

IMPLEMENTASI *FRAMEWORK* COBIT 5.0 FOKUS DOMAIN *DELIVERY, SUPPORT, DAN SERVICE* PADA PT.XYZ

Yunda Heningtyas¹, Indah Mayatika Sihaloho², Akmal Junaidi³

Universitas Lampung

Jl. Prof. Dr. Sumantri Brojonegoro No. 1 Bandar Lampung Telp: 0721-701609 Fax: 0721-702767

yunda.heningtyas@fmipa.unila.ac.id¹, indah.mayatika1069@students.unila.ac.id²,
akmal.junaidi@fmipa.unila.ac.id

Abstract

XYZ company has implemented information technology in the company's operations. Information technology management audits are needed to find out whether the application of information technology is in accordance with the company's control standards. The framework used in this research was COBIT 5.0 domain that is DSS (Delivery, support, dan service) because the DSS domain includes has IT management scope, data management scope, and facility operational scope. This research aimed to evaluate information technology management at the company. Audit results shows that the company's capability level in 4th level (Predictable Process). Predictable Process means that DSS domain process has been standarized, do the IT process, and achieved process. Capability level that the company wants to be achieve is 5th level (Optimizing Process). To achieve this level, companies must innovate and make sustainability improvements.

Keywords: *COBIT 5.0 Framework, Delivery, support, dan service, DSS Domain, IT Management of Audit*

Abstrak

PT. XYZ adalah perusahaan yang telah menerapkan teknologi informasi dalam operasional perusahaan. Audit manajemen teknologi informasi diperlukan untuk mengetahui apakah penerapan teknologi informasi sudah sesuai dengan standar control perusahaan. Framework yang digunakan dalam penelitian ini adalah COBIT 5.0 domain yang DSS (Delivery, support, dan service) karena domain DSS mencakup pengelolaan layanan teknologi informasi, pengelolaan data, dan operasional fasilitas. Penelitian ini bertujuan untuk mengevaluasi manajemen teknologi informasi pada perusahaan tersebut. Berdasarkan hasil audit, capability level perusahaan berada pada level 4 (Predictable Process). Predictable Process diartikan proses domain DSS pada perusahaan telah terstandarisasi, melakukan proses sesuai dengan standar yang ditetapkan, dan mencapai hasil dari proses tersebut. Namun, expected level yang ingin dicapai perusahaan adalah level 5 (Optimizing Process). Untuk mencapai level tersebut, perusahaan harus membuat inovasi dan melakukan perbaikan yang berkelanjutan.

Kata kunci: *Audit Manajemen Teknologi Informasi, Delivery, support, dan service, Domain DSS, Framework COBIT 5.*

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) memberikan manfaat yang potensial dalam lingkungan bisnis yang sangat kompetitif [1]. Penggunaan TI yang tepat dapat mendukung tercapainya sasaran visi, misi, dan tujuan perusahaan. TI yang diimplementasikan dengan baik pada perusahaan akan meningkatkan kualitas layanan yang kompleks dan terintegrasi. Salah satu perusahaan yang telah lama menerapkan TI dalam kegiatan operasional perusahaan adalah PT XYZ. PT. XYZ merupakan perusahaan yang bergerak dalam jasa penjualan, perawatan, perbaikan dan suku cabang salah satu merk sepeda motor di Indonesia. Salah satu peran TI di PT. XYZ adalah adanya sistem informasi yang membantu proses penyelenggaraan operasional perusahaan. Sistem informasi tersebut adalah sistem informasi TEDS. TEDS merupakan sistem informasi yang digunakan untuk operasional, *backoffice*, serta pemasaran.

Kegiatan bisnis perusahaan mendapat dukungan penuh dari bidang TI dengan cara memperbaiki layanan TI perusahaan seperti menyelesaikan masalah *system error* dan koneksi internet perusahaan yang terkadang mengalami kendala. Bidang TI memegang peranan penting pada perkembangan bisnis perusahaan sehingga perusahaan harus melakukan evaluasi secara berkala terhadap standar kontrol bidang TI. Salah satu cara untuk melakukan evaluasi terhadap standar kontrol bidang TI adalah melakukan audit manajemen TI. Namun, PT XYZ belum pernah mengevaluasi apakah standar kontrol bidang TI telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis sesuai dengan *business processes* perusahaan.

Untuk dapat mengetahui sejauh mana pengelolaan layanan TI, layanan data, dan operasional fasilitas pada perusahaan berjalan dengan efektif dan efisien, *framework* yang dapat digunakan adalah COBIT 5.0 dengan fokus domain DSS (*Delivery, support, dan service*) [2]. COBIT 5.0 juga mendukung adanya penilaian resiko perusahaan berdasarkan tingkat kemampuan perusahaan dalam melakukan proses-proses yang telah didefinisikan [3]. Penilaian resiko tersebut dikenal dengan istilah *capability model* [3].

Audit TI pada layanan konsumen di PT XYZ ini bertujuan untuk mengetahui apakah layanan TI yang diberikan kepada konsumen sudah mengimplementasikan seluruh *business processes* perusahaan secara efektif dan efisien. Berdasarkan hasil temuan dan analisis yang dilakukan, penelitian ini diharapkan dapat memberikan rekomendasi yang tepat untuk meningkatkan layanan konsumen pada PT XYZ.

2. METODOLOGI PENELITIAN

Fokus domain pada *framework* COBIT 5.0 yang dibahas dalam penelitian ini adalah DSS. Tahap pelaksanaan audit diawali dengan mengumpulkan data-data yang diperlukan dalam proses audit. Pengumpulan data dilakukan melalui observasi, wawancara, dan kuisisioner. Observasi dilakukan untuk mengetahui kondisi nyata layanan TI perusahaan. Wawancara dilakukan secara langsung kepada supervisor TI PT XYZ. Pertanyaan yang diajukan selama proses wawancara

berkaitan dengan *business processes* dan penerapan sistem informasi TEDS. Selain itu, proses wawancara juga dilakukan untuk mendapatkan data berupa profil perusahaan, struktur organisasi, *job desk*, dan proses bisnis perusahaan.

Tahap selanjutnya adalah menentukan objek yang akan terlibat dalam kegiatan audit menggunakan RACI (*Responsible, Accountable, Consulted, Informed*) *Chart*. RACI *Chart* merupakan matrik aktivitas dan wewenang pada organisasi yang membantu dalam mengambil keputusan [4]. RACI *Chart* dilakukan untuk mendapatkan data yang akurat melalui penyebaran kuisisioner. Kuisisioner hanya dibagikan kepada stakeholder dengan status R (*Responsible*) dalam RACI *Chart*. Status R merupakan pelaksana yang memiliki tanggung jawab kegiatan operasional, memenuhi kebutuhan dan menciptakan hasil yang diinginkan dari organisasi [4]. Hasil pemetaan menggunakan RACI *Chart* mendapatkan 5 orang responden yaitu manager TI, admin/*helpdesk* TI, supervisor TI, *Network and Infrastructur* TI, dan staf *sales* promosi (bisnis). Penyebaran kuisisioner ini dilakukan untuk mendapatkan tanggapan dari 5 orang responden untuk mengetahui kondisi nyata pada bagian TI perusahaan.

Tahap selanjutnya adalah penentuan *capability level*. *Capability level* merupakan proses penilaian berdasarkan tingkat kemampuan organisasi dalam melakukan proses-proses yang telah didefinisikan dalam model *assessment* [5]. *Capability level* memiliki 6 tingkatan dengan rentang nilai seperti Tabel 1.

Tabel 1. Pemetaan Rentang Nilai Kapabilitas [6]

Rentang Nilai	<i>Capability level</i>	Nilai Kapabilitas
0 – 0,50	0 – <i>Incomplete Process</i>	0,00
0,51 – 1,50	1 – <i>Performed Process</i>	1,00
1,51 – 2,50	2 – <i>Managed Process</i>	2,00
2,51 – 3,50	3 – <i>Established Process</i>	3,00
3,51 – 4,50	4 – <i>Predictable Process</i>	4,00
4,51 – 5,00	5 – <i>Optimizing Process</i>	5,00

Berikut ini merupakan penjelasan untuk masing-masing tingkatan dalam *capability model*, yaitu [8]:

a. Level 0 - *Incomplete Process*

Incomplete Process tidak diimplementasikan atau gagal untuk mencapai tujuan prosesnya. Pada level ini hanya ada sedikit atau tidak ada bukti pencapaian sistematis dari tujuan proses.

b. Level 1 - *Performed Process*

Tujuan dari *Performed Process* umumnya tercapai, tetapi pencapaian mungkin tidak direncanakan dan dilacak secara ketat. Ada produk-produk kerja yang dapat diidentifikasi untuk proses, dan ini membuktikan pencapaian tujuan tersebut.

c. Level 2 - *Managed Process Proses*

Managed Process Proses ini diimplementasikan dengan cara yang terkelola (direncanakan, dimonitor, dan disesuaikan) dan produk-produk kerjanya ditetapkan secara tepat, dikontrol dan dipelihara.

d. Level 3 - *Established Process*

Established Process Proses diimplementasikan menggunakan proses yang ditentukan yang didasarkan pada proses standar dan mampu mencapai hasil prosesnya.

e. Level 4 - *Predictable Process*

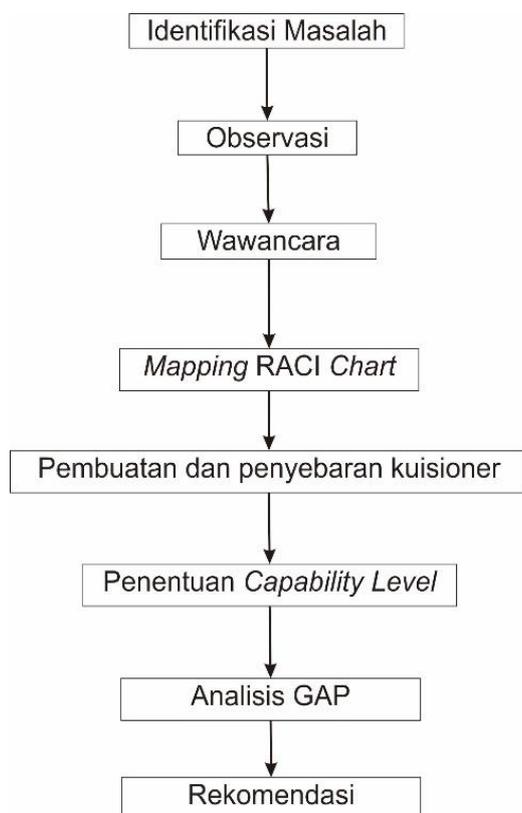
Predictable Process Proses yang didefinisikan dilakukan secara konsisten dalam praktik dan batasan kontrol yang ditentukan untuk mencapai tujuan proses yang dibutuhkan.

f. Level 5 - *Optimizing Process*

Proses terus ditingkatkan untuk memenuhi sasaran bisnis yang relevan dan yang diproyeksikan.

Penentuan *capability level* perusahaan berdasarkan hasil kuisisioner. Selanjutnya, hasil *capability level* diverifikasi oleh auditor. Proses verifikasi dilakukan untuk menyesuaikan kondisi nyata perusahaan dengan hasil kuisisioner berdasarkan bukti yang diberikan kepada auditor. Hasil verifikasi selanjutnya disebut dengan hasil temuan. Hasil temuan auditor divalidasi langsung oleh supervisor TI PT XYZ.

Tahap selanjutnya adalah menganalisis adanya gap antara hasil responden, hasil temuan, dan nilai ekspektasi perusahaan. Rekomendasi diberikan berdasarkan hasil analisis gap. Alur metodologi penelitian diilustrasikan pada Gambar 1 yang tertera di bawah ini.



Gambar 1. Alur Penelitian Audit TI COBIT 5.0

3. HASIL DAN PEMBAHASAN

3.1. Pengolahan Data Responden

Pertanyaan kuisiонер fokus pada domain DSS dengan subdomain *manage operations*, *manage service request incident*, *manage problem*, *manage continuity*, *manage security service*, dan *manage business process control*. Kuisiонер untuk subdomain *manage operation* diberikan kepada 1 orang responden. Responden menilai bahwa pengelolaan operasional perusahaan dalam bidang TI berada pada level 4 dengan rata-rata nilai 4,4. Perusahaan telah memiliki standar operational tertulis untuk subdomain *manage operation* dan telah dikelola dengan baik.

Kuisiонер untuk subdomain *manage service request and incident* diberikan kepada 3 orang responden dengan pembagian subsubdomain yang berbeda untuk masing-masing responden. Subsubdomain *defined incident and service request classification schemes* diberikan kepada 3 orang responden. Subsubdomain *record, classify and prioritise request and incidents* diberikan kepada 2 orang responden. Subsubdomain *verify, approve, and fulfil service request* diberikan kepada 3 orang responden. Subsubdomain *investigate, diagnose and allocate incident* diberikan kepada 2 orang responden. Subsubdomain *resolve and recover from incident* diberikan kepada 2 orang responden. Subsubdomain *close service requests and incidents* dan subsubdomain *track status and produce reports* masing-masing diberikan kepada 1 orang responden. Ketiga orang responden memberikan nilai

rata-rata 4,9 untuk subdomain *manage service request and incident*. Perusahaan berada pada level 4 yang berarti perusahaan telah memiliki standar operasional tertulis untuk pengelolaan layanan *service and incident* dan menerapkannya sesuai dengan standar yang ditetapkan.

Kuisisioner untuk subdomain *manage problems* diberikan kepada 3 orang responden dengan pembagian subsubdomain yang berbeda untuk masing-masing responden. Subsubdomain *identify and classify problems* diberikan kepada 3 orang responden. Subsubdomain *investigate and diagnose problems* dan *raise known errors* masing-masing diberikan kepada 1 orang responden. Subsubdomain *resolve and close problems* dan *perform proactive and close problems* masing-masing diberikan kepada 1 orang responden. Ketiga orang responden memberikan nilai rata-rata 4,6 untuk subdomain *manage problems*. Perusahaan berada pada level 4 yang berarti perusahaan telah memiliki standar operasional tertulis untuk penanganan masalah bidang TI dan menerapkannya sesuai dengan standar yang ditetapkan.

Kuisisioner untuk masing-masing subsubdomain pada subdomain *manage continuity* diberikan kepada 4 orang responden kecuali untuk subsubdomain *manage backup arrangements* hanya diberikan kepada 2 orang responden. Rata-rata penilaian responden adalah 4,6 sehingga *manage continuity* perusahaan dalam bidang TI berada pada level 4. Perusahaan telah memiliki standar operasional tertulis untuk subdomain *manage continuity* dan telah dikelola dengan baik.

Kuisisioner untuk subdomain *manage security service* diberikan kepada 3 orang responden dengan pembagian subsubdomain yang berbeda untuk masing-masing responden. Subsubdomain *protect against malware, manage network and connectivity security, manage endpoint security, dan manage sensitive documents and output devices* masing-masing diberikan kepada 1 orang responden. Subsubdomain *manage user identity and logical access* dan *monitor the infrastructure for security related events* masing-masing diberikan kepada 2 orang responden. Subsubdomain *manage physical access to IT assets* diberikan kepada 3 orang responden. Responden memberikan nilai rata-rata 4,6 untuk subdomain *manage security service*. Perusahaan berada pada level 4 yang berarti perusahaan telah memiliki standar operasional tertulis untuk penanganan pelayanan keamanan bidang TI dan menerapkannya sesuai dengan standar yang ditetapkan.

Kuisisioner untuk masing-masing subsubdomain pada subdomain *manage bussines process control* diberikan kepada 1 orang responden kecuali untuk subsubdomain *manage roles, responsibilitie, access privileges and level of authority* yang diberikan kepada 2 orang responden. Rata-rata penilaian responden adalah 5 sehingga *manage bussines process control* perusahaan dalam bidang TI berada pada level 5. Perusahaan telah memiliki prosedur tertulis untuk *manage bussines process control* yang terstandarisasi, proses bisnis telah dilaksanakan sesuai dengan standar yang ada, konsisten dan selalu diperbaharui sesuai dengan kondisi yang ada dilapangan.

Hasil rekapitulasi nilai responden dapat dilihat pada Tabel 2. Subdomain DSS COBIT 5.0 disimbolkan dengan huruf D, *capability level* responden disimbolkan dengan CL, dan *expected level* dengan EL.

Tabel 2 Rekapitulasi *Capability level* Responden

D	Proses	CL	EL
DSS 01	<i>Manage operations</i>	4,4	5
DSS 02	<i>Manage service request and incident</i>	4,9	5
DSS 03	<i>Manage Problems</i>	4,6	5
DSS 04	<i>Manage Continuity</i>	4,6	5
DSS 05	<i>Manage security service</i>	4,6	5
DSS 06	<i>Manage bussines process control</i>	5,0	5
Rata-Rata		4,68	5

Hasil *capability level* responden pada Tabel 2 menyatakan bahwa subdomain *manage bussines process control* telah memenuhi target *expected level* perusahaan. Nilai *capability level* pada subdomain DSS lainnya belum memenuhi target *expected level* perusahaan. Perusahaan harus melakukan perubahan-perubahan pada beberapa bagian proses yang belum optimal untuk mencapai target *expected level* perusahaan. Secara keseluruhan, *capability level* untuk domain DSS pada layanan konsumen di PT XYZ berada pada level 4.

3.2. Analisa GAP

Analisis gap dilakukan untuk mengetahui kesenjangan (gap) antara hasil kuisioner dengan kondisi nyata operasional perusahaan dan mencari penyebabnya. Tabel 3 merupakan perbandingan antara *capability level* (CL) perusahaan, hasil temuan auditor (HT) dan target *expected level* perusahaan. Hasil temuan diperoleh berdasarkan kondisi perusahaan saat proses audit. Nilai pada hasil temuan diperoleh berdasarkan bukti-bukti pendukung yang dimiliki perusahaan dan telah mendapatkan persetujuan dari perusahaan.

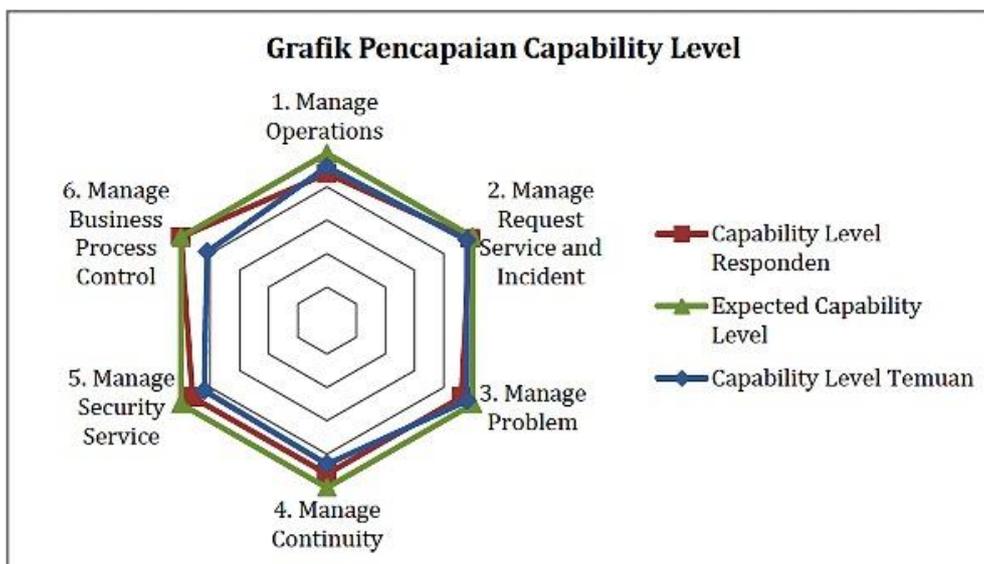
Tabel 3. Analisis GAP domain DSS

Sub Domain	CL	HT	EL
DSS01 <i>Manage operations</i>	4,4	4,6	5
DSS02 <i>Manage service request and incident</i>	4,9	4,8	5
DSS03 <i>Manage Problem</i>	4,6	4,8	5
DSS04 <i>Manage Continuity</i>	4,6	4,3	5
DSS05 <i>Manage security service</i>	4,6	4,2	5
DSS06 <i>Manage business process control</i>	5,0	4,1	5
Rata-Rata	4,68	4,46	5

Perubahan nilai pada hasil temuan subdomain *manage operations*, *manage service request incident*, *manage problem*, *manage continuity*, dan *manage security service* tidak mempengaruhi hasil akhir *capability level* perusahaan. Hasil temuan pada *manage business process control* mengalami penurunan level. Setelah dilakukan verifikasi, perusahaan telah memiliki prosedur standar secara tertulis namun perusahaan belum melakukan peninjauan secara rutin terhadap aktifitas bisnis perusahaan terkait TI dengan SOP perusahaan. Peninjauan tersebut meliputi pengelolaan penyalarsan aktifitas, pengelolaan pemrosesan informasi, pengelolaan hak akses, penanganan error, dan pengelolaan asset-aset informasi.

Pada proses *manage operations*, ditemukan perbedaan versi *Office Application* pada beberapa cabang perusahaan. Hal ini terjadi karena tidak adanya peninjauan secara berkala terhadap pemakaian *Office Application* pada cabang perusahaan. Pada proses *manage request service and incident*, perusahaan belum melakukan konfirmasi kepada *user* terhadap kepuasan atas pemenuhan permintaan layanan dan insiden. Pada proses *manage problem*, perusahaan belum melakukan laporan penyelesaian masalah secara berkala. Pada proses *manage continuity*, perusahaan belum melakukan pemeriksaan kegiatan terhadap standar operasional perusahaan mengenai hasil dari backup data. Pada proses *manage security service*, perusahaan belum melakukan pemeriksaan secara rutin dalam mengontrol hak akses yang digunakan user.

Gambar 2 menggambarkan posisi pencapaian *capability level*, nilai temuan dan *expected level* perusahaan pada domain DSS. Nilai kematangan yang diharapkan (*expected level*) dalam mengelola layanan TI pada proses *manage operations*, *manage request service and incident*, *manage problem*, *manage continuity*, *manage security service*, dan *manage business process control* adalah pada level 5. Level 5 (*optimizing process*) adalah level dimana perusahaan telah melakukan inovasi-inovasi dan melakukan perbaikan yang berkelanjutan.



Gambar 2. Grafik Pencapaian *Capability level* pada domain DSS (*Delivery, support, dan service*)

3.3. Rekomendasi

Hasil analisis gap menunjukkan adanya ketidakseuaian antara hasil responden, hasil temuan dan *expected level* pada layanan TI perusahaan. Berdasarkan hasil responden dan hasil temuan menyatakan bahwa *capability level* perusahaan yang sesungguhnya berada pada tingkat 4. Perusahaan telah menjalankan proses TI sesuai dengan SOP yang telah ditetapkan. Namun, perusahaan harus melakukan inovasi dan perbaikan yang berkelanjutan untuk dapat mencapai target level yang diinginkan. Adapun rekomendasi yang diberikan untuk perbaikan perusahaan di masa depan dijelaskan pada Tabel 4.

Tabel 4. Rekomendasi Hasil Audit

Sub Domain	Masalah yang Terjadi	Rekomendasi
DSS01 <i>Manage operations</i>	Belum terstandarisasinya pemakaian <i>Office Application</i> di <i>desktop</i> aplikasi yang ada di tiap cabang.	Bidang TI PT. XYZ harus selalu memperbaharui versi <i>office</i> yang digunakan untuk setiap cabang perusahaan. Kegiatan ini harus diimbangi dengan pengawasan oleh setiap staf cabang untuk memastikan sudah dilakukan dengan benar.
DSS02 <i>Manage service request and incident</i>	Belum adanya verifikasi SOP/ <i>form</i> yang diberikan kepada pihak pengguna yang meminta layanan kepada bidang TI untuk menyelesaikan masalah layanan.	Pembuatan <i>form</i> verifikasi terselesaikannya masalah oleh bidang TI ketika penanganan masalah layanan telah terselesaikan. <i>Form</i> ini dibagikan kepada pihak yang mengajukan <i>form</i> layanan.
DSS03 <i>Manage Problem</i>	Belum adanya laporan yang menyimpan keseluruhan <i>error</i> sistem.	Pembuatan fungsi <i>troubleshooter</i> (penangkap masalah) oleh bidang TI pada sistem informasi perusahaan untuk mengetahui kesalahan/ <i>error</i> yang terjadi dan menyimpan setiap insiden kerusakan secara otomatis.
	Belum adanya <i>form</i> peninjauan laporan kemajuan penyelesaian masalah. <i>Form</i> layanan ini penting, untuk mengetahui sudah sejauh mana masalah pada layanan IT sedang diselesaikan.	Pembuatan <i>form</i> peninjauan kemajuan masalah oleh bidang TI mengenai kemajuan penanganan masalah yang sedang diselesaikan. <i>Form</i> ini sebaiknya dibuat dalam bentuk aplikasi <i>website internal</i> supaya pihak-pihak yang terkait dengan masalah mengetahui perkembangan masalah tersebut.

Sub Domain	Masalah yang Terjadi	Rekomendasi
DSS04 <i>Manage Continuity</i>	Belum adanya jadwal rutin oleh bidang TI untuk melakukan pemeriksaan <i>backup</i> data yang dilakukan.	Pembuatan <i>backup</i> data otomatis oleh bidang TI dan pembuatan jadwal rutin secara berkala untuk memastikan proses <i>backup</i> data sudah ter-cover dengan aman di <i>backup tape rotation method</i> yang digunakan.
	Belum adanya evaluasi oleh bidang TI terhadap BCP (<i>Business Continuity Plan</i>).	Bidang TI membuat <i>form</i> daftar apa yang perlu dievaluasi. Hal ini, dilakukan oleh staf khusus untuk membuat jadwal evaluasi dan mengevaluasi kegiatan dengan SOP yang ada. <i>Form</i> daftar evaluasi ini dapat membantu mengetahui hal apa saja yang sudah terpenuhi dan membuat inovasi-inovasi bisnis selanjutnya.
DSS05 <i>Manage security service</i>	Belum adanya jadwal piket untuk melakukan pemeriksaan rutin terhadap antivirus pada komputer kerja.	Bidang TI membuat jadwal piket untuk melakukan pemeriksaan terhadap <i>update</i> semua <i>software</i> . Hal ini harus dilakukan secara konsisten dan optimal guna memastikan data perusahaan pada komputer aman dan tidak terdeteksi serangan virus.
	Belum adanya standar operasional mengenai otorisasi terhadap <i>devices</i> yang boleh mengakses informasi perusahaan dan jaringan perusahaan.	Pembuatan standar operasional yang terdokumentasi dan melakukan <i>setting</i> otorisasi terhadap <i>devices</i> yang boleh mengakses informasi perusahaan dan jaringan perusahaan.
DSS06 <i>Manage business process control</i>	Belum adanya kebijakan bagi pegawai ketika melakukan pelanggaran dalam penggunaan teknologi informasi.	PT. XYZ menentukan saksi pelanggaran terhadap pegawai yang melakukan pelanggaran dalam penggunaan teknologi informasi. Kegiatan ini harus diterapkan secara konsisten guna menghindari kerusakan - kerusakan teknologi pada perusahaan.
	Belum adanya standar operasional, dan kegiatan perusahaan mengenai pemeriksaan serta evaluasi rutin terhadap keamanan aset informasi.	Pembuatan standar operasional yang terdokumentasi oleh bidang TI serta pembuatan <i>form</i> daftar pemeriksaan dan evaluasi keamanan aset informasi. Kegiatan ini harus dilakukan secara konsisten dan optimal untuk menghindari pencurian data perusahaan yang sifatnya <i>private</i> dan <i>confidential</i> .

4. SIMPULAN

Hasil audit pada PT. XYZ menggunakan *framework* COBIT 5.0 dengan fokus domain DSS adalah PT XYZ berada pada *capability level 4* yaitu *Predictable Process*. Layanan bidang TI PT. XYZ telah melakukan proses-proses TI yang terstandarisasi, dilakukan, dan sudah mencapai hasil yang diinginkan. Namun, perusahaan harus mempertahankan proses yang sudah berjalan dengan baik, dan melakukan peninjauan secara rutin pada setiap proses sesuai dengan standar operasional prosedur. Selain itu, perusahaan diharapkan dapat membuat inovasi-inovasi layanan dan melakukan perbaikan yang berkelanjutan untuk mencapai *expected level 5*.

DAFTAR PUSTAKA

- [1] Sarno, R., "**Audit Sistem dan teknologi Informasi**", ITS Pres, Surabaya, 2009.
- [2] ISACA, "**COBIT 5 Enabling Process**", ISACA, United States, 2012.
- [3] ISACA, "**COBIT 5 A Business Framework for the Governance and**
- [4] **Management Enterprise IT**", ISACA, United States, 2012.
- [5] ISACA, "**COBIT 5 Implementation**", ISACA, United States, 2012.
- [6] ISACA, "**COBIT 5 Process Assessment Model (PAM)**", ISACA, United States, 2012.
- [7] Surendro, K., "**Pengembangan Rencana Induk Sistem Informasi, Bandung: Penerbit Informatika**", 2009.
- [8] ISO/IEC 15504-2, "**Information Technology - Process Assessment - Part 2: Performing an Assessment**", ISO/IEC, Switzerland, 2003.