**PROSES AUDIT**

Dalam melakukan penilaian *capability level* proses pada COBIT 5, masing-masing proses dianalisis secara bertahap apakah proses tersebut telah memenuhi persyaratan-persyaratan yang harus dipenuhi pada masing-masing *level*, mulai dari *level* 1 hingga *level* 5. Selain itu, terdapat ketentuan kategori dari hasil penilaian di tiap *level*nya, yaitu suatu proses cukup meraih kategori *Largely achieved* (L) dengan *range* nilai berkisar 50-85% atau *Fully achieved* (F) dengan *range* nilai berkisar 85%-100% untuk dapat dinyatakan bahwa proses tersebut telah meraih suatu *capability level* tersebut, namun proses tersebut harus meraih kategori *Fully achieved* (F) untuk dapat melanjutkan penilaian ke *capability level* berikutnya.

Tabel ringkasan pencapaian *capability level* ditunjukkan pada tabel di bawah ini:

Tabel 4.1 Ringkasan pencapaian *capability level*

|  |  |
| --- | --- |
| **Tujuan** | **[ deskripsi tujuan dari proses ]** |
| **Proses****[nama proses]** | ***Level* 0**  | ***Level* 1** | ***Level* 2** | ***Level* 3** | ***Level* 4** | ***Level* 5** |
|  |  | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Rating berdasarkan persentase dan warna** |  |  |  |  |  |  |  |  |  |  |

Deskripsi :

N = *Not achieved* ( 0 % - 15 % )

P = *Particaly achieved* ( 15 % - 50 % )

L = *Largely achieved* ( 50 % - 85 % )

F = *Fully achieved* ( 85 % - 100 % )

# N (*Not achieved* / tidak tercapai)

# Dalam kategori ini tidak ada atau hanya sedikit bukti atas pencapaian atribut proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar 0-15%.

# P (*Partially achieved* / tercapai sebagian)

# Dalam kategori ini terdapat beberapa bukti mengenai pendekatan, dan beberapa pencapaian atribut atas proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar 15-50%.

# L (*Largely achieved* / secara garis besar tercapai)

# Dalam kategori ini terdapat bukti atas pendekatan sistematis, dan pencapaian signifikan atas proses tersebut, meski mungkin masih ada kelemahan yang tidak signifikan. *Range* nilai yang diraih pada kategori ini berkisar 50-85%.

# F (*Fully achieved* / tercapai penuh)

# Dalam kategori ini terdapat bukti atas pendekatan sistematis dan lengkap, dan pencapaian penuh atas atribut proses tersebut. Tidak ada kelemahan terkait atribut proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar 85-100%.

# Penjelasan secara rinci penilaian *capability level*  pada masing-masing proses akan dijelaskan pada sub bab berikutnya.

DSS05 (***Manage Security Services* )**

adalah proses melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan agar tetap bisaditerima sesuai dengan kebijakan keamanan. Menetapkan peran, hak, dan melakukan pemantauan kemanan. Proses ini merupakan tanggung jawab dari Divisi *IT Operation > System Operation,*karena salah satu tanggung jawabnya adalah mengatur hak akses atau *privilege* bagi setiap *user* yang ada di perusahaan agar penggunaan hak akses sesuai dengan aturan dan kewenangan yang berlaku di perusahaan.

Tabel 4.141 *Manage Security Services* DSS05 Level 1

|  |
| --- |
| ***DSS05*** *(****Manage Security Services )*** |
| ***Management practice*** | ***Oututs*** | ***Exits***  | ***Score*** |
| **DSS05.01***Protect against malware* | *Malicious software prevention policy* |  |  |
| *Evaluations of potential threats* |  |
| **DSS05.02***Manage network and connectivity security* | *Connectivity security policy* |  |  |
| *Results of penetration tests* |  |
| **DSS05.03***Manage endpoint Security* | *Security policies for endpoint devices* |  |  |
| **DSS05.04***Manage user identity and logical access* | *Approved user access rights* |  |  |
| *Results of reviews of users accounts and privileges* |  |
| **DSS05.05***Manage physical access to IT assets* | *Approved access requests* |  |  |
| *Access logs* |  |
| **DSS05.06***Manage sensitive documents and output devices* | *Inventory of sensitive documents and devices* |  |  |
| *Access privileges* |  |
| **DSS05.07***Monitor the infrastructure for securityrelated Events* | *Security event logs* |  |  |
| *Security incident Characteristics* |  |
| *Security incident tickets* |  |
| *Average score* |  |

**4.1.27.1 *Protect against malware***

Proses “*Protect against malware*”

membahas mengenai software antivirus yang digunakan untuk menjaga keamanan, update yang dilakukan terhadap *antivirus*, serta mengenai *firewall* yang dimiliki dan mengenai pemblokan software-software yang dianggap menggangu dan peraturan yang hanya memperbolehkan user menginstall software untuk printer. Selain itu terdapat juga *Policy IT Security* yang membahas mengenai peraturan peraturan standar untuk mencegah penyebaran *malware* untuk mengancam kemanan.

Adanya evaluasi mengenai ancaman yang berpotensi menyerang sistem

**4.1.27.2 *Manage network and connectivity security***

Proses “*Manage network and connectivity security*”

membahas tentang wewenang login yang dimiliki user

Secara periodik dilakukan *penetration test*

**4.1.27.3 *Manage endpoint security***

Proses “*Manage endpoint security*”

membahas tentang kewajiban user untuk melakukan *lock* terhadap komputer masing-masing pada saat tidak menggunakan komputer.

**4.1.27.4 *Manage user identity and logical access***

Proses “*Manage user identity and logical access*”

membahas mengenai dokumen tertulis yang menunjukkan seluruh kegiatan *operational* hak akses yang diberikan pada setiap user .

melakukan tinjauan ulang mengenai hal yang disebutkan pada point 1

**4.1.27.5 *Manage physical access to IT assets***

Proses “*Manage physical access to IT assets*”

*Approved access request* terdapat pada ruang server yang memiliki pencatatan siapa yang memasuki ruang server dan memiliki peraturan yang boleh memasuki ruangan server hanya bagian infrastruktur,

*Access logs* juga mengenai catatan karyawan yang masuk ke dalam ruang server tersimpan pada database yang hanya bisa diakses melalui login .

**4.1.27.6 *Manage sensitive documents and output devices***

Proses “*Manage sensitive documents and output devices*”

membahas tentang pengumpulan dan penyimpanan segala informasi, ketentuan IT dalam

bentuk *hardcopy* maupun *softcopy* sebagai bukti dan keterangan yang dapat dipergunakan sebagai acuan dalam *system* kerja IT.

*Access priveleges*

**4.1.27.7 *Monitor the infrastructure for security-related events***

Proses “*Monitor the infrastructure for security-related events*”

mengenai dokumentasi kejadian yang menyangkut dengan keamanan sistem

mengenai adanya dokumentasi pengelompokan setiap karakteristik setiap kejadian yang menyangkut kemanan sistem

mengenai prosedur yang harus dilakukan ketika gangguan terjadi

Dari hasil penilaian capability *level*, apabila proses lulus dari *level* 1, karena proses ini memperoleh status *fully achieved* sebesar 100% sehingga proses ini dapat melakukan penilaian untuk *level* 2. Berikut ini adalah tabel untuk penilaian pada *level* 2 :

Tabel 4.4 Penilaian *capability level* 2.1proses

|  |
| --- |
| ***2.1 Performance Management*** |
| ***Generic practices*** | ***Exist*** | ***Score*** |
| *Identify the Objectives* |  |  |
| *Plan and monitor the performance* |  |  |
| *Adjust the performance* |  |  |
| *Define responsibilities* |  |  |
| *Identify and make available* |  |  |
| *Manage the interfaces* |  |  |
| ***Average Score*** |  |

 *:*

1. Semua anggota perusahaan telah mengerti terhadap tujuan dari semua kegiatan yang dilakukannya.
2. Perusahaan telah memiliki sistem penilaian yang tercantum dalam sebuah dokumen DP3 (Daftar Penilaian Pelaksanaan Pekerjaan).
3. Setiap kegiatan yang disetujui sudah ditentukan pelaksanaannya. Namun, perusahaan belum memiliki sistem Penilaian KPI (*Key Performance Indicator*) perusahaan. Sehingga performa setiap proses hanya diawasi oleh SPI (Satuan Pengawasan Internal) dalam mengawasi dan mengendalikan setiap proses.
4. Tanggung jawab setiap proses telah ditentukan, seperti yang tercantum dalam dokumen TUPOKSI ( Tugas pokok dan Fungsi ) setiap bagian.
5. menyediakan sumber daya yang dibutuhkan dalam melakukan kegiatan-kegiatan dalam perusahaan.
6. melakukan hubungan baik dengan pihak lain yang telah ditentukan tatacara pelaksanaannya.

 Setelah melakukan penilaian pada *level* 2.1 selanjutnya akan dilakukan penilaian pada *level* 2.2. Penilaian dapat dilihat pada tabel 4.5 dibawah ini :

Tabel 4.5 Penilaian *capability level* 2.2proses

|  |
| --- |
| ***2.2 Work Product Management*** |
| ***Generic practices*** | ***Exist*** | ***Score*** |
| *Define the requirements for the work products* |  |  |
| *Define the requirements for documentation and control* |  |  |
| *Identify,document and control* |  |  |
| *Review and adjust work products* |  |  |
| ***Average Score*** |  |

 dinyatakan lulus pada *level* 2.2 *Work Product Management* karena :

1. Perusahaan telah menentukan bentuk dokumen hasil kerja sebagai *template* laporan. Standardisasi format pelaporan dibuat oleh sub bidang analisa, desain dan integrasi sistem.
2. Setiap dokumen yang telah dibuat mencantumkan nama pembuat serta nama pihak yang menyetujui.
3. Setiap dokumen yang dibuat juga mencantumkan nomor revisi sehingga dokumen dikontrol denngan baik.
4. Perusahaan menyatakan tidak keberatan untuk merubah format dokumen bila dibutuhkan dalam rangka meningkatkan efektifitas dan efisiensi perusahaan.

CARA PENILAIAN

Perhitungan dilakukan dengan cara sebagai berikut :

$$capability level=\frac{\left(0\*y\_{0}\right)+\left(1\*y\_{1}\right)+\left(2\*y\_{2}\right)+…(5\*y\_{5})}{z }$$

$$y\_{n}=jumlah proses yang ada di dalam level n$$

*z = jumlah proses yang dievaluasi*

 Berdasarkan data pencapaian *level* oleh masing-masing proses, CONTOH nilai capability rata-rata perusahaan adalah sebagai berikut :

$$capability level=\frac{\left(0\*2\right)+\left(1\*4\right)+\left(2\*4\right))}{ 10}=1.2$$