SISTEM TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI BERBASIS FRAMEWORK COBIT 5 (STUDI KASUS : SMA NEGERI 1 PALEMBANG)

Nanda Aftaa Aulia[1)], Darius Antoni[2)], Dedy Syamsuar[3)], Widya Cholil[4)]
Program Studi Magister Teknologi Informasi, Bina Darma, Palembang
nanda_aftaa@yahoo.com[1)], darius.antoni@binadarma.ac.id[2)],
dedy_syamsuar@binadarma.ac.id[3)], widya@binadarma.ac.id[4)]

ABSTRAK

SMA Negeri 1 Palembang merupakan Sekolah Menengah Atas Negeri favorit yang terletak di kota Palembang yang pengelolaan sistem belajar mengajarnya membutuhkan teknologi informasi yang berperan untuk mendukung tujuan sistem pembelajaran dan visi misi sekolah . Penelitian ini menentukan domain proses pada Control Objectives for Information and Related Technology (COBIT 5) dan Pengukuran Capability Level Tata Kelola Keamanan Teknologi Informasi. Metode yang digunakan yang digunakan yaitu deskriptif, kualitatif dan metode análisis menggunakan Balance Score Card (BSC) dan COBIT 5. Berdasarkan hasil penelitian ini ditemukan bahwa proses domain COBIT Framework 5 yang digunakan sesuai dengan Keamanan Teknologi Informasi adalah : (1). APO (Align, Plan and Organise) yaitu : APO13 dan pada domain (2). DSS (Deliver, Service and Support) yaitu : (a). DSS02, (b). DSS050. Hasil dari analisis Capability Level adalah: (1) APO13 : berada pada level 2 – Managed Process, (2) DSS02 : berada pada level 2 – Managed Process, dan (3) DSS05 : berada pada level 2 – Managed Process.

Kata kunci: COBIT Framework 5, Balace Score Card, Domain Process

ABSTRACT

SMA Negeri 1 Palembang is a favorite national high school located in Palembang. This school applies technology of information in its teaching system to support learning system dan school's vision and mision. This study determined the domain process in control objectives for information and related technology (COBIT 5) and the measurement of capability level of in formation technology security management. Methods used are descriptive, cualitative and balance score card (BSC) analysis and COBIT 5. Based on The result of the study, it is found out that the domain process of cobit framework 5 which is appropriately used with the information technolgy security system are: (1). APO13 level 2-managed process,. (2). DSS02 level 2- managed process and (3). DSS05 level 2 -managed process.

Keywords: COBIT Framework 5, Balace Score Card, Domain Process

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini menjadi penting dalam kehidupan sehari-hari. Hampir di setiap kegiatan dan layanan publik pemerintah telah dihubungkan dengan teknologi informasi dan komunikasi. SMA Negeri 1 Palembang merupakan Sekolah Menengah Atas Negeri favorit di kota Palembang yang merupakan salah satu instansi yang pengelolaan sistem belajar mengajarnya membutuhkan keterlibatan teknologi informasi yang berperan untuk mendukkung tujuan sistem pembelajaran dan visi misi sekolah.

Terkhusus di masa pandemi yang kini berlangsung, yaitu pandemi Corona Virus Disease 2019 (COVID-19), yang telah menimbulkan dampak global yang sangat luas bagi seluruh lapisan masyarakat, termasuk dalam pelaksanaan pada bidang pendidikan. Sehingga bagi SMA Negeri 1 Palembang, berdampak pada sistem kegiatan belajar mengajar tatap muka beralih menjadi online.

Teknologi informasi juga dibutuhkan SMA Negeri 1 Palembang dalam pengolahan dan perlindungan data-data penting yang dimiliki, seperti data-data keuangan, informasi priibadi siswa, aset-aset yang dimiliki dan lainnya yang bersifat penting. Sehingga, dibutuhkan sustu sistem yang dapat membantu dalam pengolahan sistem tata kelola teknologi informasi di SMA Negeri 1 Palembang. Maka dari itu, penulis bermaksud melakukan Sistem Tata Kelola Keamanan Teknologi Informasi Berbasis Framework COBIT 5 (Studi Kasus SMA Negeri 1 Palembang).

Identifikasi Masalah

1. Belum adanya sistem yang mengelola keamanan teknologi informasi
2. Belum adanya sumber daya manusia yang bertanggung jawab dalam mengelola sistem manajemen pendataan informasi
3. Belum adanya keamanan sistem yang melindungi akses-akses khusus pengguna dalam menggunakan aplikasi

Rumusan Masalah

1. Bagaimana tingkat kapabilitas tata kelola keamanan teknologi informasi di SMA Negeri 1 Palembang?
2. Bagaimana rekomendasi langkah perbaikan yang harus dilakukan agar tercapai tingkat kapabilitas yang lebih baik?

LANDASAN TEORI

Manajemen Resiko

Manajemen risiko adalah suatu pendekatan terstruktur atau metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman dan merupakan suatu rangkaian aktifitas manusia termasuk: penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan sumberdaya.

Strategi yang dapat diambil antara lain adalah memindahkan risiko kepada pihak lain, menghindari risiko, mengurangi efek risiko dan menampung sebagian atau semua konsekuensi risiko tertentu. Manajemen risiko tradisional terfokus pada risiko-risiko yang timbul oleh

penyebab fisik atau legal seperti bencana alam atau kebakaran, kematian, serta tuntutan hukum.

Sasaran dari pelaksanaan manajemen risiko adalah untuk mengurangi risiko yang berbeda-beda yang berkaitan dengan bidang yang telah dipilih pada tingkat yang dapat diterima oleh masyarakat. Hal ini dapat berupa ancaman yang disebabkan oleh lingkungan, teknologi, manusia, organisani dan politik. Di sisi lain pelaksanaan manaejmen risiko melibatkan segala cara yang tersedia bagi manusia, khususnya, bagi entitas manajemen risiko (manusia, staff dan organisasi).

COBIT

COBIT (*Control Objectives for Information and related Technology)* adalah kumpulan dokumentasi untuk tata kelola teknologi informasi yang membantu auditor, pengguna dan manajemen untuk menjembatani gap antara resiko bisnis, kebutuhan kontrol dan masalah teknis teknologi informasi. (Sanyoto, 2007).

COBIT 5 adalah kerangka *end-to-end* yang menggabungkan banyak kerangka kerja serta dirancang untuk memenuhi kebutuhan *stakeholder*. COBIT 5 fokus pada tata kelola dan manajemen informasi perusahaan. COBIT 5 mengadopsi pandangan ISO 38500 mengenai perlunya tata kelola TI dan manajemen TI dan menggunakan model *Evaluate, Direct and Monitor* ISO 38500.

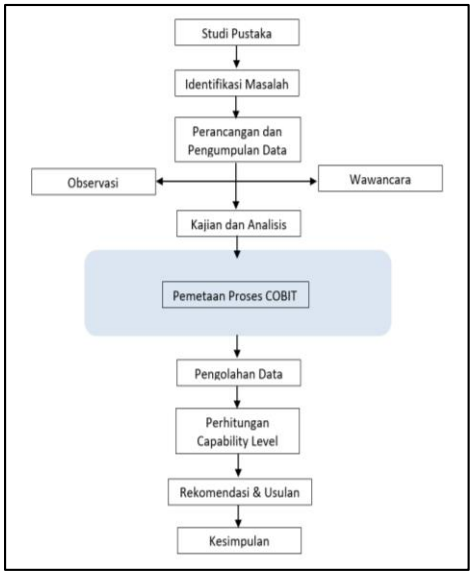
Balanced Scoredcard

BSC *(Balanced Scorecard)* merupakan konsep manajemen untuk mengukur setiap aktivitas yang dilakukan oleh suatu perusahaan dalam rangka merealisasikan tujuan perusahaan tersebut.

Perspektif pada Balanced Scoredcard :

a. Perspektif Keuangan
b. Perspektif Pelanggan
c. Perspekif Proses Bisnis (Internal)
d. Perspektif Pembelajaran & Pertumbuhan

METODOLOGI PENELITIAN



Gambar 1. Metodologi Penelitian

Gambar 1 menjelaskan alur tahapan-tahapan yang dlakukan pada penenlitian. Tahapan pertama yang dilakukan adalah dengan melakukan studi pustaka, yaitu dengan mencari penelitian-penelitian terdahulu, buku-buku terkait yang relevan dengan penelitian yang dilakukan. Tahapan berikutnya adalah melakukan identifikasi masalah yang akan diteliti lalu merancangnya dan mengumpulkan data. Pengumpulan data dilakukan melalui observasi dan wawancara secara informal terhadap responden. Data yang didapatkan, lalu dikaji dan dianalisis untuk dilakukan pemetaan proses domain COBIT dengan template yang telah disediakan oleh COBIT 5. Setelah dilakukan pemetaan, akan

didapatkan data berupa persentase di setiap level kapabilitas yang tercapai, yang kemudian dirangkum dan hitung nilai kapabilitasnya. Nilai kapabilitas yang didapatkan ini kemudian dapat membantu menentukan rekomendasi langkah terbaik apa yang selanjutnya dapatr dilakukan untuk perbaikan dalam sistem tata kelola keamanan teknologi informasi di SMA Negeri 1 Palembang.

PEMBAHASAN

Mapping dan Pemilihan Domain

Proses pemilihan domain ini diawali dengan melihat objektivitas tata kelola, yaitu optimalisasi keamanan informasi untuk optimasi risiko *(Risk Optimisation),* optimalisasi ini berkaitan dengan sistem yang mendukung integrasi SMA Negeri 1 Palembang dalam mengelola sistem keamanan teknologi informasi. Hal ini dapat dilihat pada tabel di bawah ini :

Tabel 1. Tujuan Strategis BSC

BSC Dimension	**Tujuan Strategis**
Finance	Penyesuaian penggunaan sarana dan prasarana terhadap pesatnya perkembangan teknologi informasi untuk pengelolaan sistem keamanan teknologi informasi dalam meningkatkan kegiatan akademik dan non akademik
Customer	Menghasilkan inovasi baru terhadap perkembangan teknologi untuk pembangunan studi dan kepentingan lainnya
Internal	1. Mengaplikasikan inovasi sistem keamanan teknologi informasi dalam bentuk pengolahan data yang terotomatisasi
	2. Pembagian otoritas dalam penggunaan database sistem yang yang digunakan dengan tujuan-tujuan tertentu yang telah ditentukan
Learning and Growh	Peningkatan kemampuan sumberdaya manusia yang memadai untuk implementasi dan perawatan sistem keamanan TI

Proses selanjutnya yang dilakukan adalah memilih *Enterprise Goals* dengan memetakannnya berdasarkan dimensi balanced scorecard, lalu pemilihan diseleksi dengan memilih objek *Primary* pada kolom *Risk Optimisation*.

Proses selanjutnya dengan melakukan seleksi terhadap 14 enterprise *goals* berpredikat primary dengan IT *related goals* yang berjumlah 17 poin. Hasil yang diperoleh, selanjutnya dipetakan kembali dengan dengan proses-proses domain pada COBIT 5.

Hasil pemetaan yang didapatkan, disesuaikan dengan tujuan strategis yang dilakukan oleh SMA Negeri 1 Palembang untuk mendukung proses integrasi yang diinginkan.

Tabel 2. Hasil Pemetaan *IT- Related Goals* dengan Domain *Process* COBIT 5

IT-Related Goals	***COBIT 5 Process***
04 - Managed IT-related decisions	*EDM03, APO10, APO12, APO13, BAI01, BAI06, DSS001, DSS02, DSS03, DSS04, DSS05, DSS06, MEA01, MEA02, MEA03*

Berdasarkan tabel di atas, proses domain COBIT yang dapat di-assessment sesuai dengan kebutuhan SMA Negeri 1 Palembang, yaitu untu

sistema tata kelola teknologi informasi, didapatkan 3 domain yaitu, APO13 *(manage security),* DSS05 *(manage security service),* dan DSS02 *(manage service request and insident).*

Deskripsi proses *COBIT* 5 hasil *assessment*

1. *Manage Security (*APO13)

Menurut ISACA (2012a), APO13 adalah sebuah proses pada COBIT 5 yang terkait dengan pendefinisian, pengoperasian dan pengawasan keamanan serta menjaga risiko keamanan informasi pada tingkatan yang dapat diterima oleh perusahaan. Proses ini memiliki fungsi untuk menjaga dampak dari risiko keamanan informasi agar tetap dalam tingkat yang telah ditetapkan oleh perusahaan.

2. *Managed Security Service* (DSS05)

DSS05 adalah sebuah proses pada COBIT 5 dengan fokus untuk mengelola layanan keamanan pada organisasi untuk mempertahankan risiko keamanan informasi berada pada batas aman yang telah ditentukan (ISACA, 2012b). Selain itu, terdapat juga pelaksanaan klasifikasi data yang telah dilaksanakan namun belum ditemukan dokumen tertulis yang menjelaskan data yang dilakukan oleh perusahaan.

3. *Managed Service Request and Insident* (DSS02)

Menurut ISACA (2012) DSS02 adalah sebuah proses yang menyediakam respon tepat waktu dan cepat terhadap permintaan layanan dan resolusi pengguna atas semua jenis insiden. Serta mampu meningkatkan produktivitas dan meminimalis gangguan melalui penanganan yang cepat atas kebutuhan personil dan insiden yang terjadi. Hal ini berkaitan dengan penyediaan layanan teknologi informasi saat pandemi terjadi, yaitu dimana kegiatan belajar mengajar dilakukan secara *online* sehingga layanan dan insiden butuh ditangani dan diminimalisir dengan baik sehingga tidak menggangu kegiatan belajar megajar, serta aktivitas guru maupun staff yang berlangsung.

Penilaian Kapabilitas Proses

Berdasarkan hasil penilaian terhadap proses DSS05, APO13 dan DSS02, dapat dirangkum hasil sebagai berikut :

Tabel 3. Proses Capability Level

ID Proses	Nama Proses	*Process Capability Level*					
		Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
DSS05	Memastikan keamanan sistem		Fully Achieved	Fully Achieved	**Partially Achieved**	Not Achieved	Not Achieved
APO13	Mengelola layanan keamanan		Fully Achieved	Fully Achieved	**Partially Achieved**	Not Achieved	Not Achieved
DSS02	Mengelola permintaan layanan dan insiden		Fully Achieved	Fully Achieved	**Partially Achieved**	Not Achieved	Not Achieved

Berdasarkan tabel-tabel penilaian kapabilitas, dapat dilihat bahwa pencapaian tingkat kapabilitas pada domain DSS05 yaitu memastikan keamanan sistem di SMA Negeri 1 Palembang dengan rata-rata penilaian 33%, pada domain APO13 yaitu untuk mengelola layanan keamanan dengan rata-rata penilaian 33%, dan domain DSS02 yaitu untuk mengelola permintaan layanan dan insiden di SMA Negeri 1 Palembang, khususnya ketika pandemi yang berlangsung kini, rata-rata penilaian yang dicapai adalah 50%.

Dari hasil penilaian *capability level*, ketiga proses yang diteliti, yaitu DSS05, APO13 dan DSS02 berhenti di level 3 karena pada salah satu atribut proses yang ada pada level 3 hanya mencapai *partially achieved* yaitu pada atribut proses 3.2 (PA3.2). Sehingga dapat disimpulkan proses penilaian berhenti pada level 2 *(Managed Process)* dengan catatan penilaian pada

level 3 (*Established Process*) atribut proses 3.1 (PA 3.1) mencapai *largely achieved* dan atribut proses 3.2 (PA 3.2) mencapai *partially achieved*. Sehingga berdasarkan penilaian proses yang dilakukan karena pada level berikutnya salah satu atribut prosesnya tidak ada yang mencapai *largely achieved.*

Berdasarkan hasil penilaian dari level masing-masing proses, dilakukan perhitungan untuk mengetahui besarnya nilai rata-rata tingkat kapabilitas dari sistem tata kelola teknologi informasi di SMA Negeri 1 Palembang, dengan acuan rumus sebagai berikut :

$$Tingkat\ kapabilitas\ level = \frac{(0 * L0) + (1 * L1) + (2 * L2) + (3 * L3) + (4 * L4) + (5 * L5)}{JP}$$

Dimana :

Ln : Jumlah proses pada level *n*

JP : Jumlah proses yang di-*assessment*

Maka, perhitungannya adalah sebagai berikut :

$$Tingkat\ kapabilitas\ level = \frac{(0 * 1) + (1 * 0) + (2 * 3) + (3 * 0) + (4 * 0) + (5 * 0)}{3}$$

$$Tingkat\ kapabilitas = 2$$

Rekomendasi Hasil Assessment

1. **APO13 (Mengelola Keamanan Layanan)**
   a. Melakukan identifikasi dan penyediaan infrastruktur yang dibutuhkan seperti pemenuhan kebutuhan jaringan internet yang memadai untuk melakukan pengelolaan keamanan layanan
   b. Meningkatkan pengetahuan keamanan informasi pada seluruh staff untuk meningkatkan pemahaman keamanan informasi sehingga hak-hak akses dapat terjaga dan terlindungi.
   c. Melakukan audit pemeliharaan sistem secara berkala, serta dapat pula melanjutkan dengan menerapkan standar keamanan informasi seperti ISO/IEC2007

2. **DSS05 (Memastikan Kemanan SIstem)**
   a. Melakukan identifikasi dan penyediaan infrastruktur yang dibutuhkan seperti pemenuhan kebutuhan jaringan internet yang memadai untuk melakukan pengelolaan keamanan layanan.
   b. Secara berkala melakukan pengumpulan data, evaluasi dan perbaikan sistem sebagai bentuk pengendalian oleh staff terkait.
   c. SMA Negeri 1 Palembang dapat mendefinisikan dan menentukan hak akses pengguna untuk masing-masing unit dalam menggunakan aplikasi, khususnya jika aplikasi tersebut berkaitan dengan log dokumen terlindungi atau dapat dilengkapi dengan dokumen Prosedur Operasi Pengelolaan Hak Akses.
   d. Melakukan pengelolaan pada dokumen penting dan perangkat keluaran seperti laptop, printer dan sejenisnya, sebagai bentuk perlindungan fisik terhadap asset yang dimiliki.
   e. Sebagai tahap lanjutan, SMA Negeri 1 Palembang dapat melakukan pemantauan infrastruktur secara detail terkait keamanan informasi dengan melakukan pemasangan CCTV pada setiap area penting yang memungkinkan risiko kegagalan keamanan sistem dapat terjadi.

3. **DSS02 (Mengelola Permintaan Layanan dan Insiden)**
   a. Menetapkan permintaan layanan yang dibutuhkan oleh user dan menyediakannya,

seperti kebutuhan layanan dalam kegiatan kelas belajar-mengajar secara online yang mebutuhkan aplikasi khusus.

b. Menyediakan akses jaringan internet yang baik dalam menunjang *performance*, dan melakukan monitoring berkala oleh staff yang berperan.

KESIMPULAN

Kesimpulan

Berdasarkan hasil analisis dalam penelitian ini, dapat disimpulkan bahwa :

1. Penilaian tingkat *capability level* pada proses tata kelola keamanan informasi yang dilakukan di SMA Negeri 1 Palembang yaitu pada domain proses DSS05 (memastikan keamanan sistem), APO13 (mengelola layanan keamanan), dan DSS02 (mengelola permintaan layanan dan insiden) berhenti pada level 3 *(establish process)* dan tidak bisa dilanjutkan untuk level berikutnya.
2. Nilai *capability level* yang dicapai pada penelitian ini yaitu berada pada level 2 untuk setiap proses yang dilakukan, dikarenakan pada penilaian capability level yang berhenti pada level 3, setiap proses hanya mencapai proses 3.2 (PA 3.2) atau *partially achieved.*
3. Penilaian proses pada level berikutnya tidak bisa dilakukan jika salah satu proses atributnya tidak mencapai *largely achieved.*

Saran

1. Pada penelitian selanjutnya diharapkan agar dapat melakukan sistem tata kelola teknologi informasi dengan level yang lebih baik.
2. Diharapkan agar dapat dapat melakukan sistem tata kelola dengan *resource optimization* sebagai kebutuhan dari *stakeholder*.

DAFTAR PUSTAKA

Alexander, D.O.T., dan Merry Christy. 2020. *Analisis Audit Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 pada Instansi X*. Yogyakarta. Universitas Teknologi Yogyakarta.

Imany, Y.D., Widhy Hayuhardika, Admaja Dwi Herlambang. 2019. *Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia).* Universitas Brawijaya.

Nugraha, B. 2017. *Analisis dan Evaluasi Sistem Informatika Akademik Menggunakan COBIT 5 PAM (Process Assessment Model) (Studi Kasus Pada Universitas Singaperbangsa Karawang).* Universitas Singaperbangsa Karawang.

Ajismanto, F. 2017. *Analisis Domain Proses COBIT Framework 5 pada Sistem Informasi Worksheet (Studi Kasus: Perguruan Tinggi STMIK, Politeknik Palcomtech).* STMIK PalComTech Palembang.

Husein, GM, Radiant Victor. 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL).*Bandung. Universitas Kristen Maranatha.