INFOTECH: JOURNAL OF TECHNOLOGY INFORMATION
DOI: https://doi.org/10.37365/jti.v9i1.153

VOL. 9 No. 1 Juni 2023
P-ISSN : 2460-2108
E-ISSN : 2620-5181

AUDIT APLIKASI PRESENSI PADA PERUSAHAAN INDUSTRI KOSMETIK MENGGUNAKAN COBIT 5

Honni[1], Francka Sakti Lee[2], M. Fauzi Isputrawan[3], Isabelle Ivana Limawal[4], Johanes Fernandes Andry[5]

[1,2,3,4,5]Sistem Informasi
[1,2,3,4,5]Universitas Bunda Mulia, Jakarta, Indonesia.
Correspondence email: jandry@bundamulia.ac.id

Article history: *Submission date: Januari 24, 2023* *Revised date: Juni 27, 2023* *Published date: Juni 30, 2023*

ABSTRACT

Attendance is essential for an institution or institution; it can assess employee salaries and performance. The company that will be audited is PT Anugerah Familindo Lestari, a company that distributes beauty and hair and body care products. This company's problem is that the fingerprint machine used has an error, which causes several employees who have been absent but are not recorded in the system. Therefore, to implement a sound fingerprint attendance system, it is necessary to carry out a checking activity known as an information system audit. In conducting data and observations, the study used questionnaires and interviews with related information and document confirmation. So far, the system has been implemented to support attendance procedures. In this study, the selected domains are Deliver Service and Support (DSS) domain and Monitor, Evaluate, and Assessment (MEA) domain with a focus on IT Process DSS01, DSS04, DSS05, and MEA02. Based on the research conducted, the writer found that the average level of the DSS01 domain was 1.6, the DSS04 domain was 1.7, the DSS05 domain was 1.7, and the MEA02 domain was 1.8. In all the domains studied, the level of capability of the domain is still below the expectation; the author concludes that from the results of this capability level, PT. Anugerah Familindo Lestari still has much to do with the management and maintenance of their attendance system to increase the current level of capability because it is still quite far from the level expected by this company.

Keywords: *Attendance, COBIT 5 Framework, Information System Audit.*

ABSTRAK

Kehadiran sangat penting bagi suatu lembaga atau lembaga; itu dapat menilai gaji dan kinerja karyawan. Perusahaan yang akan diaudit adalah PT Anugerah Familindo Lestari, perusahaan yang mendistribusikan produk kecantikan dan perawatan rambut dan tubuh. Permasalahan perusahaan ini adalah mesin sidik jari yang digunakan mengalami error, yang menyebabkan beberapa karyawan yang absen namun tidak tercatat di sistem. Oleh karena itu, untuk menerapkan sistem absensi sidik jari yang baik, perlu dilakukan kegiatan pengecekan yang dikenal dengan audit sistem informasi. Dalam melakukan data dan observasi, penelitian ini menggunakan kuesioner dan wawancara dengan informasi terkait dan konfirmasi dokumen. Sejauh ini, sistem tersebut telah diterapkan untuk mendukung prosedur absensi. Pada penelitian ini domain yang dipilih adalah domain *Deliver Service and Support* (DSS) dan domain Monitor, *Evaluate, and Assessment* (MEA) dengan fokus pada IT Process DSS01, DSS04, DSS05, dan MEA02. Berdasarkan penelitian yang dilakukan, penulis menemukan bahwa rata-rata level domain DSS01 adalah 1,6, domain DSS04 adalah 1,7, domain DSS05 adalah 1,7, dan domain MEA02 adalah 1,8. Pada semua domain yang diteliti, tingkat kapabilitas domain tersebut masih di bawah harapan; penulis menyimpulkan bahwa dari hasil tingkat kapabilitas ini, PT. Anugerah Familindo Lestari masih banyak melakukan pengelolaan dan pemeliharaan sistem absensi mereka untuk meningkatkan level kapabilitas saat ini karena masih cukup jauh dari level yang diharapkan oleh perusahaan ini.

Kata Kunci: Kehadiran, COBIT 5 *Framework*, Audit Sistem Informasi.

PENDAHULUAN

PT. Anugerah F. Lestari, perusahaan yang mendistribusikan produk untuk mempercantik diri dan melakukan berbagai perawatan untuk rambut dan anggota tubuh berdiri pada akhir tahun 2017, perusahaan ini lahir dari PT Anugerah Familindo Utama (pabrik produk kecantikan dan perawatan tubuh). PT Anugerah Familindo Utama memiliki pengalaman mengerjakan produk-produk brand ternama hingga saat ini. Produk perusahaan adalah Cultusia, Valenno, Missmay, Jinju, dan lain-lain, banyak brand yang bermunculan dari perusahaan ini. Perusahaan yang kami teliti menggunakan sistem pengenalan sidik jari.

Dengan di gunakannya teknologi dan sistem informasi sudah memiliki peran yang amat sangat strategis pada era sekarang ini dalam membantu untuk memenangkan persaingan dalam era digital ini. Selain itu pemanfaatannya juga dapat digunakan dalam membantu absensi (Croteau & Bergeron, 2001). Presensi adalah kumpulan data kehadiran, tentunya adalah bagian dari berbagai pelaporan kegiatan suatu organisasi, atau komponen perusahaan itu sendiri yang berisi record kehadiran yang disusun dan diatur sedemikian rupa sehingga dapat mempermudah untuk dicari dan digunakan untuk keperluan kapan saja serta diperuntukkan oleh pihak yang dapat bertanggung jawab.

Sidik jari merupakan alat yang digunakan sebagai pengenal ciri-ciri, melindungi personal komputer asal data, atau penggunaan personal komputer sang orang yg tidak bertanggung jawab. menggunakan sidik jari menjadi pengganti tanda tangan bisa mengetahui identitas pemilik berasal sidik jari (Olagunju, Adeniyi, & Oladele, 2018). Sistem absensi pengenalan sidik jari banyak digunakan untuk banyak tujuan lain dan merupakan teknik yang sangat nyaman dan dapat diandalkan untuk memverifikasi identitas seseorang. Diyakini bahwa tidak ada dua orang yang memiliki sidik jari yang sama di dunia ini. Efisiensi menjadi dasar penggunaan sistem absensi sidik jari, yang membantu organisasi buat berhemat energi atau tenaga sekaligus menjamin keamanan (Saraswat, Kumar, & Engineering, 2010; Sequeira & Cardoso, 2015). Sistem absensi pengenalan sidik jari memiliki beberapa keunggulan yaitu mengatasi kecurangan dalam proses prestise. Membantu manajemen bergengsi menjadi lebih baik dan lebih akurat. Itu menghasilkan data yang lebih akurat, meningkatkan disiplin kehadiran karyawan, dan menghindari manipulasi absensi. Namun dalam penerapannya, sidik jari itu sendiri masih memiliki beberapa kendala (Mulyadi, 2020).

Awal mula tujuan dari audit sistem berita ialah buat mengetahui proses absensi sistem absensi perusahaan yang waktu ini sedang diuji dengan menggunakan standar COBIT (Budiarta, Iskandar, Sudarma, & Technology, 2016). COBIT adalah kerangka kerja atau panduan untuk praktik terbaik manajemen dan teknologi informasi. Penelitian ini akan menggunakan framework COBIT 5 yang merupakan framework COBIT terbaru (Firdaus, 2018).

COBIT 5 ialah salah satu kerangka kerja bisnis dan IT untuk menaikkan tata kelola serta manajemen perusahaan. Versi evolusi TI ini sudah menggabungkan persepsi teranyar pada tata kelola perusahaan serta menyediakan prinsip, praktik, alat buat menganalisis, dan contoh kerangka kerja yang diterima secara umum buat membantu mengoptimalkan sistem presensi, contoh pada penilaian teknologi informasi COBIT 5 memiliki cakupan yang sangat luas (Aisyah, Cakranegara, & Sani, 2022; Drljača & Latinović, 2017). COBIT 5 dipilih karena memiliki framework layanan yang komprehensif untuk membantu perusahaan mengatasi permasalahan yang terdapat pada absensi perusahaan. COBIT 5 juga akan memberikan gambaran dan keamanan informasi pada perusahaan yang mengalami masalah absensi dan menaikkan kegunaan akibat penilaian kapabilitas proses. Versi terbaru ini menyampaikan dasar buat penilaian yang lebih formal dan menyeluruh (Moeller, Erek, Loeser, & Zarnekow, 2013).

METODE PENELITIAN

Ruang lingkup penelitian ini terbatas pada pengauditan pada aplikasi presensi dan Proses Identifikasi absensi pada PT. Anugerah F. Lestari khususnya di Kantor Cabang Pembantu Bogor. Pada tahap ini, penetapan proses teknologi informasi sesuai dengan standar COBIT 5 yang telah diolah sesuai studi kasus. Cakupan TI domain yang diaudit pada aplikasi presensi, terlihat pada Tabel 1. Lingkup TI Domain yang Diaudit.

Tabel 1. Lingkup TI Domain yang Diaudit

Sub-domain	Keterangan
DSS01	Manage operation
DSS04	Manage keberlanjutan
DSS05	Monitor, Evaluaasi, internal sistem control

Prosedur Penelitian merupakan kegiatan yang harus dilakukan dalam melakukan penelitian. Adapun tahapan dan prosedur penelitian adalah diperlihatkan pada Gambar 1. Tahapan Penelitian.

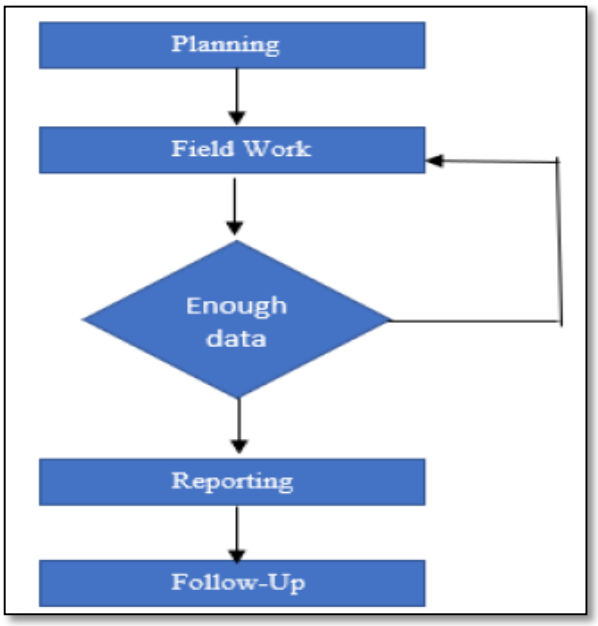
1) *Planning*

Planning atau perencanaan artinya termin awal dalam penelitian yg penulis lakukan. sebab di termin ini adalah ruang lingkup, objek yg akan diaudit, standar penilaian akibat audit serta komunikasi dengan yg bersangkutan akan organisasi/perusahaan yg akan diaudit menggunakan analisis visi, misi, tujuan, serta sasaran suatu objek, dan kebijakan yg terkait menggunakan

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbud No.105/E/KPT/2022, 7 April 2022. Diterbitkan oleh LPPM STMIK Widuri

DOI: https://doi.org/10.37365/jti.v9i1.153
VOL. 9 No. 1 Juni 2023
P-ISSN : 2460-2108
E-ISSN : 2620-5181

pemrosesan pemeriksaan. di termin perancangan mencakup beberapa aktivitas yaitu penentuan ruang lingkup dan tujuan audit, pengorganisasian tim audit, pemahaman operasi usaha klien, review akibat audit, serta penyusunan acara audit (Gatrad, 2000; Sani et al., 2020).



Sumber: (Honni et al., 2023)
Gambar 1. Tahapan Penelitian.

2) *Field Work*
Pada tahapan atau sesi ini, penulis bertujuan untuk memperoleh informasi dengan mengumpulkan data dengan dan dari pihak-pihak yang terkait. Sebab hambatan tersebut, penulis menggunakan beberapa metode yang dapat dilakukan, seperti; mewawancara, membuat kuesioner, dan melakukan survei secara langsung ke tempat penelitian yang dilakukan. Data-data tersebut nantinya dapat bermanfaat untuk membantu auditor menganalisis organisasi/perusahaan yang diaudit. Jika informasi yang dibutuhkan sudah cukup, maka lanjutkan ke langkah berikutnya atau langkah pelaporan, dan jika tidak, kembali ke langkah kerja lapangan (Corfield, 2008). Untuk diolah dan dlakukan perhitungan berdasarkan perhitungan tingkat kapabilitas.

Pada sesi ini, penulis akan memberikan informasi berupa hasil audit. Perhitungan tingkat kemampuan dilakukan tentang hasil yang di dapat pada wawancara, melakukan survei, dan melakukan perhitungan hasil rekapitulasi dari penyebaran Kuesioner. Berdasarkan nilai tingkat kapabilitas, hasilnya nanti akan mencerminkan berapa tingkat kapabilitas saat ini dan standar kinerja atau cita-cita yang diharapkan dapat menjadi pedoman dalam melakukan analisis kesenjangan (gap) lebih lanjut. Hal ini dilakukan untuk mengetahui seberapa besar *gap* tersebut dan mengetahui apa yang menyebabkan terjadinya *gap* tersebut. Dengan adanya report audit yang baik maka permasalahan akan lebih jelas terlihat dimana letak kesalahan pada sistem tersebut (Musa, 2017).

3) Tindak Lanjut
Setelah pelaporan atau pelaporan adalah memberikan laporan hasil audit berupa rekomendasi tindakan korektif kepada manajemen objek yang diperiksa, untuk selanjutnya kewenangan perbaikan menjadi tanggung jawab pengendalian item yang dibahas apakah akan diterapkan atau hanya menjadi acuan untuk perbaikan di masa mendatang (Stewart, 2007).

4) Tingkat Kemampuan Proses
Pada setiap level, kemampuan hanya dapat dicapai jika level di bawahnya tercapai sepenuhnya. Sebagai contoh, tingkat kapabilitas proses 3 yang, Ditetapkan, memerlukan tingkat sebelumnya Proses terkelola sekarang diimplementasikan menggunakan proses yang ditentukan yang mampu mencapai hasil proses, dan atribut untuk kapabilitas proses tingkat 2 harus diselesaikan sepenuhnya.
Dalam setiap proses yang dinilai memiliki empat tingkatan penilaian, sebagai berikut:
a) Tidak Tercapai (N): Bila hasil penilaian berdasarkan analisis antara 0% - 15%.
b) Partially Achieved (P): Kondisi tercapai pada saat hasil penilaian berada pada 15% - 50%.
c) Sangat Tercapai (L): Kondisi tercapai jika hasil penilaian mencapai 50% - 85%.
d) Tercapai Penuh (P): Jika hasil penilaian sudah mencapai 85% - 100%. Ada enam tingkat kemampuan yang dapat dicapai suatu proses, dan itu juga termasuk menetapkan 'proses yang tidak lengkap' jika praktiknya tidak mencapai tujuan proses yang diinginkan.

Table 2. COBIT 5 *Capability Levels Model*

Level	Description
Level 0: Incomplete	Proses tidak dilaksanakan atau gagal mewujudkan tujuannya. Pada tingkat ini, hanya ada sedikit atau tidak ada bukti pencapaian tujuan secara sistematis.
Level 1: Performed	Proses yang diterapkan sudah mencapai tujuannya. Proses ini memiliki satu atribut proses yaitu Process Performance.
Level 2: Managed	Proses yang dilakukan sekarang diimplementasikan dan dikelola (direncanakan, dipantau, dan disesuaikan). Proses ini memiliki dua atribut proses yaitu Performance Management dan Work Product Management.
Level 3: Established	Proses yang dikelola sekarang diimplementasikan dalam proses yang ditentukan yang dapat mencapai hasil prosesnya. Proses ini memiliki dua atribut proses yaitu Process Definition dan Process Deployment.

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbud No.105/E/KPT/2022, 7 April 2022. Diterbitkan oleh LPPM STMIK Widuri

Level	Description
Level 4: Predictable	Proses yang ditetapkan sekarang beroperasi dalam batas yang ditentukan untuk mencapai hasil prosesnya. Proses ini memiliki dua atribut proses yaitu Process Management dan Process Control.
Level 5: Optimizing	Proses yang dapat diprediksi sekarang terus ditingkatkan untuk memenuhi tujuan bisnis yang relevan saat ini dan yang diproyeksikan. Proses ini memiliki dua atribut proses yaitu Process Innovation dan Process Optimization..

Sumber: (Honni et al., 2023)

HASIL DAN PEMBAHASAN

1. DSS01 *Manage Operations*

Mengoordinasikan dan mengimplementasikan kegiatan dan prosedur operasional jika diperlukan untuk menyediakan layanan TI internal dan outsourcing, pemeliharaan infrastruktur, lingkungan, dan fasilitas, serta penerapan prosedur operasi standar dan kegiatan pemantauan yang akan diperlukan. Berikut ini adalah tujuan proses dari DSS01 (*Manage Operations*):

1. Kegiatan operasional dilakukan sesuai kebutuhan dan terjadwal.
2. Operasi dipantau, diukur, dilaporkan, dan diperbaiki.

1.1 DSS01.01 *Perform Operational Procedures*

Memelihara dan menjalankan prosedur operasional dan tugas operasional secara handal dan konsisten. Berikut adalah kegiatan dari proses tersebut:

1. Dengan menjaga dan melaksanakan prosedur operasional dan tugas operasional dengan baik, handal dan konsisten.
2. Dengan mengembangkan, memelihara prosedur operasional dan kegiatan terkait untuk mendukung semua layanan yang diberikan.
3. Dengan menjaga jadwal kegiatan operasional, melaksanakan kegiatan dengan tepat, dan mengelola kinerja dan hasil kegiatan yang dijadwalkan.
4. Verifikasi bahwa setiap data yang diharapkan untuk diproses diterima dan diproses secara lengkap, akurat, dan tepat waktu. Memberikan output mengikuti persyaratan perusahaan. Mendukung kebutuhan restart dan pemrosesan ulang. Pastikan bahwa pengguna menerima keluaran yang tepat selama cara yang aman dan tepat waktu.
5. Pastikan bahwa standar keamanan yang berlaku dipenuhi untuk penerimaan, pemrosesan, penyimpanan, dan keluaran pengetahuan dengan cara yang memenuhi tujuan perusahaan, kebijakan keamanan perusahaan, dan persyaratan peraturan.
6. Menjadwalkan, mengambil, dan mencatat pencadangan mengikuti kebijakan dan prosedur yang ditetapkan.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS01.01, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa PT Anugerah Familindo Lestari telah menerapkan service level yang tepat dimana sistem yang memadai selalu memfasilitasi kebutuhan absensi namun belum memiliki manajemen untuk memantau proses absensi menggunakan sidik jari di perusahaan. Tingkat kemampuan subdomain ini adalah level satu, Performed.

1.2 DSS01.02 *Manage Outsourced IT Services*

Kelola operasi layanan TI yang dialihdayakan untuk melindungi informasi perusahaan dan keandalan penyampaian layanan. Berikut adalah kegiatan dari proses tersebut:

1. Pastikan bahwa persyaratan perusahaan untuk keamanan proses data dipatuhi mengikuti kontrak dan SLA dengan hosting atau penyedia layanan pihak ketiga.
2. Pastikan bahwa bisnis operasional perusahaan dan persyaratan pemrosesan serta prioritas untuk pemberian layanan dipatuhi mengikuti kontrak dan SLA dengan hosting atau penyedia layanan pihak ketiga.
3. Rencanakan audit independen dan jaminan lingkungan operasional penyedia outsourcing untuk memverifikasi bahwa persyaratan yang disepakati telah ditangani secara memadai.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS01.02, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa PT Anugerah Familindo Lestari telah menerapkan service level yang tepat dimana sistem yang memadai selalu memfasilitasi kebutuhan absensi namun belum memiliki manajemen untuk memantau proses absensi menggunakan sidik jari di perusahaan. Level kapabilitas sudah mencapai level dua, Managed.

1.3 DSS01.03 *Monitor IT Infrastructure*

Pantau infrastruktur TI dan acara terkait. Menyimpan informasi kronologis yang memadai dalam log operasi untuk memungkinkan rekonstruksi, peninjauan, dan pemeriksaan urutan waktu operasi dan aktivitas lain di sekitar atau fungsi pendukung. Berikut adalah kegiatan dari proses tersebut:

1. Mencatat peristiwa, mengidentifikasi sejauh mana data yang akan direkam, mendukung pertimbangan risiko dan kinerja.
2. Identifikasi dan pertahankan inventaris aset infrastruktur yang perlu dipantau untuk kekritisan

DOI: https://doi.org/10.37365/jti.v9i1.153
VOL. 9 No. 1 Juni 2023
P-ISSN : 2460-2108
E-ISSN : 2620-5181

layanan yang didukung dan hubungan antara item konfigurasi dan layanan
3. Dengan mendefinisikan dan menerapkan aturan yang mengidentifikasi, mencatat pelanggaran ambang serta kondisi kejadian yang ada. Selain itu, ada keseimbangan antara membuat peristiwa kecil palsu dan tonggak sejarah sehingga log peristiwa tidak akan dibebani dengan informasi yang tidak perlu.
4. Dengan membuat log peristiwa dan menyimpannya di tempat yang sesuai untuk periode yang sesuai guna membantu penyelidikan di masa mendatang.
5. Dengan menetapkan prosedur dengan tujuan memantau event log dan melakukan review secara berkala.
6. Pastikan bahwa tiket insiden dibuat segera pada saat pemantauan mengidentifikasi penyimpangan dari ambang batas yang telah ditentukan.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS01.03, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa dalam hal kepengurusan tanggung jawab khususnya sistem absensi di PT Anugerah Familindo Lestari sudah berjalan. Masih belum memenuhi elemen proses yang ditentukan karena tidak ada manajemen yang bertanggung jawab atas manajemen sistem. Tingkat kemampuan subdomain ini adalah level satu, Performed.

1.4 DSS01.04 *Manage The Environment*

Pertahankan langkah-langkah perlindungan terhadap faktor lingkungan. Instal semua peralatan dan perangkat khusus untuk memantau dan mengontrol lingkungan. Berikut adalah kegiatan dari proses tersebut:
1. Mengidentifikasi bencana alam dan ulah manusia, yang mungkin terjadi di dalam area di mana fasilitas TI berada. Menilai efek potensial pada fasilitas TI.
2. Dengan mengidentifikasi bagaimana peralatan TI, termasuk peralatan bergerak dan di luar lokasi, telah dilindungi dari ancaman lingkungan yang diantisipasi. Pastikan bahwa kebijakan tersebut membatasi atau mengecualikan makan, minum, dan merokok di area sensitif, dan melarang penyimpanan alat tulis dan perlengkapan lain yang menimbulkan bahaya kebakaran di dalam ruang komputer.
3. Menempatkan dan membangun semua fasilitas TI untuk meminimalkan dan mengurangi kerentanan dari ancaman lingkungan.
4. Dengan memantau dan juga memelihara perangkat yang mendeteksi ancaman lingkungan secara berkala. Contohnya termasuk api, air, asap, dan kelembaban.
5. Memastikan bahwa lokasi tersebut dibangun dan dirancang untuk meminimalkan dampak risiko lingkungan. Contohnya termasuk pencurian, udara, kebakaran, teror, vandalisme, bahan kimia, dan bahan peledak. Pertimbangkan juga zona keamanan khusus dan sel tahan api (misalnya, menempatkan lingkungan/server produksi dan pengembangan jauh dari satu sama lain).

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS01.04, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit diperoleh dari kehadiran tingkat operasional sistem di PT Anugerah Familindo Lestari; Ini sudah pada tahap yang cukup baik tetapi belum berhasil menyelesaikan masalah abses seperti pemeliharaan sistem. Level kapabilitas sudah mencapai level dua, Managed.

1.5 DSS01.05 *Manage Facilities*

Kelola fasilitas, termasuk peralatan listrik dan komunikasi, sejalan dengan undang-undang dan peraturan, persyaratan teknis dan bisnis, spesifikasi vendor, serta panduan kesehatan dan keselamatan. Berikut adalah kegiatan dari proses tersebut:
1. Periksa persyaratan fasilitas TI untuk melindungi dari fluktuasi dan pemadaman listrik, sehubungan dengan persyaratan perencanaan kesinambungan bisnis lainnya. Dapatkan peralatan pasokan tak terputus yang sesuai (misalnya, baterai, generator) untuk mendukung perencanaan kesinambungan bisnis yang telah ditentukan.
2. Secara teratur menguji mekanisme catu daya tak terputus dan memastikan bahwa daya sering dialihkan ke ketersediaan tanpa pengaruh signifikan pada operasi bisnis.
3. Pastikan fasilitas yang menampung sistem TI memiliki cukup satu sumber untuk utilitas yang bergantung (mis, daya, telekomunikasi, air, gas). Pisahkan pintu masuk fisik setiap utilitas.
4. Pastikan Pengkabelan dan penambalan fisik (data dan telepon) terstruktur dan teratur. Struktur kabel dan saluran harus didokumentasikan atau direkam (misalnya, cetak biru rencana bangunan serta diagram pengkabelan).
5. Dengan mencatat, memantau, mengelola, dan menyelesaikan insiden fasilitas sejalan dengan proses manajemen insiden TI. Selain itu, ini juga menyediakan laporan tentang insiden fasilitas di mana pengungkapan diperlukan dalam masalah hukum dan peraturan.
6. Menganalisis perubahan fisik terhadap situs atau tempat untuk menilai kembali risiko lingkungan (misalnya, kerusakan akibat kebakaran atau air). Laporkan hasil analisis yang ada kepada kelangsungan bisnis serta manajemen fasilitas.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-*domain* DSS01.05, terdapat temuan audit

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbud No.105/E/KPT/2022, 7 April 2022. Diterbitkan oleh LPPM STMIK Widuri

berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa pemantauan level dari PT Anugerah Familindo Lestari cukup bermanfaat karena memberikan solusi bagi karyawan ketika mengalami kendala saat melakukan sidik jari, dan manajemen sudah memilikinya. Level kapabilitas sudah mencapai level dua, Managed.

Untuk memudahkan pemahaman secara jelas, dapat dilakukan pemetaan atribut proses (PA). Pemetaan ini dilakukan untuk mengetahui pencapaian sistem informasi yang ada berdasarkan hasil wawancara dan analisis di perusahaan. Proses pemetaan atribut ini diperlukan untuk mendapatkan tingkat kapabilitas dari setiap subproses dalam suatu domain. Setiap proses atribut harus seluruhnya atau sebagian besar dapat dicapai untuk naik ke tingkat berikutnya. Untuk setiap PA yang hanya berada pada level pertama (misal 2.1, 3.1, 4.1 dan 5.1), level ability yang didapatkan adalah 1 level di bawah PA. Jadi proses dengan PA 2.1 hanya memiliki tingkat kemampuan 1.

Table 3. *Mapping Process Attributes Form* (DSS01)

IT Processes	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
DSS01-01	F	N	N	N	N	N	N	N	N
DSS01-02	F	F	F	N	N	N	N	N	N
DSS01-03	F	F	N	N	N	N	N	N	N
DSS01-04	F	F	F	N	N	N	N	N	N
DSS01-05	F	F	F	N	N	N	N	N	N

Sumber: (Honni et al., 2023)

Berdasarkan hasil wawancara dan kuesioner yang dilakukan, yang dituangkan dalam Tabel 3, setiap proses TI mencapai atribut proses yang berbeda. DSS01.02 mencapai PA 2.2 (sepenuhnya tercapai) sehingga level kapabilitas berada pada level 2. Sedangkan pada subproses DSS01.03 hanya mencapai PA 2.1 yang menandakan level kapabilitas belum mencapai level 2 dan hanya level 1.

Table 4. *Results of DSS01 Manage Operations*

No	Sub Domain	Process Attributes	Capability Level	Expected Level
DSS01-01	Perform Operational Procedures	1,1	1	3
DSS01-02	Manage Outsourced IT Services	2,2	2	3
DSS01-03	Monitor IT Infrastructure	2,1	1	3
DSS01-04	Manage The Environment	2,2	2	3
DSS01-05	Manage Facilities	2,2	2	3
	Average		1,6	3

Sumber: (Honni et al., 2023)

2. DSS04 *Manage Continuity*

Pada tahap ini, penulis akan menganalisis pengoperasian sistem absensi kritis berkelanjutan dan menjaga ketersediaan informasi pada tingkat yang dapat diterima perusahaan jika terjadi gangguan yang signifikan, dengan deskripsi proses, mengatur dan memelihara rencana untuk memungkinkan sistem dan TI untuk menanggapi insiden dan gangguan untuk melanjutkan operasi. Proses sistem kritis dan layanan TI yang diperlukan serta menjaga ketersediaan informasi pada tingkat yang dapat diterima oleh perusahaan. Tingkat kapabilitas proses yang diharapkan dari DSS04 Manage Continuity adalah level 3. Berikut adalah tujuan proses dari DSS04 (*Manage Continuity*) :

1. Informasi penting bisnis tersedia untuk bisnis sesuai dengan tingkat layanan minimum yang disyaratkan.
2. Ketahanan yang memadai tersedia untuk layanan kritis.
3. Dengan menguji kesinambungan layanan, yang telah memverifikasi keefektifan rencana tersebut.
4. Perencanaan keberlanjutan baik untuk mencerminkan kebutuhan bisnis saat ini.
5. Pihak internal dan eksternal dilatih dalam rencana kesinambungan.

2.1 DSS4.01 *Define The Business Continuity Policy, Objectives, And Scope*

Menetapkan kebijakan dan ruang lingkup bisnis yang sejalan dengan tujuan perusahaan dan pemangku kepentingan. Berikut adalah kegiatan dari proses tersebut:

1. Mengidentifikasi proses bisnis internal, pengalihdayaan, dan aktivitas layanan yang penting bagi operasi perusahaan atau diperlukan untuk memenuhi kewajiban hukum.
2. Dengan mengidentifikasi siapa pemangku kepentingan utama dan peran serta tanggung jawab mereka untuk menguraikan dan menyepakati kebijakan dan ruang lingkup keberlanjutan.
3. Dengan menentukan dan mendokumentasikan tujuan dan ruang lingkup kebijakan minimum yang disepakati untuk melakukan bisnis dan menanamkan perlunya perencanaan kesinambungan dalam budaya perusahaan.
4. Identifikasi semua proses bisnis pendukung serta layanan TI terkait.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS04.01, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa PT Anugerah Familindo Lestari telah sudah diterapkan namun belum memiliki manajemen luar biasa untuk mengawasi proses absensi menggunakan sidik jari. Tingkat kemampuan subdomain ini adalah level satu, Performed.

2.2 DSS04.02 *Maintain A Continuity Strategy*

Mengevaluasi opsi manajemen kesinambungan bisnis dan memilih strategi yang hemat biaya dan layak yang

DOI: https://doi.org/10.37365/jti.v9i1.153
VOL. 9 No. 1 Juni 2023
P-ISSN : 2460-2108
E-ISSN : 2620-5181

akan memastikan pemulihan dan kelancaran operasi perusahaan dalam menghadapi peristiwa yang tidak diinginkan atau gangguan signifikan lainnya. Berikut adalah kegiatan dari proses tersebut:

1. Identifikasi skenario potensial yang cenderung menimbulkan peristiwa yang akan menyebabkan insiden gangguan yang signifikan.
2. Melakukan analisis dampak bisnis untuk mengukur dampak dari waktu ke waktu dari gangguan terhadap fungsi bisnis penting dan karenanya, serta dampak dari gangguan yang ada.
3. Dengan menetapkan waktu minimum yang diperlukan untuk memulihkan dan memperbaiki proses bisnis untuk mendukung periode gangguan bisnis yang sesuai dan pemadaman listrik yang dapat ditoleransi secara maksimal.
4. Menilai kemungkinan ancaman yang dapat menyebabkan kegagalan kelangsungan usaha dan mengidentifikasi tindakan yang akan mengurangi kemungkinan dan dampak dengan meningkatkan pencegahan dan meningkatkan ketahanan.
5. Menganalisis persyaratan kontinuitas untuk melihat kemungkinan opsi bisnis dan teknis strategis.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS04.02, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit dalam hal menjaga kehadiran sistem di PT Anugerah Familindo Lestari sudah dilakukan, namun belum ada manajemen yang mendukung sistem tersebut. Tingkat kemampuan subdomain ini adalah level satu, Performed.

2.3 DSS04.03 *Develop And Implement A Business Continuity Response*

Mengembangkan rencana kelangsungan bisnis (BCP) berdasarkan strategi yang menjalankan prosedur dan informasi yang ada dalam kesiapan untuk digunakan agar perusahaan dapat melanjutkan aktivitas kritisnya. Berikut adalah kegiatan dari proses tersebut:

1. Dengan menentukan respon insiden dan tindakan komunikasi yang perlu dilakukan jika terjadi gangguan. Menentukan peran dan tanggung jawab terkait, termasuk akuntabilitas untuk kebijakan dan implementasi.
2. Mengembangkan dan memelihara BCP operasional yang berisi prosedur untuk mengikuti kemungkinan operasi berkelanjutan dari proses bisnis penting dan pengaturan pemrosesan sementara, termasuk tautan ke rencana penyedia layanan outsourcing.
3. Pastikan pemasok utama dan mitra outsourcing memiliki rencana kesinambungan yang efektif di lokasi. Memperoleh bukti yang diaudit sesuai kebutuhan.
4. Menentukan kondisi dan prosedur pemulihan yang memungkinkan dimulainya kembali proses bisnis, termasuk pemutakhiran dan rekonsiliasi database informasi untuk menjaga integritas informasi.
5. Menentukan dan mendokumentasikan sumber daya yang diperlukan untuk mendukung prosedur kontinuitas dan pemulihan, mengingat orang, fasilitas, dan infrastruktur TI.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan aktivitas COBIT 5 sub-domain DSS04.03, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: berjalan cukup baik dengan pemantauan dari Kantor Pusat, dan telah dipantau oleh Kantor Pusat. Level kapabilitas sudah mencapai level dua, Managed.

2.4 DSS04.04 *Exercise, Test, And Review The BCP*

Menguji pengaturan kesinambungan secara teratur untuk melaksanakan rencana pemulihan terhadap hasil yang telah ditentukan dan memungkinkan solusi inovatif dikembangkan, dan memverifikasi bahwa proyek akan berjalan seperti yang diharapkan. Berikut adalah kegiatan dari proses tersebut:

1. Dengan menentukan tujuan untuk melatih dan menguji sistem bisnis, teknis, logistik, administrasi, prosedural dan operasional keputusan untuk memverifikasi kelengkapan BCP dalam memenuhi risiko bisnis.
2. Tetapkan dan setujui latihan dengan pemangku kepentingan yang realistis, validasi prosedur kontinuitas, dan sertakan peran dan tanggung jawab serta pengaturan penyimpanan data yang menyebabkan gangguan terkecil pada proses bisnis.
3. Menetapkan peran dan tanggung jawab untuk melakukan latihan dan uji rencana kesinambungan.
4. Jadwalkan latihan dan aktivitas pengujian sebagaimana ditentukan dalam rencana kesinambungan.
5. Melakukan pembekalan dan analisis pasca latihan untuk memikirkan pencapaian.
6. Mengembangkan rekomendasi untuk meningkatkan rencana kesinambungan yang ada. Mendukung hasil review.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS04.04, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa pelatihan sistem TI telah dilaksanakan diimplementasikan sepenuhnya untuk karyawan PT Anugerah Familindo Lestari. Namun hanya sedikit karyawan yang terikat tanggung jawab yang memahami proses dan teknik penggunaan sistem TI. Level kapabilitas sudah mencapai level dua, *Managed*.

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbud No.105/E/KPT/2022, 7 April 2022. Diterbitkan oleh LPPM STMIK Widuri

Table 5. Mapping Process Attributes Form (DSS04)

IT Processes	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
DSS04-01	F	N	N	N	N	N	N	N	N
DSS04-02	F	N	N	N	N	N	N	N	N
DSS04-03	F	F	F	N	N	N	N	N	N
DSS04-04	F	F	F	N	N	N	N	N	N
DSS04-05	F	F	F	N	N	N	N	N	N
DSS04-06	F	F	F	N	N	N	N	N	N
DSS04-07	F	F	F	N	N	N	N	N	N

Sumber: (Honni et al., 2023)

2.5 DSS04.05 *Review, Maintain And Improve The Continuity Plan*

Lakukan semua tinjauan manajemen sehingga kemampuan kontinuitas diatur untuk memastikan kesesuaian, kecukupan, dan kekhasan yang berkelanjutan. Berikut adalah kegiatan dari proses tersebut:

1. Meninjau rencana kesinambungan dan kemampuan setiap hari terhadap setiap asumsi yang dibuat dan tujuan operasional dan strategis bisnis saat ini.
2. Pertimbangkan apakah penilaian dampak bisnis yang direvisi juga diperlukan, dengan mengandalkan karakter perubahan.
3. Merekomendasikan dan mengkomunikasikan perubahan yang ada dalam kebijakan, rencana, prosedur, infrastruktur, serta peran dan tanggung jawab untuk memperoleh persetujuan dan pemrosesan manajemen melalui proses manajemen perubahan.
4. Tinjau rencana kesinambungan setiap hari untuk memikirkan dampak perubahan terbaru atau signifikan terhadap organisasi perusahaan, proses bisnis, pengaturan alih daya, teknologi, infrastruktur, sistem operasi, dan sistem aplikasi.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS04.05, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa pelatihan sistem TI telah dilaksanakan diimplementasikan sepenuhnya untuk karyawan PT Anugerah Familindo Lestari. Namun hanya sedikit karyawan yang terikat tanggung jawab yang memahami proses dan teknik penggunaan sistem TI. Level kapabilitas sudah mencapai level dua, Managed.

2.6 DSS04.06 *Conduct Continuity Plan Training*

Menyediakan semua pihak internal dan eksternal yang berkepentingan dalam sesi pelatihan reguler mengenai peran dan tanggung jawab mereka ketika terjadi masalah di perusahaan. Berikut adalah kegiatan dari proses tersebut:

1. Tetapkan dan pertahankan semua persyaratan dan rencana pelatihan bagi mereka yang memiliki perencanaan perkusi, penilaian dampak, penilaian risiko, komunikasi media, dan respons insiden. Pastikan bahwa rencana pelatihan mempertimbangkan frekuensi pembinaan dan mekanisme penyampaian pelatihan.
2. Mengembangkan kompetensi yang didukung pelatihan praktis, termasuk keikutsertaan dalam latihan dan tes.
3. Memantau keterampilan dan kompetensi yang didukung latihan dan hasil tes.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan aktivitas COBIT 5 sub-domain DSS04.06, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan pemulihan layanan TI telah dilaksanakan dengan benar. Namun, dibutuhkan sumber daya manusia yang ahli dalam hal ini. Sehingga tidak semua karyawan dapat melakukan IT recovery jika diperlukan. Level kapabilitas sudah mencapai level dua, *Managed*.

2.7 DSS04.07 *Manage Backup Arrangements*

Menjaga ketersediaan informasi penting bisnis. Berikut adalah kegiatan dari proses tersebut:

1. Salin sistem, aplikasi, data dan dokumentasi sesuai dengan jadwal yang telah digariskan.
2. Pastikan bahwa sistem, aplikasi, data, dan dokumentasi yang dipelihara atau diproses oleh pihak ketiga dilindungi atau diamankan secara memadai. Pertimbangkan untuk meminta pengembalian cadangan dari pihak ketiga. Pertimbangkan pengaturan eskro atau setoran.
3. Dengan menetapkan persyaratan untuk penyimpanan data cadangan di lokasi dan di luar lokasi yang memenuhi persyaratan bisnis yang ada. Pertimbangkan aksesibilitas yang diperlukan untuk menyalin data.
4. Meluncurkan kesadaran dan pelatihan BCP.
5. Menguji dan menyegarkan data arsip dan data cadangan secara teratur.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS04.07, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan penyimpanan dan pengarsipan data telah telah berjalan dan dilaksanakan dengan baik. Level kapabilitas sudah mencapai level dua, Managed. Tabel 5 menjelaskan atribut pemetaan proses IT Processes DSS04 dan penentuan nilai kapabilitas.

Berdasarkan hasil wawancara dan kuesioner yang dilakukan, yang dituangkan dalam Tabel 5, dapat dilihat pada proses IT DSS04.03, DSS04.04, DSS04.05, DSS04.06, dan DSS04.07 mencapai PA 2.2 (sepenuhnya tercapai) sehinggacapability level berada pada level 2. Sedangkan pada sub proses DSS04.01 dan DSS04.02

DOI: https://doi.org/10.37365/jti.v9i1.153
VOL. 9 No. 1 Juni 2023
P-ISSN : 2460-2108
E-ISSN : 2620-5181

baru mencapai PA 1.1 yang menandakan bahwacapability level belum mencapai level 2 dan hanya level 1.

Pada Tabel 6, hasil DSS04 (Manage Continuity) menunjukkan tingkat kapabilitas keseluruhan pada subproses DSS04 dan hasil rata-rata untuk Proses TI DSS04 itu sendiri.

Table 6. *Results of DSS04 Manage Continuity*

No	Sub Domain	Process Attributes	Capability Level	Expected Level
DSS 04-01	Define The Business Continuity Policy, Objectives, And Scope	1,1	1	3
DSS 04-02	Maintain A Continuity Strategy	1,1	1	3
DSS 04-03	Develop And Implement A Business Continuity Response	2,2	2	3
DSS 04-04	Exercise, Test, And Review The BCP	2,2	2	3
DSS 04-05	Review, Maintain And Improve The Continuity Plan	2,2	2	3
DSS 04-06	Conduct Continuity Plan Training	2,2	2	3
DSS 04-07	Manage Backup Arrangements	2,2	2	3
	Average		1,7	3

Sumber: (Honni et al., 2023)

3. DSS05 *Manage Security Services*

Pada tahap ini, penulis akan menganalisis meminimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional, dengan deskripsi proses melindungi informasi perusahaan untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan mengikuti kebijakan keamanan. Menetapkan dan memelihara peran keamanan informasi dan hak akses serta melakukan pemantauan keamanan. Tingkat kapabilitas proses yang diharapkan dari DSS05 manage security services adalah level 3, Didirikan. Berikut ini adalah tujuan proses dari DSS05 (Manage Security Services):

1. Keamanan jaringan dan komunikasi harus memenuhi persyaratan bisnis yang ditetapkan.
2. Informasi yang telah diproses, disimpan, dan dikirim oleh perangkat endpoint diperlukan dan harus dilindungi.
3. Semua pengguna dapat diidentifikasi secara unik dan juga memiliki hak akses sesuai peran bisnisnya.
4. Tindakan fisik diterapkan untuk menjaga informasi dari akses, kerusakan, dan interferensi yang tidak sah saat diproses, disimpan, atau dikirim.
5. Informasi elektronik diamankan secara memuaskan saat disimpan, dikirim, atau dimusnahkan.

3.1 DSS05.01 Protect Against Malware

Terapkan dan pertahankan proses pencegahan, detektif, dan korektif yang ada (kebanyakan patch keamanan dan kontrol virus terbaru) di seluruh perusahaan untuk melindungi sistem dan teknologi informasi dari malware (mis., virus, worm, spyware, spam). Berikut adalah kegiatan dari proses tersebut:

1. Komunikasikan kesadaran akan perangkat lunak berbahaya serta terapkan prosedur pencegahan dan tanggung jawab.
2. Instal dan aktifkan alat perlindungan perangkat lunak berbahaya di semua fasilitas pemrosesan yang ada, dengan file definisi perangkat lunak berbahaya yang diperbarui sesuai kebutuhan perusahaan.
3. Dengan mendistribusikan semua perangkat lunak perlindungan secara terpusat menggunakan konfigurasi terpusat dan manajemen perubahan.
4. Dengan secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau nasihat keamanan produk dan layanan vendor).
5. Melakukan pelatihan berkala tentang malware dalam penggunaan email dan internet. Latih pengguna untuk tidak menginstal perangkat lunak yang dibagikan atau tidak disetujui.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan aktivitas COBIT 5 sub-domain DSS05.01, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit manajemen keamanan IT cukup baik bagus. Hal ini terlihat dari organisasi TI yang terorganisir dan keamanan data yang terjamin dengan aplikasi keamanan yang aman. Level kapabilitas sudah mencapai level dua, *Managed*.

3.2 DSS05.02 *Manage Network And Connectivity Security*

Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi keseluruhan metode konektivitas informasi. Berikut adalah kegiatan dari proses tersebut:

1. Penilaian risiko yang didukung dan persyaratan bisnis menetapkan dan memelihara kebijakan untuk keamanan konektivitas.
2. Izinkan hanya perangkat resmi yang memiliki akses ke informasi perusahaan dan oleh karena itu, jaringan perusahaan. Konfigurasikan perangkat ini untuk memaksa entri kata sandi.

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbud No.105/E/KPT/2022, 7 April 2022. Diterbitkan oleh LPPM STMIK Widuri

3. Menerapkan mekanisme penyaringan jaringan, seperti firewall dan perangkat lunak pendeteksi intrusi, dengan kebijakan yang sesuai untuk mengatur lalu lintas masuk dan keluar.
4. Mengenkripsi informasi dalam perjalanan sesuai dengan klasifikasinya.
5. Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.
6. Melakukan pengujian keamanan sistem secara berkala untuk mengetahui kecukupan perlindungan sistem.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS05.02, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa PT Anugerah Familindo Lestari telah melakukan perencanaan keamanan data dan pembaruan perangkat lunak. Level kapabilitas sudah mencapai level dua, *Managed*.

3.3 DSS05.03 *Manage Endpoint Security*

Pastikan bahwa titik akhir (misalnya, laptop, desktop, server, dan perangkat atau perangkat lunak seluler dan jaringan lainnya) diamankan pada tingkat yang sama dengan atau lebih besar dari persyaratan keamanan yang ditentukan oleh informasi yang diproses, disimpan, atau dikirim. Berikut adalah kegiatan dari proses tersebut:
1. Konfigurasikan sistem operasi dengan cara yang aman.
2. Terapkan mekanisme penguncian perangkat.
3. Mengenkripsi informasi dalam penyimpanan sesuai dengan klasifikasinya.
4. Kelola akses dan kontrol jarak jauh.
5. Kelola konfigurasi jaringan dengan cara yang aman.
6. Menerapkan pemfilteran lalu lintas jaringan pada perangkat endpoint.
7. Lindungi integritas sistem.
8. Berikan perlindungan fisik pada perangkat endpoint.
9. Hilangkan perangkat endpoint dengan aman.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS05.03, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit adalah seluruh kegiatan yang berkaitan dengan akses aplikasi dan proses absensi menggunakan sidik jari berbasis IT yang direkam dan dipantau. Level kapabilitas sudah mencapai level dua, Managed.

3.4 DSS05.04 *Manage User Identity and Logical Access*

Memastikan bahwa semua pengguna memiliki hak akses terhadap informasi yang harus sesuai dengan kebutuhan bisnisnya dan berkoordinasi dengan unit bisnis yang mengelola hak aksesnya dalam proses bisnis. Berikut adalah kegiatan dari proses tersebut:
1. Menjaga hak akses pengguna dengan mengikuti fungsi bisnis dan persyaratan proses yang telah ditentukan sebelumnya. Selain itu, juga harus menyelaraskan manajemen identitas dan hak akses dengan peran dan tanggung jawab yang telah ditentukan sebelumnya, didukung prinsip-prinsip yang paling tidak diistimewakan, perlu dimiliki dan perlu diketahui.
2. Secara unik mengidentifikasi semua kegiatan ilmu informasi berdasarkan peran fungsional, berkoordinasi dengan unit bisnis untuk memastikan bahwa setiap peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam aplikasi proses bisnis.
3. Otentikasi semua akses ke aset informasi yang mendukung klasifikasi keamanannya, berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan dalam proses bisnis untuk memastikan bahwa kontrol otentikasi dikelola dengan tepat.
4. Mengelola semua perubahan terhadap hak akses (penciptaan, modifikasi dan penghapusan) yang berlaku pada waktu yang dapat diterima hanya berdasarkan transaksi yang disetujui dan didokumentasikan yang disahkan oleh individu manajemen yang ditunjuk.
5. Dengan melindungi jejak audit dari akses ke informasi yang tergolong sangat sensitif.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS05.04, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa setiap pegawai yang bertanggung jawab untuk pengguna aplikasi memiliki akun tersendiri yang merupakan bagian dari tanggung jawab karyawan. Setiap karyawan dengan posisi yang berbeda memiliki akses yang berbeda. Tingkat kemampuan subdomain ini adalah level satu, Performed.

3.5 DSS05.05 *Manage Physical Access to IT Assets*

Menentukan dan melaksanakan prosedur untuk menyediakan, membatasi, dan mencabut akses bangunan, bangunan, dan area sesuai dengan kebutuhan bisnis di suatu perusahaan, termasuk keadaan darurat. Akses ke tempat, fasilitas, dan tempat harus dibenarkan, disahkan, dicatat, dan juga akan dipantau. Ini harus berlaku untuk semua orang yang telah memasuki lokasi, termasuk staf, staf sementara, klien, vendor, pengunjung, atau pihak ketiga lainnya. Berikut adalah kegiatan dari proses tersebut:
1. Mengelola permintaan dan juga memberikan akses ke fasilitas komputasi. Selain itu, permintaan akses formal harus diselesaikan dan disahkan oleh manajemen situs TI, dan oleh karena itu catatan permintaan disimpan. Formulir tersebut harus secara khusus mengidentifikasi area di mana individu diberikan akses.

DOI: https://doi.org/10.37365/jti.v9i1.153
VOL. 9 No. 1 Juni 2023
P-ISSN : 2460-2108
E-ISSN : 2620-5181

2. Pastikan profil akses tetap terkini. Mendasarkan akses ke situsnya (ruang server, gedung, area, atau zona) pada fungsi dan tanggung jawab pekerjaan.
3. Masuk dan pantau semua titik masuk ke situsnya. Daftarkan semua pengunjung, termasuk kontraktor dan vendor, ke lokasi.
4. Instruksikan semua personel untuk menampilkan identifikasi yang terlihat sesedikit mungkin. Mencegah penerbitan kartu identitas atau lencana tanpa otorisasi yang tepat.
5. Mengharuskan pengunjung dikawal sesingkat mungkin saat berada di lokasi. Jika tanpa pendamping, individu asing yang tidak memakai tanda pengenal staf, petugas keamanan waspada.
6. Lakukan pelatihan kesadaran keamanan fisik secara teratur.

Table 7. *Mapping Process Attributes Form* (DSS05)

IT Processes	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
DSS05-01	F	F	F	N	N	N	N	N	N
DSS05-02	F	F	F	N	N	N	N	N	N
DSS05-03	F	F	F	N	N	N	N	N	N
DSS05-04	F	F	N	N	N	N	N	N	N
DSS05-05	F	N	N	N	N	N	N	N	N
DSS05-06	F	F	F	N	N	N	N	N	N
DSS05-07	F	F	F	N	N	N	N	N	N

Sumber: (Honni et al., 2023)

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS05.05, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit pada PT Anugerah Familindo Lestari, selalu dilakukan dengan menguji dan memantau keamanan data terkait TI. Proses bisnis ini dibuktikan dengan pemeliharaan rutin oleh TI yang dilakukan minimal satu kali setiap bulan, namun belum ada manajemen yang mengatur proses tersebut. Tingkat kemampuan subdomain ini adalah level satu, Performed.

3.6 DSS05.06 *Manage Sensitive Documents And Output Devices*

Tetapkan perlindungan fisik yang sesuai dengan praktik akuntansi dan manajemen inventaris untuk aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan, printer tujuan khusus, atau sistem keamanan. Berikut adalah kegiatan dari proses tersebut:
1. Menetapkan prosedur untuk mengontrol penerimaan, penggunaan, penghapusan dan pembuangan formulir-formulir tertentu dan alat-alat keluaran ke dalam, di dalam dan di luar perusahaan.
2. Menetapkan hak akses ke dokumen sensitif dan perangkat keluaran yang mendukung prinsip hak istimewa, menyeimbangkan risiko dan persyaratan bisnis.
3. Buat daftar dokumen sensitif dan perangkat keluaran dan lakukan rekonsiliasi secara teratur.
4. Tetapkan perlindungan fisik yang sesuai atas bentuk-bentuk tertentu dan perangkat sensitif.
5. Hancurkan informasi sensitif, dan lindungi perangkat (misalnya, degaussing media elektronik, penghancuran fisik perangkat memori, sediakan mesin penghancur kertas atau keranjang kertas yang dikunci untuk membatasi formulir tertentu dan kertas rahasia lainnya).

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan kegiatan COBIT 5 sub-domain DSS05.06, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit adalah setiap kejadian atau kejadian di setiap cabang akan direview di departemen lain dan menjadi pelajaran agar tidak terjadi lagi. Level kapabilitas sudah mencapai level dua, Managed.

3.7 DSS05.07 *Monitor The Infrastructure For Security-Related Events*

Menggunakan alat deteksi intrusi, pantau infrastruktur untuk akses data yang tidak kompatibel, dan verifikasi setiap insiden yang terintegrasi dengan pemantauan insiden umum dan manajemen insiden. Berikut adalah kegiatan dari proses tersebut:
1. Mencatat peristiwa terkait keamanan yang dilaporkan oleh alat pemantauan keamanan infrastruktur, mengidentifikasi sejauh mana data yang akan direkam didukung pertimbangan risiko. Pertahankan mereka untuk jangka waktu yang tepat untuk membantu penyelidikan di masa depan.
2. Mendefinisikan dan mengkomunikasikan karakter dan karakteristik insiden terkait keamanan yang potensial sehingga sering mudah dikenali, dan dampaknya dipahami untuk memungkinkan respons yang proporsional.
3. Tinjau log peristiwa secara teratur sehingga kami dapat mengetahui tentang potensi insiden.4. Pertahankan prosedur pengumpulan bukti sejalan dengan aturan bukti forensik lokal dan pastikan bahwa semua staf dibuat sadar akan keinginan tersebut.
4. Pastikan tiket insiden keamanan dibuat tepat waktu saat pemantauan mengidentifikasi potensi insiden keamanan.

Berdasarkan hasil observasi, wawancara, dan kuesioner yang telah dilakukan berdasarkan aktivitas COBIT 5 sub-domain DSS05.07, terdapat temuan audit berdasarkan kondisi organisasi sebagai berikut: Hasil audit menunjukkan bahwa keamanan aplikasi sistem

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbud No.105/E/KPT/2022, 7 April 2022. Diterbitkan oleh LPPM STMIK Widuri

yang digunakan oleh PT Anugerah Familindo Lestari berguna, membatasi akses untuk setiap karyawan dan keamanan aplikasi yang terjamin. Level kapabilitas sudah mencapai level dua, Managed. Pada Tabel 7 menjelaskan atribut pemetaan proses IT *Processes* DSS05 dan penentuan nilai kapabilitas.

Table 8. DSS05 *Managed Security Services*

No.	Sub Domain	Process Attributes	Capability Level	Expected Level
DSS05-01	Protect Against Malware	2,2	2	3
DSS05-02	Manage Network And Connectivity Security	2,2	2	3
DSS05-03	Manage Endpoint Security	2,2	2	3
DSS05-04	Manage User Identity And Logical Access	2,1	1	3
DSS05-05	Manage Physical Access To IT Assets	1,1	1	3
DSS05-06	Manage Sensitive Documents And Output Devices	2,2	2	3
DSS05-07	Monitor The Infrastructure For Security-Related Events	2,2	2	3
	Average		1,7	3

Sumber: (Honni et al., 2023)

KESIMPULAN

Proses absensi sidik jari sudah berjalan namun belum optimal, diharapkan PT. Anugerah Familindo Lestari dapat menggunakan penelitian ini sebagai referensi untuk pengembangan selanjutnya. Saran untuk penelitian selanjutnya Audit Sistem Informasi dapat dilakukan secara rutin setiap periode tertentu, dan dapat dicapai level yang diinginkan secara keseluruhan, tidak hanya pada sistem absensi, sehingga semua aspek operasional kerja juga dapat dievaluasi sehingga dapat meningkatkan kinerja perusahaan/instansi.

DAFTAR PUSTAKA

Aisyah, S., Cakranegara, P. A., & Sani, A. J. R. R. d. E.-J. M. I. K. (2022). Pengaruh Lingkungan Kerja dan Insentif Terhadap Kinerja Karyawan PT. Capella Medan. *6*(4), 864-874.

Budiarta, K., Iskandar, A. P. S., Sudarma, M. J. I. J. o. E., & Technology, E. (2016). Audit Information System Development using COBIT 5 Framework. *1*(1), 3-7.

Corfield, L., Schizas, A., Williams, A., and Noorani, A. (2008). Non-attendance at the colorectal clinic: A prospective audit," Ann. R. Coll. Surg. Engl. doi:10.1308/003588408X301172Croteau, A.-M., & Bergeron, F. J. T. j. o. s. i. s. (2001). An information technology trilogy: business strategy, technological deployment and organizational performance. *10*(2), 77-99.

Drljača, D., & Latinović, B. J. J.-A. (2017). Frameworks for audit of an information system in practice. *12*(2).

Firdaus, D., Widya Nurwahyuni Propitari. (2018). Attendance Record Program With Web-Based Design For Field Employees In Pt. Putra Maju Lestari. *International Research Journal of Computer Science, 3*.

Gatrad, A. J. A. o. D. i. C. (2000). A completed audit to reduce hospital outpatients non-attendance rates. *82*(1), 59-61.

Moeller, B., Erek, K., Loeser, F., & Zarnekow, R. (2013). How sustainable is COBIT 5? Insights from theoretical analysis and empirical survey data.

Mulyadi, D. (2020). The Impact of Fingerprint Attendance and Compensation Systems toward Discipline and Performance of Employees. *International Journal of Advanced Science and Technology, 29(7), 1773 - 1784.*

Musa, S. S. D., Kamardin, N. D., dan Malak, H. A. (2017). Audit committee attendance and Earnings Management in Nigeria. *Asian J. Multidiscip. Stud., vol. 5, no. 3, p. 8.*

Olagunju, M., Adeniyi, A., & Oladele, T. J. I. J. o. C. A. (2018). Staff attendance monitoring system using fingerprint biometrics. *179*(21), 8-15.

Sani, A., Budiyantara, A., Haryanto, T., Wiliani, N., Manaf, K., Firmansyah, E. J. T. E., & Management. (2020). Influences of the Environmental Context on the Acceptance and Adoption Technology among SMEs in Indonesia. *83*, 22283-22293.

Saraswat, C., Kumar, A. J. I. J. o. C. S., & Engineering. (2010). An efficient automatic attendance system using fingerprint verification technique. *2*(02), 264-269.

Sequeira, A. F., & Cardoso, J. S. J. S. (2015). Fingerprint liveness detection in the presence of capable intruders. *15*(6), 14615-14638.

Stewart, J., and Munro, L. (2007). The Impact of Audit Committee Existence and Audit Committee Meeting Frequency on the External Audit: Perceptions of Australian Auditors," Int. J. Audit. doi:10.1111/j.1099-1123.2007.00356.x

Wijaya, R., and Andry, J. F. (2017). Performance measurement of JP soft application using COBIT 5 framework. Regist. J. Ilm. Teknol. Sist. Inf., . doi:10.26594/register.v3i2.1121