemen Perubahan
Petunjuk terhadap prosedur manajemen perubahan organisasi yang digunakan. – untuk menguatkan pemenuhan persyaratan. Termasuk juga didalamnya target untuk penerimaan, penanganan dan implementasi RFC, biasanya tergantung pada kategori atau prioritas perubahan.

Service Continuity
Petunjuk terhadap *Service Continuity Plan* organisasi, termasuk didalamnya bagaimana satu buah SLA mempengaruhi SLA lainnya.

Keamananan
Petunjuk terhadap kebijakan keamanan organisasi dan rincian pertanggungjawaban dari kedua belah pihak.

Printing
Rincian dari kondisi spesial ketika layanan membutuhkan alat pencetak.

Pertanggungjawaban
Rincian dari tanggung jawab mulai dari penyedia layanan, pelanggan dan pengguna.

Charging
Rincian dari formula tagihan yang digunakan, periode taginan, dan referensi dokumen aturan tagihan, bersamaan dengan prosedur faktur pembayaran.
Dalam formula tagihan pun mungkin untuk dimasukkan aturan ketika tagihan terlambat untuk dibayarkan.

Pelaporan dan Peninjauan Layanan
Konten, frekuensi, waktu dan distribusi laporan layanan, dan frekuensi forum pembahsan layanan. Termasuk juga di dalambanya bagaimana dan kapan target SLA ditinjau dan direvisi (jika dimungkinkan), termasuk didalamnya aturan siapakah yang akan menjalankannya dan rincian kapasitas wewenangnya.

Glosarium
Penjelasan terhadap singkatan-singkatan yang digunakan

Amandemen
Catatan perubahan yang dilakukan.

6.3 OPERATIONAL LEVEL AGREEMENT (OLA)

Operational Level Agreement (OLA) merupakan sebuah kerangka persetujuan yang menjadi dasaran organisasi untuk menyampaikan atau menjalankan layanan sesuai dengan kualitas yang telah disepakati dalam SLA.

a. Komponen OLA

Sebuah OLA minimal mampu mendeskripsikan beberapa komponen di bawah ini :

1. Pernyataan Persetujuan (Antara Pihak A dengan Pihak B)
2. Deskripsi Layanan Singkat
3. Jangka waktu berlaku
4. Perencanaan Pemeriksanaan (review per x / tahun)
5. Persetujuan (tanda tangan)
6. Penjabaran lengkap dari SLA :
   - Penjabaran Layanan
   - Ruang lingkup
   - Waktu Penyediaan Layanan
   - Target Layanan
7. Daftar Kontak yang dapat di hubungi
8. *Service Desk* :
   - Waktu respon terhadap insiden
   - Tanggung jawab insiden
9. *Problem Management* :
   - Waktu respon terhadap masalah
   - Tanggung jawab masalah
10. *Change Management*
11. *Release Management*
12. *Configuration Management*
13. *Information security management*
14. *Capacity management*
15. *Service level management*
16. *Supplier Management*
17. Daftar Pustaka
18. Dokumentasi Perubahan

b. Contoh OLA

Persetujan ini dibuat antara …….. dan ……..

Perjanjian ini meliputi penyediaan dukungan layanan XYZ ……..(deskripsi singkat layanan).

Perjanjian ini berlaku selama 12 bulan sejak (tanggal) sampai (tanggal).
Perjanjian ini akan ditinjau rutin setiap tahun. Setiap perubahan kecil direkam pada formulir perubahan yang dilampirkan di akhir dokumen perjanjian, dengan melampirkan dukungan perubahan oleh kedua belah pihak dan dikelola melalui proses Manajemen Perubahan.
Persetujuan :

Nama……Posisi……Tanggal……

Nama……Posisi……Tanggal……

Rincian Perubahan Sebelumnya
Deskripsi Layanan Pendukung:
Penjelasan yang komprehensif dan rinci dari layanan pendukung yang disediakan.

Ruang Lingkup Perjanjian:
Meliputi seluruh deskripsi dari komponen apa saja yang tercakup dalam perjanjian dan apa yang menjadi pengecualian.

Waktu Layanan:
Penjelasan mengenai waktu layanan yang diberikan.

Target Layanan:
Target penyediaan layanan dan pelaporan-tinjauan terhadap proses dan frekuensi layanannya.

Tingkatan Kontak:
Rincian kontak untuk setiap pihak yang terlibat dalam perjanjian dan proses eskalasi dari titik utama kontak.

***Service Desk* dan Respon terhadap Insiden :**
Daftar Penanggungjawaban dan target yang disepakati untuk kemajuan dan resolusi dan dukungan dalam menghadapi insiden.oleh *Service Desk*.

Problem Response Times :
Tanggung jawab dan target yang disepakati untuk kemajuan dan resolusi bagi organisasi dalam menyelesaikan masalah.

Manajemen Perubahan:
Tanggung jawab dan target yang disepakati untuk kemajuan dan pelaksanaan perubahan.

Manajemen Rilis:
Tanggung jawab dan target yang disepakati untuk kemajuan dan pelaksanaan rilis layanan.

Manajemen Konfigurasi:
Tanggung jawab untuk kepemilikan, penyediaan dan pemeliharaan informasi akurat manajemen konfigurasi.

Manajemen Keamanan Informasi:
Tanggung jawab dan target yang disepakati untuk mendukung Kebijakan Keamanan dan proses Manajemen Keamanan Informasi.

Manajemen Ketersediaan:
Tanggung jawab untuk memastikan bahwa semua komponen dalam *support domain* dikelola dan didukung untuk bertemu dan terus memenuhi semua layanan dan ketersediaan komponen target.

Manajemen Keberlanjutan Layanan :
Tanggung jawab untuk memastikan bahwa semua komponen dalam *support domain* yang dimiliki *up-to-date* dan rencana pemulihan yan teruji mendapat dukungan, disetujui, dan seluruh kebutuhan bisnisnya didokumentasikan.
Proses ini juga termasuk pengembangan teknis penilaian risiko dan manajemen mitigasi.

Manajemen Kapasitas:
Tanggung jawab untuk mendukung kapasitas kebutuhan proses manajemen kapastas sesuai ruang lingkup yang disepakati.

Service Level Management:
Definisi dan persetujuan target sesuai dalam SLA, SLR dan OLA, mengenai komponen dalam ruang lingkup teknis *service domain*.

Manajemen *Supplier*:
Bantuan dengan pengelolaan kontrak pemasok, terutama dalam ruang lingkup *technical domain*nya.

Ketersediaan Informasi:
Penyediaan dan pemeliharaan informasi yang akurat, termasuk data keuangan untuk semua komponen dalam ruang lingkup yang disepakati.

Daftar Istilah:
Penjelasan dari setiap singkatan yang tidak dapat dihindari untuk membantu pemahaman istilah yang ada di dalam perjanjian.

Amandemen :
Penyertaan catatan amandemen yang disepakati, dengan rincian amandemen, tanggal dan penandatangan persetujuan perubahan. Hal ini juga harus berisi rincian sejarah perubahan lengkap akan dokumen dan revisinya.

7. *Assessment* Manajemen Keamanan Layanan

Assessment adalah suatu proses sistematis, mandiri, dan terdokumentasi untuk mengevaluasinya secara objektif guna menentukan sejauh mana capaian telah dipenuhi.

Di dalam prosesnya, selain rekomendasi standar operasinal yang baik, dilengkapi juga dengan prosedur dan panduan pelaksanaan *assessment* agar manajemen keamanan layanan yang sudah direncanakan dapat dipantau dan adanya tindakan keberlanjutan.

Panduan TI dan prosedur yang terkait ini dimaksudkan untuk memenuhi persyaratan dokumentasi sistem manajemen TI organisasi. Manajer departemen dan supervisor bertanggung jawab untuk mengidentifikasi setiap dokumen tambahan yang diperlukan untuk memastikan perencanaan, operasi dan pengendalian proses berjalan sesuai dengan strategi organisasi.

Rincian dokumentasi bervariasi berdasarkan ukuran departemen atau organisasi yang terlibat dan jenis kegiatan yang dilakukan. Prosedur pengembang harus mempertimbangkan kompleksitas proses dan interaksinya, juga kompetensi personel yang terlibat.

Sistem manajemen TI perusahaan menggunakan bentuk standar dan memberikan kontrol dan akuntabilitas. Supervisor harus meninjau rekaman data TI yang di-*posting* lengkap dengan dokumen sumber dan dokumen pengolahan. Dokumen dalam bentuk media apapun termasuk program perangkat lunak, *file* teks elektronik, atau *hardcopy* dokumen. pelaksanaan *assessment* manajemen keamanan layanan yang dipandu oleh tim auditor internal dalam menggunakan indeks sangat dianjurkan untuk menjamin independensi dan ke-*valid*-an hasil penilaian.

LAMPIRAN C
KUISIONER PENERIMAAN PENGGUNA

Halaman ini sengaja dikosongkan.

Keterangan

- **STS** : Sangat Tidak Setuju
- **TS** : Tidak Setuju
- **N** : Netral
- **S** : Setuju
- **SS** : Sangat Setuju

No.	Pertanyaan	STS	TS	N	S	SS
	Kebermanfaatan					
1.	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* mempercepat saya dalam memahami manajemen keamanan layanan di banding melakukan *review* sendiri.	1	2	3	4	5
2.	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan kinerja karena menghemat waktu dan uang yang saya keluarkan.	1	2	3	4	5
3.	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan produktifitas karena saya dapat menemukan informasi kekurangan manajemen keamanan layanan dalam waktu yang singkat.	1	2	3	4	5
4.	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan efektifitas karena saya lebih mudah mendapatkan informasi	1	2	3	4	5

	tindakan yang sesuai dengan fokusan manajemen.					
5.	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* sangat bermanfaat bagi saya dalam menentukan tindakan yang sesuai dengan fokusan manajemen	1	2	3	4	5
6.	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan hasil keputusan penentuan strategi keamanan lanjutan organisasi.	1	2	3	4	5
Kemudahan Penggunaan						
1.	Saya mudah menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
2.	Saya mudah mempelajari cara menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
3.	Saya merasa mudah menemukan langkah perbaikan yang saya inginkan melalui *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
4.	Saya merasa mudah membandingkan kesiapan organisasi saat ini dengan pengembangan perencanaan dengan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
5.	Saya merasa fleksibel dalam melakukan pengembangan manajemen keamanan layanan dengan menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5

Sikap Terhadap Penggunaan						
1.	Saya merasa nyaman menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
2.	Saya merasa senang melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
3.	Saya merasa senang mencari kelemahan dan kekurangan manajemen keamanan layanan dengan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
4.	Saya merasa senang saat menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	1	2	3	4	5
5.	Saya rasa melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* adalah ide yang bagus.	1	2	3	4	5
6.	Saya rasa melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* adalah pilihan yang bijak.	1	2	3	4	5
7.	Saya rasa melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* adalah hal yang positif.	1	2	3	4	5

Kecenderungan untuk menggunakan						
1	Kemungkinan saya akan menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* untuk melakukan penilaian kesiapan manajemen layanan organisasia	1	2	3	4	5
2	Saya berniat untuk menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* pada penilaian selanjutnya	1	2	3	4	5
3	Saya berharap untuk menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* pada penilaian selanjutnya	1	2	3	4	5

Menurut Anda hal apa yang perlu ditingkatkan dan diperbaiki dari *Indeks Penilaan Kesiapan Manajemen Layanan :*

……
……
……
……
……

Hasil dari kuisioner penerimaan pengguna adalah sebagai berikut :

No.	Pertanyaan	Responden 1	Responden 2	Responden 3	Responden 4
	Kebermanfaatan				
1	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* mempercepat saya dalam memahami manajemen keamanan layanan di banding melakukan *review* sendiri.	**5**	**-**	**4**	**4**
2	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan kinerja karena menghemat waktu dan uang yang saya keluarkan.	**5**	**-**	**4**	**4**
3	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan produktifitas karena saya dapat menemukan informasi kekurangan manajemen keamanan layanan dalam waktu yang singkat.	**5**	**-**	**4**	**4**
4	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan efektifitas karena saya lebih mudah mendapatkan informasi tindakan yang sesuai dengan fokusan manajemen.	**5**	**-**	**4**	**4**
5	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* sangat bermanfaat bagi saya dalam menentukan tindakan yang sesuai dengan fokusan manajemen	**5**	**-**	**4**	**4**
6	Menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* dapat meningkatkan hasil keputusan penentuan strategi keamanan lanjutan organisasi.	**5**	**-**	**4**	**4**

Kemudahan Penggunaan					
1	Saya mudah menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	**3**	**-**	**3**	**3**
2	Saya mudah mempelajari cara menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	**4**	**-**	**3**	**3**
3	Saya merasa mudah menemukan langkah perbaikan yang saya inginkan melalui *Indeks Penilaan Kesiapan Manajemen Layanan*	**4**	**-**	**3**	**3**
4	Saya merasa mudah membandingkan kesiapan organisasi saat ini dengan pengembangan perencanaan dengan *Indeks Penilaan Kesiapan Manajemen Layanan*	**5**	**-**	**3**	**3**
5	Saya merasa fleksibel dalam melakukan pengembangan manajemen keamanan layanan dengan menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	**5**	**-**	**3**	**3**

Sikap Terhadap Penggunaan					
1	Saya merasa nyaman menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	**5**	**-**	**3**	**3**
2	Saya merasa senang melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	**5**	**-**	**3**	**3**
3	Saya merasa senang mencari kelemahan dan kekurangan manajemen keamanan layanan dengan *Indeks Penilaan Kesiapan Manajemen Layanan*	**5**	**-**	**3**	**2**
4	Saya merasa senang saat menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan*	**4**	**-**	**3**	**3**

5	Saya rasa melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* adalah ide yang bagus.	**4**	**-**	**3**	**3**
6	Saya rasa melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* adalah pilihan yang bijak.	**5**	**-**	**3**	**3**
7	Saya rasa melakukan penilaian menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* adalah hal yang positif.	**5**	**-**	**3**	**3**

Kecenderungan untuk menggunakan					
1	Kemungkinan saya akan menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* untuk melakukan penilaian kesiapan manajemen layanan organisasia	**4**	**-**	**4**	**4**
2	Saya berniat untuk menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* pada penilaian selanjutnya	**4**	**-**	**4**	**4**
3	Saya berharap untuk menggunakan *Indeks Penilaan Kesiapan Manajemen Layanan* pada penilaian selanjutnya	**4**	**-**	**4**	**4**

Masukan dari pihak LPTSI untuk pengembangan indeks penilaian manajemen keamanan layanan :

Masukan	Tindak Lanjut	Validasi
Seharusnya ada dokumen prosedur serta ditaati dan dievaluasi secara berkala (Responden 3)	Pembuatan Rekomendasi pembuatan prosedur dan panduan penggunaan Indeks Penilaian	√
• *Struktur Penilaian Sebaiknnya dikelompokkan berdasarkan core & Support Process, diruntunkan berdasarkan proses bisnis.* • *Penilaian sebaiknya bukan dalam bentuk rentang presepsi, akan sangat baik bila dalam bentuk scorecard yang spesifik untuk setiap item penilaian.*	Rekomendasi untuk Penelitian Selanjutnya dimasukkan ke dalam panduan.	√

Pembahasan hasil kuisioner :

1. Rata-rata untuk kategori pertanyaan Kebermanfaatan Indeks, adalah 4 yaitu **Setuju** bahwa indeks penilaian kesiapan manajemen keamanan bermanfaat untuk organisasi terkait.
2. Rata-rata untuk kategori pertanyaan Kemudahan penggunaan Indeks, adalah 3 yaitu **Netral** bahwa indeks penilaian kesiapan manajemen keamanan mudah untuk digunakan / dioperasikan dalam organisasi terkait.
3. Rata-rata untuk kategori pertanyaan Sikap terhadap pengguna Indeks, adalah 3 yaitu **Netral** bahwa setiap pengguna indeks penilaian kesiapan manajemen keamanan bersikap netral dalam menggunakan / dioperasikan dalam organisasi terkait.
4. Rata-rata untuk kategori pertanyaan Kecenderungan untuk penggunaan Indeks, adalah 4 yaitu **Setuju** bahwa organisasi terkait setuju untuk menggunakan indeks penilaian kesiapan manajemen keamanan sebagai salah satu alat evaluasi keamanan layanan di organisasinya.
5. Rekomendasi telah dipenuhi dalam **Lampiran B.**

Halaman ini sengaja dikosongkan.

LAMPIRAN D
PEMETAAN INDEKS PENILAIAN

Halaman ini sengaja dikosongkan.

	Strategy				Service						Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 1 - Define and Manage Service Levels																									
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 2 - Manage Third-Party Services																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	N	N	N	Y	N	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition								Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 3 - Manage Performance and Capacity																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 4 - Ensure Continuous Service																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition								Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 5 - Ensure Systems Security																											
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition								Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 6- Identify and Allocate Costs																											
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 7 - Educate and Train Users																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 8 - Manage Service Desk and Incident																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfillment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 9 - Manage the Configuration																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N	
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 10 - Manage Problems																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 11 - Manage Data																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	N	N	N	Y	N	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition							Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 12 - Manage Physical Environment																										
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

	Strategy				Service							Transition						Operation					Continual		
	Strategy Generation	IT Financial Management	Service Portfolio Mgmt	Demand Mgmt	Service Catalogue Mgmt	Service Level Mgmt	Availability Mgmt	Capacity Mgmt	IT Service Continuity Mgmt	Information Security Mgmt	Supplier Mgmt	Transition Planning and Support	Change Mgmt	Service Asset & Configuration Mgmt	Release & Deployment Mgmt	Service Validation & Testing	Evaluation	Knowledge Mgmt	Incident Management	Event Mgmt	Request Fulfilment	Problem Mgmt	Access Mgmt	Service Reporting	Service Measurement & Control	Return on Investment on CSI
COBIT DS 13 - Manage Operations																									
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communication and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	N	N	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N
Information System Acquisition, Development and Maintenance	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	N
Compliance	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Keterangan	
COBIT 4.1	
BERHUBUNGAN	Y
TIDAK BERHUBUNGAN	N

Halaman ini sengaja di kosongkan.

LAMPIRAN E
VERIFIKASI INDEKS

Halaman ini sengaja dikosongkan.

No	*ITIL Prespective*	ITIL	ISO		ISO	COBIT	COBIT
	Service Strategy						
1	*Strategy Generation*	*Define the market*	-	-	-	-	-
2		*Develop the offerings*	ISO2	1.1.1 1.1.2 1.1.3	*Management commitment to information security* *Information security co-ordination* *Allocation of information security responsibilities*	-	-
3		*Develop strategic assets*		2.1.4 2.1.5 2.1.6	*Authorization process for information processing facilities* *Confidentiality agreements* *Contact with authorities* *Contact with special interest groups*	-	-
4		*Prepare for execution*		2.1.7	*Independent review of information security*	-	-

5	*IT Financial Management*	*Service Valuation*	-	-	-	DS6	*Identify and Allocate Costs*
6		*Service Provisioning models and analysis*	-	-	-	-	-
7		*Funding*	-	-	-	-	-
8		*Business Impact Analysis (Financial Value)*	-	-	-	-	-
9		*Chargeback*	ISO2	2.3.1	*Security requirements in outsourcing contracts*	DS6	*Cost Model and Charging*
10		*Return on Investment*	-	-	-	-	-
11	*Service Portfolio Management*	*Define Services & Ensure Business Case*	ISO11	10.2.1	*Compliance with Legal Requirement*	-	-
12		*Analyse portfolio Value & prioritize*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
13		*Approve & Authorize Services and Resources*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
14		*Charter Services and allocate Resources*	ISO4	4.1.1 4.1.2 4.1.3 4.1.4	*Roles and responsibilities* *Screening* *Terms and conditions of employment*	-	-

15	*Demand Management*	*Core Services and Support Services*	ISO1	1.1.1	*Information Security Policy Document*	-	-
16		*Developing differentiated Offerings*	-	-	-	-	-
17		*Service Level Packages (SLPs)*	-	-	-	-	-
18		*Segmentation*	ISO2	2.1.2	*Information security co-ordination*	-	-

No	*ITIL Prespective*	ITIL	ISO		ISO	COBIT	COBIT
	Service Design						
19	*Service Catalogue Management*	*Agreeing and documenting a service definition*	ISO1	1.1.1	*Information Security Policy Document*	DS1	*Define of Service*
20		*Interfacing with Service Portfolio Management*	ISO2	2.1.2	*Information security co-ordination*	DS1	*Service Level Management Frameworks*
21		*Producing and Maintaining a Service Catalogue*	ISO4	4.1.2	*Terms and conditions of employment*	DS1	*Service Level Management Frameworks*
22			ISO5	5.1.4	*Information security awareness, education, and training*		
24		*Interfacing with Business & IT Service Continuity Mgmt*	-	-	-	DS1	*Service Level Management Frameworks*
25		*Interfacing with support teams, suppliers and configuration mgmt*	ISO8	8.1.1	*Documented operating procedures*	DS1	*Service Level Management Frameworks*
26	*Service Level Management*	*Designing SLA frameworks*	ISO9	6.1.3	*Reporting information security events*	DS1	*Service Level Framework*
27		*Determine, document and agree requirements & produce SLRs*		6.1.3	*Reporting security weaknesses*	DS1	*Service Level Agreement*

28		*Monitor service performance against SLA*		6.1.3	*Responsibilities and procedures*	DS1	*Monitoring and Reporting of SLA*
29		*Collate, measure and improve customer satisfaction*		4.3.4	*Learning from information security incidents*	DS1	*Monitoring and Reporting of SLA*
30		*Produce service reports*		4.3.1	*Reporting Security Incident*	DS1	*Monitoring and Reporting of SLA*
31		*Conduct service reviews and instigate improvements within an SIP*	-	7.2.4	*User Management*	DS1	*Review of SLA and Contracts*
32		*Review and revise SLAs, Service Scope and underpinning agreements*	-	10.2.1	*Input Data Validation*	DS1	*Review of SLA and Contracts*
33		*Develop contacts and relationship*	-	2.1.6	*Co-operation between organisations*	-	
34		*Compliants and compliments*	-	10.2.1	*Compliance with security policy*	-	
35		*Determine Legel Requirements, Compliance*	-	10.1.1	*Security Requirements analysis and specification*	-	
36	*Availability Management*	*Monitor, measure, analyse and report service and component*	ISO6	6.1.1	*Documented operating procedures*	DS3	*Resource Availability*

		availability					
37		*Unavailability analysis*		6.2.1	*capacity planning*	DS3	*Resource Availability*
38		*The expanded incident lifecycle*		6.1.3	*Confidentiality agreements*	DS3	*Resource Availability*
39		*Service failure analysis*		6.4.3	*Fault Logging*	DS3	*Resource Availability*
40		*Identifying Vital Business Functions (VBF)*	ISO7	7.7.1	*Event logging*	DS3	*Resource Availability*
41		*Designing for availability*		6.5.1	*Network Control*	DS3	*Resource Availability*
42		*Designing for recovery*		6.4.3	*Fault Logging*	DS3	*Resource Availability*
43		*Risk Analysis and Management (for availability of Services)*		6.4.1	*Information Back-up*	DS3	*Resource Availability*
44		*Planned and preventive maintenance*	ISO6	6.4.1	*Information Back-up*	DS3	*Resource Availability*
45		*Production of the Projected Service Outage (PSO) document*		6.6.2	*Disposal of Media*	DS3	*Resource Availability*
46		*Availability Testing Schedule*		6.4.1	*Information Back-up*	DS3	*Resource Availability*
47	*Capacity Management*	*Business Capacity Management*	ISO3	3.1.1	*Inventory of Assets*	DS3	*Performance and Capacity Planning*

48		*Service Capacity Management*		5.1.4	*working in secure areas*	DS3	*Current Performance and Capacity*
49		*Component Capacity Management*	ISO5	5.1.3	*Securing Offices, rooms and facilities*	DS3	*Future Performance and Capacity*
50		*Utilization Monitoring*		5.2.3	*Cabling Security*	DS3	*Monitoring and Reporting*
51		*Response Time Monitoring*	ISO9	9.1.3	*Writing and implementing continuity plan*	DS3	*Monitoring and Reporting*
52		*Exploitation of new technology*	ISO1	2.1.4	*Authorization process for information processing facilities*	DS3	*Monitor Future Trends and Regulation*
53		*Threshold management and control*	ISO5	5.1.1	*Physical Security Perimeter*	DS3	*Monitoring and Reporting*
54		*Demand Management*	-	-	-	DS3	*Future Performance and Capacity*
55		*Modelling and trending*	-	-	-	DS3	*Future Performance and Capacity*
56		*Application sizing*	-	-	-	DS3	*Future Performance and Capacity*
57	*IT Service Continuity Management*	*Initiation - Policy setting*	ISO1	1.1.2	*Review and Evaluation*	DS4	*IT Continuity Framework*
58		*Specify terms of reference and scope*	ISO3	3.1.1	*Inventory of Assets*	DS4	*IT Continuity Framework*
59		*Allocate resources*	ISO4	4.1.2	*Personal Screening and Policy*	DS4	*IT Continuity Framework*

60		*Define the project organization and control structure*	ISO3	3.2.1	*Classification Guidelines*	DS4	*IT Continuity Framework*
61		*Agree project and quality plans*	ISO4	4.1.4	*Terms and conditions of employment*	DS4	*IT Continuity Framework*
62		*Business Impact Analyses for requirements*	ISO9	9.1.2	*business continuity and impact analysis*	DS4	*IT Continuity Framework*
63		*Risk analysis*	ISO9	9.1.3	*Writing and implementing continuity plan*	-	-
64		*IT Service Continuity Strategy*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
65		*Risk response measures*	ISO9	9.1.2	*business continuity and impact analysis*	DS4	*IT Continuity Plan*
66		*Implementation Risk reduction and Standby arrangements*	ISO10	10.1.1	*identification of applicable legislation*	-	-
67		*Organization and Disaster Recovery Planning*	ISO9	9.1.2	*business continuity and impact analysis*	DS4	*Maintenance of the IT Continuity Plan*
68		*Initial and ongoing testing*	ISO6	6.1.5	*separation of development and operational facilities*	DS4	*Testing of the continuity plan*

69		*Ongoing Education, Awareness and training*	ISO4	4.2.1	*information security education and training*	DS4	*IT Continuity Plan Training*
70		*Regular Reviews*	ISO7	7.2.4	*review of user access rights*	DS4	*Post-resumption Review*
71		*Change Management*	ISO6	6.1.2	*operational change control*		
72	*Information Security Management*	*Production, review and revision of an overall Information Security Policy*	ISO1	1.1.1	*Information Security Policy Document*	DS5	*Management of IT Security*
73		*Communication, Implementation and enforcement of Security Policy*	ISO1	1.1.2	*Review and Evaluation*	DS5	*IT Security Plan*
74		*Assessment and classification of all information assets and documentation*	ISO3	3.1.1	*Inventory of Assets*	-	-
75		*Implementation, review and revision and improvement security controls*	ISO6	6.1.1	*Documented operating procedures*	DS5	*Management of IT Security*
76		*Monitor and management of all security breaches and*	ISO6	6.3.1	*Control against malicious software*	DS5	*Malicious Software Prevention, Detection and Correction*

		major security incidents					
77		*Analysis, reporting and reduction of the volumes and impact of security breaches and incidents*	ISO6	6.1.3	*Incident Management Porcedures*	DS5	*Malicious Software Prevention, Detection and Correction*
78		*Schedule and completion of security reviews, audits and penetration tests*	ISO7	7.2.4	*review of user access rights*	DS5	*IT Security Plan*
79	*Supplier Management*	*Evaluation of new suppliers and contracts*	ISO2	2.2.1	*identification of risks from third party*	DS2	*Identification of all Supplier Relationships*
80		*Supplier categorization and maintenance Supplier and Contracts Database (SCD)*	ISO2	2.3.1	*Security requirements in outsourcing contracts*	DS2	*Supplier Risk Management*
81		*Establishing new suppliers and contracts*	ISO2	2.2.1	*identification of risks from third party*	DS2	*Supplier Relationship Management*
82		*Supplier and Contract Management and performance*	ISO2	2.3.1	*Security requirements in outsourcing contracts*	DS2	*Supplier Relationship Management*
83		*Contract renewal and/or termination*	ISO2	2.2.2	*security requirements in third party contracts*	DS2	*Supplier Performance Monitoring*

No	*ITIL Prespective*	ITIL	ISO		ISO	COBIT	COBIT
	Service Transition						
84	*Transition Planning & Support*	*Transition Strategy*	-	-	-	-	-
85		*Prepare for Service Transition*	-	-	-	-	-
86		*Planning and coordinating Service Transition*	-	-	-	-	-
87	*Change Management*	*Planning and controlling changes*	ISO6	6.1.2	*operational change control control*	-	-
88		*Change and release scheduling*	-	-	-	-	-
89		*Communications*	-	-	-	-	-
90		*Change decision making and change authorization*	ISO6	6.1.2	*operational change control control*	-	-
91		*Ensuring there are remediation plans*	-	-	-	-	-
92		*Chang Advisory Board*	-	-	-	-	-
93		*Emergency Change Handling*	-	-	-	-	-

94		*Measurement and control*	-	-	-	-	-
95		*Management Reporting*	-	-	-	-	-
96		*Understanding the impact of change*	-	-	-	-	-
97		*Continual improvement*	-	-	-	-	-
98	*Service Asset & Configuration*	*Configuration Management and Planning*	-	-	-	DS9	*Configuration Repository and Baseline*
99		*Configuration Identification*	-	-	-	DS9	*Identification and Maintenance of Configuration Items*
100		*Configuration Control*	-	-	-	DS9	*Configuration Repository and Baseline*
101		*Status accounting and reporting*	-	-	-	DS9	*Configuration Repository and Baseline*
102		*Verification and audit*	ISO8	8.2.4	*Output Data Validation*	DS9	*Configuration Integrity review*
103	*Release & Deployment Management*	*Release and deployment planning*	ISO6	6.1.5	*separation of development and operational facilities*	-	-

104		*Preparation for build, test and deployment*	ISO8	8.1.1	*Security Requirements analysis and specification*	-	-
105		*Build and test*	ISO8	8.5.2	*technical review of operationg system changes*	-	-
106		*Service testing and pilots*	ISO8	8.5.1	*change control procedures*	-	-
107		*Plan and prepare for deployment*	ISO8	8.1.1	*Security Requirements analysis and specification*	-	-
108		*Perform transfer, deployment and retirement*	-	-	-	-	-
109		*Verify deployment*	-	-	-	-	-
110		*Early life support*	-	-	-	-	-
111		*Review and close deployment*	-	-	-	-	-
112		*Review and close Service Transition*	-	-	-	-	-
113	*Service Validation and Testing*	*Validation and Test Management*	-	-	-	-	-
114		*Plan and Design Test*	-	-	-	-	-

115		*Verify test plan and test design*	-	-	-	-	-
116		*Prepare test environment*	-	-	-	-	-
117		*Perform tests*	-	-	-	-	-
118		*Evaluate exit criteria and report*	-	-	-	-	-
119		*Test clean up and close*	-	-	-	-	-
120	*Evaluation*	*Evaluation plan*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
121		*Understanding the intended effect of a change*	ISO9	9.1.3	*Writing and implementing continuity plan*	-	-
122		*Factors for considering the effect of a service change*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
123		*Evaluation of predicted and actual performance*	ISO9	9.1.1	*business continuity management process*	-	-
125		*Risk assessment*	ISO9	9.1.2	*busniess continuity and impact analysis*	-	-

126	*Knowledge Management*	*Knowledge Management Strategy*	ISO4	4.2.1	*information security education and training*	-	-
127		*Knowledge Transfer*	ISO4	4.2.1	*information security education and training*	-	-
128		*Data and Information Management*	ISO3	3.2.2	*information labeling and handling*	-	-
129		*Using the service knowledge management system*	ISO6	6.7.6	*publucly available systems*	-	-

No	*ITIL Prespective*	ITIL	ISO		ISO	COBIT	COBIT
	Service Operation						
130	*Incident Management*	*Incident Identification*	ISO6	6.1.3	*Incident Management Porcedures*	DS8	*Registration of Customer Queries*
131		*Incident Logging*		6.1.3	*Incident Management Porcedures*	DS8	*Registration of Customer Queries*
132		*Incident categorization*		6.1.3	*Incident Management Porcedures*	DS8	*Registration of Customer Queries*
133		*Incident prioritization*		6.1.3	*Incident Management Porcedures*	DS8	*Registration of Customer Queries*
134		*Initial diagnosis*	ISO4	4.3.4	*Learning from incident*	DS8	*Registration of Customer Queries*
135		*Incident escalation*	ISO6	6.1.3	*Incident Management Porcedures*	DS8	*Incident Escalation*
136		*Investigation and diagnosis*	ISO10	10.1.7	*collection of evidence*	DS8	*Incident Escalation*
137		*Resolution and recovery*	-	-	-	DS8	*Incident Escalation*
138		*Incident closure*	-	-	-	DS8	*Incident Closure*
139	*Event Management*	*Event occurs*	-	-	-	DS13	*IT Infrastructure Monitoring*
140		*Event notification*	ISO6	6.3.1	*Incident Management*	DS13	*IT Infrastructure*

					Porcedures		*Monitoring*
141		*Event detection*	ISO6	6.4.2	*operator logs*	DS13	*IT Infrastructure Monitoring*
142		*Event filtering*	-	-	-	DS13	*IT Infrastructure Monitoring*
143		*Significance of events*	ISO6	6.4.3	*Fault Logging*	DS13	*IT Infrastructure Monitoring*
144		*Event correlation*	-	-	-	DS13	*IT Infrastructure Monitoring*
145		*Trigger*	ISO6	6.3.1	*Control against malicious software*	DS13	*IT Infrastructure Monitoring*
146		*Response selection*	ISO6	6.3.1	*Control against malicious software*	DS13	*IT Infrastructure Monitoring*
147		*Review and actions*	ISO6	6.4.1	*Information Back-up*	DS13	*IT Infrastructure Monitoring*
148		*Close event*	-	-	-	DS13	*IT Infrastructure Monitoring*
149	*Request Fulfilment*	*Menu selection*	ISO2	2.1.5	*specialist information security advise*	DS8	*Service Desk*
150		*Financial approval*	-	-	-	DS8	*Service Desk*
151		*Other approval*	ISO2	2.1.5	*specialist information security advise*	DS8	*Service Desk*

152		*Fulfilment*	ISO2	2.1.5	*specialist information security advise*	DS8	*Service Desk*
153		*Closure*	ISO2	2.1.5	*specialist information security advise*	DS8	*Service Desk*
154	*Problem Management*	*Problem detection*	ISO6	6.4.3	*Fault Logging*	DS10	*Identification and Classification of Problems*
155		*Problem logging*	ISO6	6.4.3	*Fault Logging*	DS10	*Identification and Classification of Problems*
156		*Problem categorization*	ISO6	6.4.2	*operator logs*	DS10	*Identification and Classification of Problems*
157		*Problem prioritization*	ISO6	6.4.2	*operator logs*	DS10	*Identification and Classification of Problems*
158		*Workarounds*	ISO5	5.1.3	*Securing Offices, rooms and facilities*	DS10	*Problem Tracking and Resolution*
159		*Raising a known Error record*	ISO8	8.2.1	*Input Data Validation*	DS10	*Problem Tracking and Resolution*
160		*Problem resolution*	ISO6	6.4.3	*Fault Logging*	DS10	*Problem Tracking and Resolution*
161		*Problem closure*	-	-	-	DS10	*Problem Closure*

162		*Major Problem review*	-	-	-	DS10	*Problem Closure*
163		*Errors detect in the development environment*	-	-	-	-	-
164	*Access Management*	*Requesting access*	ISO2	2.1.4	*authorisation process for information processing facilities*	DS5	*User Account Management*
165		*Verification*	ISO2	2.1.7	*Independent review of information security*	DS5	*Identity Management*
166		*Providing rights*	ISO10	10.2.1	*Compliance with security policy*	DS5	*User Account Management*
167		*Monitoring identity status*	ISO10	10.2.1	*Compliance with security policy*	DS5	*User Account Management*
168		*Logging and tracking access*	ISO10	10.1.5	*preventive of misuse of information processing facility*	DS5	*User Account Management*
169		*Removing or restricting rights*	ISO10	10.1.1	*identification of applicable legislation*	DS5	*User Account Management*

No	*ITIL Prespective*	ITIL	ISO		ISO	COBIT	COBIT
	Continual Service Improvement						
170	*Reporting*	*Define targeted Audience*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
171		*Define Business Views*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
172		*Agreement on what to monitor and report*	ISO10	10.1.1	*identification of applicable legislation*	-	-
173		*Monitor against Service Level targets*	ISO10	10.1.1	*identification of applicable legislation*	-	-
174		*Reporting workloads, trends non-compliance*	ISO9	9.1.1	*business continuity management process*	-	-
175	*Service Measurement & Control*	*Developing a Service Management Framework*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
176		*Defining what to measure*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
177		*Setting targets*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-

178		*Service Management process measurement*	ISO9	9.1.4	*Business Continuity Planning Framework*	-	-
179		*Creating a measurement framework grid*	-	-	-	-	-
180		*Interpreting and using metrics*	-	-	-	-	-
181		*Interpreting metrics*	-	-	-	-	-
182		*Using measurement and metrics*	-	-	-	-	-
183		*Creating scorecard and reports*	-	-	-	-	-
184	*Return on Investment on CSI*	*Creating a return on Investment*	-	-	-	-	-
185		*Establishing the business case*	-	-	-	-	-
186		*Measuring benefits achieved*	-	-	-	-	-

Halaman ini sengaja dikosongkan.