TATA KELOLA TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT 4.1 PADA PT.DUNIA SAFTINDO

[1]Hendry Himayadi, [2]Johanes Fernandes Andry
[1,2]Sistem Informasi, Fakultas Teknik dan Desain, Universitas Bunda Mulia,
Jl. Lodan Raya No. 2 Ancol, Jakarta Utara 14430, telp (021) 690 9090/fax Fax: (021) 690-9712
Email: hendryhimayadi14 @gmail.com, jandry@bundamulia.ac.id

(Diterima: 5 Maret 2019, direvisi: 13 Mei 2019, disetujui: 21 Juli 2019)

ABSTRAK

PT.Dunia Saftindo adalah perusahaan yang bergerak di bisnis ritel yang berlokasi di Superblock Mega Kemayoran Jakarta Pusat. Perusahaan ini menjual berbagai alat kesehatan dan keselamatan seperti masker, tandu dan alat gas pemadam kebakaran. Masalah yang terjadi dalam organisasi adalah seringnya laporan gangguan kecil dari user ketika waktu kerja dan ada beberapa masalah yang tidak terlalu penting membuat departemen TI datang ke tempat untuk menyelesaikannya, dan sering kali serangan virus di seperti Denial Of Service (DOS) atau malware yang sering dikirim ke email perusahaan yang dapat mengganggu kinerja perusahaan. Sistem informasi audit dilakukan untuk mengetahui bagaimana perusahaan mengkoordinasikan kegiatan operasional dan mengelola masalah yang ada dengan mengevaluasi efektivitas sistem informasi. Penelitian ini menggunakan model kerangka kerja COBIT 4.1 dengan sub-domain PO9, AI3, AI4, DS5. Berdasarkan penelitian ini, ditemukan bahwa rata-rata sub-domain memiliki level kematangan Defined Process, artinya PT Dunia Saftindo memiliki tingkat kemampuan yang baik. Namun perlunya perhatian khusus pada bagian securitas untuk meingkatkan mutu dari sistem keamanan karena banyak serangan yang dilakukan dari pihak luar yang dapat mengganggu sistem operasional perusahaan dan untuk pengembangan bisnis diharapkan perusahaan dapat mengembangkan dengan menggunakan Enterprise Resource Planning (ERP) untuk meningkatkan mutu perusahaan serta mencegah terjadinya error untuk segala aktivitas operasional perusahaan.

Kata Kunci: PT Dunia Saftindo, Cobit 4.1, ERP

1 PENDAHULUAN

Bisnis retail merupakan kegiatan pemasaran yang untuk memenuhi kebutuhan perseorangan atau rumah tangga, bisnis retail tidak hanya dalam kategori makanan melainkan dapat berupa jasa dan barang [1]. Banyak perusahaan sekarang yang bergerak dalam bidang retail karena dilihatnya memiliki peluang bisnis yang cukup baik ,perkembangan bisnis retail dapat dilihat dari banyaknya pembukaan gerai-gerai baru baik perusahaan dalam negeri ataupun asing [2].

Perusahaan pada era sekarang membutuhkan suatu alat yang dapat membantunya dalam mencapai tujuan perusahaan, sala satu cara yang dapat dilakukan untuk membantu masalah tersebut adalah penerapan sistem informasi untuk menunjang aktifitas proses bisnis tersebut [3]. Saat ini sistem informasi merupakan suatu kebutuhan mutlak untuk kelangsungan sebuah perusahaan, sistem informasi bertugas mengelola seluruh data perusahaan dengan cepat dan akurat serta aman [4]. Keamanan data, keefektifan, keefisienan, kerahasiaan data, dan ketersediaan data harus dapat di kontrol dengan baik, sala satunya dengan COBIT *(Control Objectives for Information and Technology*) adalah kerangka dari best practices manajemen TI yang membantu organisasi untuk memaksimalkan keuntungan bisnis dari organisasi teknologi informasi (TI) mereka [5].

COBIT adalah sekumpulan dokumentasi *best practice* untuk tata kelola IT (IT *Governace)* yang dapat membantu sebagai pedoman pelaksanaan control manajemen proses dan prosedur dalam mencapai hasil yang baik bagi perusahaan, dalam cobit memiliki tingkat kematangan jika perusahaan belum mencapai tingkat kematangan yang diharapkan dari implementasi sistem maka diharapkan adanya perbaikan dari sistem yang berjalan [6]. Cobit 4.1 merupakan generasi kelima setelah Cobit 1 yang ditemukan pada tahun 1996, Cobit 2 ditemukan pada tahun 1998 [7].

Tata kelola TI Dijelaskan bahwa merupakan bagian dari pengelolaan perusahaan secara keseluruhan yang terdiri dari kepemimpinan dan struktur organisasi dari proses yang ada untuk

memastikan kelanjutan TI organisasi dan pengembangan strategi dan tujuan organisasi untuk dapat mengambil keuntungan, sehingga mendapatkan keuntungan yang kompetitiv [8]. Cobit sangat erat hubungannya dengan Information Technology Infrastructure Library (ITIL), ITIL merupakan serangkaian dokumen yang berisi serangkaian praktik terbaik untuk mengimplementasikan kerangka kerja seperti Cobit [9].

PT.Dunia Saftindo dapat disebut DSI merupakan perusahaan yang bergerak pada bisnis retail yang berlokasi pada superblock mega kemayoran jakarta pusat,perusahaan ini menjual berbagai alat kesehatan dan keamanan seperti masker, tandu dan gas pemadam kebakaran.perusahaan ini juga mengikuti perkembangan jaman dengan melibatkan sistem informasi dalam bisnisnya yaitu dengan membuat website dengan tujuan untuk dapat bersaing dipasar dan membatu perusahaan untuk bekerja lebih efektiv dan efesien sesuai dari tujuan penerapan sistem informasi. Penerapan sistem infromasi berkaitan dengan Tata kelola TI karena jika Tata kelola TI dalam perusahaan tidak berjalan dengan baik maka manfaat dari penerapan sistem informasi tidak akan maksimal, pada dasarnya tata kelola TI adalah memberikan penilaian terhadap managemen rersiko atas penerapan strategi bisnis dan TI dalam perusahaan [10]. Adapun tujuan dari penerapan audit sistem ini adalah untuk mengevaluasi dan menjadikan hasil audit sebagai masukan atau tolak ukur untuk perusahaan dikedepannya,jika memiliki tingkat kematangan yang kurang pada domain tertentu maka perusahaan dapat meningkatkan kualitas pada bagian tersebut.

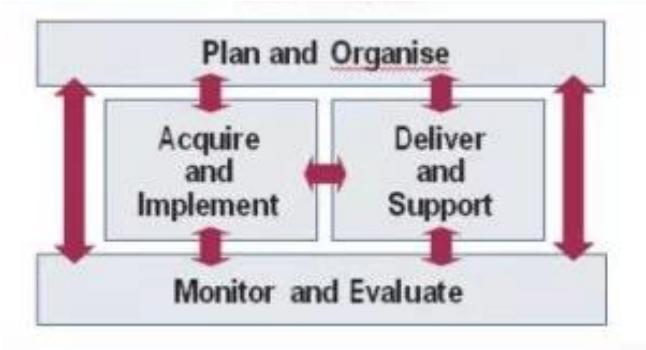
2 TINJAUAN PUSTAKA

2.1 Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi adalah tanggung jawab yang diberikan kepada dewan direksi dan manajemen eksekutif organisasi, yang merupakan bagian dari perusahaan yang mencakup kepemimpinan, struktur serta proses organisasi dan diperlukan adanya perubahan peran TI, dari peran efisiensi ke peran strategik yang memastikan bahwa teknologi informasi perusahaan dapat digunakan untuk mempertahankan dan memperluas strategi serta membantu mencapai tujuan dari organisasi [11].

2.2 Cobit 4.1

COBIT 4.1 adalah salah satu *framework* yang dapat menjadi standar dalam pelaksanaan proses auditing yang terdiri dari empat *domain* dan merupakan sebuah proses yang dapat digunakan dalam melaksanakan suatu aktivitas auditing [12]. Aktivitas teknologi informasi pada COBIT 4.1 terdapat empat domain yaitu *Plan and Organise* (PO), *Deliver and Support* (DS), *Acquire and Implement* (AI), *Monitor and Evaluate* (ME) dari keempat domain tersebut saling berhubungan pada proses auditing siklus domain dapat dilihat pada Gambar 1. siklus domain Cobit 4.1 [13].



Gambar 1. Siklus *Domain* Cobit 4.1 [13]

2.3 Tingkat Kematangan

Salah satu alat pengukur dari kinerja suatu sistem teknologi informasi adalah model kematangan (*maturity level*), model kematangan digunakan untuk mengontrol proses-proses teknologi informasi dan menentukan penilaian sekarang (*current score*) menggunakan framework COBIT 4.1 dengan informasi menggunakan metode penilaian/*scoring* [14]. Indeks penilaian Tingkat Kematangan Pengelolaan terdapat pada Tabel 1. *Maturity Level*.

Tabel 1. *Maturity Level* [14]

Level kematangan yang terdapat pada Tabel 1. *Maturity Level* memiliki penjelasan yang dapat dijabarkan sehingga perusahaan dapat mengetahui dengan level kematangan yang ada memiliki penjelasan [15]. Penjalasan level kematangan dapat dilihat pada bagian bawah ini.

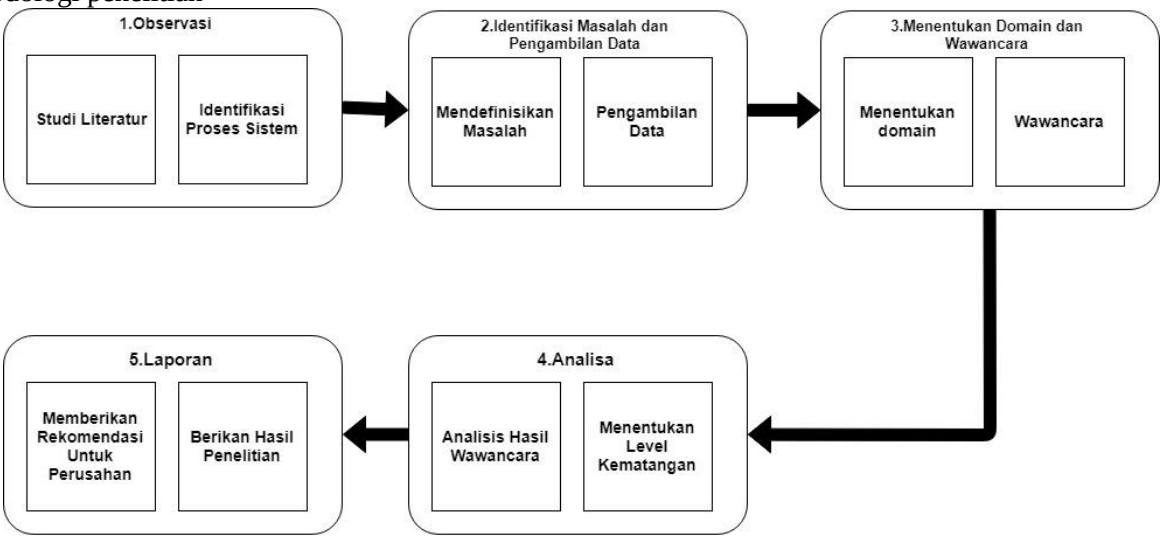
Indeks kematangan	Level Kematangan
0.00-0.49	0.*Non-Existent*
0.50-1.49	1.*Initial/Ad Hoc*
1.50-2.49	2.*Repeatable But Intutive*
2.50-3.49	3.*Defined Process*
3.50-4.49	4.*Menaged and Measurable*
4.50-5.00	5.*Optimized*

(1) Level 0 (*Non-existent*) Perusahaan tidak mengetahui dan tidak perduli sama sekali terhadap proses teknologi informasi di perusahaannya.
(2) Level 1 (*Initial Level*) Pada level ini, perusahaan pada umumnya tidak menyediakan lingkungan yang stabil untuk mengembangkan suatu produk baru. Ketika suatu organisasi memiliki kekurangan pengalaman manajemen, keuntungan dari mengintegrasikan pengembangan produk tidak dapat ditentukan. Proses pengembangan tidak dapat diprediksi dan bersifat tidak stabil, karena proses secara teratur berubah selama pengerjaan berjalan beberapa *form* dari satu proyek ke proyek lain. Kinerja tergantung pada kemampuan individual dan variasi keahlian yang dimilikinya.
(3) Level 2 (*Repeatable Level*) Pada level ini, adanya suatu kebijakan untuk mengatur pengembangan suatu proyek dan prosedur dalam mengimplementasikan kebijakan tersebut. Tingkat efektif suatu proses manajemen dalam mengembangankan proyek adalah dengan kemungkinkan perusahaan mengulangi pengalaman yang berhasil dalam mengembangkan proyek dari sebelumnya, walaupun terdapat proses yang berbeda.
(4) Level 3 (*Defined Level*) Pada level ini, proses standar dalam pengembangan suatu produk baru telah didokumentasikan, proses ini didasari pada proses pengembangan produk yang telah diintegrasikan. Proses-proses ini digunakan untuk membantu seluruh *stakeholder* pengembangan sehingga bekerja dengan lebih efektif.
(5) Level 4 (*Managed Level*) Pada level ini, perusahaan membuat suatu matrik untuk suatu produk, yang berfungsi sebagai alat ukur proses dan hasil. Proyek mempunyai kontrol terhadap produk dan proses untuk mengubah variasi proses kerja sehingga terdapat batasan yang dapat diterima.
(6) Level 5 (*Optimized Level*) Pada level ini, seluruh organisasi difokuskan pada proses peningkatan secara terus-menerus. Teknologi informasi yang digunakan sudah terintegrasi dan terotomatis pada proses bisnis perusahaan dan mampu meningkatkan kualitas, efektifitas, serta kemampuan beradaptasi perusahaan. Dengan adanya tingkatan *Maturity Model*, maka perusahaan dapat mengetahui posisi kematangannya saat ini, dan secara terus menerus berusaha untuk meningkatkan levelnya sampai tingkat tertinggi.

3 METODE PENELITIAN

Makalah ini menggunakan studi literatur dengan melakukan survei terlebih dahulu dengan menganalisis visi dan misi perusahaan, rencana strategis perusahaan serta kebijakan yang terkait dengan manajemen investasi TI dan pengamatan pada Layanan TI. Data yang dikumpulkan adalah kualitatif, berarti bahwa pertanyaan tersebut berfokus pada orang yang diwawancarai dari departemen TI tertinggi di perusahaan [16]. Setelah itu data akan diproses untuk dihitung berdasarkan perhitungan tingkat kematangan standar Cobit 4.1. Hasil audit berisi tingkat kematangan saat ini. Kemudian penulis memberikan daftar rekomendasi untuk tindakan di masa depan agar memperbaiki kelemahan perusahaan saat ini serta meningkatkan layanan TI. Fokus dari penelitian ini adalah *domain* AI 3(*Acquire and Implement*) *Acquire and Maintain Technology Infrastructure*, AI 4 *Enable Operation and Use*, PO 9 (*Plan and Organise*) *Assess and Manage IT Risks*, DS 5 (*Deliver and Support*) *Ensure Systems Security*. Pemilihan domain diberikan setalah penulis melakukan pembahasan singkat tentang Cobit 4.1 serta *domain* dan *sub-domainnya* pada manager IT DSI sehingga pemilihan domain dilakukan

oleh pihak perusahaan karena terkait masalah *privacy* perusahaan dan ketersediaan data yang diberikan. Penulis menggambarkan urutan proses dari awal sampai akhir, yang ditunjukkan pada Gambar 2 metodologi penelitian



Gambar 2. Metodologi Penelitian [16]

Pada bagian ini penulis akan menjelaskan sehubungan dengan metodologi penelitian yang ada yang dibagi menjadi 5 bagian:

(1) Pengamatan

Fase 1, penulis melakukan studi literatur yang berkaitan dengan penelitian yang akan dilakukan pada DSI.

Fase 2, penulis mengidentifikasi proses kerja hingga aplikasi berjalan pada DSI.

(2) Identifikasi Masalah dan Kumpulkan Data

Fase 1, penulis mendefinisikan masalah yang terjadi di perusahaan.

Fase 2, penulis melakukan wawancara dengan manajer departemen TI pada DSI.

(3) Tentukan Domain dan Wawancara

Fase 1, penulis menentukan domain dan proses yang relevan dengan penelitian ini.

Fase 2, penulis membuat daftar pertanyaan untuk disampaikan kepada manajer TI dan wawancara segera.

(4) Analisis

Fase 1, penulis menganalisis hasil wawancara bersama Manager IT

Fase 2, penulis menghitung tingkat kematangan dengan standar Cobit 4.1

(5) Pelaporan

Fase 1, penulis memberikan rekomendasi untuk meningkatkan kemampuan perusahaan.

Fase 2, penulis memberikan hasil laporan yang telah dibuat kepada perusahaan untuk mendapatkan umpan balik.

4 HASIL DAN PEMBAHASAN

Hasil Analisis data mencakup tentang pengukuran kinerja tingkat kematangan terhadap keamanan sistem teknologi informasi dan proses kerja yang berjalan di DSI. Data yang didapat dari hasil wawancara diolah sesuai metode COBIT 4.1. untuk mengetahui tingkat kematangan saat ini dan mengetahui tingkat kematangan yang diharapkan kedepan sehingga akan diketahui *gap* diantara tingkat kematangan saat ini dengan tingkat kematangan yang diharapkan. Berdasarkan hasil pengurukuran tersebut akan menghasilkan hasil audit yang dapat memberikan saran dan rekomendasi untuk DSI. Dalam proses audit ini domain yang menentukan dari pihak DSI karena berhubungan dengan *privacy* data perusahaan dan ketersediaan informasi untuk dapat dikelola oleh peneliti, *domain* yang digunakan adalah PO9, AI3, AI4, DS5.

PO9 (*Plan and organize) Assess and Manage IT Risks*

Pada domain ini menjelaskan tentang penilaian dan Mengelola Risiko, kerangka kerja TI manajemen risiko dibuat dan dipelihara. Kerangka kerja ini mendokumentasikan tingkat risiko TI yang umum dan disepakati dan risiko residual (selisih nilai). Setiap dampak potensial pada sasaran organisasi yang disebabkan oleh peristiwa yang tidak direncanakan perlu diidentifikasi, dianalisis dan dinilai. Strategi risiko digunakan untuk meminimalkan risiko yang diterima. Hasil dari penilaian dapat dipahami oleh para pemangku kepentingan terutama mengenai keuangan, untuk memungkinkan para pemangku kepentingan menyelaraskan risiko dengan rencana solusi dari dampak yang akan terjadi

PO9.1 *IT Risk Management Framework*

Menetapkan kerangka kerja manajemen risiko TI yang selaras dengan kerangka kerja manajemen risiko organisasi (perusahaan). Dari hasil wawancara ditemukan data bahwa DSI tidak memiliki kerangka kerja managemen risiko yang tertulis dan diimplementasikan pada organisasi tetapi DSI telah memiliki alternativ solusi untuk resiko yang akan datang, seperti penggunaan ISP (*internet Service Provider*) pada perusahaan memiliki 3 untuk menghindari kejadian jika salah satu ISP mengalami gangguan dan memiliki ISP pengganti agar aktivitas perusahaan tetap berjalan karena internet pada DSI tidak boleh *offline* lebih dari 10 menit atau perusahaan akan mengalami kerugian disebabkan segala transaksi pada DSI menggunakan internet. Dari hasil analisis data yang ada memiliki maturity level 2 karena DSI belum memiliki kerangka kerja managemen risiko yang didokumentasikan dan diimplementasikan sehingga menggunakan pengalaman sebelumnya untuk menyelesaikan suatu masalah yang ada.

PO9.2 *Establishment of Risk Context*

Pembentukan Konteks Risiko Tetapkan konteks di mana kerangka kerja penilaian risiko diterapkan untuk memastikan hasil yang sesuai. Ini harus mencakup menentukan konteks internal dan eksternal dari setiap penilaian risiko, tujuan penilaian, dan kriteria terhadap risiko yang mana dievaluasi. Dari hasil wawancara ditemukan data bahwa DSI belum ada konteks risiko untuk dapat menilai risiko yang akan terjadi sehingga tidak dapat mengevaluasi tingkat risiko yang terjadi tetapi DSI memiliki planning risiko untuk menaggulanginya pada saat risiko terjadi seperti untuk infrastruktur internal maupun external seperti jaringan eror yang dapat langsung diperbaiki oleh departemen IT dan kerusakan pada *hardware* dapat di *swipe* (diganti) dengan mesin baru. Untuk layanan ISP jika terjadi *error* akan dilimpahkan pada pihak ketiga untuk memperbaikinya atau pada layanan ISP itu sendiri dengan cara mengadu (*complain*). Dari hasil data tersebut DSI *memiliki maturity level* 3, karena penilaian risiko dan evaluasi risiko tidak ada karena tidak memiliki kerangka konteks risiko yang ditetapkan, solusi untuk risiko diselesaikan pada saat peristiwa terjadi.

PO9.3 *Event Identification*

Identifikasi Peristiwa Identifikasi peristiwa (ancaman realistis penting yang mengeksploitasi kerentanan signifikan yang berlaku) dengan potensi dampak negatif pada tujuan atau operasi perusahaan, termasuk bisnis, peraturan, hukum, teknologi, mitra dagang, sumber daya manusia dan aspek operasional. Tentukan sifat dampak dan pertahankan informasi ini. Catat dan pertahankan risiko yang relevan dalam risiko registrasi. . Dari hasil wawancara ditemukan data bahwa DSI sudah dapat mengidentifikasi ancaman yang dapat terjadi dan berdampak negative untuk operasional perusahaan dapat dilihat dari penggunaan ISP 3 jenis untuk menghindari risiko gangguan pada salah satu layanan, DSI juga melakukan filtering untuk karyawan yang melamar kerja ada standar kriteria karyawan pada perusahaan untuk menghindari ketidaksesuaian SDM (sumber daya manusia) untuk proses bisnis perusahaan dan ada juga training untuk pegawai baru atau aplikasi baru sebelum diimplemntasikan untuk menghindari kesalahan user dalam penggunaan aplikasi yang dapat merugikan perusahaan berdasarkan data maturity level pada sub-domain ini adalah 3 karena secara keseluruhan DSI sudah sigap akan peristiwa yang dapat merugikan perusahaan sehingga adanya tindakan khusus untuk mengurangi dampak risiko terjadi.

PO9.4 *Risk Assessment*

Tugas beresiko Menilai secara berulang kemungkinan dan dampak dari semua risiko yang diidentifikasi, menggunakan metode kualitatif dan kuantitatif. Kemungkinan dan dampak yang terkait dengan risiko *inheren* dan residual harus ditentukan secara individual, berdasarkan kategori dan pada portofolio dasar. Dari hasil wawancara yang dilakukan, DSI tidak menggunakan metode kualitatif dan kuantitatif untuk menilai semua risiko yang dapat terjadi, penilaian risiko yang dilakukan DSI adalah menggunakan pengalaman sebelumnya agar tidak terjadi kemungkinan hal yang sama. Nilai *maturity level* untuk *sub-domain* ini adalah 2 karena Pendekatan penilaian risiko yang berkembang ada dan

diimplementasikan atas kebijakan manajer IT dan stakeholder lain. Manajemen risiko ada pada tingkat tinggi serta dampak yang sangat besar untuk perusahaan dan biasanya hanya diterapkan pada proyek-proyek besar.

PO9.5 *Risk Response*

Kembangkan dan pertahankan proses respons risiko yang dirancang untuk memastikan bahwa pengendalian yang hemat biaya memitigasi risiko terhadap dasar berkelanjutan. Proses respons risiko harus mengidentifikasi strategi risiko seperti penghindaran, pengurangan, pembagian atau penerimaan, menentukan tanggung jawab terkait dan pertimbangkan tingkat toleransi risiko. Dari hasil wawancara, DSI memiliki aktivitas penghematan biaya dalam ruang penyimpanan data dengan pemakaian *database external* dan *internal* dapat di *restore* untuk *backup* data jika ada suatu kendala pada data perusahaan yang tersimpan pada *database*, DSI juga memiliki *Server* sendiri sehingga memudahkan pengolaan data perusahaan dan menghemat biaya jika menyewa ruang penyimpanan di *cloud* yang dikenakan biaya cukup lumayan karena *storage* yang dibutuhkan DSI banyak dan penghindaran terhadap keamanan data yang belum tentu terjamin jika penyewaan dari luar . Sehingga DSI memiliki *maturity level* 3 karena sejauh ini perusahaan sudah melakukan respon risiko yang cukup baik dengan pengendalian hemat biaya melalui setiap kegiatan operasional perusahaan.

PO9.6 *Maintenance and Monitoring of a Risk Action Plan*

Prioritaskan dan rencanakan kegiatan pengendalian di semua tingkatan untuk mengimplementasikan respons risiko yang diidentifikasi perlu, termasuk identifikasi biaya, manfaat dan tanggung jawab untuk pelaksanaan. Dapatkan persetujuan untuk tindakan yang direkomendasikan dan penerimaan risiko residual, dan memastikan bahwa tindakan yang dilakukan diketahui oleh pemilik proses yang terkena dampak.

Dari hasil wawancara yang dilakukan didapatkan data bahwa DSI memiliki maintance dan *monitoring* secara berkala untuk *hardware* dan *software* yang ada pada perusahaan agar operasional berjalan secara optimal dan untuk anggaran biaya perawatan jika terjadi kerusakan pada *hardware* atau *software* dan memungkinkan untuk adanya pembelian alat baru Manager IT meminta pada direktur utama untuk persetujuan terhadap pembelian alat. Tanggug jawab dari *maintance* dan *monitoring* dilimpahkan pada departemen IT sehingga pertanggung jawaban akan diminta berupa laporan secara berkala yang harus diberikan pada direktur utama mengenai maintance dan segala biaya yang terkait. Dari data tersebut DSI memiliki *maturity level* 3 karena DSI telah melakukan *maintance* dan *monitoring* terhadap hardware maupun software yang memiliki fungsi penting dalam operasional perusahaan dengan adanya *monitoring* tersbut dapat dikatakan sebagai rencana tindakan risiko karena dapat mengurangi risiko yang tidak diinginkan terjadi.

Dari hasil analisa audit tersebut, di peroleh Maturity Level dari setiap *sub – domain* yang ada pada PO 9 Assess *and Manage IT Risks* dan hasil proses nya dapat di lihat pada Tabel 2 *Assess and Manage IT Risks.*

Rekomendasi untuk DSI *sub-domain* PO9 *Assess and Manage IT Risks* dieperlukan kerangka managemen risiko IT pada perusahaan agar perusahaan dapat membuat perencanaan untuk mengurangi dampak dari risiko kedepanya dan para pegawai dapat mengikuti prosedur yang ada untuk menanggulanginya jika terjadi suatu masalah dalam perusahaan dan pentingnya ada penilaian terhadap risiko yang terjadi agar hal yang sama tidak terjadi lagi dan dapat merencanakan untuk proses perbaikan dari kelemahan yang pernah terjadi. Suatu kebijakan perlu seperti peraturan tertulis tentang batasan dan wewenang dari setiap pegawai dan setiap divisi dalam penggunaan segala aset dalam perusahaan seperti pemakaian aplikasi dan memasuki ruangan agar tidak terjadi masalah antar divisi karena sudah ada peraturan tertulis dan update teknologi sangat diperlukan untuk pengembangan perusahaan lebih maju. Suatu penilaian risiko secara dokumentasi agar mudah dianalisa dan dilakukan secara berkala untuk menilai resiko yang sering terjadi dan risiko yang jarang serta dampak yang pernah diterima perusahaan dengan tujuan memprediksi dan merencakan solusi kedepannya untuk menguragi risiko kejadian yang sama terjadi dan kerugian yang diterima perusahan, perlunya suatu pelimpahan tanggung jawab terhadap divisi tertentu atau pegawai tertentu untuk melakukan pengawasan dan pengendalian atas risiko yang dapat terjadi pada aktivitas perusahaan dan dapat berdampak kerugian.

Tabel 2. *Assess and Manage IT Risks*

NO	Sub Domain	Current	Expected
PO 9.1	IT Risk Management Framework	2	3
PO 9.2	Establishment of Risk Context	3	4
PO 9.3	Event Identification	3	4
PO 9.4	Risk Assessment	2	4
PO 9.5	Risk Response	3	4
PO 9.6	Maintenance and Monitoring of a Risk Action Plan	3	4
	Rata-rata	2.6	3.8
	Gap Current dengan Expected	1.2	

Berdasarkan Tabel 2. *Assess and Manage IT Risks* terdapat adanya current yang artinya nilai sekarang dan expected artinya nilai yang diharapkan kepada perusahaan untuk dapat mencapainya dengan melakukan peningkatan dan pengembangan dari sebelumnya, rekomendasi yang diberikan penulis dapat dijadikan bahan pertimbangan untuk pengambilan keputusan atau perencanaan dikedepannya. Adanya *Gap* artinya selisih antar nilai yang dihaarapkan dengan nilai sekarang untuk DSI pada domain PO 9 terjadi *Gap* 1.2 adanya harapan untuk DSI mampu meningkatkan atau pengembangan sampai mencapai nilai *expected.*

AI3 *Acquire and Maintain Technology Infrastructure*

Organisasi memiliki proses untuk implementasi dan melakukan peningkatan infrastruktur **t**eknologi. Ini membutuhkan pendekatan yang direncanakan untuk akuisisi, pemeliharaan dan perlindungan infrastruktur sejalan dengan strategi teknologi yang disepakati dan penyediaan pengembangan dan lingkungan pengujian. Ini memastikan bahwa ada dukungan teknologi yang berkelanjutan untuk aplikasi bisnis.

AI3.1 Technological Infrastructure Acquisition Plan

Menghasilkan rencana untuk akuisisi, implementasi dan pemeliharaan infrastruktur teknologi yang memenuhi standard persyaratan fungsional dan teknis bisnis dan sesuai dengan arahan tujuan organisasi.

AI3.2 *Infrastructure Resource Protection and Availability*

Menerapkan kontrol internal, keamanan dan tindakan auditabilitas selama konfigurasi, integrasi dan pemeliharaan perangkat keras dan perangkat lunak untuk melindungi sumber daya dan memastikan ketersediaan dan integritas. Tanggung jawab untuk menggunakan infrastruktur oleh mereka yang mengembangkan dan mengintegrasikan komponen infrastruktur. Penggunaannya harus dipantau dan dievaluasi.

AI3.3 *Infrastructure Maintenance*

Mengembangkan strategi dan rencana untuk pemeliharaan infrastruktur, dan memastikan bahwa perubahan sesuai dengan prosedur manajemen. Termasuk pemantauan berkala terhadap kebutuhan bisnis, manajemen tambalan, peningkatan strategi, risiko, penilaian terhadap kerentanan keamanan.

AI3.4 *Feasibility Test Environment*

Membangun lingkungan pengembangan dan pengujian untuk mendukung kelayakan dan integrasi antar komponen infrastruktur menjadi efektif dan efisien.

Dari hasil wawancara yang dilakukan didapatkan data bahwa DSI memiliki perencanaan jadwal maintance terhadap software dan hardware secara berkala, DSI juga memiliki *firewall* dan *antivirus* untuk setiap komputer *user*, untuk perlingdungan dan mencegah adanya masalah dari luar. DSI memiliki software monitoring untuk melacak komputer mana yang jaringannya terputus sehingga IT support dapat memastikan kondisi masalah tanpa datang ketempat, aplikasi yang digunakan adalah Microtic The Dude. Dari hasil analisis DSI memiliki *maturity level* secara keseluruhan 3 karena DSI sudah memiliki perencanaan yang teratur dan diimplementasikan terhadap *maintance* dan *monitoring* infrastruktur IT dalam perusahaan dan DSI juga perduli akan kelangsungan infrastruktur IT dengan memberikan sekuritas terhadap beberapa infrastruktur seperti *database*, komputer, mesin *server*, *email* perusahaan sehingga dapat menjaga kegiatan operasional perusahaan tetap berjalan stabil.

Rekomendasi untuk DSI pada *sub-domain* AI3 *Acquire and Maintain Technology Infrastructure* adalah dan perlu adanya tes kelayakan atas aplikasi atau sistem yang sedang dipakai untuk memastikan aplikasi yang dipakai berjalan secara maksimal dan untuk perencanaan pengembangan jika ada aplikasi atau tambahan mesin yang dibutuhkan perusahaan untuk menunjang proses bisnis DSI semakin maju.

Dari hasil analisa audit tersebut, di peroleh *Maturity Level* dari setiap *sub-domain* yang ada pada AI3 *Acquire and Maintain Technology Infrastructure* dan hasil proses nya dapat di lihat pada Tabel 3. *Acquire and Maintain Technology Infrastructure*.

Tabel 3. *Acquire and Maintain Technology Infrastructure.*

NO	*Sub Domain*	*Current*	*Expected*
AI3.1	*Technological Infrastructure Acquisition Plan*	3	4
AI3.2	*Infrastructure Resource Protection and Availability*	3	4
AI3.3	*Infrastructure Maintenance*	3	4
AI3.4	*Feasibility Test Environment*	3	4
	Rata-rata	3	4
	Gap Current dengan *Expected*	1	

Berdasarakan Tabel 3. *Acquire and Maintain Technology Infrastructure* terdapat adanya *current* yang artinya nilai sekarang dan *expected* artinya nilai yang diharapkan kepada perusahaan untuk dapat mencapainya dengan melakukan peningkatan dan pengembangan dari sebelumnya, rekomendasi yang diberikan penulis dapat dijadikan bahan pertimbangan untuk pengambilan keputusan atau perencanaan dikedepannya. Adanya *Gap* artinya selisih antar nilai yang diharapkan dengan nilai sekarang untuk DSI pada domain AI3 terjadi *Gap* 1 adanya harapan untuk DSI mampu meningkatkan atau pengembangan sampai mencapai nilai *expected*.

AI4 *Enable Operation and Use*

Pengetahuan tentang sistem baru. Proses ini membutuhkan pembuatan dokumentasi dan panduan manual untuk pengguna TI, dan menyediakan pelatihan untuk memastikan penggunaan serta pengoperasian aplikasi dilakukan dengan tepat dan benar.

AI4.1 *Planning for Operational Solutions*

Mengembangkan rencana untuk mengidentifikasi dan mendokumentasikan semua aspek teknis, operasional, dan penggunaan sehingga semua orang yang akan mengoperasikan, menggunakan dan melaksanakan tanggung jawab mereka.

AI4.2 *Knowledge Transfer to Business Management*

Memberikan pengetahuan ke manajemen bisnis untuk memungkinkan individu-individu untuk mengambil hak atas sistem dan data dan tanggung jawab untuk kualitas layanan, kontrol internal, dan administrasi aplikasi.

AI4.3 *Knowledge Transfer to End User*

Memberikan pengetahuan dan keterampilan untuk memungkinkan *user* menggunakan sistem secara efektif dan efisien dalam mendukung proses bisnis.

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

Memberikan pengetahuan dan keterampilan untuk memungkinkan staf operasional dan bagian teknis untuk secara efektif dan efisien memberikan, mendukung dan memelihara sistem infrastruktur terkait.

Dari hasil wawancara yang dilakukan didapatkan bahwa DSI memiliki standar prosedur untuk setiap *user* baru akan dilatih terlebih dahulu sebelum langsung menggunakan aplikasi yang ada pada perusahaan untuk mencegah terjadinya kesalahan dalam penggunaaan aplikasi dan untuk aplikasi baru akan di demo kepada seluruh *user* sebelum diimplemtasikan agar *user* dapat menggunakan aplikasi yang baru dengan benar. Tanggung jawab yang diserahkan pada divisi tertentu seperti IT yang memiliki tanggung jawab atas kualitas *software*, *hardware*, jaringan, *database* dan permintaan dari user untuk pembuatan program yang membantu aktivitas atau proses kerja dalam perusahaan. Divisi IT memiliki peran besar dalam DSI sehingga semua kontrol baik pengelolaan ataupun pemeliharaan terhadap infrastruktur IT perusahaan dipegang oleh divisi IT. Dari analisa data yang didapatkan *maturity level*

DSI adalah 2.75 karena DSI sudah memiliki prosedur yang tetap dengan adanya pelatihan pada *user* baru dan adanya tanggung jawab yang dilimpahkan pada divisi untuk sebagai pusat pengendalian terhadap infrastruktur dalam perusahaan.

Rekomendasi untuk DSI pada *sub-domain* AI4 *Enable Operation and Use* adalah perlunya batasan akses terhadap *user* dalam hal kecil seperti pencolokan *flashdisk* ke komputer perusahaan yang dapat berdampak buruk seperti pencemaran virus, hal kecil perlu juga mendapat perhatian karena dapat berdampak juga pada kinerja perusahaan. Dari hasil analisa audit tersebut, di peroleh *Maturity Level* dari setiap sub–domain yang ada pada AI4 *Enable Operation and Use* dan hasil proses nya dapat di lihat pada Tabel 4. *Enable Operation and Use*.

Tabel 4. *Enable Operation and Use*

NO	*Sub Domain*	*Current*	*Expected*
AI4.1	*Planning for Operational Solutions*	3	4
AI4.2	*Knowledge Transfer to Business Management*	3	4
AI4.3	*Knowledge Transfer to End User*	3	4
AI4.4	*Knowledge Transfer to Operations and Support Staff*	2	3
	Rata-rata	2.75	3.75
	Gap Current dengan *Expected*	1	

Berdasarakan Tabel 4 *Enable Operation and Use* terdapat adanya *current* yang artinya nilai sekarang dan *expected* artinya nilai yang diharapkan kepada perusahaan untuk dapat mencapainya dengan melakukan peningkatan dan pengembangan dari sebelumnya, rekomendasi yang diberikan penulis dapat dijadikan bahan pertimbangan untuk pengambilan keputusan atau perencanaan dikedepannya. Adanya *Gap* artinya selisih antar nilai yang diharapkan dengan nilai sekarang untuk DSI pada *sub-domain* AI4 terjadi *Gap* 1 adanya harapan untuk DSI mampu meningkatkan atau pengembangan sampai mencapai nilai *expected*.

DS5 *Ensure Systems Security*

Kebutuhan untuk menjaga integritas informasi dan melindungi aset TI memerlukan proses manajemen keamanan. Proses ini termasuk menetapkan dan memelihara peran dan tanggung jawab keamanan TI, kebijakan, standar, dan prosedur. Keamanan manajemen juga termasuk melakukan pemantauan keamanan dan pengujian berkala dan menerapkan tindakan korektif untuk diidentifikasi kelemahan atau insiden keamanan. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis dari kerentanan keamanan dan insiden.

DS5.1 *Management of IT Security*

Kelola keamanan TI pada tingkat organisasi tertinggi yang sesuai, sehingga pengelolaan tindakan keamanan sejalan dengan proses bisnis.

DS5.2 *IT Security Plan*

Identifikasi persyaratan bisnis, risiko dan kepatuhan ke dalam rencana keamanan keseluruhan TI, dengan mempertimbangkan infrastruktur TI dan lingkungan keamanan. Pastikan bahwa rencana tersebut diimplementasikan dalam kebijakan dan prosedur keamanan bersama dengan yang sesuai investasi dalam layanan, personel, perangkat lunak, dan perangkat keras. Mengkomunikasikan kebijakan dan prosedur keamanan kepada para pemangku kepentingan dan pengguna.

DS5.3 *Identity Management*

Pastikan bahwa semua pengguna (internal, eksternal dan sementara) dan aktivitas mereka pada sistem TI (aplikasi bisnis, lingkungan TI, operasi sistem, pengembangan dan pemeliharaan) dapat dikontrol. Aktifkan identitas pengguna melalui mekanisme otentikasi. Adanya konfirmasi setiap penggunaan hak akses dalam perusahaan yang menunjukan bahwa memang pemiliknya saja yang dapat mengaksesnya.

DS5.4 *User Account Management*

serangkaian prosedur manajemen pengguna. Prosedur persetujuan yang menjabarkan data atau pemilik sistem yang memberikan akses hak istimewa. Prosedur ini harus berlaku untuk semua pengguna, termasuk administrator (pengguna istimewa) dan pengguna internal dan eksternal, untuk kasus normal dan darurat. Hak dan kewajiban relatif terhadap akses ke sistem dan informasi perusahaan

seharusnya diatur secara kontrak untuk semua jenis pengguna. Lakukan tinjauan manajemen secara teratur terhadap semua akun dan hak akses yang terkait.

DS5.5 *Security Testing, Surveillance and Monitoring*

Menguji dan memantau implementasi keamanan TI secara proaktif. Keamanan TI harus diakreditasi ulang tepat waktu untuk memastikan bahwa garis dasar keamanan informasi perusahaan dapat dipertahankan.

DS5.6 *Security Incident Definition*

Mendefinisikan karakteristik masalah keamanan potensial dengan jelas sehingga dapat diklasifikasikan dengan benar dan ditangani oleh manajemen masalah.

DS5.7 *Protection of Security Technology*

Buat teknologi terkait keamanan tahan terhadap gangguan, dan jangan dokumentasi keamanan yang tidak perlu

DS5.8 *Cryptographic Key Management*

Menentukan bahwa ada kebijakan dan prosedur untuk mengatur masalah perubahan, pencabutan, penghapusan, distribusi, sertifikasi, penyimpanan, pemasukan, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.

DS5.9 *Malicious Software Prevention, Detection and Correction*

Letakkan langkah-langkah pencegahan, deteksi dan korektif di tempat (terutama *patch* keamanan terbaru dan kontrol virus) di seluruh organisasi untuk melindungi sistem dan teknologi informasi dari malware (mis, *virus, worm, spyware, spam*).

DS5.10 *Network Security*

Gunakan teknik keamanan dan prosedur manajemen (mis, Firewall, peralatan keamanan, segmentasi jaringan, intrusideteksi) untuk mengesahkan akses dan mengontrol arus informasi ke jaringan.

DS5.11 *Exchange of Sensitive Data*

Tukar data transaksi sensitif hanya melalui jalur atau media tepercaya dengan kontrol untuk memberikan keaslian konten.

Dari hasil wawancara didapatkan data DSI memiiki sistem keamanan atau batasan akses setiap penggunaan seperti ruang server yang tidak dapat dimasuki oleh semua user hanya pemangku jabatan penting dan manager IT karena menggunakan *card access* yang berbeda yang dimiliki oleh pemangku jabatan penting, setiap ruangan divisi memiliki *card access* sehingga tidak semua divisi dapat masuk keruangan divisi lain. Sistem absesnsi pada DSI adalah menggunakan teknologi *Fingerprint*, aktivitas pengelolaan bisnis menggunakan *Accurate* 4 sistem kemanan untuk database menggunakan securitas bawaan dari *Accurate* yang memiliki password yang diketahui oleh Manager IT dan direktur utama, setiap computer *user* memiliki user id dan *Password* yang hanya diketahui oleh pemiliknya sehingga tidak setiap user dapat mengakses komputer lain selain miliknya dan *password* diwajibkan diganti setiap 2 mnggu sekali berdasarkan dari kebijakan divisi IT untuk selalu *update* sistem keamanan. Adapun pembatasan terhadap penggunaan internet yaitu pemblokiran terhadap jejaring sosial yang tidak berhubungan dengan aktvitas perusahaan seperti: *youtube*, *facebook*, *instagram* dan media sosial lainnya pemblokiran *by system* artinya secara otomatis tidak dapat dibuka pada saat user membuka *link* tesebut, adapun keamanan *software* menggunakan *firewall* dari *Accurate*, *antivirus*, *firerwall* bawaaan *windows* untuk mencegah serangan dari luar yang dapat merusak sistem. Dari data tersebut *maturity level* pada domain ini adalah 2.7 *Defined Process* karena secara keseluruhan DSI telah menerapkan keamanan sistem yang baik dan adanya batasan akses untuk setiap user dalam aktivitas perusahaan.

Rekomendasi untuk DSI pada sub-domain DS5 *Ensure Systems Security* adalah perlunya planning kedepannya pada bagian securitas seperti *firewall* berbentuk mesin agara keamanan lebih terjamin karena dikelola dan dikontol oleh pihak perusahaan sendiri, diperlukan *testing security* agar mengetahui kekuatan sistem keamanan pada perusahaan dengan cara itu kita dapat mengetahui kekurangan yang ada pada sistem sekuritas perusahaan dan penting juga untuk pemakaian antivirus yang original bukan bajakan agar keamanan lebih terjamin. Untuk proses bisnis dapat dikembangkan ke tahap pemakaian *Enterprise Resource Planning* (ERP). Pada perusahaan yang tidak menerapkan sistem ERP, umumnya menggunakan sistem *database* yang terpisah. setiap divisi memiliki *database* tersendiri seperti pemasaran, *human resource development*, *purchasing* memiliki *database* yang berbeda dan sering terjadi masalah yaitu ketidaksesuaian data input dengan output sehingga sulit untuk pengelolaannya.

ERP dapat mengintegrasikan dari keseluruhan sistem sehingga meminimalkan kemungkinan terjadi kesalahan atau *error*. Dari hasil analisa audit tersebut, di peroleh *Maturity Level* dari setiap *sub – domain* yang ada pada DS5 *Ensure Systems Security* dan hasil prosesnya dapat di lihat pada Tabel 5 *Ensure Systems Security.*

Tabel 5 *Ensure Systems Security*

NO	*Sub Domain*	*Current*	*Expected*
DS5.1	*Management of IT Security*	3	4
DS5.2	*IT Security Plan*	2	3
DS5.3	*Identity Management*	3	4
DS5.4	*User Account Management*	3	4
DS5.5	*Security Testing, Surveillance and Monitoring*	2	3
DS5.6	*Security Incident Definition*	2	3
DS5.7	*Protection of Security Technology*	3	4
DS5.8	*Cryptographic Key Management*	3	4
DS5.9	*Malicious Software Prevention, Detection and Correction*	3	4
DS5.10	*Network Security*	3	4
DS5.11	*Exchange of Sensitive Data*	3	4
	Rata-rata	2.7	3.7
	Gap Current dengan *Expected*	1	

Berdasarakan Tabel 5 *Ensure Systems Security* terdapat adanya *current* yang artinya nilai sekarang dan *expected* artinya nilai yang diharapkan kepada perusahaan untuk dapat mencapainya dengan melakukan peningkatan dan pengembangan dari sebelumnya, rekomendasi yang diberikan penulis dapat dijadikan bahan pertimbangan untuk pengambilan keputusan atau perencanaan dikedepannya. Adanya *Gap* artinya selisih antar nilai yang diharapkan dengan nilai sekarang untuk DSI pada *domain* DS5 terjadi *Gap* 1 adanya harapan untuk DSI mampu meningkatkan atau pengembangan sampai mencapai nilai *expected*

5 KESIMPULAN

Berdasarkan hasil analisis penelitian ini, kesimpulan diperoleh bahwa sistem informasi di DSI telah berjalan dengan baik. Hampir semua proses telah dilakukan secara efektif, proses operasional dan manajemen masalah dilaksanakan dengan baik. Mereka mengerti cara memperbaiki masalah yang terjadi dan memiliki jalur alternatif saat masalah terjadi. Aset infrastruktur telah dikelola dan dikendalikan dengan baik dan secara berkala dan mereka juga melakukan pemeliharaan secara teratur untuk menjaga hal-hal tak terduga yang terjadi. Tetapi perusahaan masih perlu membuat beberapa perbaikan di bagian manajemen akses yang memiliki kelemahan karena hal-hal kecil juga perlu mendapat perhatian karena dapat berdampak pada kinerja perusahaan serta monitoring untuk aplikasi yang sedang berjalan untuk medeteksi gejala yang aneh atau suatu gerakan mencurigakan yang memiliki potensi buruk untuk kemanan sistem agar perusahaan dapat mencegahnya sebelum kejadian terjadi. Secara keseluruhan dari *sub-domain* PO9 mencapai nilai maturity level 2.6, AI3 mencapai nilai maturity level 3, AI4 mencapai nilai maturity level 2.75, DS5 mencapai nilai *maturity level* 2.7 artinya dari *sub-domain* teresebut ada pada level *Defined Process* yang cukup baik sehingga perlu pengembangan untuk mencapai nilai ekspektasi. DSI perlu memiliki perencanaan masa depan dengan pengembangan bisnis lebih tinggi seperti menggunakan ERP dalam proses bisnisnya agar proses bisnis lebih terstruktur dan terintegrasi satu sama lain yang mengurangi risiko yang dan dapat membuat profit untuk perusahaan karena bisnis berjalan dengan efektif dan efisien.

REFERENSI

[1] Istiatin & Sudarwati, "Analisis Strategi Pemasaran Bisnis Retail Di Lottemart Surakarta (Dosen Fakultas Ekonomi Manajemen UNIBA)," *J. Paradig.*, vol. 12, no. 02, pp. 21–31, 2015.

[2] E.Soliha, "Analisis Industri Ritel," *Anal. Ind. Ritel Di Indones.*, vol. 15, no. 2, pp. 128–142, 2008.

[3] Fenny and J. F. Andry, "Audit Sistem Informasi Menggunakan Framework Cobit 4.1 Pada Pt. Aneka Solusi Teknologi," *Pros. Semnastek*, vol. 0, no. 0, pp. 1–2, 2017.

[4] R. Anderson, K. Kevin, and J. F. Andry, "Audit Aplikasi Inventori Menggunakan Framework Cobit 4.1 Pada Store Nonna," *It J. Res. Dev.*, vol. 3, no. 1, p. 1, 2018.

[5] Fauzan, "Audit Tata Kelola Teknologi Informasi Untuk Mengontrol Manajemen Kualitas Menggunakan Cobit 4.1 (Studi Kasus : PT Nikkatsu Electric Works)," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 3, pp. 235–244, 2015.

[6] G. Ayu, T. Krisanthi, I. M. Sukarsa, and I. P. A. Bayupati, "Governance Audit of Application Procurement Using Cobit Framework 1 Gusti Ayu Theresia Krisanthi, 2 I Made Sukarsa, 3 I Putu Agung Bayupati," vol. 59, no. 2, pp. 342–351, 2005.

[7] Winalia, F. Renaldi, and A. I. Hadiana, "Pengukuran Tingkat Kematangan Teknologi Informasi menggunakan COBIT 4.1 Pada Universitas Jenderal Achmad Yani," *Semin. Nas. Apl. Teknol. Inf. 2017*, pp. 31–36, 2017.

[8] I. D. Lesmono and D. Erca, "Tata Kelola Teknologi Informasi Dengan Metode COBIT 4.1 (Studi Kasus : PT.IMI)," *J. Kaji. Ilm.*, vol. 18, no. 1, 2018.

[9] M. M. Mohammadi, A. Z. Ravasan, and H. Hamidi, "Investigating Critical Success Factors in Implementing ITIL Framework," *Int. J. Stand. Res.*, vol. 13, no. 1, pp. 74–91, 2016.

[10] R. A. Khther and M. Othman, "Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review," *Int. J. Inf. Technol. Converg. Serv.*, vol. 3, no. 1, pp. 21–29, 2013.

[11] A. Y. Zafarina, M. Arief, and R. Mulyana, "Analisis Dan Perancangan Tata Kelola Ti Menggunakan Cobit 4.1 Domain Plan and Organize Dan Acquire and Implement: Studi Kasus Pt Xyz," *J. Sist. Inf.*, vol. 12, no. 2, p. 64, 2016.

[12] J. F. Andry, Y. M. Geasela, A. Wailan, B. A. Matjik, A. Kurniawan, and J. Junior, "Penggunaan COBIT 4.1 Dengan Domain ME Pada Sistem Informasi Absensi (Studi Kasus: Universitas XYZ)," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 13, no. 2, p. 97, 2019.

[13] A. Arumana, "Analisis Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4.1 pada Fakultas Teknik Undip," *J. Teknol. dan Sist. Komput.*, 2014.

[14] D. Darwis and . Yuniarwati, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 4.1 sebagai Upaya Peningkatan Keamanan Data pada Dinas Pendidikan dan Kebudayaan Kabupaten Pesawaran," *Explore*, vol. 7, no. 1, 2016.

[15] Wisda, "Pengukuran Tingkat Kematangan IT Governance Pada Layanan Akademik STMIK AKBA Dengan Framework Cobit 4 . 1 (Studi Kasus : STMIK AKBA Makassar)," *J. Speed*, vol. 8, no. 1, pp. 14–21, 2016.

[16] B. H. Mesa and J. F. Andry, "Evaluasi Tingkat Efektivitas Sistem Informasi Menggunakan Framework COBIT 5 Evaluation of Information System Effectiveness Level Using COBIT Framework 5," no. June, pp. 148–159, 2018.