KAJIAN PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SISTEM INFORMASI PADA PENGOLAHAN DATA ELEKTRONIK (PDE) MENGGUNAKAN FRAMEWORK COBIT 4.1 STUDI KASUS: SMK NEGERI 24 JAKARTA

Furnia Sari Dewi Kencanawati[1], Yahdi Kusnadi[2]
Program Studi Manajemen Informatika
Akademi Manajemen Informatika dan Komputer Bina Sarana Informatika
Jl. Margonda Raya No. 8 Depok
[1]furn14@gmail.com
[2]yahdi_k@yahoo.com

ABSTRACT

Electronic Data Processing (PDE) at SMK Negeri 24 Jakarta has a significant role in supporting the work processes as well as teaching and learning in schools. Its existence as one of the utilization of technology in the field of Information Technology (IT) has brought a new wind to the development progress of the inner workings of Administration (TU). However, the application of ICT, particularly PDE, in addition to bringing fresh air for IT development also brings the values that will lead to a negative thing if the awareness of IT security for each individual user's PDE is not maximized. Measuring the level of maturity on the PDE by using the COBIT framework 4.1 and domain DS5, Deliver and support system, are expected to provide information on the extent to which awareness of the security system on each user's information, measure the maturity level of information system security in PDE, to know the findings and constraints on system as well as members of the problem and alternative solutions based on the measurement results of the questionnaire results.

Keywords: Electronic Data Processing (PDE), Measurement, Maturity, Security

I. Pendahuluan

Sistem Informasi sebagai sebuah alternatif pengelolaan data dan informasi, memiliki peranan yang cukup signifikan seiring dengan kemajuan teknologi baik dalam bidang informasi maupun komunikasi. Keberadaan sistem informasi mampu mengatasi semua hambatan yang menjadi kendala dalam era sebelumnya.

Bagi sebuah organisasi/perusahaan besar dimana informasi menjadi hal yang sangat vital, keberadaan sistem informasi dirasakan banyak manfaatnya. Sistem Informasi yang sudah mulai berkembang mengikuti perkembangan teknologi, dirasa sebagai hal yang sangat membantu namun disisi lain memiliki keterbatasan yang dapat merugikan organisasi/perusahaan itu sendiri. Keberadaan sistem informasi dengan didukung oleh teknologi menjadi hal yang sangat penting dikarenakan mampu mendukung proses kerja menjadi optimal. Sekolah dimana keberadaan informasi sering dipandang sebelah mata, pun membutuhkan informasi dan teknologi untuk mendukung optimalisasi proses belajar dan mengajar disekolah tersebut. SMK Negeri 24 Jakarta yang merupakan sekolah yang berstandar nasional turut merasakan pentingnya informasi dan teknologi dalam mendukung proses kerja yang mampu mengoptimalisasi tercapainya tujuan belajar mengajar di sekolah.

Berdirinya program keahlian RPL pada tahun 2004 di SMK Negeri 24 Jakarta memberikan banyak pengaruh terhadap penerapan ICT bagi proses kegiatan belajar mengajar (KBM). Disinilah dimulai proses kerja yang terintegrasi dan terpusat yang dikenal dengan istilah Pengolahan Data Elektronik (PDE) yang diterapkan pada bagian Tata Usaha (TU).

Meningkatnya pengelolaan Teknologi Informasi (TI) pada kegiatan sekolah, menuntut diadakannya *audit* sistem informasi atau teknologi informasi, yang berfokus pada keamanan sistem dan manajemen data di TU khususnya bidang PDE, untuk menilai apakah pengendalian umum dan keamanan sistem informasi mampu memenuhi tujuannya. Isu utama dalam pengelolaan Teknologi Informasi (TI) masa kini adalah bagaimana menyelaraskan strategi bisnis sekolah dengan TI. Isu tersebut merupakan bagian dari fokus pembahasan Tata Kelola TI.

Pengolahan Data Elektronik (PDE) atau EDP menurut Jogiyanto (2007, p. 23). adalah manipulasi dari data ke dalam bentuk yg lebih

berarti berupa suatu informasi dgn menggunakan suatu alat elektronik yaitu komputer..

Menurut Sanyoto (2007, p.276), CoBIT adalah sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, pengguna (*user),* dan manajemen, untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI. CoBIT bermanfaat bagi auditor karena merupakan teknik yang dapat membantu dalam identifikasi *IT control issues*. CoBIT berguna bagi para IT *user* karena memperoleh keyakinan atas kehandalan sistem aplikasi yang dipergunakan. Sedangkan para manajer memperoleh manfaat dalam keputusan investasi di bidang TI serta infrastrukturnya,

COBIT (*Control Objectives For Information & Related Technology*) merupakan seperangkat praktik terbaik (*best practice*) bagi pengelolaan teknologi informasi. COBIT merupakan standar yang sekarang banyak digunakan dan merupakan panduan yang lengkap dari praktek-praktek terbaik untuk manajemen pengendalian internal TI yang mencakup empat *domain* yaitu : *planning & organization, acquisition & implementation, delivery & support and monitoring,* yang dirinci menjadi 34 high level control objectives.

Sekolah Menengah Kejuruan Negeri 24 Jakarta adalah sekolah standar nasional yang memiliki proses kerja yang cukup kompleks dan penting dengan menggunakan teknologi informasi yang mendukungnya. Hal ini adalah salah satu alasan untuk melakukan evaluasi penerapan tata kelola TI pada SMK Negeri 24 Jakarta. Dikarenakan bagian Tatau Usaha (TU) merupakan core atau sentral proses dari keseluruhan kegiatan yang mendukung proses belajar dan mengajar disekolah. Pengelolaan yang kurang baik pada teknologi informasi akan mengakibatkan dukungan terhadap proses lain disekolah tersebut, terutama kegiatan belajar mengajar sekolah menjadi kurang optimal. Oleh karena itu, teknologi informasi harus dikelola dengan baik dengan mengacu pada standar tata kelola yang sudah diakui secara internasional.

CobIT dianggap sebagai kerangka kerja yang tepat untuk dipakai dalam melakukan proses *audit* tata kelola TI yang ada di SMK Negeri 24 Jakarta karena CobIT menyediakan standar dalam kerangka kerja *domain* yang terdiri dari sekumpulan proses TI yang merepresentasikan aktivitas yang dapat dikendalikan dan terstruktur. Sehingga cocok diterapkan di SMK Negeri 24 Jakarta yang fokus tata kelola IT-nya saat ini masih sebagai kontrol dari proses yang mendukung kegiatan belajar mengajar sekolah.

II. Tinjauan Pustaka

a. Keamanan Sistem Informasi

Keamanan informasi ditujukan untuk mendapatkan kerahasiaan, ketersediaan, serta integritas pada semua sistem informasi perusahaan, bukan hanya piranti keras dan data (McLeod dan P. Schell, 2008:269).

Keamanan Informasi yang diartikan secara harfiah Keamanan (Bahasa Indonesia) dan Security (Bahasa Inggris), berasal dari bahasa yunani "Secure" yang berarti adalah aman. Sedangkan Informasi dan Information berasal dari "To-Inform" yang berarti adalah memberitahu.

Istilah keamanan informasi (information security) digunakan untuk mendeskripsikan perlindungan baik peralatan komputer dan non komputer, fasilitas, data dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang (McLeod dan P. Schell, 2008:270).

Dasar untuk keamanan terhadap ancaman oleh orang- orang tak berwewenang adalah pengendalian akses. Alasannya sederhana (McLeod dan P. Schell, 2008,p.280) : jika orang-orang tak berwewenang ditolak aksesnya ke sumber daya informasi, maka perusakan tidak dapat dilakukan. Pengendalian akses terdiri dari tiga cara, yaitu:

1. Identifikasi Pengguna
   Merupakan identifikasi pertama dengan cara memberikan sesuatu yang mereka ketahui, misalnya kata sandi. Identifikasi dapat pula mencakup lokasi penggun, seperti nomor telepon atau titik masuk jaringan.
2. Otentikasi Pengguna
   Verifikasi hak akses pengguna dengan otentifikasi, yang merupakan identifikasi dengan memberikan sesuatu yang mereka miliki, seperti smart card atau chip identifikasi. Dapat juga dilaksanakan dengan dengan cara memberikan sesuatu yang menjadi identitas diri, seperti tanda tangan, suara atau pola suara.
3. Otorisasi Pengguna
   Setelah pemeriksaan identifikasi dan autentifikasi dilalui pengguna, akan didapatkan otorisasi untuk memasuki tingkat atau derajat pengguna tertentu.

Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu (McLeod dan P. Schell, 2008,p.270) :

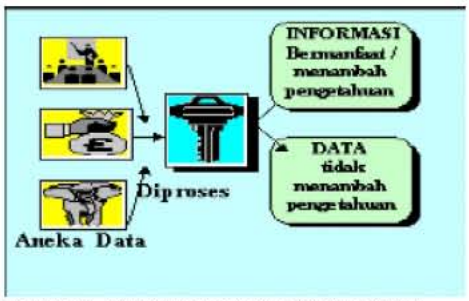
1. Kerahasiaan
   Perusahaan/organisasi berusaha untuk melindungi data dan informasinya dari

pengungkapan kepada orang-orang yang tidak berwenang.

2. Ketersediaan
   Tujuan dari infrastruktur informasi adalah menyediakan data dan informasi sedia bagi pihak-pihak yang memiliki wewenang untuk menggunakannya.
3. Integritas
   Semua system informasi harus memberikan representasi akurat atas system fisik yang direpresentasikannya.

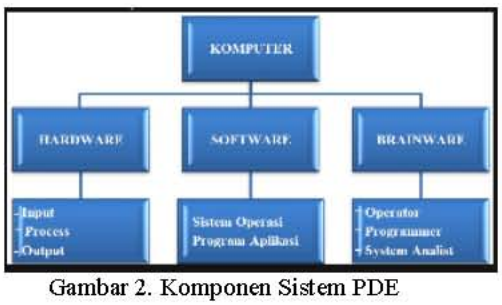
b. Pengolahan Data Elektronik (PDE)

Electronic Data Processing (EDP) atau pengolahan data elektronik (PDE) adalah manipulasi dari data ke dalam bentuk yang lebih berarti berupa suatu informasi dengan menggunakan suatu alat elektronik yaitu komputer (Wahyudie, 2006). Secara umum dikatakan Sistem PDE adalah suatu system pengolahan data dengan menggunakan Komputer.



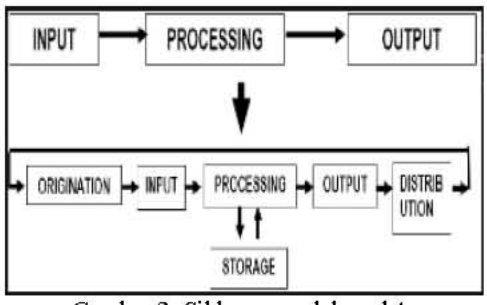
Gambar 1. Gambaran Umum Sistem PDE

Sistem PDE memiliki komponen seperti perangkat keras (hardware), perangkat lunak (software), prosedur, basis data (database), jaringan komputer dan komunikasi data serta pengguna (user).



Gambar 2. Komponen Sistem PDE

Komponen-komponen tersebut saling berinteraksi membentuk sebuah system PDE, yang berfungsi mengolah data. Siklus pengolahan tersebut tampak seperti gambar 3 dibawah ini.



Gambar 3. Siklus pengolahan data

Statement On *Audit*ing Standard No. 48 (Pujiwidodo:2007), "Pengaruh proses komputer dalam pemeriksaan laporan keuangan" mengidentifikasikan beberapa perbedaan karakteristrik antara sistem
PDE dengan manual, yaitu meliputi :

1. Terkadang tidak memerlukan dokumen masukan atau Transaction Trail. Catatan dan dokumen pendukung pelaksanaan transaksi terkadang dapat dihapuskan dalam sistem PDE, karena dalam sistem PDE banyak catatan dan dokumen yang tidak diperlukan lagi. Misalnya : Suatu perusahaan menggunakan pencatat waktu yang dihubungkan langsung (on-line) dengan komputer, sehingga karyawan hanya tinggal menekan tombol tertentu dan secara otomatis sistem tersebut akan mengumpulkan dan memindahkan jumlah jam kerja pada akun tenaga kerja dan upah masing-masing.
2. Keseragaman pemrosesan transaksi dengan menggunakan komputer biasanya dilakukan secara seragam.
3. Pemisahan tugas. Dalam Sistem PDE, potensi untuk melakukan kesalahan dan ketidakberesan cukup besar, sehingga perlu diadakan tambahan pengendalian, seperti pemberian "password".

c. Cobit 4.1

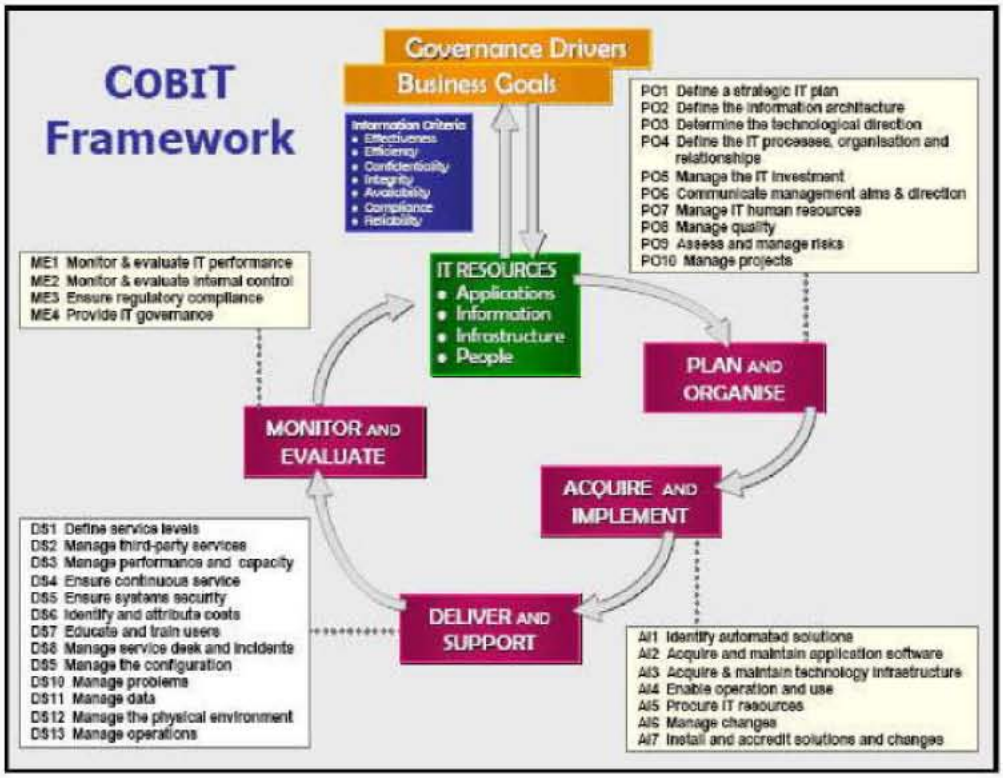
COBIT 4.1 merupakan versi terakhir dari seperangkat tujuan pengendalian (*control objectives*) untuk TI. Versi pertama diluncurkan oleh yayasan ISACF pada tahun 1996 yang menekankan pada bidang *audit*. COBIT edisi kedua, merefleksikan suatu peningkatan sejumlah dokumen sumber,

COBIT, *Control Objectives For Information & Related Technology* adalah seperangkat pedoman praktik terbaik pengelolaan teknologi informasi *(IT Management*). COBIT berguna bagi pengguna TI karena memperoleh keyakinan atas sistem aplikasi dan teknologi yang dipergunakan. Sedangkan bagi manajer memperoleh manfaat dalam keputusan investasi di bidang TI serta infrastrukturnya dan keputusan atas

procurement (pengadaan/ pembelian) sumber daya TI. Disamping itu dengan kehandalan sistem informasi yang dimiliki perusahaan diharapkan berbagai keputusan bisnis dapat didasarkan atas informasi yang ada.

COBIT menyediakan standar dalam kerangka kerja *domain* yang terdiri dari sekumpulan Proses TI yang merepresentasikan aktivitas yang dapat dikendalikan dan terstruktur. Kerangka kerja tersebut memfokuskan pada lebih banyak kontrol dan sedikit eksekusi sehingga kepentinganya lebih ditujukan kepada pendefinisian strategi dan kontrol yang biasanya dilakukan oleh manajemen tingkat atas, namun tidak detil menjelaskan bagaimana memenuhi keduanya yang dapat dipakai sebagai acuan pengguna yang langsung terkait dengan pengelolaan TI.

Aktivitas teknologi informasi dalam CobIT didefinisikan kedalam model proses yang generik dan dikelompokkan dalam 4 *Domain* dan 34 High Level Control Objectives. Framework CobIT secara keseluruhan dapat dilihat pada gambar berikut. Melalui gambar tersebut dapat dilihat model proses CobIT yang terdiri dari 4 *Domain* dan 34 macam proses.



Gambar 5. Ilustrasi konsep Cobit Framework

III. Metode Penelitian

Dengan mengimplementasikan framework CobIT 4.1 pada *Control Objective* ke-5 dari *Domain Delivery and Support* (DS), *Ensuring System Security* (Memastikan Keamanan Sistem) untuk menjamin integritas sistem informasi di PDE TU SMKN 24, dan dengan beberapa metode sebagai berikut :

1. **Wawancara dan diskusi**
   Wawancara dilakukan dengan mengadakan tanya jawab secara langsung kepada pihak yang berwenang yaitu Ibu Sri Nuryani, BA, selaku Kabag. Tata Usaha (TU) Sekolah Menengah Kejuruan Negeri 24 Jakarta.
2. **Observasi**
   Observasi dilakukan dengan mengamati keseharian para pegawai di lingkungan TU bidang PDE Sekolah Menengah Kejuruan Negeri 24 Jakarta.
3. **Dokumentasi**
   Dokumentasi merupakan pengumpulan data dan pencarian data yang mendukung permasalahan dengan jalan menyalin laporan-laporan, dan catatan - catatan yang berkaitan dengan masalah yang dibahas termasuk mengisi *checklist* berdasarkan hasil wawancara.

IV. HASIL DAN PEMBAHASAN

a. Check List yang Digunakan Dalam Wawancara

Framework CobIT 4.1 pada *Control Objective* ke-5 dari *Domain Delivery and Support* (DS), *Ensuring System Security* (Memastikan Keamanan Sistem) untuk menjamin integritas sistem informasi. Check List yang digunakan pada saat wawancara seperti dibawah ini:

Kuesioner
DS5-MENJAMIN KEAMANAN SISTEM

Nama Responden :
Bidang :
Jabatan :

LEVEL 0 - Non Existent

NO	PERTANYAAN	Y	T
1	Organisasi mengetahui kebutuhan akan keamanan TI		
2	Tanggung jawab dan akuntabilitas dilakukan untuk memastikan keamanan		
3	Ukuran untuk mendukung manajemen keamanan TI di implementasikan		
4	Adanya pelaporan keamanan TI dan proses respon untuk pelanggaran keamanan TI		
5	Apakah kekurangan akan proses administrasi keamanan sistem diketahui		

Gambar 6. Kuesioner Level 0 – Non Existent

LEVEL 1 - Initial/ Ad-hoc

NO	PERTANYAAN	Y	T
1	Organisasi mengetahui kebutuhan keamanan TI		
2	Kesadaran akan kebutuhan untuk keamanan tergantung pada masing-masing individu		
3	Keamanan TI dilaksanakan berdasarkan reaksi atas permasalahan		
4	Keamanan TI terstrutur		
5	Pelanggaran keamanan TI yang terdeteksi menyebabkan saling melempar tanggung jawab karena tidak jelasnya pelimpahan pelaksana		
6	Respon terhadap pelanggaran TI dapat diprediksi		

Gambar 7. Kuesioner Level 1 – Initial/Ad-hoc

LEVEL 2 - Repeatable but intuitive

NO	PERTANYAAN	Y	T
1	Tanggung jawab dan akuntabilitas akan keamanan TI ditugaskan kepada seorang koordinator keamanan TI, walaupun kewenangan pengelolaan koordinator tersebut dibatasi		
2	Kesadaran akan kebutuhan keamanan dipecah-pecah dan dibatasi		
3	Analisis terhadap hasil informasi yang relevan terhadap keamanan yang dihasilkan oleh sistem		
4	Layanan dari pihak ketiga memenuhi kebutuhan keamanan organisasi		
5	Kecukupan peralatan dan keahlian dalam pengembangan kebijakan keamanan		
6	Pelaporan keamanan TI yang lengkap, berhubungan dan terarah		
7	Training keamanan telah tersedia tetapi pelaksanaannya tergantung pada masing-masing orang		
8	Keamanan TI dilihat sebagai sebuah tanggung jawab dari pihak TI dan pihak organisasi/sekolah melihat bahwa keamanan TI sebagian dari areanya		

Gambar 8. Kuesioner Level 2 – Repeatable but intuitive

LEVEL 3 - Define process

NO	PERTANYAAN	Y	T
1	Kesadaran akan keamanan telah ada, dan dipromosikan oleh manajemen		
2	Prosedur keamanan TI telah didefinisikan dan sejalan dengan kebijakan keamanan TI		
3	Tanggung jawab keamanan TI telah ditugaskan dan dimengerti, tetapi dijalankan secara konsisten		
4	Sebuah rencana dan solusi keamanan TI ada karena adanya analisis resiko		
5	Pelaporan keamanan mencakup fokus bisnis yang jelas		
6	Testing keamanan ad hoc (misal testing penyusupan) telah dilakukan		
7	Training keamanan telah tersedia untuk TI dan bisnis tetapi hanya dijadwalkan dan diatur secara informal		

Gambar 9. Kuesioner Level 3 – Define Process

LEVEL 4 - Manage and measureable

NO	PERTANYAAN	Y	T
1	Tanggung jawab untuk keamanan TI telah di tugaskan secara jelas, teratur, dan dijalankan		
2	Analisis resiko dan dampak keamanan TI dilakukan secara konsisten		
3	Kebijakan dan praktik dari keamanan dilengkapi dengan baseline keamanan tertentu		
4	Pengungkapan metode untuk mempromosikan kesadaran akan keamanan dianggap penting		
5	Identifikasi pengguna, otentifikasi dan otorisasi terstandar		
6	Sertifikat keamanan disarankan untuk staf yang bertangunag jawab untuk audit dan manajemen keamanan		
7	Testing keamanan dipenuhi menggunakan standard dan proses formal menuju peningkatan tingkat kemananan		
8	Proses keamana TI dikoordinasikan dengan seluruh fungsi keamanan sekolah/organisasi		
9	Pelaporan keamanan TI dikaitkan dengan tujuan sekolah/organisasi		
10	Training keamanan TI dilakukan baik dalam lingkup TI maupun bisnis		
11	Training keamanan TI direncanakan dan diatur agar mampu merespon kebutuhan bisnis dan profil resiko keamanan yang telah didefinisikan		
12	Tujuan dan matrix untuk manajemen keamanan telah didefinisikan tetapi belum diukur		

Gambar 10. Kuesioner Level 4 – Manage and measurable

LEVEL 5 - Optimised

NO	PERTANYAAN	Y	T
1	Keamanan TI adalah tanggung jawab bersama pihak manajemen sekolah, bagian PDE dan terintegrasi dengan tujuan bisnis keamanan sekolah/organisasi		
2	Kebutuhan keamanan TI didefinisikan dengan jelas, dioptimasi dan dimasukan ke dalam rencana keamanan yang telah disetujui		
3	Pengguna dan pelanggan makin akuntable dalam mendefinisikan kebutuhan keamanan dan fungsi keamanan terintegrasi dengan aplikasi pada saat tahap desain		
4	Insiden keamanan ditangani dengan prosedur respons insiden yang formal yang didukung oleh tool yang terotomatisasi		
5	Penilaaian kemanan periodik dilaksanakan untuk mengevaluasi efektivitas implementasi dari rencana keamanan		
6	Informasi akan ancaman dan kerentanan secara sistematis dikumpulkan dan dianalisis		
7	Kontrol yang cukup untuk mengurangi resiko telah dikomunikasikan dan diimplementasikan		
8	Testing keamanan, root cause analisys akan insiden keamanan dan identifikasi secara proaktif akan resiko, digunakan untuk meningkatkan proses secara berkelanjutan		
9	Proses keamanan dan teknologi terintegrasi di seluruh lini organisasi/sekolah		
10	Metrik untuk manajemen keamanan diukur, dikumpulkan dan dikomunikasikan		
11	Manajemen menggunakan hasil ukuran metrik+B37 untuk menyesuaikan rencana keamanan dalam proses peningkatan yang berkelanjutan		

Gambar 10. Kuesioner Level 5 – Optimized

b. Hasil Perhitungan Maturity Level

Berdasarkan hasil kuesioner yang telah disebarkan kepada staf disekolah yang menggunakan fasilitas PDE, didapat hasil perhitungan sebagai berikut:

Tabel 1. Perhitungan Maturity

Hasil Perhitungan Maturity Level

Domain	Level	Pertanyaan	Jawaban						Total	
			R1	R2	R3	R4	R5	R6	Ya	Tidak
DS5	0	P1	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P2	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P3	Ya	Ya	Ya	Ya	Tidak	Ya	5	1
		P4	Ya	Ya	Ya	Ya	Tidak	Ya	5	1
		P5	Ya	Ya	Ya	Ya	Ya	Ya	6	0
	1	P6	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P7	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P8	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P9	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P10	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P11	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
	2	P12	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P13	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P14	Ya	Ya	Ya	Tidak	Tidak	Tidak	3	3
		P15	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P16	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
		P17	Ya	Ya	Ya	Ya	Tidak	Tidak	4	2
		P18	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
		P19	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
	3	P20	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P21	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P22	Ya	Ya	Ya	Ya	Tidak	Tidak	4	2
		P23	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P24	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P25	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P26	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
	4	P27	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
		P28	Ya	Ya	Ya	Ya	Tidak	Ya	5	1
		P29	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P30	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P31	Ya	Ya	Ya	Ya	Tidak	Ya	5	1
		P32	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P33	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
		P34	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P35	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P36	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
		P37	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P38	Ya	Ya	Ya	Ya	Ya	Ya	6	0
	5	P39	Ya	Ya	Ya	Tidak	Tidak	Tidak	3	3
		P40	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P41	Ya	Ya	Ya	Tidak	Tidak	Tidak	3	3
		P42	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
		P43	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P44	Ya	Ya	Tidak	Tidak	Tidak	Tidak	2	4
		P45	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P46	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P47	Ya	Ya	Ya	Ya	Ya	Ya	6	0
		P48	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6
		P49	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	0	6

Tabel 2. Hasil Perhitungan Maturity

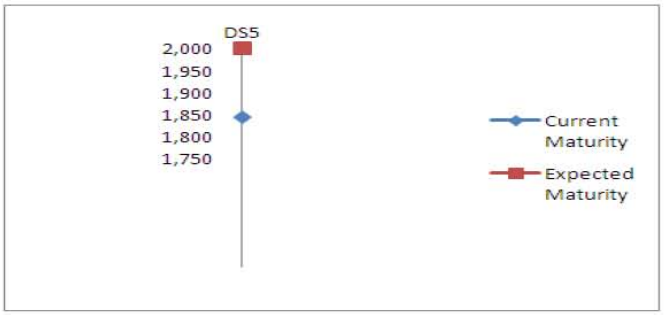
Hasil Perhitungan Maturity Level

Domain	Responden	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Maturity Level
DS5	R1	0,000	0,125	0,439	0,430	0,586	0,570	**2,151**
	R2	0,000	0,125	0,439	0,430	0,586	0,570	**2,151**
	R3	0,000	0,157	0,315	0,540	0,420	0,429	**1,860**
	R4	0,000	0,174	0,261	0,597	0,464	0,158	**1,655**
	R5	0,000	0,246	0,246	0,631	0,327	0,223	**1,673**
	R6	0,000	0,192	0,192	0,494	0,512	0,175	**1,565**
Maturity Level =		**0,000**	**1,020**	**1,892**	**3,123**	**2,895**	**2,126**	1,843

Dari hasil perhitungan maturity diatas, didapat Current Maturity 1,843. Jika Expected Maturity yang diharapkan adalah 2, maka didapat hasil perhitungan radar sebagai berikut:

Radar DS

Domain	Proses	*Current Maturity*	*Expected Maturity*
DS5	*Ensure systems security*	1,843	2



Gambar 11. Radar hasil perhitungan maturity

Dari hasil perhitungan *checklist* seperti yang terlihat dari tabel diatas. Sekolah Menengah Kejuruan Negeri 24 Jakarta termasuk dalam kategori Maturity Level 2 yaitu *Repeatable but Intuitive*.

c. Temuan-temuan

1. Hasil Observasi Lapangan

Hasil observasi lapangan dan wawancara yang dilakukan oleh peneliti adalah pengelolaan teknologi informasi pada aspek DS 5 terkait dengan memastikan sistem keamanan TI yaitu:

a) Penerapan sistem keamanan pada sistem informasi manajemen sekolah dilakukan dengan cara, *user* dalam menggunakan hak aksesnya dibatasi dengan *security matrix* dimana semua pengguna komputer menerima otorisasinya berdasarkan *role*. *Role* yang diberikan disesuaikan dengan kebutuhan pengguna sesuai dengan job description tiap-tiap pengguna komputer. *Role* ini dimaksudkan untuk membatasi apa saja yang dapat dilakukan oleh program-program tersebut. Pengaksesan Sistem Aplikasi hanya dapat dilakukan oleh orang-orang yang terotorisasi dan diberi wewenang untuk mengakses. Misalnya, data apa yang dapat diakses, data mana yang hanya dapat dilihat (*read only*), ditambah, diubah atau dihapus, apabila pengaturan *role* ini tidak tepat, maka akan banyak pihak-pihak yang tidak berwenang dapat mengakses data tertentu, sehingga jika itu terjadi maka keyakinan akan integritas data akan menjadi berkurang dan juga akan terjadi banyak perubahan-perubahan data yang tidak diinginkan.
b) Setiap user login menggunakan *password,* dengan kombinasi angka dan huruf, password yang dimasukan tidak terlihat dan secara otomatis akan lock user apabila terjadi 3 kali kesalahan login yang dilakukan oleh user, sistem aplikasi menampilkan pesan jika verifikasi login tidak valid dan yang dapat membuka kembali lock user adalah Administrator sehingga dengan adanya pembatasan sistem kesalahan dalam penginputan login akses ini akan mempersulit bagi orang- orang yang tidak memiliki otoritas untuk mengakses ke sistem aplikasi. Penggunaan password bertujuan untuk mencegah kepada pihak-pihak yang tidak mempunyai hak akses atas aplikasi dan data-data dalam PDE.
c) Untuk melindungi akses dari luar, digunakan VPN (*virtual private network*), dimana untuk login lewat internet, maka user akan memasukkan password untuk melakukan akses.
d) Untuk mengantisipasi perkembangan virus telah dipasang anti virus pada setiap komputer yang update signature nya setiap ada virus baru, virus internasional dipergunakan antivirus *Kespersky* 2010 yang update secara otomatis dan virus lokal dipergunakan antivirus Smadav Pro yang update secara otomatis ketika terhubung internet.
e) Untuk keamanan aset-aset fisik, dalam tata usaha (TU) disediakan 2 buah pemadam kebakaran yang diletakkan masing- masing pada bagian PDE dan bagian Kepegawaian, hal ini dilakukan jika sewaktu-waktu ada kebakaran yang mungkin disebabkan oleh hubungan arus listrik pendek atau akibat yang lain.

f) Bidang PDE beroperasi 8 jam setiap harinya (kecuali hari minggu/ hari libur), di monitoring seorang administrator yang memiliki staff TI sebanyak tiga orang yang kompeten dibidangnya, sehingga komputer di dalam PDE selalu ada pengawasan.
g) PDE menggunakan *Uninterupable Power Supply* (UPS) yang digunakan untuk menstabilkan tegangan listrik, UPS ini juga berfungsi sebagai pengamanan data apabila listrik mati mendadak, UPS dapat bertahan kurang lebih 3 jam, sehingga dalam jangka waktu tersebut Administrator dapat melakukan back up data - data sekolah untuk disimpan di tempat yang lebih aman dan melakukan shut down sesuai dengan prosedur.

Untuk pencegahan kerusakan perangkat keras, PDE melakukan kontrak pemeliharaan dengan pihak ketiga dimana pekerjaan pemeliharaan dilakukan oleh pihak ketiga 2 kali setahun yaitu bulan November dan bulan April yang pelaksanaannya ditetapkan oleh sekolah, apabila hardware ada masalah pihak ketiga menyediakan pelayanan 24 jam dan pihak ketiga menjamin dapat menyelesaikan perbaikan masing -masing hardware dalam jangka waktu paling lama 3x24 jam, sedangkan untuk software, perusahaan membeli software yang berlisensi sehingga jelas legalitasnya.

Dari hasil observasi, wawancara dan pengamatan langsung dilapangan, SMK Negeri 24 Jakarta, didapat temuan sebagai berikut: 1. Registry Editor

Gambar 12. Bukti penguncian Registry Editor

2. Server

Gambar 13. Server yang digunakan untuk sistem PDE

2. Hasil Kuesioner perhitungan Cobit

Dari hasil kuesioner dan perhitungan berdasarkan Cobit DS5, Keamanan Sistem Informasi, didapat temuan-temuan sebagai berikut:

Tabel 3. Temuan berdasarkan level 0 – Non Existen

Temuan-temuan berdasarkan kuesioner
DS5-MENJAMIN KEAMANAN SISTEM

LEVEL 0 - Non Existent

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Organisasi mengetahui kebutuhan akan keamanan TI	6	1	Adanya pembatasan hak akses; Penggunaan Password untuk setiap user/account; Sekolah telah berlangganan antivirus
2	Tanggung jawab dan akuntabilitas dilakukan untuk memastikan keamanan	6	1	Tiap user memiliki hak akses yang berbeda; Tiap user/account memiliki password
3	Ukuran untuk mendukung manajemen keamanan TI di implementasikan	5	0,833	Keamanan TI diimplementasikan, tapi masih belum menyeluruh
4	Adanya pelaporan keamanan TI dan proses respon untuk pelanggarann keamanan TI	5	0,833	Ada respon tapi belum ada pelaporan untuk respon
5	Apakah kekurangan akan proses administrasi keamanan sistem diketahui	6	1	Diketahui; belum ada kebijakan umur password; adanya penyalahgunaan pemakaian account milik orang lain

Maturity Level = 0,000

Tabel 4. Temuan berdasarkan level 1 – Initial/Ad-hoc

LEVEL 1 - Initial/ Ad-hoc

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Organisasi mengetahui kebutuhan keamanan TI	0	0	Sebenarnya mengetahui namun disepelekan
2	Kesadaran akan kebutuhan untuk keamanan tergantung pada masing-masing individu	6	1	Tiap user memiliki hak akses yang berbeda; Tiap user/account memiliki password
3	Keamanan TI dilaksanakan berdasarkan reaksi atas permasalahan	6	1	Sudah ada respon sebagai reaksi atas permasalahan keamanan TI
4	Keamanan TI terukur	0	0	Belum terukur
5	Pelanggaran keamanan TI yang terdeteksi menyebabkan saling melempar tanggung jawab karena tidak jelasnya pelimpahan	6	1	Belum ada seksi untuk security sistem di bagian Pengolahan Data Elektronik (PDE)
6	Respon terhadap pelanggaran TI dapat diprediksi	0	0	Tidak dapat diprediksi

Maturity Level = 1,020

Tabel 5. Temuan berdasarkan level 2 – Repeatable but intuitive

LEVEL 2 - Repeatable but intuitive

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Tanggung jawab dan akuntabilitas akan keamanan TI ditugaskan kepada seorang koordinator keamanan TI, walaupun kewenangan pengelolaan koordinator tersebut dibatasi	0	0	Tidak ada koordinator untuk keamanan TI di bagian Pengolahan Data Elektronik (PDE)
2	Kesadaran akan kebutuhan keamanan dipecah-pecah dan dibatasi	6	1	Sudah sesuai
3	Analisis terhadap hasil informasi yang relevan terhadap keamanan yang dihasilkan oleh sistem	3	0,5	Keamanan yang dihasilkan sistem tidak semua berdasar pada hasil analisa
4	Layanan dari pihak ketiga memenuhi kebutuhan keamanan organisasi	6	1	Ada perjanjian dengan pihak ke-3 untuk melakukan maintenance 2 kali setahun; adanya karyawan honorer yang bertanggung jawab dibagian PDE.
5	Kecukupan peralatan dan keahlian dalam pengembangan kebijakan keamanan	2	0,333	Peralatan dan keahlian belum mencukupi
6	Pelaporan keamanan TI yang lengkap, berhubungan dan terarah	4	0,667	Ada dokumentasi tapi tidak lengkap
7	Training keamanan telah tersedia tetapi pelaksanaannya tergantung pada masing-masing orang	2	0,333	Tidak ada training khusus untuk keamanan, tetapi ada himbauan dan pemberitahuan yang didalamnya berisi tentang keamanan meskipun sedikit
8	Keamanan TI dilihat sebagai sebuah tanggung jawab dari pihak TI dan pihak sekolah/organisasi melihat bahwa keamanan TI sebagian dari areanya	2	0,333	Keamanan TI belum dianggap sebagai hal yang utama, dikarenakan pelanggaran TI sering terjadi

Maturity Level = 1,892

Tabel 6. Temuan berdasarkan level 3 – Define process

LEVEL 3 - Define process

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Kesadaran akan keamanan telah ada, dan dipromosikan oleh pihak sekolah/organisasi	6	1	Telah ada dan dipromosikan
2	Prosedur keamanan TI telah didefinisikan dan sejalan dengan kebijakan keamanan TI	6	1	Telah didefinisikan dan sejalan dengan kebijakan keamanan TI
3	Tanggung jawab keamanan TI telah ditugaskan dan dimengerti, tetapi dijalankan secara konsisten	4	0,667	Telah ditugaskan dan (mungkin) dimengerti, tetapi belum sepenuhnya konsisten
4	Sebuah rencana dan solusi keamanan TI ada karena adanya analisis resiko	6	1	Terdapat analisis resiko untuk rencana keamanan TI
5	Pelaporan keamanan mencakup fokus bisnis yang jelas	0	0	Pelaporan keamanan belum ada
6	Testing keamanan ad hoc (misal testing penyusupan) telah dilakukan	0	0	Belum ada testing ad hoc
7	Training keamanan telah tersedia untuk TI dan bisnis tetapi hanya dijadwalkan dan diatur secara informal	0	0	Tidak ada training khusus untuk keamanan, tetapi ada pelatihan yang didalamnya berisi tentang penggunaan PDE dan sedikit mengenai keamanan

Maturity Level = 3,123

Tabel 7. Temuan berdasarkan level 4 – Manage and measurable

LEVEL 4 - Manage and measureable

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Tanggung jawab untuk keamanan TI telah di tugaskan secara jelas, teratur, dan dijalankan	2	0,333	Dijalankan, belum ditugaskan dan diatur
2	Analisis resiko dan dampak keamanan TI dilakukan secara konsisten	5	0,833	Analisis resiko telah dilakukan, tetapi belum konsisten
3	Kebijakan dan praktik dari keamanan dilengkapi dengan baseline keamanan tertentu	0	0	Kebijakan praktek keamanan tidak berdasarkan baseline tertentu
4	Pengungkapan metode untuk mempromosikan kesadaran akan keamanan dianggap penting	0	0	Keamanan TI belum dianggap sebagai hal yang penting, dikarenakan pelanggaran TI jarang terjadi
5	Identifikasi pengguna, otentifikasi dan otorisasi terstandar	5	0,833	Ada tetapi belum terstandar
6	Sertifikat keamanan disarankan untuk staf yang bertangunag jawab untuk audit dan manajemen keamanan	0	0	Tidak ada
7	Testing keamanan dipenuhi menggunakan standard an proses formal menuju peningkatan tingkat kemananan	2	0,333	Belum ada testing khusus keamanan
8	Proses keamana TI dikoordinasikan dengan seluruh fungsi keamanan sekolah/organinsasi	0	0	Tidak dikoordinasikan dengan seluruh fungsi keamanan organisasi
9	Pelaporan keamanan TI dikaitkan dengan tujuan sekolah/organisasi	6	1	Belum ada pelaporan keamanan
10	Training keamanan TI dilakukan baik dalam lingkup TI maupun bisnis	2	0,333	Training yang mencakup keamanan hanya terbatas pada kalangan tertentu
11	Training keamanan TI direncanakan dan diatur agar mampu merespon kebutuhan bisnis dan profil resiko keamanan yang telah didefinisikan	0	0	Tidak ada training khusus keamanan
12	Tujuan dan matrix untuk manajemen keamanan telah didefinisikan tetapi belum diukur	6	1	Telah didefinisikan tetapi belum diukur

Maturity Level = 2,895

Tabel 8. Temuan berdasarkan level 5 –Optimised

LEVEL 5 - Optimised

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Keamanan TI adalah tanggung jawab bersama pihak manajemen sekolah, bagian PDE dan terintegrasi dengan tujuan bisnis keamanan sekolah/organisasi	3	0,5	TI belum menjadi bagian dari strategic plan bisnis disekolah, tetapi IT plan telah dibuat (ada)
2	Kebutuhan keamanan TI didefinisikan dengan jelas, dioptimasi dan dimasukan ke dalam rencana keamanan yang telah disetujui	0	0	Keamanan TI belum dianggap hal yang penting, dikarenakan pelanggaran IT tidak sering terjadi
3	Pengguna dan pelanggan makin akuntable dalam mendefinisikan kebutuhan keamanan dan fungsi keamanan terintegrasi dengan aplikasi pada saat tahap desain	3	0,5	Tidak semua pengguna sadar akan keamanan sistem informasi
4	Insiden keamanan ditangani dengan prosedur respons insiden yang formal yang didukung oleh tool yang terotomatisasi	2	0,333	Telah tersedia tool untuk mengatasi insiden walau tidak lengkap dan belum semua terotomatisasi
5	Penilaaian kemanan periodik dilaksanakan untuk mengevaluasi efektivitas implementasi dari rencana keamanan	0	0	Tidak ada penilaian keamanan secara periodik
6	Informasi akan ancaman dan kerentanan secara sistematis dikumpulkan dan dianalisis	2	0,333	Sedikit dikumpulkan dan dianalisis
7	Kontrol yang cukup untuk mengurangi resiko telah dikomunikasikan dan diimplementasikan	0	0	Kontrol yang dilakukan belum cukup (masih terbatas) dan belum ada bagian khusus untuk keamanan TI
8	Testing keamanan, root cause analisys akan insiden keamanan dan identifikasi secara proaktif akan resiko, digunakan untuk meningkatkan proses secara berkelanjutan	0	0	Belum ada testing keamanan
9	Proses keamanan dan teknologi terintegrasi di seluruh lini organisasi/sekolah	6	1	Proses keamanan baru terlaksana di bagian PDE
10	Metrik untuk manajemen keamanan diukur, dikumpulkan dan dikomunikasikan	0	0	Belum terukur
11	Manajemen menggunakan hasil ukuran metrik+B37 untuk menyesuaikan rencana keamanan dalam proses peningkatan yang berkelanjutan	0	0	Belum ada

Maturity Level = 2,126

d. Identifikasi Resiko

Ancaman/Sumber	Resiko	Pengendalian
Password/login diketahui oleh orang yang tidak berhak	Terjadi perubahan, dan bahkan penghapusan data sekolah	Sekolah membuat kebijakan pembatasan umur password
Tidak adanya pembatasan *role* untuk setiap user	User dapat mengakses data dan aplikasi lainnya yang bukan tanggung jawabnya	Pengguna dalammenggunakanhak aksesnyadibatasi dengan *security matrix* dimana semua user menerima otorisasinya berdasarkan *role*. *Role* yang diberikan disesuaikan dengan kebutuhan *user* sesuai dengan *job description*.
Tidak adanya perlindungan untuk akses lewat internet	Hacker dapat masuk dan mengutak-atik data sekolah, baik nilai siswa maupun data lainnya	Membuat *firewall* berlapis untuk akses lewat internet
Antivirus di sekolah tersebut tidak dapat mencegah masuknya virus ke komputer	Virus akan masuk dan dapat merusak data-data sekolah	Sekolah membeli virus lokal dan virus internasional dengan berlangganan
Listrik mati mendadak	Proses bisnis sekolah dapat terhenti	Penggunaan *Uninterupable Power supply*
Terjadi kebakaran	Mengakibatkan data-data sekolah hilang	Pemasangan pemadam kebakaran ditempat yang mudah dijangkau.
Kerusakan perangkat keras	Proses bisnis sekolah dapat berhenti apabila tidak dilakukan tindakan yang lebih lanjut	Sekolah melakukan perjanjian pemeliharaan perangkat keras dengan pihak ketiga

e. Hasil Observasi dan Perhitungan Maturity

Dari hasil perhitungan *checklist* didapat Sekolah Menengah Kejuruan Negeri 24 Jakarta termasuk dalam kategori Maturity Level 2 yaitu *Repeatable but Intuitive*.

Level 2 (*Repeatable but Intuitive*) adalah ketika tanggung jawab dan penanggung jawab keamanan TI ditentukan dalam koordinator keamanan TI, walaupun manajemen otoritasnya terbatas. Kesadaran akan kebutuhan keamanan terpecah dan terbatas. Walaupun informasi terkait dengan keamanan diproduksi oleh sistem, namun tidak dianalisis. Layanan dari pihak ketiga mungkin tidak memenuhi kebutuhan keamanan perusahaan secara spesifik. Kebijakan keamanan sedang dikembangkan tetapi keahlian dan perakatan tidak mencukupi. Pelaporan keamanan TI tidak lengkap, cenderung membingungkan atau tidak berhubungan. Pelatihan keamanan tersedia namun dilakukan umumnya karena inisiatif individu. Keamanan TI terutama terlihat sebagai tanggung jawab dan area TI sementara bisnis tidak melihat keamanan TI dalam areanya.

f. Rekomendasi

Dalam kaitannya dalam menjamin integritas keamanan sistem informasi yang ada di Sekolah Menengah Kejuruan Negeri 24 Jakarta, sebaiknya pihak Tata Usaha (TU) Sekolah yang membawahi bidang Pengolahan Data Elektronik (PDE) mempunyai target tingkat maturity level yang ingin dicapai. Misalkan saat ini PDE Sekolah masih berada di maturity level 2, dalam jangka 5 tahun ke depan TU mentargetkan untuk mencapai maturity level 3. Akan tetapi dengan terlebih dahulu menyempurnakan level tingkat kedewasaan yang semula 1,8 menjadi 2.

V. PENUTUP

5.1. Kesimpulan

Keamanan teknologi informasi di Pengolahan Data Elektronik (PDE) SMK Negeri 24 Jakarta berdasarkan *domain Delivery and Support* (DS) *Control Objective Ensuring System Security* telah mencapai maturity level 2 (*Repeatable but Intuitive*).

Untuk level Sekolah, level ini sudah termasuk kategori cukup optimal, hal ini dapat dilihat dari adanya pembatasan hak akses *user* yang didasarkan pada job description masing-

masing pegawai, setiap *user login* menggunakan password dengan kombinasi angka dan huruf, password yang dimasukan tidak terlihat dan secara otomatis akan lock user apabila terjadi 3 kali kesalahan login yang dilakukan oleh user.

5.2. Saran

Pengukuran tingkat maturity Pengolahan Data Elektronik (PDE) pada bagian TU ini masih jauh dari sempurna, untuk kedepannya diharapkan diadakan pengukuran kembali dengan menyempurnakan checklist yang telah ada dan mengembangkan *domain* pengukurannya, tidak hanya DS5. Selain itu, untuk pengisian kuesioner diharapkan yang mengisi adalah orang-orang yang benar-benar mengetahui system PDE dengan didampingi pengisian kuesionernya oleh orang yang lebih ahli dibidang pengukuran maturity (Cobit).

Daftar Pustaka

Dwiyatmoko Pujiwidodo, *Struktur Pengendalian Intern Terhadap Sistem Pengolahan Data Elektronik (PDE).* PERSPEKTIF VOL. V NO. 2. APRIL 2007

IT Governance Institute. 2007. *COBIT 4.1.* USA: IT Governance Institute.

McLeod, Jr, Raymond, dan P. Schell, George. 2008. *Management Information Systems, Sistem Informasi Manajemen.* Jakarta: Salemba Empat.

Yudhie. 2011. *http://www.yudhie-sitte.co.cc/index.php?option=com_content&view=article&id=35:is-it-possible-to-change-the-types-of-menu-entries&catid=31:tentang-komputer&Itemid=46*, Tanggal akses 18 maret 2011.

Cameron, Debra. (1998). *E-Commerce Security Strategies: Protecting the Enterprise.* Computer
Technology Research Corp. Charleston, SC.

Enger, Norman L & Hawerton, Paul W. (1980). *Computer Security: A Management Audit Approach.* Amacom.

Fraser. B..(1997). *Network Working Group. Site Security Handbook.*

Gullati,VP and Dube DP (2005), *Information System Audit and Assurance,*Tata McGraw-Hill
Publishing Company Ltd.

Gondodiyoto, S. (2007). *Audit Sistem Informasi + Pendekatan COBIT.* Edisi Revisi. PT. Mitra Wacana Media. Jakarta.

Hall, James A. (2001). *Sistem Informasi Akuntansi.* Buku ke-1, Edisi ke-1. Terjemahan Jusuf, A.A. Salemba Empat, Jakarta.

IT Governance Institute.(2007).*COBIT 4.1.* United State of America.

Jones, Frederick L & Rama, Dasaratha V. (2003). *Accounting Information System, A Business Process Approach.* Thomson. South-Western.

O'Brien, James.A.(2005). *Introduction to Information Systems.* Edisi ke-12. Salemba Empat, Jakarta.

Onno Purbo dan Aang Arif Wahyudi, (2001) *Mengenl E-Commerce*, PT Elex Media Komputindo Jakarta.

Ron Weber,(2002) *Information System Control and Audit*, Willey.

Robbins, P. Stephen & Coulter, Mery. (1999). *Manajemen.* Sixth Edition. Diterjemahkan oleh Drs. T. Hermaya. Jilid 1. PT Prenhallindo, Jakarta.