Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, Vol. 4, No. 2, Agustus 2018, Hal. 163-171
e-ISSN 2502-8995, p-ISSN 2460-8181

AUDIT SISTEM INFORMASI ABSENSI PADA PT SINAR PRATAMA AGUNG MENGGUNAKAN KERANGKA KERJA COBIT 4.1

[1]Michelle Angelia, [2]Kristanto, [3]Yohanes Setevannus, [4]Johanes Fernandes Andry
[1,2,3,4]Program Studi Sistem Informasi, Fakultas Teknik dan Desain, Universitas Bunda Mulia
Jl. Lodan Raya No. 2 Ancol, Jakarta Utara 14430.
Email: [1]michelleangelia198@gmail.com, [2]ktanto13@gmail.com,
[3]setevannusy@gmail.com, [4]jandry@bundamulia.ac.id.

ABSTRAK

PT. Sinar Pratama Agung merupakan perusahaan yang bergerak di bidang *garment* dan sepatu yang menerapkan suatu sistem informasi pada aspek kerjanya di perusahaan untuk meningkatkan kegiatan operasional kerja yaitu menggunakan alat yang terkomputerisasi yaitu *fingerprint* untuk mencatat daftar kehadiran setiap karyawan di perusahaan. Sistem yang digunakan harus mampu mengelola, menyampaikan dan menjaga keamanan informasi dengan baik. Maka, perlu dilakukan audit bertujuan untuk mengevaluasi tata kelola sistem informasi yang berjalan. Penelitian dilakukan mengikuti standar Kerangka Kerja COBIT 4.1 untuk tata kelola IT. Penelitian berfokus pada sub-domain AI4, DS1, DS4, DS5, DS10, dan ME2. Keenam sub-domain tersebut penting dibahas karena berkaitan dengan penilaian dari karyawan, perlengkapan, keamanan fisik, regulasi, dan sebagainya. Untuk pengumpulan data, penelitian ini menggunakan teknik observasi, wawancara dan kepustakaan. Teknik analisis data yang digunakan adalah *Maturity level*. Dari hasil penelitian, ditemukan bahwa DS5 berada pada level 3,09; DS4 dan DS10 berada pada level 3 (*Defined Process*); DS1 berada pada level 2,83; AI4 berada pada level 2,75 (*Repeatable but Intuitive*); sedangkan ME2 berada pada level 1,71 (*Initial/ad Hoc*). Nilai tertinggi berada pada DS5 (*Ensure Systems Security*) dengan nilai 3,09 dan nilai terendah pada ME2 (*Monitor and Evaluate Internal Control*) dengan nilai 1,71.
Kata Kunci: absensi, COBIT 4.1, PT Sinar Pratama Agung.

A. PENDAHULUAN

Dengan perkembangan teknologi yang semakin maju menuntun dunia usaha untuk bersaing secara kompetitif yang secara efektif dan efisien [1]. PT sinar pratama agung adalah salah satu perusahaan yang bergerak di bidang *garment* dan sepatu telah menempatkan teknologi dalam mencapai tujuannya untuk meningkatkan kegiatan operasional kerja sesuai dengan sasaran visi misi dan tujuan perusahaannya [2]. Dengan adanya teknologi, perusahaan ini menerapkan sistem informasi untuk mendukung proses bisnisnya seperti penggunaan sistem informasi absensi pada perusahan. Perlu melakukan evaluasi terhadap sistem dan prosesnya yang bertujuan memastikan sistem informasi absensi yang di gunakan pada perusahaan memberi kemudahan dalam proses bisnis perusahaan serta meningkatkan tata kelola IT yang baik sesuai dengan visi misi perusahaan. Dapat dilakukan audit yang dapat bertanggung jawab terhadap penilaian tata kelola TI yang efisiensi sesuai dengan prosedur yang diterapkan pada perusahaan [3][4][5]. Audit SI/TI dalam kerangka kerja COBIT atau *IT Assurance* adalah salah satu audit yang dapat memberikan masukan terhadap perbaikan pengelolaan sistem di masa yang akan datang [6][7]. Audit Sistem Informasi berdasarkan standar *framework* COBIT 4.1. *Control Objective for Information and Related Technology* (COBIT) adalah sebuah kerangka kerja dan *supporting toolset* yang dapat membantu manajer pada perusahaan menjembatani jarak antara tujuan keperluan perusahaan terhadap pengendalian, resiko bisnis yang di hadapi dan disetiap permasalahan teknik, serta mengomunikasikan level pengendalian kepada *stakeholder* [8][9]. COBIT terdapat 4 domain utama [10]: *Planning and Organization* (PO), *Acquisition and Implementation* (AI), *Delivery and Support* (DS) dan *Monitoring and Evaluation* (ME) yang memiliki proses (*sub-domain*). Jumlah proses yang dari setiap *sub-domain* adalah 34 proses.

Oleh karena itu, penelitian ini menggunakan beberapa domain yaitu AI, DS, dan ME. Khususnya pada sub-sub domainnya seperti AI4, DS1, DS4, DS5, DS10, dan ME2. Penelitian ini memilih *sub domain* ini karena berkaitan dengan hal yang akan diberikan penilaian, yaitu mulai dari karyawan, perlengkapan, keamanan fisik, dan regulasi yang ada di perusahaan, serta menemukan gap atau kesenjangan yang menetapkan tingkat kematangan pada penerapan sistem informasi absensi dan mencari tahu keselarasan proses kerjanya terhadap prosedur absensi di perusahaan [11].

B. LANDASAN TEORI

B.1. Audit Sistem Informasi

Proses mengumpulkan dan evaluasi suatu bukti menentukan apakah sistem aplikasi

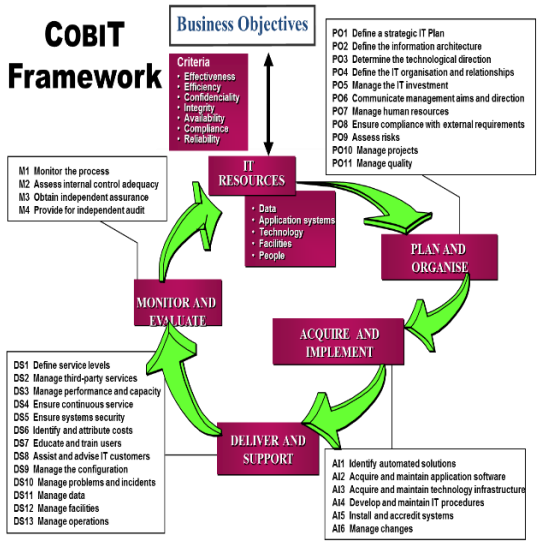
terkomputerisasi menetapkan serta menerapkan sistemnya dalam pengendalian *intern* secara memadai, terjamin integritas datanya dan penyelenggaraan sistem informasi berbasis *computer* secara efektif [12][13].

B.2. Absensi

Sistem absensi merupakan sistem yang mencatat daftar kehadiran serta identitas setiap karyawan atau anggota instansi dalam sebuah perusahaan [14]. *Fingerprint* adalah alat yang digunakan untuk memudahkan sebuah proses kegiatan absensi di perusahaan. Selain itu juga berfungsi untuk menghindari manipulasi data absensi yang sangat mudah dilakukan jika proses kegiatan absensi secara manual.

B.3. COBIT 4.1

COBIT merupakan sebuah kerangka kerja dan *supporting toolset* yang membantu manajer untuk pengendalian, permasalahan teknik dan risiko bisnis serta komunikasi kepada *stakeholder* mengenai level pengendalian [15][16]. Merupakan metode kerangka dasar dalam menciptakan TI sesuai keinginan organisasi [17]. Metode ini merupakan *framework* yang terdiri dari domain serta proses mengatur aktivitas dan *logical structure* [18]. COBIT *framework* dapat dilihat pada Gambar 1.



Gambar 1. COBIT *framework* [19][20]

B.4. *Maturity Level*

Dalam pengukuran tingkat kematangan untuk tingkat manajemen dan para manajer harus diatur sebab untuk mengetahui pengelolaan dan proses sebuah TI di organisasi agar dapat diketahui pada tingkatan mana pengelolaannya [19][20].

Adapun *maturity model* yang digunakan adalah:

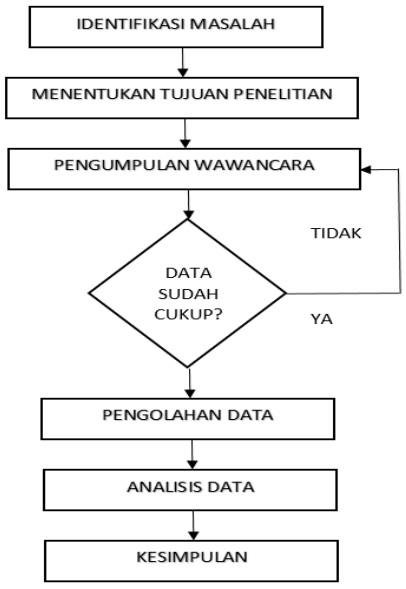
(1) 0 - *Non-existent* – Tidak terlihat sama sekali adanya proses.
(2) 1 - *Initial/Ad Hoc* - Ada bukti perusahaan menyadari bahwa adanya masalah dan harus dikaji tetapi belum adanya standarisasi.
(3) 2 - *Repeatable but Intuitive* - Proses dikembangkan pada tahap dimana prosedur yang mirip diikuti oleh bermacam-macam orang yang melaksanakan tugas.
(4) 3 - *Defined Process* - Prosedur telah terstandarisasi dan terdokumentasi, serta komunikasi melalui *training*.
(5) 4 - *Managed and measurable* - Manajemen memantau dan mengukur kesesuaian prosedur serta mengambil tindakan dimana proses terlihat tidak berjalan efektif.
(6) 5 - *Optimised* - Proses dirancang sampai tingkat pelaksanaan yang baik, berdasarkan hasil dari pengembangan berkelanjutan dan *maturity modelling* dengan perusahaan lain.

C. METODOLOGI PENELITIAN

Pada penelitian ini, lingkup penelitian dibatasi pada audit sistem informasi absensi pada PT. Sinar Pratama Agung dan Identifikasi Proses Sistem Informasi Absensi.

Tabel 1. Cakupan IT Domain yang di audit

Sub Domain	Descriptions
AI4	*Enable Operations 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

Tahap ini, ditetapkan proses teknologi informasi yang sesuai dengan standar COBIT yang diolah sesuai dengan studi kasus. Cakupan IT

domain yang diaudit pada sistem informasi absensi diperlihatkan pada Tabel 1. Metodologi penelitian yang dilakukan dan tahapan dalam memperoleh data dari sumber, mulai dari survei awal dan wawancara ditujukan pada Gambar 2.

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

(1) *Planning* (Perencanaan)

Planning merupakan tahap awal dalam prosedur penelitian yang dilakukan. Karena tahap ini ditentukan 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. Tahap perancangan meliputi beberapa aktifitas utama yakni penetapan ruang lingkup dan tujuan audit, pengorganisasian tim audit, pemahaman mengenai operasi bisnis klien, pengkajian ulang hasil audit sebelumnya, serta 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 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)

Dengan adanya pelaporan pada suatu masalah maka akan dapat terlihat jelas dimanakah letak kesalahannya. Setelah itu peneliti akan menganalisa dan menyimpulkan hasil. Peneliti memberi laporan hasil audit dalam hal merekomendasi tindak perbaikan dan wewenang perbaikan kepada pihak *management* objek penelitian, dapatkah penelitian ini akan diterapkan secara langsung atau hanya menjadi acuan untuk perbaikan dimasa yang akan datang.

(4) *Follow-Up* (Tindak Lanjut)

Dengan adanya pelaporan pada suatu masalah maka akan dapat terlihat jelas dimanakah letak kesalahannya. Setelah itu peneliti akan menganalisa dan menyimpulkan hasil. Peneliti memberi laporan hasil audit dalam hal merekomendasi tindak perbaikan dan wewenang perbaikan kepada pihak *management* objek penelitian, dapatkah penelitian ini akan diterapkan secara langsung atau hanya menjadi acuan untuk perbaikan dimasa yang akan datang.

D. Proses Sistem Informasi Absensi

Proses berjalannya Sistem Informasi Absensi di PT Sinar Pratama Agung menggunakan *fingerprint*:

(1) tahapan pertama adalah dimana para karyawan mulai datang ke perusahaan;
(2) tahapan kedua adalah dimana para karyawan mulai melakukan kegiatan absensi dengan menempelkan sidik jarinya di *fingerprint* yang dimiliki oleh perusahaan;
(3) tahapam kedua, terdapat kondisi dimana bila sidik jari dari karyawan tersebut sedang dibaca oleh *fingerprint*, apakah sidik tersebut dapat terdeteksi oleh *fingerprint*? Jika ya, maka sidik jari karyawan tersebut berhasil terdata pada absensi tesebut. Sedangkan jika tidak, maka si karyawan harus menempelkan kembali sidik jarinya agar dapat terdeteksi pada *fingerprint*;
(4) tahapan keempat, setelah sidik jari tersebut terdeteksi maka data absensi karyawan tersebut langsung terinput ke personalia;
(5) Tahapan kelima, setelah data absensi karyawan terinput ke personalia, data tersebut terinput ke dalam *database* dan selesai.

E. HASIL AUDIT DAN PEMBAHASAN

Pada bagian ini, membahas sistem informasi absensi dengan pendekatan COBIT *framework* pada PT. Sinar Pratama Agung. Disini menganalisa lingkungan yang terjadi dalam IT departemen, mulai dari karyawan, perlengkapan, keamanan fisik dan regulasi.

E.1. AI4 *Enable Operation and Use*

Proses memerlukan dokumentasi dan manual standar yang digunakan *users* dan IT, serta pelatihan diadakan menjamin aplikasi dan infrastruktur yang digunakan serta dijalankan dengan tepat [21].

E.1.1. AI4.1 *Planning for Operational Solutions*

Perencanaan solusi operasional dengan mengembangkan rencana, mengidentifikasi dan mendokumentasikan, aspek teknis operasional dan penggunaan agar semua orang yang mengoperasikan, menggunakan dan mempertahankan solusi otomatis dapat melaksanakan tanggung jawabnya.

E.1.2. AI4.2 *Knowledge Transfer to Business Management Transfer*

Pengetahuan manajemen bisnis dengan mentransfer pengetahuan untuk manajemen bisnis memungkinkan individu mengambil kepemilikan sistem dan data, tanggung jawab penyediaan layanan dan kualitas, pengendalian internal, dan aplikasi administrasi.

E.1.3. AI4.3 *Knowledge Transfer to End Users Transfer*

Pengetahuan pengguna akhir dengan mentransfer pengetahuan serta keterampilan memungkinkan pengguna akhir secara efektif dan efisien menggunakan sistem untuk mendukung proses bisnis. Di tahapan ini prosedur telah terstandarisasi dari pengetahuan dan keterampilan karyawan sudah baik.

E.1.4. AI4.4 *Knowledge Transfer to Operations and Support Staff Transfer*

Pengetahuan operasional dan staff pendukung transfer pengetahuan dan keterampilan memungkinkan operasi serta staf pendukung teknis secara efektif dan efisien memberi dukungan serta memelihara sistem dan infrastruktur yang terkait.

Dari hasil analisa audit AI4 *Enable operation and use*, diperoleh level kematangan dari setiap proses yang ada dalam tahap dan proses-prosesnya dapat dilihat pada Tabel 2 Hasil *Maturity* AI4 *Enable Operation and Use.*

Tabel 2. Hasil *Maturity* AI4 *Enable Operation and Use*

	AI4 Enable operation and use	***Maturity Level***
AI4.1	*Planning for Operational Solutions*	3
AI4.2	*Knowledge Transfer to Business Management*	2
AI4.3	*Knowledge Transfer to End Users*	3
AI4.4	*Knowledge Transfer to Operations and Support Staff*	3
AI4	**Rata-rata**	**2,75**

E.2. DS1 *Define and Manage Service Levels*

Komunikasi efektif antara manajemen IT dan pelanggan bisnis mengenai jasa yang dibutuhkan, disanggupi oleh definisi serta persetujuan layanan IT dan tingkat layanan yang didokumentasikan. Proses ini mencakupi pemantauan dan pelaporan secara berkala pada *stakeholder* untuk pemenuhan tingkat layanan. Proses memungkinkan keselarasan antara layanan IT dan persyaratan bisnis terkait [21].

E.2.1. DS1.1 *Service Level Management Framework*

Tetapkan sebuah kerangka yang menyediakan tingkat layanan manajemen proses antara pelanggan dan penyedia layanan. Kerangka menjaga keselarasan antara kebutuhan bisnis dan prioritas, serta menfasilitasi pemahaman yang sama antara pelanggan dan penyedia. Kerangka mencakup proses untuk menciptakan kebutuhan layanan, definisi layanan, SLA, OLA dan sumber pendanaan.

E.2.2. DS1.2 *Definition of Services*

Definisi karakteristik pelayanan dan kebutuhan bisnis, serta memastikan terorganisasi dan disimpan secara terpusat melalui implementasi pendekatan portofolio katalog layanan.

E.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.

E.2.4. DS1.4 *Operating Level Agreements*

Menetapkan OLA yang menjelaskan bagaimana layanan yang akan disampaikan secara teknis untuk mendukung SLA secara optimal.

E.2.5. DS1.5 *Monitoring and Reporting of Service Level Achievements*

Memantau kriteria kinerja tingkat layanan tertentu serta melaporkan pencapaian tingkat layanan dalam bentuk yang lebih berarti bagi *stakeholder*. Hasil *statistic* pemantauan tersebut dianalisis untuk mengetahui kelebihan dan kekurangannya sehingga mampu meningkatkan layanan.

E.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 memastikan efektif dan *up to date* serta perubahan dalam persyaratan telah diperhitungkan. Dari hasil analisa audit DS1 *Define and manage service levels*, diperoleh level kematangan dari setiap proses yang ada dalam tahap dan proses-prosesnya dapat dilihat pada Tabel 3.

Tabel 3. Hasil *Maturity* DS1 *Define And Manage S*

	DS1 Define And Manage Service Levels	***Maturity Level***
DS1.1	*Service Level Management Framework*	3
DS1.2	*Definition of Services*	2
DS1.3	*Service Level Agreements*	3
DS1.4	*Operating Level Agreements*	3
DS1.5	*Monitoring and Reporting of Service Level Achievements*	3
DS1.6	*Review of Service Level Agreements and Contracts*	3
DS1	**Rata-rata**	**2,83**

E.3. DS4 *Ensure Continuous Service*

Kebutuhan menyediakan layanan IT yang berkesinambungan membutuhkan pengembangan, mempertahankan dan pengujian rencana kontinuitas IT, memanfaatkan penyimpanan *offsite backup* dan memberikan pelatihan rencana kelangsungan secara periodik [21].

E.3.1. DS4.1 *IT Continuity Framework*

Kerangka kerja membahas struktur organisasi manajemen kontinuitas, meliputi peran, tugas dan tanggung jawab penyedia layanan internal dan eksternal, manajemen dan pelanggan, proses perencanaan yang menciptakan aturan dan struktur dokumen, pengujian dan melaksanakan pemulihan bencana IT dan rencana kontinjensi.

E.3.2. DS4.2 *IT Continuity Plans*

Rencana didasarkan pada pemahaman risiko potensi dampak bisnis dan membahas persyaratan untuk ketahanan, pengolahan alternatif dan kemampuan pemulihan dari semua layanan IT kritis.

E.3.3. DS4.3 *Critical IT Resources*

Fokus perhatian pada item yang dispesifikasi sebagai yang paling kritis dalam rencana kelangsungan IT untuk membangun ketahanan dan menetapkan prioritas dalam situasi pemulihan.

E.3.4. DS4.4 *Maintenance of the IT Continuity Plan*

Mendorong manajemen IT mendefinisikan dan mengeksekusi prosedur kontrol perubahan untuk memastikan rencana kontinuitas IT terus berkembang dan mencerminkan kebutuhan bisnis yang sebenarnya secara terus-menerus.

E.3.5. DS4.5 *Testing of the IT Continuity Plan*

Menguji rencana kontinuitas IT secara teratur memastikan sistem IT dapat pulih secara efektif, menangani kekurangan dan menjaga rencana tetap relevan.

E.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.

E.3.7. DS4.7 *Distribution of the IT Continuity Plan*

Menentukan adanya pendefinisian dan pengelolaan strategi distribusi memastikan rencana didistribusi dengan benar dan aman serta tersedia bagi pihak berwenang yang berkepentingan, kapan dan dimana diperlukan.

E.3.8. DS4.8 *IT Services Recovery and Resumption*

Aktivasi dari situs cadangan, inisiasi proses alternatif, komunikasi pelanggan dan *stakeholder*, dan prosedur penerusan.

E.3.9. DS4.9 *Offsite Backup Storage*

Penyimpanan *offsite* semua backup media kritis, dokumentasi dan sumber daya IT lainnya diperlukan untuk rencana kontinuitas pemulihan dan bisnis IT.

E.3.10. DS4.10 *Post-resumption Review*

Mentukan apakah manajemen IT menetapkan prosedur untuk menilai kecukupan dari rencana dalam penerusan keberhasilan fungsi IT setelah bencana, dan memperbarui rencana yang sesuai. Dari hasil analisa audit DS4 *Ensure continuous service*, diperoleh level kematangan dari setiap proses yang ada dalam tahap dan proses-prosesnya dapat dilihat pada Tabel 4 Hasil Maturity DS4 *Ensure continuous service*.

Tabel 4. Hasil *Maturity* DS4 *Ensure Continuous Service*

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

E.4. DS5 *Ensure Systems Security*

Proses meliputi membangun dan mempertahankan peran dan tanggung jawab keamanan IT, kebijakan, standar, dan prosedur. Manajemen keamanan termasuk melakukan pemantauan keamanan dan pengujian berkala serta mengimplementasikan tindakan perbaikan untuk mengidentifikasi kelemahan atau insiden keamanan. Manajemen keamanan efektif melindungi semua aset IT meminimalkan dampak bisnis dari kerentanan dan insiden keamanan [21].

E.4.1. DS5.1 *Management of IT Security*

Mengelola keamanan TI pada tingkat tertinggi organisasi yang tepat, sehingga manajemen tindakan keamanan sejalan dengan kebutuhan bisnis.

E.4.2. 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.

E.4.3. DS5.3 *Identity Management*

Memastikan semua pengguna (internal, eksternal dan sementara) dan aktivitas di sistem IT (aplikasi bisnis, lingkungan IT, operasi sistem, pengembangan dan pemeliharaan) dapat diidentifikasi secara unik. Konfirmasi user memiliki hak akses ke sistem dan data yang sesuai dengan kebutuhan bisnis didefinisikan dan didokumentasikan dan persyaratan kerja yang melekat pada identitas user.

E.4.4. 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*.

E.4.5. DS5.5 *Security Testing, Surveillance and Monitoring*

Menguji dan memantau pelaksanaan keamanan IT dengan cara proaktif. Keamanan IT diakreditas ulang pada waktu yang tepat memastikan dasar informasi keamanan perusahaan yang disetujui tetap terjaga. Fungsi *logging* dan pengawasan memungkinkan pencegahan dini dan/atau deteksi dan pelaporan tepat waktu akan kegiatan yang tidak biasa dan/atau abnormal yang mungkin perlu ditangani.

E.4.6. DS5.6 *Security Incident Definition*

Mendefinisikan dan mengkomunikasikan karakteristik insiden keamanan yang potensial dengan jelas sehingga mereka dapat diklasifikasikan dan diobati oleh peristiwa dengan benar dan proses manajemen masalah.

E.4.7. DS5.7 *Protection of Security Technology*

Membuat teknologi yang berhubungan dengan keamanan yang tahan terhadap gangguan.

E.4.8. DS5.8 *Cryptographic Key Management*

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

E.4.9. 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*).

E.4.10. DS5.10 *Network Security*

Menggunakan 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.

E.4.11. DS5.11 *Exchange of Sensitive Data*

Pertukaran data transaksi sensitif melalui jalur dipercaya atau menengah dengan kontrol memberikan keaslian konten, bukti pengiriman, bukti penerimaan dan tidak ada penolakan. Dari hasil analisa audit DS5 *Ensure Systems Security*, diperoleh level kematangan dari setiap proses yang ada dalam tahap dan proses-prosesnya dapat dilihat pada Tabel 5.

Tabel 5. Hasil *Maturity* DS5 *Ensure Systems Security*

DS5 Ensure Systems Security		***Maturity Level***
DS5.1	*Management of IT Security*	3
DS5.2	*IT Security Plan*	3
DS5.3	*Identify Management*	3
DS5.4	*User Account Management*	3
DS5.5	*Security Testing, Surveillance and Monitoring*	2
DS5.6	*Security Incident Definition*	4
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*	4
DS5.11	*Exchange of Sensitive Data*	3
DS5	**Rata-rata**	**3,09**

E.5. DS10 *Manage Problem*

Manajemen data efektif membutuhkan identifikasi kebutuhan data. Proses manajemen data meliputi pembangungan prosedur secara efektif mengelola perpustakaan media, backup dan *recovery* dari data, dan pembuangan media yang layak. Manajemen data efektif membantu menjamin kualitas, ketepatan waktu dan ketersediaan data bisnis [21].

E.5.1. DS10.1 *Identification and Classification of Problems*

Mengimplementasi proses untuk melaporkan dan mengklasifikasi masalah yang diidentifikasikan sebagai bagian manajemen insiden. Langkah-langkah ini terlibat dalam klasifikasi masalah mirip dengan langkah-langkah dalam klasifikasi insiden. Langkah-langkah tersebut yakni menentukan kategori, dampak, urgensi, dan prioritas. Mengelompokkan masalah selayaknya pada grup atau domain terkait (contoh: *hardware*, *software*, *software* pendukung). Kelompok-kelompok ini disesuaikan dengan tanggung jawab organisasi dari pengguna dan basis konsumen dan harus menjadi dasar dari alokasi masalah untuk mendukung staf.

E.5.2. DS10.2 *Problem Tracking and Resolution*

Memastikan sistem manajemen masalah menyediakan fasilitas audit *trail* yang cukup 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 mengeskalasi masalah, mungkin menyertakan manajemen senior untuk meningkatkan prioritas dari laporan atau mengimplementasikan perubahan yang penting sesuai kebutuhan. Memantau kemajuan dari resolusi masalah sesuai SLA.

E.5.3. DS10.3 *Problem Closure*

Membuat prosedur untuk menyelesaikan laporan masalah yang dijalankan saat konfirmasi dari *error* diselesaikan atau setelah persetujuan dengan pihak bisnis bagaimana jalur alternatif untuk menghadapi masalah.

E.5.4. DS10.4 *Integration of Configuration, Incident and Problem Management*

Mengintegrasikan proses terkait konfigurasi, insiden dan manajemen masalah memastikan manajemen efektif dari masalah dan memudahkan perkembangan. Dari hasil analisa audit DS10 *Manage Problems*, diperoleh level kematangan dari setiap proses yang ada dalam tahap dan proses-prosesnya dapat dilihat pada Tabel 6 Hasil *Maturity* DS10 *Manage Problems*.

Tabel 6. Hasil *Maturity* DS10 *Manage Problems*

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

E.6. ME2 *Monitor and Evaluate Internal Control*

Membangun program kontrol internal efektif untuk IT membutuhkan proses pemantauan yang terdefinisi dengan baik. Proses 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 [21].

E.6.1. ME2.1 *Monitoring of Internal Control Framework*

Meningkatkan IT mengendalikan lingkungan dan kerangka kontrol untuk memenuhi tujuan organisasi.

E.6.2. ME2.2 *Supervisory Review*

Memantau dan mengevaluasi efisiensi dan efektivitas IT internal kontrol tinjauan manajerial.

E.6.3. ME2.3 *Control Exceptions*

Mengidentifikasi kontrol pengecualian, serta menganalisis dan mengidentifikasi penyebab yang mendasari *root*. Meningkat kontrol pengecualian dan melaporkan tepat kepada *stakeholder*. Institut tindakan korektif yang diperlukan.

E.6.4. ME2.4 *Control Self-assessment*

Mengevaluasi kelengkapan dan efektivitas pengendalian manajemen atas proses IT, kebijakan dan kontrak melalui terus program penilaian diri.

E.6.5. ME2.5 *Assurance of Internal Control*

Memperoleh sesuai kebutuhan serta kepastian lebih lanjut akan kelengkapan dan efektivitas pengendalian internal melalui pihak ketiga tinjauan.

E.6.6. ME2.6 *Internal Control at Third Parties*

Menilai status kontrol internal penyedia layanan eksternal. Memastikan penyedia layanan eksternal mematuhi hukum dan peraturan persyaratan dan kewajiban kontrak.

E.6.7. ME2.7 *Remedial Actions*

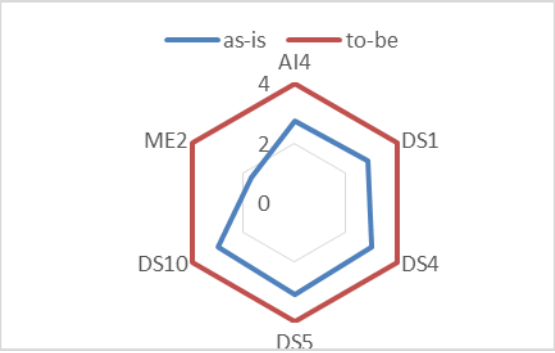
Mengidentifikasi, melacak dan menerapkan tindakan perbaikan yang timbul dari penilaian pengendalian dan pelaporan.

Dari hasil analisa audit ME2 *Monitor and Evaluate Internal Control*, diperoleh level kematangan dari setiap proses yang ada dalam tahap dan proses-prosesnya dapat dilihat pada Tabel 7.

Tabel 7. Hasil *Maturity* ME2 *Monitor and Evaluate Internal Control*

ME2 Monitor and Evaluate Internal Control		*Maturity Level*
ME2.1	*Monitoring of Internal Control Framework*	2
ME2.2	*Supervisory Review*	3
ME2.3	*Control Exceptions*	3
ME2.4	*Control Self-assessment*	2
ME2.5	*Assurance of Internal Control*	0
ME2.6	*Internal Control at Third Parties*	0
ME2.7	*Remedial Actions*	2
ME2	**Rata-rata**	**1,71**

Dari hasil audit sistem informasi absensi diatas, maka *sub domain* rata-rata hasil perhitungan *maturity level*, diperlihatkan pada Tabel 8. 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 8 rata-rata perhitungan *maturity level*, maka dibuat gambarnya menggunakan diagram *spider*, diperlihatkan pada Gambar 4.



Gambar 4. Diagram Spi*der Maturity Level as-is vs to-be*

Tabel 8. Rata-rata Hasil Perhitungan *Maturity* Level

Proses TI	*Descriptions*	*Maturity Level*
AI4	*Enable operation and use*	2,75
DS1	*Define And Manage Service Levels*	2,83
DS4	*Ensure Continuous Service*	3
DS5	*Ensure Systems Security*	3,09
DS10	*Manage Problem*	3
ME2	*Monitor and Evaluate Internal Control*	1,71

F. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian yang telah dilakukan adalah sebagai berikut: (1) PT. Sinar Pratama Agung sudah memiliki tata kelola sistem informasi yang telah dilakukan secara berulang, namun tata kelola yang diterapkan sudah memenuhi harapan. Keberadaan tata kelola sistem informasi pada PT. Sinar Pratama Agung terdefinisi dengan baik dan formal, ada prosedur maupun panduan baku dari pihak manajemen dan (2) berdasarkan hasil pengukuran menggunakan *maturity level* diketahui bahwa DS5 berada pada level 3,09 dan DS4 dan DS10 berada pada level 3 (*Defined Process*), sedangkan DS1 berada pada level 2,83 dan AI4 berada pada level 2,75 (*Repeatable but Intuitive*), sedangkan ME2 berada pada level 1,71 (*Initial/ad Hoc*). Nilai tertinggi berada pada DS5 (*Ensure Systems Security*) dengan nilai 3,09 dan nilai terendah pada ME2 (*Monitor and Evaluate Internal Control*) dengan nilai 1,71. Dengan itu diketahui bahwa Tata Kelola Sistem Informasi Absensi di PT. Sinar Pratama Agung berada *expected level* yang diharapkan pada level 3.

REFERENSI

[1] Rinawati dan P. Candrawati. Vol.7, No. 2, Desember 2013. *Sistem Informasi Absensi Karyawan Pada Pt Harja Gunatama Lestari Bandung*. Jurnal *Computech* & Bisnis, Vol.7. 96-105.

[2] R. K. Candra, I. Atastina dan Y. Firdaus. No.1 April 2015. *Audit Teknologi Informasi menggunakan Framework COBIT 5 Pada Domain DSS (Delivery, Service, and Support) (Studi Kasus: iGracias Telkom University)*. e-Proceeding of Engineering: Vol.2.

[3] Jelvino dan J. F. Andry. Nomor 2 Agustus 2017. *Audit Sistem Informasi Absensi pada PT. Bank Central Asia Tbk menggunakan COBIT 4.1*. Jurnal Teknik Informatika dan Sistem Informasi Volume 3.

[4] G. Hardy. 2009. *The Role of the IT Auditor in IT Governance*. ISACA Jurnal 1.

[5] H. Setiawan dan K. Mustofa. 2013. *Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia*. IPTEK-KOM, Vol. 15 No. 1 Juni, pp.1-15, ISSN 1410 – 3346,

[6] J. F. Andry. 2016. *Audit Tata Kelola Ti Di Perusahaan (Studi Kasus XYZ Cargo)*. Seminar Nasional Teknologi Informasi.

[7] Fitrianah, Devi, Sucahyo dan Yudho Giri. *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.

[8] T. Pradini dan J. F. Andry. 2018. *Audit Sistem Informasi Front Office Pada World Hotel Menggunakan Kerangka Kerja Cobit 4.1*. IKRAITH-INFORMATIKA, VOL. 2, NO. 1.

[9] M. K. Tanugara. 2015. *Perancangan Pedoman Audit Sistem Informasi Pada Industri Perhotelan dengan Studi Kasus Hotel Bintang 4 Berbasis Framework COBIT 4.1 menggunakan Domain Delivery and Support*. Makalah disajikan dalam Seminar Nasional Aplikasi dan Pengembangan Teknologi Informasi, Surabaya: Universitas Ciputra Surabaya 2.Buyens, Jim, 2001. *Web Database Development*. Jakarta: PT. Elex Media Komputindo.

[10] I. S. Rozas dan D. A. R. Effendy. 2012. *Mengukur Efektifitas Hasil Audit Teknologi Informasi Cobit 4.1 Berdasarkan Perspektif End User*. JURANAL LINK VOL 17/No. 2/September.

[11] Juliandarini dan S. Handayaningsih, S. 2013. *Audit Sistem Informasi Pada Digilib Universitas XYZ Menggunakan Kerangka Kerja COBIT 4.0*. Jurnal Sarjana Teknik Informatika, Jurnal Sarjana Teknik Informatika e-ISSN: 2338-5197 Volume 1 Nomor 1, Juni.Budiawan, Tiyo. 2011. *Mobile Tracking GPS (Global Positioning System) Melalui Media SMS (Short Message Service)*. [SKRIPSI] Universitas Diponegoro.

[12] I R. Widayanti dan L. Purnamawati. 2013. *Audit Sistem Informasi Pada Aplikasi Sistem Manajemen Pemeriksaan (Smp) Badan Pemeriksa Keuangan Republik Indonesia*. Forum Ilmiah Volume 10 Nomor 2, Mei.

[13] Weber, Ron. 2000. *Information System Control and Audit*", *Printice Hall,, Inc. New Jersey*.
[14] A. S.Rintjap, Sherwin R.U.A, Sompie ST, MT dan Oktavian Lantang ST., MTI. 2014. *Aplikasi Absensi Siswa Menggunakan Sidik Jari di Sekolah Menengah Atas Negeri 9 Manado*. *e-journal* Teknik Elektro dan Komputer), ISSN: 2301-8402.
[15] T. Pradini dan J. F. Andry. 2018. *Audit Sistem Informasi Front Office Pada World Hotel Menggunakan Kerangka Kerja Cobit 4.1*. IKRAITH-INFORMATIKA, VOL. 2, NO. 1.
[16] M. K. Tanugara. 2015. *Perancangan Pedoman Audit Sistem Informasi Pada Industri Perhotelan dengan Studi Kasus Hotel Bintang 4 Berbasis Framework COBIT 4.1 menggunakan Domain Delivery and Support*. Makalah disajikan dalam Seminar Nasional Aplikasi dan Pengembangan Teknologi Informasi, Surabaya: Universitas Ciputra Surabaya 2.
[17] Muthmainnah, S. Kom., M. Kom. 2015. *Model Perancangan Tata Kelola Teknologi Informasi (It Governance) Pada Proses Pengelolaan Data Di Universitas Malikussaleh Lhokseumawe*. Techsi Vol. 6 No.1, April.
[18] D. T. Yulianti dan M. C. Patria. 2011. *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.
[19] I. B. Sukmajaya dan J. F. Andry. 2017. *Audit Sistem Informasi Pada Aplikasi Accurate Menggunakan Model Cobit Framework 4.1 (Studi Kasus: Pt. Setia Jaya Teknologi)*. Vol. 2.
[20] Rajasa, A. 2015. *Predicting the Intention to Re-Use on Accounting Application Software, The International Journal of Business & Management*, Vol.3, No.8, p.207, August.
[21] Andry, J.F. Christianto, K. 2018. *Audit Menggunakan COBIT 4.1 dan COBIT 5 dengan Case Study.* Yogyakarta: TEKNOSAIN.