

# Audit Sistem Informasi Absensi pada PT. Bank Central Asia Tbk menggunakan COBIT 4.1

Jelvino<sup>#1</sup>, Johanes Fernandes Andry<sup>#2</sup>

<sup>#1,2</sup>Program Studi Sistem Informasi, Universitas Bunda Mulia  
Jl. Lodan Raya No. 2 Ancol, Jakarta Utara 14430

<sup>1</sup>vinozhou90@gmail.com

<sup>2</sup>jandry@bundamulia.ac.id

**Abstract** — BCA is a national bank established in 1957 and has continued to grow. Nowadays the bank has supported business processes in various companies, such as the use of attendance information systems. During this system implementation, it has been running to support the procedures of attendance activities. The purpose of this research is to get an overview of the performance of information technology governance in order to determine the extent of maturity level which is currently running, with a few aspects to consider such as effectiveness and, efficiency. The conclusion that can be drawn from the research that has been done is IT governance at the BCA has been done, although still run optimally within each IT process contained in the sub domain Monitor Evaluate Assess (MEA) on average was at 3.0 (defined process) for sub domain DS1, DS5, DS10 and ME2.

**Keywords**— Audit SI, Absensi, BCA, COBIT 4.1

## I. PENDAHULUAN

Perkembangan sistem informasi sampai saat ini telah mendukung proses bisnis diberbagai perusahaan, seperti penggunaan sistem informasi absensi pada PT. Bank Central Asia.Tbk (BCA). Untuk itu diperlukan suatu evaluasi atas penggunaan sistem informasi absensi yang dimiliki BCA untuk memastikan bahwa sistem informasi yang dimiliki telah memberi kemudahan bagi perusahaan. Selama ini implementasi sistem telah berjalan untuk mendukung prosedur kegiatan absensi. Diharapkan dengan dilakukannya audit sistem informasi ini, agar sistem absensi yang ada pada BCA akan menjadi lebih baik. Auditor TI bertanggung jawab atas penilaian efisiensi tata kelola TI dengan tingkatan prosedur dalam pelaksanaannya. Auditor TI (dari dalam organisasi atau independen) dapat melakukan sejumlah peran kunci [1], [2].

Rekomendasi dari hasil audit adalah perbaikan dan peningkatan sistem informasi absensi dan tata kelola teknologi informasi di BCA khususnya pada KCP Mangga Besar, Jakarta.

## II. TINJAUAN PUSTAKA

### A. Audit Sistem Informasi

Audit SI/TI dalam kerangka kerja COBIT lebih sering disebut dengan istilah IT Assurance ini bukan hanya dapat memberikan evaluasi terhadap keadaan tata kelola Teknologi Informasi di BCA tetapi dapat juga memberikan masukan yang dapat digunakan untuk perbaikan pengelolaannya di masa yang akan datang [3]. Audit Sistem Informasi adalah proses untuk mengumpulkan dan mengevaluasi bukti dalam menentukan apakah sistem informasi telah dibangun sehingga memelihara integritas data, menjaga aset, membuat sasaran organisasi dapat tercapai secara efektif, dan menggunakan sumber daya yang efisien [4], [5].

### B. Absensi

Absensi dapat dikatakan suatu pendataan kehadiran yang merupakan bagian dari aktifitas pelaporan yang ada dalam sebuah institusi. Absensi disusun dan diatur sehingga mudah untuk dicari dan dipergunakan ketika diperlukan oleh pihak yang berkepentingan. Secara umum, jenis-jenis absensi menurut cara penggunaannya dapat dikelompokkan menjadi dua, yaitu :

- Absensi Manual, yang merupakan cara penulisan kehadiran dengan cara menggunakan pena berupa tanda tangan
- Absensi non manual, yang merupakan cara penulisan kehadiran dengan menggunakan alat yang terkomputerisasi, bisa menggunakan kartu RFID ataupun fingerprint [6].

### C. COBIT 4.1

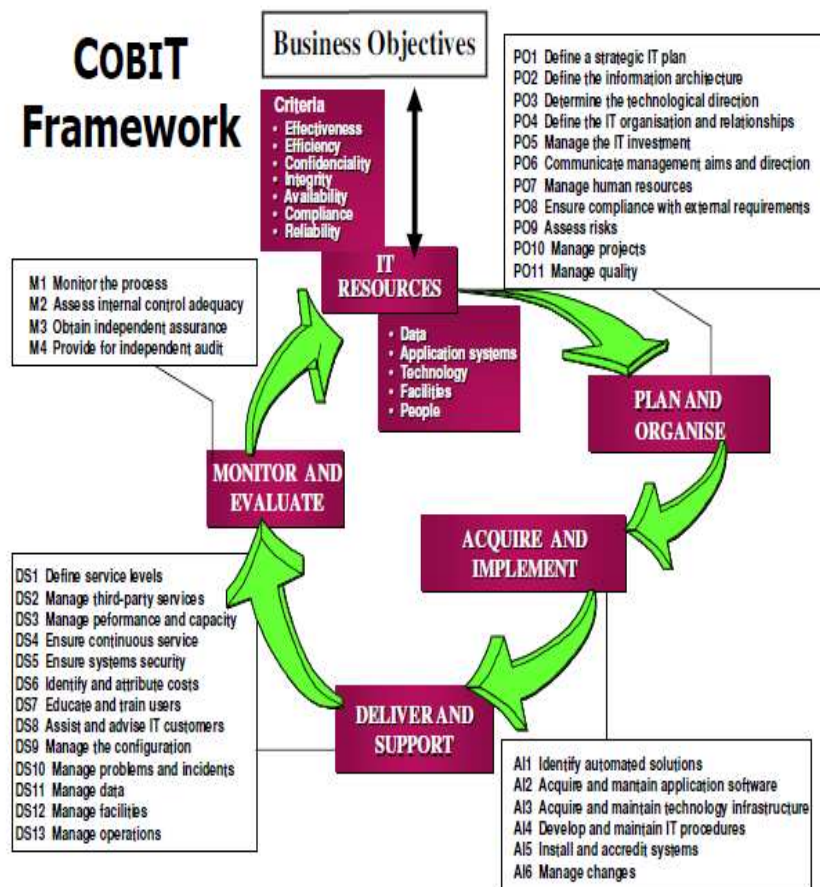
Metode COBIT 4.1 (*Control Objective for Information and related Technology*) merupakan suatu *framework* yang terdiri dari domain dan proses yang digunakan untuk mengatur aktivitas dan *logical structure*. Metode COBIT dapat berguna untuk teknologi informasi membuat hubungan kerja kebutuhan bisnis, organisasi teknologi informasi dapat membuat proses model, mengidentifikasi sumber daya teknologi informasi, dapat mengarahkan objektif kontrol Manajemen [7], [8]. Keseluruhan *Framework COBIT 4.1* diperlihatkan pada gambar 1.

COBIT membantu menyokong pengembangan kebijakan yang jelas dan langkah-langkah praktis terbaik yang dapat

diambil untuk pengendalian teknologi informasi di seluruh perusahaan. COBIT dirancang antara lain untuk mendukung:

- Manajemen eksekutif dan dewan direksi.
- Bisnis dan manajemen teknologi informasi.

- Pengelolaan, *assurance*, pengendalian dan *security professionals* (IT Governance Institute, 2005) [9], [11], [12].



Gambar 1. Framework COBIT (COBIT 4.1 Excerpt, Executive Summary Framework, 2008) [9], [10], [11], [12], [13].

#### D. Maturity Level

Adapun *generic maturity model* yang digunakan adalah

• 0 *Non-existent* – tidak ada sama sekali proses yang terlihat. Perusahaan belum menyadari bahwa ada masalah yang harus dikaji.

• 1 *Initial/Ad Hoc* – Ada bukti bahwa perusahaan telah menyadari ada masalah yang ada dan harus dikaji namun belum ada standarisasi. Tetapi, ada pendekatan *ad hoc* yang cenderung diaplikasikan sesuai kasus. Pendekatan manajemen secara umum tidak terstruktur.

• 2 *Repeatable but Intuitive* – Proses telah dikembangkan pada tahap dimana prosedur yang mirip telah diikuti oleh bermacam-macam orang yang melaksanakan tugas ini. Tidak ada training atau komunikasi secara formal tentang prosedur standard dan tanggung jawabnya jatuh pada individu. Ada ketergantungan yang tinggi pada individu dan sering terjadi *error*.

• 3 *Defined Process* – Prosedur telah terstandarisasi dan terdokumentasi, dan komunikasi lewat training. Merupakan keharusan bahwa proses tersebut harus diikuti. Tetapi, sedikit deviasi yang terjadi. Prosedur tersebut tidak rumit tetapi formalisasi dari practice yang sekarang

• 4 *Managed and measurable* – manajemen memantau dan mengukur kesesuaian dengan prosedur dan mengambil tindakan dimana proses terlihat tidak berjalan efektif. Proses dikembangkan secara berkelanjutan dan memberikan practice yang baik. Otomasi dan alat bantu digunakan dalam cara yang terbatas dan terpecah-pecah.

• 5 *Optimised* – proses telah dirancang sampai tingkat pelaksanaan yang baik, berdasarkan hasil dari pengembangan berkelanjutan dan *maturity modelling* dengan perusahaan lain. IT digunakan dalam cara terintegrasi untuk mengotomasi alur kerja, menyediakan alat bantu untuk meningkatkan kualitas dan efektifitas, membuat perusahaan mudah diadaptasi [9], [11], [12].

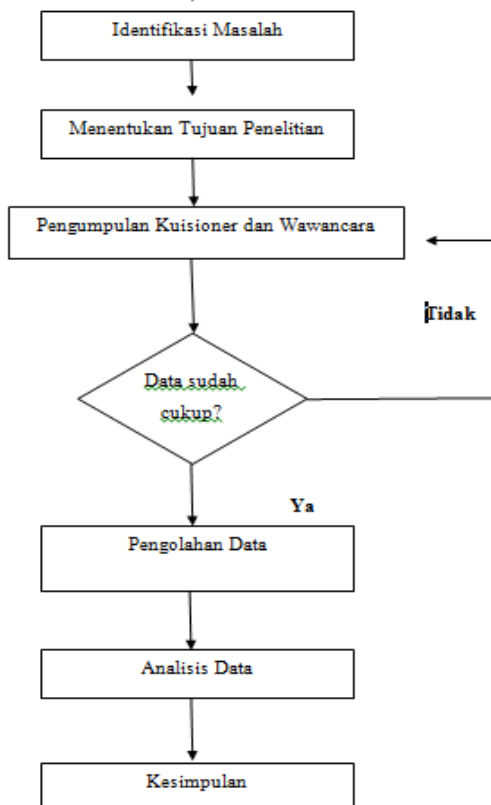
III. METODOLOGI PENELITIAN

Metodologi penelitian yang dilakukan dan tahapan-tahapan penulis dalam mengambil ataupun memperoleh data dari sumber, mulai dari survei awal, wawancara dan kuisisioner ditujukan pada Gambar 2. Diagram Alir Penelitian.

Lingkup dari penelitian ini dibatasi pada audit sistem informasi absensi pada PT.Bank Central Asia,Tbk khususnya pada Kantor Cabang Pembantu (KCP) Mangga Besar, Jakarta dan Identifikasi Proses Sistem Informasi Absensi. Pada tahap ini, menetapkan proses teknologi informasi yang sesuai dengan standar COBIT yang telah diolah sesuai dengan studi kasus. Cakupan IT domain yang di audit pada sistem informasi absensi, diperlihatkan pada Tabel I Cakupan IT Domain Yang Di Audit.

TABEL I  
CAKUPAN IT DOMAIN YANG DI AUDIT

Sub Domain	Descriptions
AI4	Enable Operation and Use
DS1	Define and Manage Service Levels
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS10	Manage Problems
ME2	Monitor and Evaluate Internal Control



Gambar 2. Diagram Alir Penelitian

Prosedur Penelitian merupakan suatu kegiatan yang harus dilakukan dalam melakukan penelitian. Adapun tahapan dan prosedur penelitiannya sebagai berikut:

1) *Planning* (Perencanaan),

Perencanaan merupakan tahapan awal dalam prosedur penelitian yang kami lakukan. Karena pada tahap ini kami dapat menentukan ruang lingkup (*scope*), sebuah objek yang akan di audit, standar evaluasi dari hasil audit serta komunikasi terhadap orang yang bersangkutan akan organisasi/perusahaan yang akan diaudit dengan menganalisa sebuah visi, misi, sasaran dan tujuan objek, dan kebijakan-kebijakan yang terkait dengan pengolahan investigasi. Pada tahap perancangan meliputi beberapa aktifitas utama yaitu penetapan ruang lingkup dan tujuan audit, pengorganisasian tim audit, pemahaman mengenai operasi bisnis klien, pengkajian ulang hasil audit sebelumnya, dan penyiapan program audit.

2) *Field Work* (Pemeriksaan Lapangan)

Pada tahap ini auditor bertujuan untuk mendapatkan informasi dengan cara mengumpulkan data dengan pihak-pihak yang terkait yang menggunakan beberapa metode yang dapat dilakukan seperti; wawancara, kuesioner, dan melakukan survey langsung ke tempat penelitian dilakukan. Data yang di dapat nantinya akan sangat berguna dalam membantu auditor melakukan analisa sebuah organisasi/perusahaan yang di audit.

3) *Reporting* (Pelaporan)

Setelah proses pengumpulan data, maka akan didapat data yang akan diproses untuk dihitung berdasarkan perhitungan *maturity level*. Pada tahap ini yang akan dilakukan auditor adalah memberikan informasi berupa hasil-hasil dari audit. Perhitungan *maturity level* dilakukan mengacu pada hasil wawancara, survey dan rekapitulasi hasil penyebaran kuesioner. Berdasarkan hasil *maturity level* yang mencerminkan kinerja saat ini (*current maturity level*) dan kinerja standard atau ideal yang diharapkan akan menjadi acuan untuk selanjutnya dilakukan analisis kesenjangan (*gap*). Hal tersebut dimaksudkan untuk mengetahui adanya *gap* tersebut serta mengetahui apa yang menyebabkan masalah akan dapat terlihat lebih jelas dimana letak kesalahannya.

4) *Follow-Up* (Tindak Lanjut)

Setelah melakukan pelaporan atau *reporting* maka hal yang dilakukan selanjutnya adalah memberikan laporan hasil audit berupa rekomendasi tindakan perbaikan kepada pihak manajemen objek yang diteliti, untuk selanjutnya wewenang perbaikan menjadi tanggung jawab manajemen objek yang diteliti apakah akan diterapkan atau hanya menjadi acuan untuk perbaikan dimasa yang akan datang.

IV. HASIL AUDIT DAN PEMBAHASAN

Pada bagian ini, akan membahas sistem informasi absensi dengan pendekatan COBIT framework pada BCA. Disini, penulis akan menganalisa lebih kepada lingkungan yang

terjadi didalam IT departemen, mulai dari karyawan, perlengkapan, keamanan fisik, regulasi, dan sebagainya.

#### 4.1 AI4 Enable Operation and Use

Proses ini memerlukan dokumentasi dan manual standar yang akan digunakan oleh users dan IT, serta pelatihan perlu diadakan untuk menjamin aplikasi dan infrastruktur digunakan serta dijalankan dengan tepat.

##### 4.1.1 AI4.1 Planning for Operational Solutions

Perencanaan untuk solusi operasional dengan mengembangkan rencana untuk mengidentifikasi dan mendokumentasikan semua, aspek teknis operasional dan penggunaan sehingga semua orang yang akan mengoperasikan, menggunakan dan mempertahankan solusi otomatis dapat melaksanakan tanggung jawab mereka. Hasil audit adalah dokumentasi data khususnya sistem absensi pada BCA belum diterapkan secara teknologi ini berarti hanya secara manual. Nilai *maturity level* 2, yaitu *Repeatable but Intuitive*.

##### 4.1.2 AI4.2 Knowledge Transfer to Business Management

*Transfer* pengetahuan untuk manajemen bisnis dengan *mentransfer* pengetahuan untuk manajemen bisnis untuk memungkinkan individu untuk mengambil kepemilikan dari sistem dan data, dan olahraga tanggung jawab untuk penyediaan layanan dan kualitas, pengendalian internal, dan aplikasi administrasi. Hasil audit adalah pelatihan kepada karyawan mengenai sistem yang dijalankan tidak diterapkan semua namun hanya sebagian saja. Sehingga apabila terjadi masalah hanya beberapa karyawan saja yang dapat menyelesaikannya. Nilai *maturity level* 2, yaitu *Repeatable but Intuitive*.

##### 4.1.3 AI4.3 Knowledge Transfer to End Users

*Transfer* pengetahuan untuk pengguna akhir dengan *mentransfer* pengetahuan dan keterampilan untuk memungkinkan pengguna akhir untuk secara efektif dan efisien menggunakan sistem untuk mendukung proses bisnis. Hasil audit adalah pelatihan kepada setiap pengguna akhir diterapkan dan berjalan dengan baik. Nilai *maturity level* 2, yaitu *Repeatable but Intuitive*.

##### 4.1.4 AI4.4 Knowledge Transfer to Operations and Support Staff

*Transfer* pengetahuan untuk operasional dan staff pendukung *transfer* pengetahuan dan keterampilan yang memungkinkan operasi dan staf pendukung teknis untuk secara efektif dan efisien memberikan, dukungan dan memelihara sistem dan infrastruktur yang terkait. Hasil audit adalah setiap pengetahuan akan produk-produk dan sistem diberikan kepada staff yang paling rendah hal ini guna meningkatkan pelayanan dan pengetahuan produk dan sistem yang berjalan di BCA. Nilai *maturity level* 3, yaitu *Defined Process*.

Dari hasil analisa audit tersebut, diperoleh level kematangan dari setiap proses yang ada dalam tahap AI4 *Enable Operation and Use* dan proses-prosesnya dapat dilihat pada Tabel II Hasil *Maturity AI4 Enable Operation and Use*.

TABEL III

HASIL MATURITY AI4 ENABLE OPERATION AND USE

AI4 Enable operation and use		Maturity Level
AI4.1	<i>Planning for Operational Solutions</i>	2
AI4.2	<i>Knowledge Transfer to Business Management</i>	2
AI4.3	<i>Knowledge Transfer to End Users</i>	2
AI4.4	<i>Knowledge Transfer to Operations and Support Staff</i>	3
AI4	Rata-rata	2.25

#### 4.2 DS1 Define and Manage Service Levels

Komunikasi yang efektif antara manajemen IT dan pelanggan bisnis mengenai jasa yang dibutuhkan, disanggupi oleh definisi dan persetujuan layanan IT dan tingkat layanan yang didokumentasikan. Proses ini juga mencakup pemantauan dan pelaporan berkala pada stakeholder pada pemenuhan tingkat layanan. Proses ini memungkinkan keselarasan antara layanan IT dan persyaratan bisnis terkait.

##### 4.2.1 DS1.1 Service Level Management Framework

Menetapkan sebuah kerangka yang menyediakan tingkat layanan manajemen proses antara pelanggan dan penyedia layanan. Kerangka harus terus menerus menjaga keselarasan antara kebutuhan bisnis dan prioritas, serta memfasilitasi pemahaman yang sama antara pelanggan dan penyedia. Kerangka tersebut harus mencakup proses untuk menciptakan kebutuhan layanan, definisi layanan, SLA, OLA dan sumber pendanaan. Hasil audit adalah BCA Menerapkan tingkat pelayanan yang baik dimana kebutuhan bisnis selalu difasilitasi oleh sistem yang memadai sehingga proses bisnis berjalan dengan baik di perusahaan tersebut. Nilai *maturity level* 3, yaitu *Defined Process*.

##### 4.2.2 DS1.2 Definition of Services

Definisi karakteristik pelayanan dan kebutuhan bisnis, serta memastikan mereka terorganisasi dan disimpan secara terpusat melalui implementasi pendekatan portofolio katalog layanan. Hasil audit adalah data-data maupun dokumen yang terkait dengan perusahaan tersimpan dan terorganisir dengan baik pada gudang arsip dan terorganisir sehingga memudahkan karyawan untuk mencari kembali dokumen tersebut. Nilai *maturity level* 4, yaitu *Managed and measurable*

##### 4.2.3 DS1.3 Service Level Agreements

Menetapkan dan menyetujui SLA untuk semua layanan IT kritis berdasarkan kebutuhan pelanggan dan kemampuan IT, seperti komitmen pelanggan, persyaratan layanan pendukung, pengaturan pendanaan dan komersial, dan sebagainya. Hasil audit adalah dari segi tanggung jawab kepengurusan terutama pada sistem absensi pada BCA sudah ada dan berjalan namun belum memenuhi *unsure defined process* dikarenakan beluma da SDM yang dikhususkan untuk bertanggung jawab terhadap pengelolaan sistem tersebut. Nilai *maturity level* 2, yaitu *Repeatable but Intuitive*.

#### 4.2.4 DS1.4 *Operating Level Agreements*

Menetapkan OLA yang menjelaskan bagaimana layanan yang akan disampaikan secara teknis untuk mendukung SLA secara optimal. Hasil audit adalah dari sisi *operation level system* absensi pada BCA sudah berada pada tahap yang baik dimana KP (Kantor Pusat) sudah mendukung operasi layanan secara optimal seperti *maintenance* sistem secara rutin. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.2.5 DS1.5 *Monitoring and Reporting of Service Level Achievements*

Memantau kriteria kinerja tingkat layanan tertentu dan melaporkan pencapaian tingkat layanan dalam bentuk yang lebih berarti bagi *stakeholder*. Hasil *statistic* pemantauan tersebut dianalisis untuk mengetahui kelebihan dan kekurangannya sehingga dapat meningkatkan layanan. Hasil audit adalah dari sisi *monitoring level* sudah terdapat audit internal maupun audit eksternal yang memonitoring setiap sistem aplikasi maupun proses bisnis yang berjalan di setiap cabang. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.2.6 DS1.6 *Review of Service Level Agreements and Contracts*

Secara teratur meninjau SLA dan kontrak fondasi (UCs) dengan penyedia layanan internal dan eksternal untuk memastikan bahwa mereka efektif dan *up to date* serta perubahan dalam persyaratan telah diperhitungkan. Hasil audit adalah pengkinian sistem selalu mengikuti perintah dari Kantor Pusat (KP) sehingga setiap aplikasi maupun sistem tergantung dari keputusan KP. Nilai *maturity level* 3, yaitu *Defined Process*.

TABEL IIIII

DS1 DEFINE AND MANAGE SERVICE LEVELS

DS1 Define And Manage Service Levels		Maturity Level
DS1.1	<i>Service Level Management Framework</i>	3
DS1.2	<i>Definition of Services</i>	4
DS1.3	<i>Service Level Agreements</i>	2
DS1.4	<i>Operating Level Agreements</i>	3
DS1.5	<i>Monitoring and Reporting of Service Level Achievements</i>	3
DS1.6	<i>Review of Service Level Agreements and Contracts</i>	3
DS1	Rata-rata	3

Dari hasil analisa audit tersebut, diperoleh level kematangan dari setiap proses yang ada dalam tahap DS1 *Define and manage service levels* dan proses-prosesnya dapat dilihat pada Tabel III Hasil *Maturity DS1 Define And Manage Service Levels*.

#### 4.3 DS4 *Ensure Continuous Service*

Kebutuhan untuk menyediakan layanan IT yang berkesinambungan membutuhkan pengembangan, mempertahankan dan pengujian rencana kontinuitas IT,

memanfaatkan penyimpanan *offsite backup* dan memberikan pelatihan rencana kelangsungan secara periodik.

#### 4.3.1 DS4.1 *IT Continuity Framework*

Kerangka kerja ini harus membahas struktur organisasi untuk manajemen kontinuitas, yang meliputi peran, tugas dan tanggung jawab penyedia layanan internal dan eksternal, manajemen mereka dan pelanggan mereka, dan proses perencanaan yang menciptakan aturan dan struktur untuk dokumen, pengujian dan melaksanakan pemulihan bencana IT dan rencana kontinjensi. Hasil audit adalah keberlangsungan IT di BCA sudah terdefinisi ini terbukti dari pengelolaan IT yang baik seperti *back up* data berkala serta *monitoring* rutin dari pihak IT sehingga didefinisikan dalam *Defined Process*. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.3.2 DS4.2 *IT Continuity Plans*

Rencana harus didasarkan pada pemahaman risiko potensi dampak bisnis dan membahas persyaratan untuk ketahanan, pengolahan alternatif dan kemampuan pemulihan dari semua layanan IT kritis. Hasil audit adalah pengembangan berkelanjutan IT khususnya sistem absensi sudah didefinisikan namun belum berjalan dengan sempurna sehingga perlu dibentuk sebuah tim yang mengurus kelanjutan pengembangan aplikasi. Nilai *maturity level* 2, yaitu *Repeatable but Intuitive*.

#### 4.3.3 DS4.3 *Critical IT Resources*

Fokuskan perhatian pada item yang dispesifikasikan sebagai yang paling kritis dalam rencana kelangsungan IT untuk membangun ketahanan dan menetapkan prioritas dalam situasi pemulihan. Hasil audit adalah fokuskan perhatian pada item yang dispesifikasikan sebagai yang paling kritis dalam rencana kelangsungan IT untuk membangun ketahanan dan menetapkan prioritas dalam situasi pemulihan. Hasil audit adalah evaluasi dan Monitoring aplikasi sudah diterapkan, namun pemulihan aplikasi sistem absen bila mengalami gangguan kritikal belum berjalan dengan baik. Nilai *maturity level* 2, yaitu *Repeatable but Intuitive*.

#### 4.3.4 DS4.4 *Maintenance of the IT Continuity Plan*

Mendorong manajemen IT untuk mendefinisikan dan mengeksekusi prosedur kontrol perubahan untuk memastikan bahwa rencana kontinuitas IT terus berkembang dan mencerminkan kebutuhan bisnis yang sebenarnya secara terus-menerus. Hasil audit adalah dari segi *maintenance* sistem absensi pada BCA belum dilaksanakan secara rutin hal ini dikarenakan sistem aplikasi absensi digunakan sebagai perangkat pendukung proses bisnis saja. Nilai *maturity level* 2, yaitu *Repeatable but Intuitive*.

#### 4.3.5 DS4.5 *Testing of the IT Continuity Plan*

Menguji rencana kontinuitas IT secara teratur untuk memastikan bahwa sistem IT dapat pulih secara efektif, menangani kekurangan dan menjaga rencana tetap relevan. Hasil audit adalah pengujian sistem TI terbukti sudah berjalan dengan baik dengan adanya pemantauan dari

Kantor Pusat. Serta laporan-laporan yang tepat waktu. Nilai maturity level 3, yaitu *Defined Process*.

#### 4.3.6 DS4.6 IT Continuity Plan Training

Menyediakan semua pihak terkait dengan sesi pelatihan reguler mengenai tata cara serta peran dan tanggung jawab mereka jika terjadi insiden atau bencana. Hasil audit adalah pelatihan mengenai sistem TI belum sepenuhnya diterapkan pada karyawan-karyawan BCA. Sehingga hanya beberapa karyawan yang terikat dengan tanggung jawab yang mengerti proses dan sistem pemakaian sistem IT. Nilai maturity level 2, yaitu *Repeatable but Intuitive*.

#### 4.3.7 DS4.7 Distribution of the IT Continuity Plan

Tentukan bahwa adanya pendefinisian dan pengelolaan strategi distribusi untuk memastikan bahwa rencana didistribusikan dengan benar dan aman serta tersedia bagi pihak berwenang yang berkepentingan, kapan dan dimana diperlukan. Hasil audit adalah distribusi kelanjutan IT pada setiap cabang berbeda-beda sehingga tergantung pada kebijakan Kantor Wilayah Bank BCA. Setiap kantor wilayah mempunyai pengembangan IT yang sedikit berbeda, dan tidak sama dengan Kantor Wilayah lain. Nilai maturity level 2, yaitu *Repeatable but Intuitive*.

#### 4.3.8 DS4.8 IT Services Recovery and Resumption

Hal ini termasuk aktivasi dari situs cadangan, inisiasi proses alternatif, komunikasi pelanggan dan *stakeholder*, dan prosedur penerusan. Hasil audit adalah pemulihan layanan IT sudah diterapkan dengan baik. Namun dalam melaksanakannya memerlukan SDM yang ahli dalam hal tersebut. Sehingga tidak semua karyawan dapat melakukan pemulihan IT apabila dibutuhkan. Nilai maturity level 2, yaitu *Repeatable but Intuitive*.

#### 4.3.9 DS4.9 Offsite Backup Storage

Penyimpanan *offsite* semua *backup* media kritis, dokumentasi dan sumber daya IT lainnya yang diperlukan untuk rencana kontinuitas pemulihan dan bisnis IT. Hasil audit adalah penyimpanan data dan arsip sudah berjalan dan diterapkan dengan sangat baik, tersusun dan tertata secara rapi pada sebuah ruangan yang disediakan, semua data dan dokumen penting tercatat dengan baik sehingga memenuhi *unsure Defined Process*. Nilai maturity level 3, yaitu *Defined Process*.

#### 4.4.10 DS4.10 Post-resumption Review

Mentukan apakah manajemen IT telah menetapkan prosedur untuk menilai kecukupan dari rencana dalam hal penerusan keberhasilan fungsi IT setelah bencana, dan memperbarui rencana yang sesuai. Hasil audit adalah pemulihan data dan rencana pemulihan setelah bencana telah memiliki prosedur dan tahapan yang baik sehingga semua perlengkapan telah disediakan apabila terjadi bencana. Nilai maturity level 3, yaitu *Defined Process*.

Dari hasil analisa audit tersebut, diperoleh level kematangan dari setiap proses yang ada dalam tahap DS4 *Ensure continuous service* dan proses-prosesnya dapat dilihat pada Tabel IV Hasil Maturity DS4 *Ensure continuous service*.

TABEL IVV

HASIL MATURITY DS4 ENSURE CONTINUOUS SERVICE

DS1	DS4 Ensure continuous service	Maturity Level
DS4.1	IT Continuity Framework	3
DS4.2	IT Continuity Plans	2
DS4.3	Critical IT Resources	2
DS4.4	Maintenance of the IT Continuity Plan	2
DS4.5	Testing of the IT Continuity Plan	3
DS4.6	IT Continuity Plan Training	2
DS4.7	Distribution of the IT Continuity Plan	2
DS4.8	IT Services Recovery and Resumption	2
DS4.9	Offsite Backup Storage	3
DS4.10	Post-resumption Review	3
DS4	Rata-rata	2.4

#### 4.5 DS5 Ensure Systems Security

Proses ini meliputi membangun dan mempertahankan peran dan tanggung jawab keamanan IT, kebijakan, standar, dan prosedur. Manajemen keamanan juga termasuk melakukan pemantauan keamanan dan pengujian berkala serta mengimplementasikan tindakan perbaikan untuk mengidentifikasi kelemahan atau insiden keamanan. Manajemen keamanan yang efektif melindungi semua aset IT untuk meminimalkan dampak bisnis dari kerentanan dan insiden keamanan.

##### 4.5.1 DS5.1 Management of IT Security

Mengelola keamanan TI pada tingkat tertinggi organisasi yang tepat, sehingga manajemen tindakan keamanan ini sejalan dengan kebutuhan bisnis. Hasil audit adalah pengelolaan IT security sudah baik ini terbukti dari organisasi IT yang tertata serta keamanan data yang terjamin dengan aplikasi keamanan yang terjamin. Nilai maturity level 3, yaitu *Defined Process*.

##### 4.5.2 DS5.2 IT Security Plan

Menerjemahkan kebutuhan bisnis, risiko dan penyesuaian ke dalam rencana keamanan IT secara keseluruhan, dengan mempertimbangkan infrastruktur IT dan budaya keamanan. Mengkomunikasikan kebijakan dan prosedur keamanan pada stakeholder dan pengguna. Hasil audit adalah perencanaan akan keamanan data serta pengkinian perangkat lunak selalu diutamakan dalam hal keamanan seperti *control* rutin dari pihak IT pada setiap cabang dan pengkinian keamanan data yang cepat. Nilai maturity level 3, yaitu *Defined Process*.

##### 4.5.3 DS5.3 Identity Management

Memastikan semua pengguna (internal, eksternal dan sementara) dan aktivitas mereka di sistem IT (aplikasi bisnis, lingkungan IT, operasi sistem, pengembangan dan pemeliharaan) dapat diidentifikasi secara unik.



Konfirmasikan bahwa user memiliki hak akses ke sistem dan data yang sesuai dengan kebutuhan bisnis didefinisikan dan didokumentasikan dan persyaratan kerja yang melekat pada identitas user. Hasil audit adalah segala kegiatan yang berkaitan dengan akses aplikasi dan transaksi dengan menggunakan aplikasi berbasis IT terekam dan diawasi oleh KP sehingga mengurangi kemungkinan terjadinya hal yang tidak diinginkan. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.4 DS5.4 User Account Management

Mengalamatkan permintaan, pembuatan, penerbitan, penangguhan, modifikasi dan penutupan *account* pengguna dan hak akses pengguna terkait dengan satu set prosedur manajemen *user account*. Hasil audit adalah setiap karyawan yang memiliki tanggung jawab terkait aplikasi yang digunakan memiliki akun tersendiri yang menjadi bagian dari tanggung jawab karyawan tersebut. Setiap karyawan dengan jabatan yang berbeda memiliki akses yang berbeda pula. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.5 DS5.5 Security Testing, Surveillance and Monitoring

Menguji dan memantau pelaksanaan keamanan IT dengan cara proaktif. Keamanan IT harus diakreditasi ulang pada waktu yang tepat untuk memastikan bahwa dasar informasi keamanan perusahaan yang telah disetujui itu tetap terjaga. Fungsi *logging* dan pengawasan akan memungkinkan pencegahan dini dan/atau deteksi dan pelaporan tepat waktu akan kegiatan yang tidak biasa dan/atau abnormal yang mungkin perlu ditangani. Hasil audit adalah *software Testing* dan *monitoring* dari pihak IT selalu dilakukan terkait keamanan data dan proses bisnis ini terbukti dari adanya *maintenance* rutin oleh pihak IT yang dilakukan setiap bulan setidaknya 2x. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.6 DS5.6 Security Incident Definition

Mendefinisikan dan menkomunikasikan karakteristik insiden keamanan yang potensial dengan jelas sehingga mereka dapat diklasifikasikan dan diobati oleh peristiwa dengan benar dan proses manajemen masalah. Hasil audit adalah setiap insiden atau kejadian baik di setiap cabang manapun akan di kaji ulang di cabang lain dan menjadi pelajaran guna mencegah hal tersebut terulang kembali. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.7 DS5.7 Protection of Security Technology

Membuat teknologi yang berhubungan dengan keamanan yang tahan terhadap gangguan. Hasil audit adalah keamanan dari sistem aplikasi yang digunakan oleh BCA sudah baik seperti membatasi akses-akses setiap karyawan dan aplikasi keamanan yang terjamin. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.8 DS5.8 Cryptographic Key Management

Menentukan bahwa kebijakan dan prosedur di tempat untuk mengatur generasi, perubahan, pencabutan, perusakan, distribusi, sertifikasi, penyimpanan, masuk, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan terhadap kunci modifikasi dan pengungkapan

yang tidak sah. Hasil audit adalah setiap kewenangan untuk mengakses data-data tertentu terbagi mulai dari pimpinan cabang yang bisa mengakses lebih luas hingga front liner dengan akses paling kecil. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.9 DS5.9 Malicious Software Prevention, Detection and Correction

Memasukan tindakan *preventif*, detektif dan korektif pada bagian (terutama patch keamanan dan pengendalian virus yang berkembang) di seluruh organisasi untuk melindungi sistem informasi dan teknologi dari *malware* (misalnya, *virus, worm, spyware, spam*). Hasil audit adalah pencegahan serangan terhadap *software* selalu diantisipasi dengan monitoring rutin dan *maintenance* rutin dari pihak IT BCA sehingga aplikasi yang mengalami gangguan akan langsung ditindak lanjuti. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.10 DS5.10 Network Security

Gunakan teknik keamanan dan prosedur manajemen terkait (misalnya, *firewall*, peralatan keamanan, segmentasi jaringan, deteksi intrusi) untuk mengotorisasi akses dan kontrol arus informasi dari dan ke jaringan. Hasil audit adalah keamanan dalam *surfing browser* juga dibatasi aksesnya guna menghindari hal-hal yang tidak diinginkan, oleh karena itu halaman web yang bisa dibuka hanya halaman web tertentu saja. Nilai *maturity level* 3, yaitu *Defined Process*.

#### 4.5.11 DS5.11 Exchange of Sensitive Data

Pertukaran data transaksi sensitif hanya melalui jalur dipercaya atau menengah dengan kontrol untuk memberikan keaslian konten, bukti pengiriman, bukti penerimaan dan tidak ada penolakan.

TABEL V

HASIL MATURITY DS5 ENSURE SYSTEMS SECURITY

DS1	Description DS4	Maturity Level
DS5.1	Management of IT Security	3
DS5.2	IT Security Plan	3
DS5.3	Identity Management	3
DS5.4	User Account Management	3
DS5.5	Security Testing, Surveillance and Monitoring	3
DS5.6	Security Incident Definition	3
DS5.7	Protection of Security Technology	3
DS5.8	Cryptographic Key Management	3
DS5.9	Malicious Software Prevention, Detection and Correction	3
DS5.10	Network Security	3
DS5.11	Exchange of Sensitive Data	3
DS5	Rata-rata	3

Hasil audit adalah setiap pertukaran atau transaksi yang dilakukan menggunakan aplikasi yang terpercaya walaupun menggunakan aplikasi dari pihak ketiga. Sehingga semua data yang tercatat dan transaksi yang dilakukan dapat

dipastikan keamanannya. Nilai *maturity level* 3, yaitu *Defined Process*.

Dari hasil analisa audit tersebut, diperoleh level kematangan dari setiap proses yang ada dalam tahap DS5 Ensure Systems Security dan proses-prosesnya dapat dilihat pada Tabel V Hasil *Maturity Acquire and Implement*.

#### 4.6 DS10 Manage Problem

Manajemen data yang efektif membutuhkan identifikasi kebutuhan data. Proses manajemen data juga meliputi pembangunan prosedur secara efektif untuk mengelola perpustakaan media, *backup* dan *recovery* dari data, dan pembuangan media yang layak. Manajemen data yang efektif membantu menjamin kualitas, ketepatan waktu dan ketersediaan data bisnis.

##### 4.6.1 DS10.1 Identification and Classification of Problems

Mengimplementasikan proses untuk melaporkan dan mengklasifikasi masalah yang telah diidentifikasi sebagai bagian dari manajemen insiden. Langkah-langkah ini yang terlibat dalam klasifikasi masalah mirip dengan langkah-langkah dalam klasifikasi insiden. Langkah-langkah tersebut adalah menentukan kategori, dampak, urgensi, dan prioritas. Mengelompokkan masalah selayaknya pada grup atau domain terkait (contoh: *hardware*, *software*, *software* pendukung). Kelompok-kelompok ini dapat disesuaikan dengan tanggung jawab organisasi dari pengguna dan basis konsumen dan harus menjadi dasar dari alokasi masalah untuk mendukung staf. Hasil audit adalah setiap identifikasi masalah dan klasifikasi masalah dicatat dan dilaporkan ke KP pada saat dan hari yang sama sehingga penanggulangan masalah akan langsung ditanggapi oleh KP dan diatasi sesingkat mungkin. Nilai *maturity level* 3, yaitu *Defined Process*.

##### 4.6.2 DS10.2 Problem Tracking and Resolution

Memastikan sistem manajemen masalah menyediakan fasilitas audit trail yang cukup yang memudahkan pelacakan, analisa dan menentukan *root cause* dari seluruh masalah yang dilaporkan menyangkut seluruh benda konfigurasi terkait, insiden dan masalah yang belum selesai, *error* yang diduga dan diketahui, pelacakan trend dari masalah. Mengidentifikasi dan menginisiasi solusi yang berkelanjutan ke *root cause*, membuat *change request* lewat proses manajemen perubahan yang telah dibangun. Selama proses resolusi, manajemen masalah harus mendapatkan laporan berkala dari manajemen perubahan dari kemajuan dalam menyelesaikan masalah dan *error*. Manajemen masalah harus memantau dampak berkelanjutan dari masalah dan *error* yang diketahui ke layanan pengguna. Dalam kejadian dimana dampak sangat berbahaya, manajemen masalah harus mengescalasi masalah, mungkin menyertakan manajemen senior untuk meningkatkan prioritas dari laporan atau mengimplementasikan perubahan yang penting sesuai kebutuhan. Memantau kemajuan dari resolusi masalah sesuai SLA. Hasil audit adalah pemantauan masalah dan solusi yang diberikan mengikuti perintah dari KP, pihak manajemen dari KP akan memberikan kebijakan

terkait masalah yang dihadapi dan setiap cabang mengikuti perintah dari KP. Nilai *maturity level* 3, yaitu *Defined Process*.

##### 4.6.3 DS10.3 Problem Closure

Membuat prosedur untuk menyelesaikan laporan masalah yang dijalankan saat konfirmasi dari error telah selesai diselesaikan atau setelah persetujuan dengan pihak bisnis bagaimana jalur alternatif untuk menghadapi masalah. Hasil audit adalah setiap masalah yang dialami oleh pihak BCA hanya diketahui oleh pihak internal saja. Sehingga kerahasiaan informasi tidak tersebar ke publik. Nilai *maturity level* 3, yaitu *Defined Process*.

##### 4.6.4 DS10.4 Integration of Configuration, Incident and Problem Management

Mengintegrasikan proses terkait dari konfigurasi, insiden dan manajemen masalah untuk memastikan manajemen yang efektif dari masalah dan memudahkan perkembangan. Hasil audit adalah pengaturan masalah dan manajemen masalah diatur secara baik dan terorganisir sehingga mengurangi dampak dari masalah tersebut dan mencegahnya terulang kembali. Nilai *maturity level* 3, yaitu *Defined Process*.

Dari hasil analisa audit tersebut, diperoleh level kematangan dari setiap proses yang ada dalam tahap DS10 *Manage Problems* dan proses-prosesnya dapat dilihat pada Tabel VI Hasil *Maturity DS10 Manage Problems*.

TABEL VI

HASIL MATURITY DS10 MANAGE PROBLEMS

DS10	Description DS10	Maturity Level
DS10.1	Identification and Classification of Problems	3
DS10.2	Problem Tracking and Resolution	3
DS10.3	Problem Closure	3
DS10.4	Integration of Configuration, Incident and Problem Management	3
DS10	Rata-rata	3

#### 4.7 ME2 Monitor and Evaluate Internal Control

Membangun program kontrol internal yang efektif untuk IT membutuhkan proses pemantauan yang terdefinisi dengan baik. Proses ini meliputi pemantauan dan pelaporan kontrol pengecualian, kumpulan penilaian dari internal dan pihak ketiga. Keuntungan kunci dari pemantauan kontrol internal adalah untuk menjamin operasi efektif dan efisien dan sesuai dengan peraturan dan hukum yang berlaku.

##### 4.7.1 ME2.1 Monitoring of Internal Control Framework

Terus monitor, benchmark dan meningkatkan IT mengendalikan lingkungan dan kerangka kontrol untuk memenuhi tujuan organisasi. Hasil audit adalah pemantauan dan *monitoring* terhadap *control internal* berjalan dengan baik dengan adanya audit internal dan audit eksternal yang



rutin *memonitoring* setiap cabang. Nilai *maturity level 3*, yaitu *Defined Process*.

4.7.2 ME2.2 *Supervisory Review*

Memantau dan mengevaluasi efisiensi dan efektivitas IT internal kontrol tinjauan manajerial. Hasil audit adalah evaluasi dan kajian setiap masalah yang dihadapi karyawan akan dievaluasi guna mendapatkan solusi dan mencegah masalah tersebut terjadi kembali. Nilai *maturity level 3*, yaitu *Defined Process*.

4.7.3 ME2.3 *Control Exceptions*

Mengidentifikasi kontrol pengecualian, dan menganalisis dan mengidentifikasi penyebab yang mendasarinya *root*. Meningkatkan kontrol pengecualian dan melaporkan tepat kepada *stakeholder*. Institut tindakan korektif yang diperlukan. Hasil audit adalah identifikasi masalah yang dihadapi dilakukan dengan meeting dan mencari solusi dari masalah tersebut. Nilai *maturity level 3*, yaitu *Defined Process*.

4.7.4 ME2.4 *Control Self-assessment*

Mengevaluasi kelengkapan dan efektivitas pengendalian manajemen atas proses IT, kebijakan dan kontrak melalui terus program penilaian diri. Hasil audit adalah pengendalian dokumen dan efektifitas kebijakan dilakukan oleh pihak KP sehingga cabang hanya menerapkan kebijakan yang diberikan. Nilai *maturity level 3*, yaitu *Defined Process*.

4.7.5 ME2.5 *Assurance of Internal Control*

Memperoleh, sesuai kebutuhan, kepastian lebih lanjut akan kelengkapan dan efektivitas pengendalian internal melalui pihak ketiga tinjauan. Hasil audit adalah BCA memiliki audit eksternal yang melakukan audit pada setiap cabang untuk mengetahui seberapa efektif proses bisnis yang berjalan disana dan memberikan ulasan dan evaluasi dari hasil temuan audit eksternal. Nilai *maturity level 3*, yaitu *Defined Process*.

4.7.6 ME2.6 *Internal Control at Third Parties*

Menilai status kontrol internal penyedia layanan eksternal. Pastikan penyedia layanan eksternal mematuhi hukum dan peraturan persyaratan dan kewajiban kontrak. Hasil audit adalah BCA memiliki pihak ketiga yang siap untuk memantau setiap proses bisnis yang berjalan disetiap cabang. Nilai *maturity level 3*, yaitu *Defined Process*.

4.7.7 ME2.7 *Remedial Actions*

Mengidentifikasi, memulai, melacak dan menerapkan tindakan perbaikan yang timbul dari penilaian pengendalian dan pelaporan. Hasil audit adalah setiap hasil audit dan temuan-temuan akan diberikan solusi dan perbaikan agar proses bisnis pada cabang tersebut akan semakin lebih baik untuk kedepannya. Nilai *maturity level 3*, yaitu *Defined Process*.

Dari hasil analisa audit tersebut, diperoleh level kematangan dari setiap proses yang ada dalam tahap ME2 *Monitor and Evaluate Internal Control* dan proses-prosesnya dapat dilihat pada Tabel VII Hasil *Maturity ME2 Monitor And Evaluate Internal Control*.

TABEL VII

HASIL MATURITY ME2 MONITOR AND EVALUATE INTERNAL CONTROL

ME2	Description ME2	Maturity Level
ME2.1	Monitoring of Internal Control Framework	3
ME2.2	Supervisory Review	3
ME2.3	Control Exceptions	3
ME2.4	Control Self-assessment	3
ME2.5	Assurance of Internal Control	3
ME2.6	Internal Control at Third Parties	3
ME2.7	Remedial Actions	3
ME2	Rata-rata	3

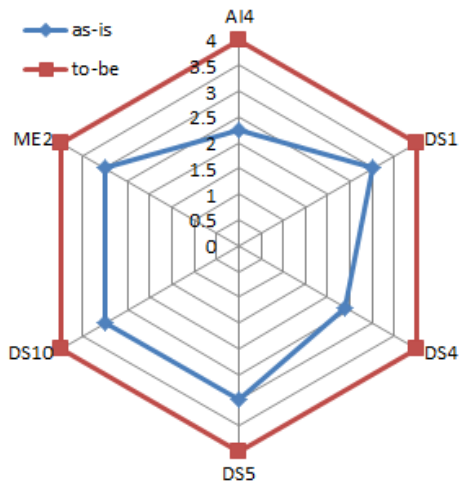
Dari hasil audit system informasi absensi tersebut diatas, maka sub domain rata-rata hasil perhitungan *maturity level*, diperlihatkan pada table VIII.

TABEL VIII

RATA-RATA HASIL PERHITUNGAN MATURITY LEVEL

Proses TI	Descriptions	Maturity Level
AI4	Enable Operation and Use	2.25
DS1	Define and Manage Service Levels	3
DS4	Ensure Continuous Service	2.4
DS5	Ensure Systems Security	3
DS10	Manage Problems	3
ME2	Monitor and Evaluate Internal Control	3

Keseluruhan maturity yang diinginkan (*to-be*) adalah pada level 4 yaitu *Managed and measurable* dibandingkan dengan *maturity* saat ini (*as-is*). Dengan data yang ada pada tabel VIII rata-rata perhitungan *maturity level*, maka dibuat gambarnya menggunakan diagram *spider*, diperlihatkan pada gambar 3.



Gambar 3. Diagram Spider Maturity Level as-is vs to-be

## V. KESIMPULAN DAN SARAN

### 5.1 Simpulan

Simpulan yang dapat diambil dari penelitian yang telah dilakukan adalah sebagai berikut:

- Audit Sistem Informasi Absensi Pada PT. Bank Central Asia Tbk Menggunakan Cobit 4.1 sudah dilakukan walaupun masih belum berjalan secara optimal karena belum mencapai pada tingkat kematangan yang diharapkan.
- Tingkat kematangan (*maturity level*) yang ada pada setiap proses TI yang terdapat dalam *sub-domain* AI4 dan DS4 masih dibawah 3 yaitu 2.25 dan 2.4 pada level *Repeatable but Intuitive &* untuk sub domain DS1, DS5, DS10 dan ME2 sudah pada level 3 yaitu *Defined Process*.
- Proses tata kelola sistem absensi telah memiliki pola yang berulang kali dilakukan. Di dalam melakukan manajemen aktivitas terkait dengan tata kelola teknologi informasi, namun keberadaannya sudah terdefinisi secara baik dan formal sehingga masih perlu perlu ditingkatkan lagi.

### 5.2 Saran

- Evaluasi tata kelola TI ini disarankan dapat dilakukan secara rutin setiap periode waktu tertentu (secara periodik), agar tingkat kematangan yang diinginkan dapat dicapai.

- Kegiatan evaluasi tata kelola TI sudah dilakukan oleh unit khusus dalam organisasi yaitu *internal audit* yang dapat dilakukan secara periodik dan akan di audit oleh *external auditor*.
- Pelatihan yang berkelanjutan tentang *COBIT 4.1* atau *5* bagi karyawan yang terlibat dalam kegiatan evaluasi tata kelola TI, beberapa karyawan sudah di *certified* oleh *ISACA*, dengan *CISA (Certified Information System Auditor)*

## DAFTAR PUSTAKA

- [1] G. Hardy, "The Role of the IT Auditor in IT Governance," *ISACA Jurnal* 1, 2009.
- [2] H. Setiawan dan K. Mustofa, "Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia," *IPTEK-KOM*, Vol. 15 No. 1 Juni, pp.1-15, ISSN 1410 – 3346, 2013.
- [3] D. Fitrihanah, Y. G. Sucahyo, "Audit Sistem Informasi/Teknologi Informasi dengan Kerangka Kerja COBIT untuk Evaluasi Manajemen Teknologi Informasi di Universitas XYZ," *Jurnal Sistem Informasi MTI-UI*, Volume 4, Nomor 1, ISBN 1412-8896.
- [4] Maniah, S. Lestari, 2008, "Model Audit Sistem Informasi Akademik Proses Penyampaian dan Dukungan Pelayanan (Studi Kasus : Universitas Widyatama)", Konferensi dan Temu Nasional Teknologi Informasi dan Komunikasi Untuk Indonesia", Jakarta, 2008.
- [5] J. F. Andry, *Audit Tata Kelola TI Di Perusahaan (Studi Kasus XYZ Cargo)*, Prosiding Seminar Nasional Teknologi Informasi (SNTI) XIII – 2016, 29 Oktober, 2016.
- [6] E. B. Setiawan, B. Kurniawan, "Perancangan Sistem Absensi Kehadiran Perkuliahan dengan Menggunakan Radio Frequency Identification (RFID)," *Jurnal CoreIT*, Vol.1, No.2, Desember, ISSN: 2460-738X, 2015.
- [7] S. Gondodiyoto, "Audit Sistem Informasi Pendekatan COBIT," Jakarta: Mitra Wacana Media, 2007.
- [8] D. T. Yulianti, M. C. Patria, "Audit Sistem Informasi Sumber Daya Manusia Pada PT X Menggunakan Cobit Framework 4.1," *Jurnal Sistem Informasi*, Vol 6, No 1, Maret, pp. 15 – 33, 2011.
- [9] J. F. Andry, "Audit Tata Kelola TI Menggunakan Kerangka Kerja COBIT Pada Domain DS dan ME Di Perusahaan Kreavi Informatika Solusindo," Seminar Nasional Teknologi Informasi dan Komunikasi 2016 (SENTIKA 2016) ISSN: 2089-9815, Yogyakarta, 18-19 Maret 2016.
- [10] H. Surbakti, "Managing Control Object For IT (COBIT) Sebagai Standar Framework Pada Proses Pengelolaan IT-Governance Dan Audit Sistem Informasi," *Jurnal Teknologi Informasi* ISSN : 1907-2430, Vol . VII Nomor 19 Maret, 2012.
- [11] J. F. Andry, "Audit Sistem Informasi Sumber Daya Manusia Pada Training Center Di Jakarta Menggunakan Framework Cobit 4.1," *Jurnal Ilmiah FIFO*, vol. VIII, no.1, pp. 28-34, 2016.
- [12] IT Governance Institute, "COBIT 4.1 Framework, Control Objective, Management Guidelines, Maturity Models," Rolling Meadows, IL 60008 USA: ITGI, 2007.
- [13] E. Maria, E. Haryani, "Audit Model Development Of Academic Information System: Case Study On Academic Information System Of Satya Wacana," *Journal of Arts, Science & Commerce*, Vol.– II, Issue –2, E-ISSN 2229-4686, ISSN 2231-4172, 2011.