PENGUKURAN MATURITY LEVEL CONTROL OBJECTIVE KE-5 DOMAIN DELIVERY AND SUPPORT : ENSURING SYSTEM SECURITY MENGGUNAKAN FRAMEWORK COBIT 4.1

Andhy Permadi

Prodi Sistem Informasi Universitas Islam Negeri Sunan Ampel Surabaya,
Jl. Ahmad Yani 117 Surabaya
andhy@uinsby.ac.id

Abstrak

Penelitian ini berfokus pada tata usaha sebagai pusat pengolahan data elektronik (PDE) di SMKN 24 dengan tujuan untuk menilai pengendalian umum apakah mampu memenuhi tujuannya dan melakukan pemetaan terhadap tahap audit TI beserta keamanannya yang kemudian diaplikasikan pada sebuah organisasi yang bergerak dibidang pendidikan, yaitu SMKN 24 Jakarta untuk melihat kinerja TI yang ada. Kerangka kerja yang digunakan sebagai acuan adalah framework CobIT 4.1 pada Control Objective ke-5 dari Domain Delivery and Support (DS), Ensuring System Security (Memastikan Keamanan Sistem) untuk menjamin integritas informasi di PDE. Bukti (evidence) digunakan untuk menentukan apakah data yang diaudit sesuai dengan kriteria dan tujuan audit dengan cara : peninjauan terhadap struktur organisasi, wawancara kepada personel yang tepat dan pengisian kuesioner. Penentuan Maturity level (tingkat kedewasaan), merupakan bagian dari pengujian kepatutan terhadap aktivitas yang ada atau dilakukan di tiap proses TI berdasarkan kerangka kerja COBIT sesuai dengan tingkatan levelnya.

Kata Kunci: *audit TI, CobIT 4.1, Domain Delivery and Support (DS), Ensuring System Security.*

Abstract

This research is focused on Administration as electronic data processing centerat SMKN 24 Jakarta, in order to assess whether it is able to meet its goals and to perform mapping toward IT audit and its security.Framework used as a reference is Cobit 4.1 on Control Objective no.5 from DomainDelivery and Support (DS), Ensuring Security System to ensure the integrity of information at PDE. Evidence is used to determine whether the data to be audited is in accordance with the criteria and the purpose of audit by: organizational structurereview, appropriate personnel interview and questionnaire filling.The determination of maturity level is part of proprietytesting on the existing activitiesor executed in each of IT process, based on COBIT framework inaptly its level.

Keywords: *audit TI, CobIT 4.1, Domain Delivery and Support (DS), Ensuring System Security.*

1. PENDAHULUAN

Sekolah Menengah Kejuruan Negeri 24 Jakarta beralamat di jalan bambu hitam, kelurahan bambu apus, kecamatan cipayung, Jakarta timur. Memiliki dua kelompok keahlian yaitu, Pariwisata (Akomodasi Perhotelan, Jasa Boga, Busana Butik), dan Teknologi Informasi & Komunikasi (Rekayasa Perangkat Lunak).

Berdirinya program keahlian RPL pada tahun 2004 memberikan banyak pengaruh terhadap penerapan ICT bagi proses kegiatan belajar mengajar (KBM), diantaranya :

- Pengisian perangkat pembelajaran seperti, Silabus dan rencana pelaksanaan pembelajaran (RPP) sudah ada *softcopy*-nya, sehingga setiap guru mengisi perangkat pembelajaran sesuai dengan jurusannya dari masing-masing kelas dikomputer sekolah atau *notebook* pribadi.
- penggunaan media pembelajaran berbasis IT, dengan menggunakan *notebook* yang berisi modul mata pelajaran, dan dengan menggunakan proyektor untuk menampilkannya dilayar, sehingga bisa dilihat seluruh siswa dikelas.
- Semua manajemen sekolah di tata usaha (TU) sudah meninggalkan mesin tik (manual), menjadi pengolahan data elektronik (PDE) yang terintegrasi.

Saat ini SMKN 24 memiliki dua lab. Komputer, satu lab. KKPI, dan sebuah server yang berisi

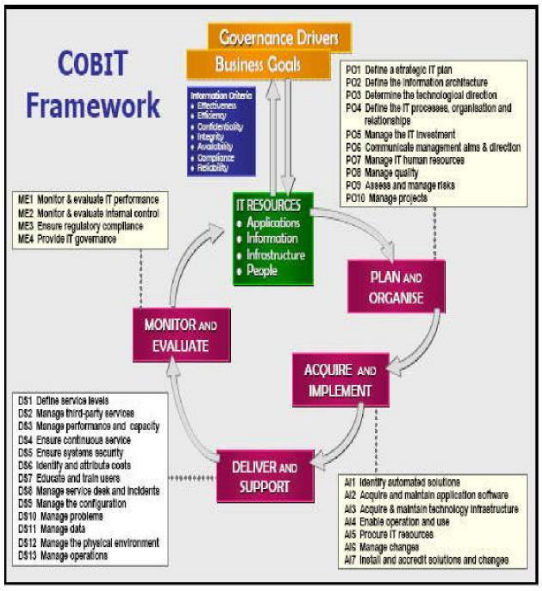
beberapa database sekolah. Meningkatnya pengelolaan teknologi informasi (TI) pada kegiatan sekolah, maka harus ada audit sistem informasi atau teknologi informasi, yang berfokus pada keamanan sistem dan manajemen data di TU bidang PDE, untuk menilai apakah pengendalian umum mampu memenuhi tujuannya.

Metodologi yang digunakan diantaranya adalah wawancara dan pengisian kuesioner terhadap *user* yang kesehariannya mengelola PDE di SMKN 24 ini dan dengan menggunakan *framework COBIT* 4.1 diharapkan mendapatkan *evidence*, namun tidak semua langkah yang ada didalam framework tersebut dilaksanakan keseluruhannya, dengan alasan mengurangi pengulangan aktivitas, maka tetap berpegang pada aturan-aturan yang bersifat umum yang telah ditetapkan oleh IT Assurance Guide [3].

2. METODE PENELITIAN

CobIT dianggap sebagai kerangka kerja yang tepat untuk dipakai dalam melakukan proses audit pengelolaan TI yang ada di PDE tata usaha (TU) SMKN 24, 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 TU yang berfokus pada tata kelola TI-nya, saat ini masih sebagai kontrol dari proses bisnis.

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 [1].



Gambar 2.1. Ilustrasi Konsep CobIT Framework [2]

2.1 Teknik Pengumpulan Data

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

a) 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.
b) Observasi
   Observasi dilakukan dengan mengamati keseharian para pegawai di lingkungan TU bidang PDE Sekolah Menengah Kejuruan Negeri 24 Jakarta.
c) 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.

2.2 Identifikasi Resiko Keamanan

Identifikasi resiko keamanan dibuat dalam bentuk tabel yakni tabel 1.1.

Tabel 1.1
Identifikasi Resiko Keamanan

Ancaman/sumber	Resiko	Pengendalian
Password logindiketahui olehorang yang tidakberhak.	Terjadi perubahan, danbahkan penghapusandata perusahaan	Perusahaanmembuatkebijakanpembatasan umur *password* . Sosialisasi penggantian password.
Tidak adapembatasan *role*pada setiap user	User dapat mengaksesdata dan aplikasilainnya yang bukantanggungjawabnya	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 perusahaan	Membuat *firewall* berlapis untuk akses lewat internet.
Anti virus pada perusahaan tidak dapat mencegah masuknya virus ke komputer.	Virus akan masuk dan dapat merusak data- data perusahaan	Perusahaan membeli virus lokal dan virus internasional secara berlangganan.
Listrik mati mendadak	Proses bisnis perusahaan dapat terhenti	Penggunaan *Uninterupable Power Supply* (UPS).
Terjadi kebakaran	Mengakibatkan data-data perusahaan hilang	Pemasangan pemadam kebakaran ditempat yang mudah dijangkau.
Kerusakan perangkat keras	Proses bisnis perusahaan dapat terhenti apa bila tidak dilakukan tindakan yang lebih lanjut.	Perusahaan melakukan perjanjian pemeliharaan perangkat keras dengan pihak ketiga.

Tabel 1.2
Checklist yang digunakan dalam Wawancara

Lampiran 1 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 pelanggan keamanan TI		
5	Apakah kekurangan akan proses administrasi keamanan sistem diketahui		

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		

LEVEL 2 - Repeatable but intuitive

NO	PERTANYAAN	Y	T
1	Tanggung jawab dan akuntabilitas akan keamanan TI ditugaskan kepada seorang koordinatorkeamanan 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 bisnis melihat bahwa keamanan TI sebagian dari arenya		

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		

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 an proses formal menuju peningkatan tingkat kemananan		
8	Proses keamana TI dikoordinasikan dengan seluruh fungsi keamanan organinsasi		
9	Pelaporan keamanan TI dikaitkan dengan tujuan bisnis		
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		

LEVEL 5 - Optimised

NO	PERTANYAAN	Y	T
1	Keamanan TI adalah tanggung jawab bersama pihak manajemen bisnis manajemen TI dan terintegrasi dengan tujuan bisnis keamanan 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		
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		

3. HASIL DAN PEMBAHASAN

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

3.1 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 Aplikasihanya dapat dilakukan oleh orang-orang yang terotorisasi dan diberi wewenang untuk mengakses. Misalnya, data apa yang dapat diakses, data mana yang hanya dapat dilihat, 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.

3.2 Setiap *user login* menggunakan *password*, dengan kombinasi angka dan huruf, *password* yang dimasukan tidak terlihat dan secara otomatisakan *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.

3.3 Untuk melindungi akses dari luar, digunakan VPN (*virtual private network*), dimana untuk *login* lewat internet, maka *user* akan memasukkan *password* untuk melakukan akses.

3.4 Untuk mengantisipasi perkembangan virus telah dipasanganti 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 ketikat erhubung internet.

3.5 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.

3.6 Bidang PDE beroperasi 8 jam setiap harinya (kecuali hari minggu/hari libur), dimonitoring seorang administrator yang memiliki staff TI sebanyak tiga orang yang kompeten dibidangnya, sehingga komputer PDE selalu ada pengawasan.

3.7 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 sekolah untuk disimpan di tempat yang lebih aman dan melakukan *shut down* sesuai dengan prosedur.

3.8 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.

Berikut tabel hasil kuesioner DS5-Menjamin Keamanan Sistem.

Tabel 1.3
Level 0 – Non Existent

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Organisasi mengetahui kebutuhan akan keamanan TI	6	1	Ada pembatasan hak akses; Sekolah telah berlangganan antivirus
2	Tanggung jawab dan akuntabilitas dilakukan untuk memastikan keamanan	6	1	Tiap user memiliki hak akses yang berbeda
3	Ukuran untuk mendukung manajemen keamanan TI di implementasikan	5	0.833	Keamanan TI diimplementasikan, tapi masih bel menyeluruh
4	Adanya pelaporan keamanan TI dan proses respon untuk pelanggan keamanan TI	5	0.833	Ada respon tapi belum ada pelaporan untuk resp
5	Apakah kekurangan akan proses administrasi keamanan sistem diketahui	6	1	Diketahui; belum ada kebijakan umur password
		Maturity	0,000	

Tabel 1.4
Level 1 – Initial Ad-hoc

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Organisasi mengetahui kebutuhan keamanan TI	0	0	Ada pembatasan hak akses; Sekolah telah berlangganan antivirus
2	Kesadaran akan kebutuhan untuk keamanan tergantung pada masing-masing individu	6	1	Tiap user memiliki hak akses yang berbeda
3	Keamanan TI dilaksanakan berdasarkan reaksi atas permasalahan	6	1	Ada respon sebagai reaksi atas permasalahan keamanan TI
4	Keamanan TI terstruktur	6	1	Belum terukur
5	Pelanggaran keamanan TI yang terdeteksi menyebabkan saling melempar tanggung jawab karena tidak jelasnya pelimpahan pelaksana	6	1	Belum ada seksi untuk security sistem di Biro TI
6	Respon terhadap pelanggaran TI dapat diprediksi	0	0	Tidak dapat diprediksi
		Maturity	1,283	

Tabel 1.5
Level 2 – Repeatable but Intuitive

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Tanggung jawab dan akuntabilitas akan keamanan TI ditugaskan kepada seorang koordinatorkeamanan TI, walaupun kewenangan pengelolaan koordinator tersebut dibatasi	0	0	Tidak ada koordinator keamanan TI
2	Kesadaran akan kebutuhan keamanan dipecah-pecah dan dibatasi	6	1	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
5	Kecukupan peralatan dan keahlian dalam pengembangan kebijakan	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 peralatan yang didalamnya berisi tentang keamanan meskipun sedikit
8	Keamanan TI dilihat sebagai sebuah tanggung jawab dari pihak TI dan pihak bisnis melihat bahwa keamanan TI sebagian dari arenya	2	0.333	Keamanan TI belum dianggap sebagai hal yang utama, dikarenakan pelanggaran TI sering terjadi
		Maturity	1,797	

Tabel 1.6
Level 3 – Define Process

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Kesadaran akan keamanan telah ada, dan dipromosikan oleh manajemen	6	1	Telah ada dan dipromosikan
2	Prosedur keamanan TI telah didefinisikan dan sejalan dengan	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 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 keamanan meskipun sedikit
		Maturity	1,951	

Tabel 1.7
Level 4 – Manage and Measurable

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 tidak sering 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	2	0.333	Belum ada testing khusus keamanan
8	Proses keamana TI dikoordinasikan dengan seluruh fungsi keamanan organinsasi	0	0	Tidak dikoordinasikan dengan seluruh fungsi keamanan organisasi
9	Pelaporan keamanan TI dikaitkan dengan tujuan bisnis	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	2,746	

Tabel 1.8
Level 5 – Optimised

NO	PERTANYAAN	Bobot	Nilai	Temuan
1	Keamanan TI adalah tanggung jawab bersama pihak manajemen bisnis manajemen TI dan terintegrasi dengan tujuan bisnis keamanan 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, tetapi belum semua terotomatisasi
5	Penilaian 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	trol yang dilakukan belum cukup (masih tas) 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	6	1	Proses keamanan baru terlaksana di divisi TI
10	Metrik untuk manajemen keamanan diukur, dikumpulkan dan	0	0	Belum terukur
11	Manajemen menggunakan hasil ukuran metrik-B37 untuk mengesuaikan rencana keamanan dalam proses peningkatan yang berkelanjutan	0	0	Belum ada
			Maturity	2,023

Tabel 1.9
Penentuan *Maturity Level* (Tingkat Kedewasaan)

Domain	Responden	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Maturity Level
DS5	R1	0.000	0.161	0.422	0.413	0.562	0.548	**2.105**
	R2	0.000	0.161	0.422	0.413	0.562	0.548	**2.105**
	R3	0.000	0.199	0.299	0.513	0.399	0.408	**1.817**
	R4	0.000	0.219	0.247	0.564	0.439	0.150	**1.619**
	R5	0.000	0.303	0.227	0.584	0.303	0.206	**1.622**
	R6	0.000	0.241	0.181	0.464	0.481	0.164	**1.531**
							Maturity Level =	**1.800**

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*.

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.

4. KESIMPULAAN

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, ini sudah cukup 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 [4]*.

DAFTAR PUSTAKA

[1] Sarno, Riyanarto. 2009. Audit Sistem & Teknologi Informasi. Edisi Pertama. Surabaya: ITS Press.

[2] IT Governance Institute. 2007. COBIT 4.1. USA: IT Governance Institute.

[3] IT Assurance Guide: Using COBIT, Chicago, 2007.

[4] Mcleod, R dan Schell, G.P.2007. Management Information System. Prentice Hall.

[5] IT Governance Institute. COBIT 4.0: Chicago, 2007.