JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1834-1841

ANALISIS TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI BERBASIS FRAMEWORK COBIT 5 (STUDI KASUS : SMA NEGERI SUMATERA SELATAN)

Aris Wibowo*[1)], Muhammad Izman Herdiansyah[2)].
1. Magister Teknik Informatika, Universita Bina Darma, Indoneisa
2. Magister Teknik Informatika, Universita Bina Darma, Indoneisa

Article Info
Kata Kunci: Balace Score Card; COBIT Framework 5; Domain Process

Keywords: *Balace Score Card; COBIT Framework 5;Domain Process*

Article history:
Received 29 September 2024
Revised 13 Oktober 2024
Accepted 4 November 2024
Available online 4 December 2024

DOI :
https://doi.org/10.29100/jipi.v9i4.5484

* Corresponding author.
Aris Wibowo
E-mail address:
Ariswibowo66@gmail.com

ABSTRAK
SMA Negeri Sumatera Selatan, sebuah sekolah menengah atas negeri terkemuka yang terletak di kota Palembang, mengandalkan teknologi informasi untuk mendukung tujuan pembelajaran dan visi misi sekolahnya. Penelitian ini menginvestigasi domain proses dalam kerangka kerja Control Objectives for Information and Related Technology (COBIT 5) serta mengukur tingkat kemampuan Tata Kelola Keamanan Teknologi Informasi. Metode deskriptif kualitatif digunakan dalam penelitian ini. Hasil penelitian menunjukkan bahwa proses dalam domain COBIT Framework 5 yang relevan dengan Keamanan Teknologi Informasi adalah APO (Align, Plan, and Organise), termasuk APO04, APO12, dan APO13, serta dalam domain DSS (Deliver, Service, and Support), termasuk DSS05. Analisis tingkat kemampuan menunjukkan bahwa APO04 berada pada level 3 – Manage Innovation, APO12 berada pada level 3 – Manage Risk, APO13 berada pada level 3 – Manage Security, dan DSS05 berada pada level 3 – Manage Service Security..

ABSTRACT

SMA Negeri Sumatera Selatan, a prominent public high school located in Palembang, relies on information technology to support its educational goals and school vision and mission. This research investigates process domains within the Control Objectives for Information and Related Technology (COBIT 5) framework and measures the level of Information Technology Governance Security capability. A qualitative descriptive method is used in this research. The results show that processes within the COBIT Framework 5 domain relevant to Information Technology Security are APO (Align, Plan, and Organize), including APO04, APO12, and APO13, as well as within the DSS (Deliver, Service, and Support) domain, including DSS05. Capability level analysis indicates that APO04 is at level 3 - Manage Innovation, APO12 is at level 3 - Manage Risk, APO13 is at level 3 - Manage Security, and DSS05 is at level 3 - Manage Service Security.

I. PENDAHULUAN

SAAT ini, Kemajuan pesat dalam bidang teknologi informasi dan komunikasi telah menjadi kebutuhan esensial dalam kehidupan sehari-hari. Hampir setiap aspek kegiatan dan layanan publik pemerintah saat ini sangat terkait dengan perkembangan teknologi informasi dan komunikasi. Salah satu contohnya terjadi di SMA Negeri Sumatera Selatan di Palembang, yang menjadi pilihan utama untuk Sekolah Menengah Atas Negeri. Sekolah ini secara aktif mengintegrasikan teknologi informasi dalam manajemen sistem pembelajarannya. Peran penting teknologi informasi ini sangat berpengaruh dalam mencapai tujuan sistem pembelajaran dan visi misi sekolah.[1]

Sekolah ini berdiri dengan maksud untuk memenuhi keperluan pendidikan yang berkualitas internasional di area Sumatera Selatan, khususnya bagi siswa-siswa dari latar belakang ekonomi yang terbatas. Pemerintah Provinsi Sumatera Selatan dan Putera Sampoerna Foundation meyakini bahwa salah satu cara terbaik untuk mengakhiri lingkaran kemiskinan dalam suatu keluarga adalah melalui pendidikan.

Agar layanan bisnis dan keamanan layanan IT di SMA Negeri Sumatera Selatan dapat dioptimalkan, diperlukan analisis dan perancangan yang mengadopsi COBIT 5 sebagai kerangka kerja untuk menjaga keamanan informasi.

Langkah ini diperlukan karena upaya tersebut belum dilaksanakan secara komprehensif di SMA Negeri Sumatera Selatan, sehingga dapat mengurangi potensi dampak risiko yang mungkin terjadi.

COBIT, yang merupakan kependekan dari *Control Objectives for Information and Related Technology*, adalah serangkaian panduan yang dapat dimanfaatkan oleh berbagai jenis organisasi, entitas pemerintah, perusahaan, atau lembaga besar untuk membantu mereka mencapai tujuan yang telah ditetapkan. COBIT 5, khususnya, menyajikan panduan yang rinci mengenai aspek keamanan informasi, yang dikenal sebagai COBIT 5 for Information Security. Bagian ini memberikan petunjuk kepada perusahaan tentang bagaimana mengelola keamanan informasi di dalam lingkungan perusahaan mereka. Dalam pengelolaan teknologi informasi, penting untuk memiliki suatu model yang berfungsi sebagai pedoman sesuai dengan strategi dan tujuan organisasi. Model tersebut berguna untuk mengukur serta mengatasi berbagai masalah yang mungkin muncul di organisasi, dan COBIT atau ITIL adalah contoh-contoh kerangka kerja yang menyediakan struktur tersebut. COBIT adalah suatu kerangka kerja IT yang dipublikasikan oleh Information System Audit and Control Association. [2].

Dalam sejumlah studi yang dilakukan oleh para akademisi dan praktisi, penilaian terhadap pengelolaan keamanan teknologi informasi (TI) menggunakan kerangka kerja COBIT 5 telah memberikan wawasan yang menarik. Konsisten dengan temuan ini, banyak lembaga pendidikan dan badan publik menghadapi tantangan dalam mencapai tingkat keterampilan yang diinginkan. Hal ini menunjukkan bahwa evaluasi terhadap proses-proses kunci dalam pengelolaan keamanan informasi, seperti memastikan keamanan sistem, manajemen layanan keamanan, dan manajemen permintaan layanan serta insiden, telah mencapai level 3 (proses terbentuk). Namun, kemajuan ke level yang lebih tinggi menjadi sulit karena beberapa atribut proses masih belum sepenuhnya terpenuhi.[3]

Penelitian lainnya menyoroti bahwa banyak instansi publik, masih berada pada level 1 dalam tata kelola TI. Untuk mencapai tingkat kapabilitas yang lebih tinggi, perbaikan yang signifikan diperlukan, termasuk evaluasi berkala terhadap potensi ancaman keamanan dan penyusunan dokumen terkait.[4]

Secara keseluruhan, kesimpulan dari berbagai penelitian ini menunjukkan bahwa meskipun banyak institusi telah mengadopsi framework COBIT 5 untuk mengelola TI, masih ada banyak tantangan yang harus diatasi untuk mencapai tingkat kapabilitas yang diharapkan. Perlunya fokus pada perbaikan proses, pemahaman yang lebih mendalam, dan komitmen untuk mengimplementasikan praktik terbaik menjadi kunci dalam meningkatkan tata kelola keamanan TI secara efektif.

COBIT 5 telah terbukti memberikan kerangka kerja yang efektif dalam mengevaluasi dan meningkatkan tata kelola TI dalam berbagai konteks, seperti yang terlihat dari sejumlah penelitian yang dilakukan di berbagai institusi pendidikan dan organisasi. Melalui pendekatan capability level yang terstruktur, COBIT 5 memungkinkan organisasi untuk secara sistematis menilai tingkat kapabilitas mereka dalam mengelola TI dan mengidentifikasi area yang memerlukan perbaikan. Selain itu, COBIT 5 juga membantu organisasi dalam menghubungkan tujuan strategis mereka dengan tujuan TI yang spesifik, sehingga mendukung pengambilan keputusan yang lebih terinformasi dan memastikan investasi TI yang efektif. Dengan demikian, COBIT 5 tidak hanya memberikan panduan yang komprehensif, tetapi juga memfasilitasi proses peningkatan berkelanjutan dalam tata kelola TI.

Untuk meningkatkan standar pelayanan bisnis dan memastikan keamanan layanan TI di Sekolah Menengah Atas Negeri Sumatera Selatan, diperlukan analisis dan perancangan yang mengintegrasikan kerangka kerja COBIT 5. Pendekatan ini dimaksudkan untuk mengamankan informasi di sekolah yang belum sepenuhnya dikelola dengan optimal, dengan tujuan mengurangi kemungkinan risiko yang timbul. Oleh karena itu, perlu dilakukan evaluasi tingkat kemampuan, dengan mempertimbangkan domain proses DSS04 (Manage Continuity) dan DSS05 (Manage Security Services), untuk menilai potensi dampak yang mungkin terjadi pada sekolah jika risiko tersebut terjadi. Langkah selanjutnya adalah melakukan audit terhadap risiko-risiko yang telah diidentifikasi, mengacu pada panduan kerangka kerja COBIT 5 untuk keamanan informasi yang telah diterbitkan.

Hasil dari studi ini berupa saran kebijakan dan solusi yang telah dipersiapkan dalam format dokumen manajemen layanan bisnis dan keamanan layanan TI. Dokumen-dokumen tersebut akan diajukan sebagai rekomendasi atau sebagai materi evaluasi bagi SMA Negeri Sumatera Selatan.

II. METODE PENELITIAN

A. Metode Penelitian

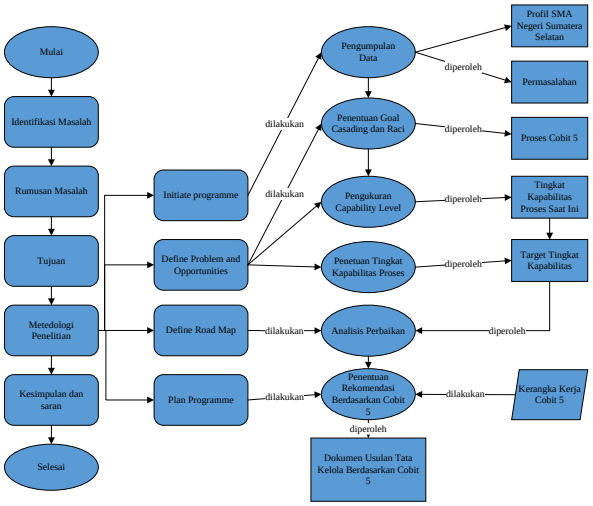
Penelitian ini menerapkan pendekatan deskriptif kualitatif dengan memanfaatkan subjek penelitian yang bersifat alami. Subyek penelitian ini merujuk pada entitas yang tidak dipengaruhi atau dimanipulasi oleh peneliti, sehingga mencerminkan keadaan sebenarnya di SMA Negeri Sumatera Selatan.Fokus penelitian terletak pada manajemen teknologi informasi di SMA Negeri Sumatera Selatan, dengan subjek penelitian terdiri dari individu yang berperan sebagai narasumber wawancara dan responden, yang merupakan bagian dari lingkungan SMA Negeri Sumatera

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1834-1841

Selatan dalam konteks penelitian ini.

B. Metode Pengumpulan Data

Gambar 1 menampilkan urutan tindakan yang terjadi selama proses penelitian. Langkah-langkah tersebut mencakup pengidentifikasian masalah yang akan diselidiki, perencanaan penelitian, dan pengumpulan data.



Gambar 1. Metodologi Penelitian

C. Tahapan Penelitian

a. Tahap 1 – Memulai program
Proses dimulai dengan mengenali segala hal yang terkait dengan tujuan, tugas, wewenang, dan konsep kerja yang sedang digunakan. Pengumpulan data dilakukan melalui observasi dan wawancara informal dengan pihak terkait.

b. Tahap 2 – Mendefinisikan Masalah dan Peluang
Pada langkah ini, tujuan cascading ditetapkan dan RACI chart disusun, diikuti dengan evaluasi tingkat kemampuan dan penetapan target kapabilitas proses. Proses dimulai dengan mengidentifikasi proses yang relevan terkait dengan tantangan yang dihadapi, dan mengevaluasi kemampuan sekolah dalam bidang Teknologi Informasi (TI). Penetapan proses dilakukan dengan mencocokkan dengan Tujuan Terkait, sedangkan evaluasi kemampuan saat ini menggunakan kuesioner kapabilitas yang mengacu pada struktur fungsional COBIT 5. Pada tahap ini, hasil penelitian tentang manajemen risiko TI, keamanan TI, dan keamanan layanan TI diuraikan secara rinci. Temuan ini digunakan untuk menilai kemampuan saat ini dari SMA Negeri Sumatera Selatan.

c. Tahap 3 – Menetapkan Rencana Perjalanan
Pada langkah ini, tujuan perbaikan ditetapkan berdasarkan hasil analisis kesenjangan yang muncul dari kuesioner kapabilitas. Ketika terjadi kesalahan, hal itu menunjukkan adanya ketidaksesuaian antara nilai kemampuan saat ini, harapan, dan realitas yang ada. Perbaikan dalam manajemen TI dijelaskan dengan memberikan prioritas pada pengembangan proyek-proyek tertentu. Hasil analisis kesenjangan ini dimanfaatkan untuk mengidentifikasi solusi potensial dalam pengelolaan teknologi informasi di SMA Negeri Sumatera Selatan. Dari hasil kuesioner yang mengukur kapabilitas, informasi tentang kemampuan saat ini dalam mengelola teknologi informasi dapat diperoleh. Kemudian, kesenjangan dapat teridentifikasi jika temuan dan penilaian tidak sejalan dengan realitas yang ada. Pada tahap ini, sasaran kemampuan yang diinginkan oleh organisasi juga dijelaskan, dengan merujuk pada Model Penilaian Proses yang meliputi level 0-5. Setelah kesenjangan terungkap dari analisis kapabilitas, peneliti mulai memetakan proses COBIT 5, yang kemudian digunakan sebagai panduan untuk menyusun rekomendasi dalam pengelolaan keamanan TI.

d. Tahap 4 - Merencanakan Program

Dalam langkah ini, program direncanakan dan proposal disusun berdasarkan hasil analisis dari wawancara dan kuesioner yang dilakukan terhadap responden di SMA Negeri Sumatera Selatan. Rencana program ini difokuskan pada area yang dipilih dari struktur kerja COBIT 5. Selain itu, program ini akan disesuaikan

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1834-1841

dengan tingkat kemampuan yang diharapkan oleh SMA Negeri Sumatera Selatan, dengan merujuk pada tahapan Siklus Hidup COBIT dalam COBIT 5.

III. HASIL DAN PEMBAHASAN

Dalam penentuan domain ini diawali dengan tahapan enterprise goal pada COBIT. Adapun tahapan pertama ialah menentunkan stakholder needsnya, dimana penelitian ini berfokus pada sisi customer dan internal serta memilih bagian *risk optimation*.

Penentuan tahapan awal ialah peneliti menentukan stakeholder yang ingin dicapai, berdasarkan latarbelakang dan rumusan masalah yang ada peneliti memilih risk optimation sebagai stakeholder need. Selanjutnya, memilih balance score card pada dimension customer dan internal dengan tujuan untuk melihat *risk optimation* pada perspektif customer dan internal

TABEL I
PEMETAAN ENTERPRISE GOAL

BSC *Dimension*	*Enterprise Goals*	*Risk Optimation*
Customer	*7. Business service continuty and availbility* *9.Information based strategic decision making*	**P**
Internal	*13. Managed business change programmes*	**P**

Setelah memahami perspektif BSC dan menetapkan tujuan organisasi seperti Business Service Continuity and Availability, Information-Based Strategic Decision Making, dan Managed Business Change Programs. Dalam konteks Business Service Continuity and Availability serta Information-Based Strategic Decision Making, kontribusi dari ITGI terlihat melalui ITG 8, yang mencakup penggunaan aplikasi, informasi, dan solusi teknologi yang memadai. Sementara dalam hal Managed Business Change Programs, ITGI 13 menekankan pengiriman program-program yang memberikan nilai tambah, tepat waktu, sesuai anggaran, dan memenuhi standar kualitas yang ditetapkan.

TABEL II
MAPPING ENTERPRISE GOAL

		Enterprise Goals		
	IT Related Goals	***7.Business service continuty and availbility***	***9.Information based strategic decision making***	***13. Managed business change programmes***
Customer	*ITG. 8 Adequate use of applications, information and technology solutions*	**S**	**S**	
Internal	*ITG.13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards*			**P**

Berdasarkan table diatas, proses domain yang sesuai dengan tujuan sehingga pada ITGI 8 yang dipilih domain APO04, APO13 dan DSS05 dan pada ITGI 13 domain APO12.

Deskripsi proses COBIT 5 sesuai dengan tujuan penelitiannya

1. Proses APO04 bertujuan untuk mengenali strategi inovasi ke depan, mencari pendekatan terbaik di mana Teknologi Informasi dapat diperbaharui melalui perkembangan terkini guna mencapai sasaran organisasi. Dalam konteks ini, APO04 melakukan penilaian dan manajemen terhadap inovasi.
2. Proses APO12 memiliki tujuan untuk menemukan strategi dan taktik, serta mencari pendekatan optimal

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1834-1841

di mana Teknologi Informasi dapat memberikan kontribusi dalam mencapai sasaran organisasi. Dalam konteks ini, APO12 melakukan evaluasi dan pengelolaan risiko TI.

3. Proses APO13 melibatkan langkah-langkah definisi, operasionalisasi, dan pengawasan sistem yang digunakan oleh sekolah untuk mengelola keamanan informasinya. Tujuan dari proses ini adalah memastikan bahwa insiden keamanan informasi dan dampaknya tetap berada dalam batas risiko yang telah ditetapkan oleh institusi. Indikator kemampuan proses ini mencakup kemampuan proses untuk mencapai tingkat kapabilitas yang telah ditetapkan diukur melalui karakteristik-karakteristik proses.
4. Proses DSS05 bertujuan untuk mengurangi dampak pada bisnis yang disebabkan oleh kerentanan keamanan informasi operasional dan insiden terkait.

Perhitungan tingkat kematangan dilakukan dengan menyusun analisis kuesioner secara terperinci, dan tingkat kematangan ditentukan berdasarkan nilai rata-rata dari setiap domain yang telah dianalisis melalui kuesioner. Data hasil perhitungan rata-rata tingkat kematangan untuk setiap domain proses dapat ditemukan dalam Tabel 3 berikut ini:

TABEL III
TINGKAT KEMATANGAN SETIAP DOMAIN

Aktivitas Proses	Deskripsi	*Capability Maturity*
APO04	*Manage Inovation*	3
APO12	*Manage Risk*	3,4
APO13	*Manage Security*	3,5
DSS05	*Manage Security Service*	3,2
	Rata-rata	**3,3**

Setelah mengevaluasi rata-rata dari setiap domain, dilakukan perhitungan rata-rata keseluruhan, dan hasilnya menunjukkan tingkat kematangan sebesar 3,3 (Proses yang Teretabil). Dari nilai ini, dapat disimpulkan bahwa manajemen keamanan TI telah terdokumentasi dan diimplementasikan sesuai dengan standar yang telah diterapkan. Meskipun demikian, diperlukan peningkatan dan pengembangan lebih lanjut dalam pengelolaan untuk mencapai tingkat kematangan pada level 4 (Proses yang Dapat Diprediksi).

Setelah menilai dan mengetahui tingkat kemampuan dalam manajemen risiko, manajemen sistem, dan layanan sistem di SMA Negeri Sumatera Selatan yang saat ini berada pada level 3 (Proses yang Teretabil), langkah berikutnya adalah melakukan analisis kesenjangan (gap). SMA Negeri Sumatera Selatan memiliki target untuk mencapai level kematangan 4 (Proses yang Dapat Diprediksi), di mana semua aktivitas berjalan sesuai dengan standar yang telah ditetapkan. Ini sesuai dengan temuan dari wawancara dengan kepala bagian pengelolaan sumber daya

Dengan mengacu pada nilai kematangan yang diperoleh melalui evaluasi kuesioner yang disampaikan kepada responden berdasarkan RACI Chart di SMA Negeri Sumatera Selatan, serta hasil wawancara dengan kepala operasional dan koordinator TI di SMA Negeri Sumatera Selatan, dapat diamati bahwa terdapat perbedaan antara tingkat kematangan yang sedang berlangsung dan tingkat kematangan yang diinginkan pada masing-masing domain.

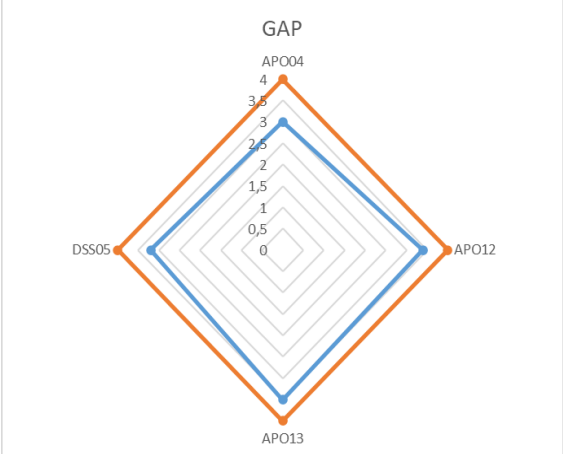
Memeriksa nilai target kematangan diharapkan dapat mempermudah pelaksanaan pengelolaan teknologi informasi secara seimbang di ketiga domain tersebut. Pihak SMA Negeri Sumatera Selatan telah menegaskan tekad mereka untuk mencapai level kematangan 4 pada tahun 2024.

TABEL IV
HASIL ANALISIS KESENJANGAN

Aktivitas Proses	Saat Ini	Yang Diharapkan	*Gap* = (Yang diharapkan – Saat ini)
APO04	3	4	4 – 3 = 1
APO12	3,5	4	4 – 3,4 = 0,6
APO13	3,4	4	4 – 3,5 = 0,5
DSS05	3,2	4	4 – 3,2 = 0,8
Jumlah			2,9

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1834-1841

Jumlah kesenjangan (gap) secara keseluruhan pada seluruh domain proses adalah sekitar 2,98, oleh karena itu, penyesuaian diperlukan pada setiap domain proses. Peneliti akan menyampaikan saran dan rekomendasi sesuai dengan pedoman COBIT 5 untuk masing-masing domain proses yang diinvestigasi. Ilustrasi kesenjangan pada setiap domain proses dapat dilihat dalam Gambar 2 berikut:



Gambar 2. Analisis Kesenjangan

Berdasarkan analisis gap diatas, dapat diketahui bahwa domain APO04 ialah domain yang paling rendah nilai capability levelnya hal tersebut dikarenakan, masih cukup kurangnya inovasi-inovasi pengembangan tata kelola kedepanya. Baik yang dilakukan oleh tim IT ataupun ide-ide pegawai lainya. Selain itu, APO12 memiliki nilai capability level yang paling baik diantara domain lainya, hal tersebut dikarenakan pengelolaan manajemen risiko sudah cukup baik dilaksanakan oleh SMA Negeri Sumatera Selatan. Hal tersebut dibuktikan adanya SOP dalam memanajemen resiko terhadap sistem yang ada di SMA Negeri Sumatera Selatan

Dengan hasil evaluasi yang telah dilakukan terhadap manajemen risiko dan tata kelola di SMAN Negeri Sumatera Selatan langkah selanjutnya adalah mengidentifikasi masalah pada tingkat kemampuan saat ini dan memberikan saran serta rekomendasi sesuai dengan kerangka kerja COBIT 5.

1. APO04 dikategorikan pada level 3 (Estabilished Process), karena berdasarkan wawancara pada SMA Negeri Sumatera Selatan belum melaksanakan penyusunan startegi untuk pengembangan inovasi tata kelola sistem kedepanya. Situasi tersebut dapat menjadi penghambat dalam meningkatkan tata kelola sistem di masa mendatang karena terbatasnya ide dan inovasi yang dapat diimplementasikan. Guna mencapai standar kematangan yang diharapkan, berikut ini adalah saran untuk meningkatkan tata kelola Teknologi Informasi (TI):
    a. Rekomendasi jangka pendeknya adalah kepala koordinator TI perlu mendalami pengetahuan mengenai penyusunan strategi TI kedepannya dan memberikan gagasan untuk setiap pegawai atau staff TI dalam berinovasi melakukan pengmbangan tata Kelola.
    b. Rekomendasi jangka panjangnya adalah kepala coordinator TI perlu mengevaluasi system untuk Menyusun perencanaan strategis kedepannya dalam jangka waktu 3-5 tahun.

2. APO12, berada pada level 3 (Proses yang Telah Terbentuk), telah melakukan evaluasi dan manajemen risiko pada setiap sistem dan TI yang dimilikinya. Namun, meskipun telah melakukan upaya tersebut, belum mencapai standar yang diinginkan, masih terdapat beberapa aspek yang belum optimal. Misalnya, evaluasi masih memerlukan bantuan dari pihak eksternal yang memiliki pemahaman yang baik tentang aturan dan prosedur evaluasi manajemen risiko. Hal ini dapat menjadi hambatan dalam meningkatkan manajemen risiko karena kurangnya pemahaman tim TI terhadap aturan dan prosedur evaluasi yang ada. Untuk mencapai tingkat kematangan yang diharapkan, telah dirumuskan rekomendasi untuk meningkatkan tata kelola TI.
    a. Rekomendasi jangka pendeknya adalah kepala koordinator TI perlu mendalami pengetahuan mengenai managemen resiko, aktivitas tersebut dapat dengan mengikuti kegiatan pelatihan managemen resiko dan Menambah jumlah karyawan di departemen TI yang memiliki pemahaman atau keahlian yang sesuai dengan manajemen risiko.

b. Rekomendasi jangka panjangnya adalah kepala kordinator TI perlu mengevaluasi system untuk mengidentifikasi managemen resiko dan mendokumendasikan SOP managemen resiko saat ini dan dimasa depan dan Koordinator TI harus mengawasi keefektifan dan kinerja manajemen risiko dalam tata kelola perusahaan TI untuk mengevaluasi apakah manajemen risiko dan mekanismenya telah diterapkan dengan baik.

3. APO013 dikategorikan pada level 3 (Estabilished Process), membuat kerangka kerja mencakup struktur dan proses manajemen keamanan TI dalam mencapai tujuanya. Hal tersebut dilakukan adanya kerangka kerja manajemen keamanan TI yang mencakup struktur dan proses aktvitas sistem. Namun kerangka kerja manajemen kemanan TI tidak seluruhnya telah dilaksanakan, karena masih ada kerangka kerja yang terlewati seperti melaksanakan evaluasi manajemen keamanan TI setiap 6 bulan atau satu tahun sekali. Hal tersebut dikarenakan evaluasi manajemen keamanan TI dilaksanakan hanya pada saat terjadi ancaman keamanan TI. Untuk mencapai tingkatan kematangan yang diinginkan, berikut adalah rekomendasi untuk meningkatkan tata kelola TI.
    a. Rekomendasi dalam jangka pendek adalah mengkomunikasikan tujuan dan arah manajemen dengan membagikan pemahaman dan kesadaran tentang mereka kepada pihak-pihak yang memiliki kepentingan dan pengguna yang tepat di SMA Negeri Sumatera Selatan.
    b. Rekomendasi dalam jangka panjangnya adalah koordinator TI harus melaksanakan peran dan tanggung jawab secara efisien. Menetapkan, menyetujui, dan mengomunikasikan peran dan tanggung jawab individu dalam Teknologi Informasi (TI), dengan penekanan pada manajemen TI, dan kepala koordinator TI perlu merencanakan untuk menjaga faktor keamanan sistem dan mengontrol lingkungan TI di SMA Negeri Sumatera Selatan, sambil memastikan integrasi dan konsistensi sistem yang ada dengan tata kelola.

4. DSS05 diperingkatkan sebagai level 3 (Proses yang Teretabil) karena berdasarkan wawancara di SMA Negeri Sumatera Selatan, mereka telah berusaha untuk meningkatkan kapasitas sumber daya guna mendukung keamanan layanan sebaik mungkin. Namun, berdasarkan wawancara dengan kepala koordinator TI, meskipun upaya untuk meningkatkan kapasitas dan sumber daya telah dilakukan dengan baik, pemeliharaan dan manajemen risiko sistem hanya dilakukan ketika terjadi kegagalan operasional sistem, dan penanganan masalah masih memerlukan dukungan dari entitas luar. Guna mencapai standar kematangan yang diinginkan, berikut adalah saran untuk meningkatkan tata kelola Teknologi Informasi (TI):
    a. Rekomendasi untuk jangka pendek adalah melakukan analisis risiko terhadap sistem yang dimiliki. Analisis ini mencakup evaluasi risiko yang telah terjadi dan peramalan potensi risiko yang mungkin terjadi.
    b. Rekomendasi dalam jangka panjang adalah membuat panduan manajemen risiko sehingga ketika terjadi kegagalan atau masalah pada sistem yang ada, SMAN Negeri Sumatera Selatan dapat menggunakan panduan tersebut sebagai acuan untuk penanganan dan pengembangan sistem di masa depan. Selain itu, koordinator juga disarankan untuk mengikuti pelatihan-pelatihan terkait manajemen risiko sistem informasi.

Dalam penelitian sebelumnya, para peneliti menggunakan COBIT 5 untuk mengevaluasi pengelolaan keamanan dengan memetakan domain dari setiap kerangka kerja dan memberikan rekomendasi perancangan yang dibutuhkan oleh masing-masing peneliti. Sebagai contoh, evaluasi pengelolaan keamanan teknologi informasi di sebuah sekolah menunjukkan bahwa beberapa proses, seperti DSS05, APO13, dan DSS02, telah mencapai level 3 (proses terbentuk). Meskipun begitu, penilaian kapabilitas menunjukkan bahwa tingkat kapabilitas untuk setiap proses berada pada level 2, karena beberapa atribut proses tidak mencapai pencapaian yang signifikan. Ini menyoroti kebutuhan akan peningkatan dalam implementasi dan dokumentasi prosedur-prosedur keamanan informasi di sekolah tersebut.3]

Hasil studi sebelumnya melibatkan evaluasi tata kelola TI di sebuah sekolah menggunakan metode capability level dalam kerangka kerja COBIT 5. Hasil evaluasi menunjukkan bahwa pada saat itu, tingkat tata kelola TI sekolah berada pada level 2 (proses dikelola) dengan skor 2,25. Oleh karena itu, saat ini sekolah memiliki capability level sebesar 2,25, sementara tingkat capability level yang diharapkan adalah 3,00. Dengan demikian, terdapat perbedaan sebesar 0,75 (gap) antara tingkat saat ini dan target yang diinginkan. Untuk mencapai tingkat capability

level yang diharapkan, sekolah perlu mengatasi kesenjangan ini dengan mengembangkan persyaratan yang sesuai dengan panduan COBIT 5 untuk seluruh proses yang belum memiliki dokumen, terutama dalam hal meningkatkan proses yang saat ini berada pada level 1 agar dapat mencapai level 2, khususnya dalam aspek manajemen keamanan informasi.[5]

Penelitian lain menunjukkan bahwa sekolah memiliki tingkat kemampuan dalam mengelola penggunaan teknologi informasi yang berada pada level 2. Secara umum, pencapaian pada setiap proses belum memenuhi standar dan belum mencapai tujuan yang diharapkan. Terutama dalam pengelolaan strategi teknologi informasi, di dalam domain align, plan, and organize (APO02), tingkat kemampuan dalam setiap proses mencapai level 2, sedangkan harapan sekolah adalah mencapai level 4. Meskipun dalam pengelolaan strategi, kemampuan masih belum optimal. Oleh karena itu, rekomendasi yang diberikan adalah untuk lebih memahami setiap proses yang harus dijalani untuk mencapai tujuan yang diinginkan. Tingkat capability level yang diharapkan secara keseluruhan ditujuan pada level 4, yang berarti proses pemanfaatan Teknologi Informasi yang telah dilakukan, dicapai, dan dikelola dengan baik harus diatur dan diterapkan secara konsisten dalam seluruh kegiatan yang berlangsung di lingkungan sekolah tersebut..[6]

IV. KESIMPULAN

Berdasarkan analisis menggunakan kerangka kerja COBIT 5, terutama di domain proses APO04, ditemukan bahwa tingkat kematangan manajemen inovasi di SMA Negeri Sumatera Selatan berada pada level 3 (Proses Terestablish), menandakan perlunya peningkatan dalam pelaksanaan pengembangan inovasi. Sebaliknya, dalam pengelolaan risiko (APO12) dan tata kelola manajemen keamanan (APO13), SMA Negeri Sumatera Selatan telah mencapai level 3 (Proses Terestablish) dengan tingkat kematangan masing-masing 3,5 dan 3,3, menunjukkan pengakuan dan pengoptimalan manajemen risiko TI serta integrasi yang baik dalam tata kelola keamanan. Demikian pula, dalam pengelolaan keamanan layanan TI (DSS05), SMA Negeri Sumatera Selatan telah mencapai level 3 (Proses yang Telah Mapan) dengan tingkat kematangan 3,2, menunjukkan dokumentasi dan komunikasi yang efektif dalam prosedur yang telah ditetapkan. Meskipun demikian, masih ada ruang untuk peningkatan dalam pengembangan inovasi untuk lebih meningkatkan efisiensi dan efektivitas keseluruhan pengelolaan SMA Negeri Sumatera Selatan.

DAFTAR PUSTAKA

[1] IT Governance Indonesia. (2019). Kupas Tuntas Tata Kelola IT (IT Governance)
[2] ISACA. (2012). COBIT, www.isaca.org, diakses : 08 Juni 2023.
[3] Aulia, N. A., Antoni, D., Syamsuar, D & Cholil, W. (2021). Tata Kelola Keamanan Sistem Teknologi Informasi dengan Basis Framework COBIT 5 (Studi Kasus: SMA Negeri 1 Palembang) dalam Jurnal Informatika, Volume 9 Nomor 2, halaman 30-37
[4] Turang, D. A. O., & Turang, M. C. (2020). Evaluasi Audit Tata Kelola Keamanan Teknologi Informasi dengan Menggunakan Kerangka Kerja COBIT 5 di Instansi X. Kumpulan Jurnal Ilmu Komputer, Volume 7, Nomor 2, halaman 130-144.
[5] As'ari, H., & Astuti, R. Analisi tata kelola. Penerapan Teknologi Informasi menggunakan Kerangka Kerja COBIT 5 di Sekolah Menengah Kejuruan Bandung.
[6] Simatupang, E., Assegaff, S., & Pahlevi, (2020) Penerapan Tata Kelola Penggunaan Teknologi Informasi dengan Menggunakan COBIT di SMPN 18 Kota Jambi, Jurnal Ilmiah Mahasiswa Sistem Informasi, Volume 2, Nomor 1, halaman 89-102.
[7] Edi Susanto. (2014). Capability Model Framewrok COBIT 5, www.erdisusanto.com, diakses : 02 Januari 2019.
[8] Hermawan, A., Hartati, T., & Wijaya, Y. (2022) Evaluasi Keamanan Data pada Platform Zahra Software dengan Menerapkan Metode Keamanan Infomasi CIA Triad. Jurnal Informatika: Jurnal Pengembangan IT, Volume 7, Nomor 3, halaman 125-130.
[9] Garg, A., Curtis, J., & Halper, H. (2003). Measuring the financial consequences of IT security incidents. Information Management & Computer Security
[10] Aliza Mustofa dan Sitaresmi Wahyu. (2017). Evaluasi Kinerja Sistem Informasi Tata Kelola Keuangan Kantor Kecamatan Kemranjen Kabupaten Banyumas dengan Menggunakan Framework COBIT 5.0 pada Domain MEA (Monitor, Evaluate, dan Assess), Jurnal Pro Bisnis Volume 10 Nomor 2.
[11] Fauziah. (2010). Pengantar Teknologi Informasi. Bandung: CV Muara Indah
[12] Jogiyanto, H., & Abdillah, W. (2014). Manajemen Sistem Informasi. Yogyakarta: ANDI.
[13] Johanes Fernandes. (2016). Process Model Kemampuan Berdasarkan Evaluasi COBIT 5 (Studi Kasus), Jurnal Jatisi Volume 3 Nomor 1.
[14] 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.
[15] Surendro,(2009), Penerapan Tata Kelola Teknologi Informasi, Yogyakarta: Penerbit Andi.
[16] ISACA, COBIT 5 for Risk. United States of America: ISACA, 2013
[17] ISACA, COBIT 5: A business framework for Governance and Management of Enterprise IT. United States of America: ISACA, 2012
[18] ITGI. IT Governance Implementation Guide, 2nd edition, The IT Governance Institute, Illinois, USA. 2007
[19] D. Oliver dan J. Lainhart, "COBIT 5: Adding Value Through Effective Geit," EDPACS, vol. 46, pp. 1-12, 2012.
[20] Whitman, M. E., & Mattord, H. J. (2012). Navigating the path to information security: A guide for IT and information security managers published by Cengage Learning.