INOTEK, Vol. 9
ISSN: 2580-3336 (Print) / 2549-7952 (Online)
Url: https://proceeding.unpkediri.ac.id/index.php/inotek/

Audit Sistem Informasi Menggunakan Kerangka Cobit 2019 Dss05

[1]Ardan Bagas Putra, [2]Reinaldha Dwi Christian, [3]Erna Daniati
[123]Sistem Informasi, Universitas Nusantara PGRI Kediri
Email:[1]hitmeup.ardanbagas@gmail.com, [2]reinaldha50@gmail.com,
[3]ernadaniati@unpkediri.ac.id
Penulis Korespondens : Erna Daniati

Abstrak— Teknologi informasi kini tengah berkembang pesat di berbagai sektor bahkan merambah dalam dunia pendidikan yang terus membawa perubahan signifikan. Sekolah kini pempergunakan sistem informasi untuk menunjang kegiatan operasional dan akademik, seperti mengolah data siswa, nilai, juga mengelola absensi. Namu, dalam penerapan sistem informasi di lingkup sekolah tidak terlepas dari risiko keamanan yang dapat mengancam integritas data. Maka dari itu, audit sistem informasi diperlukan untuk mengetahui sejauh mana sistem tersebut dikelola secara aman dan efektif. Penelitian ini bermaksud mengukur tingkat kematangan tata kelola TI pada sistem akademik yang ada dengan menggunakan framework Cobit 2019, khususnya domain DSS05 (Manage Security Service). Setelah penelitian, menunjukkan hasil audit berada di level 1 (Performed Process) yang berarti proses keamanan telah dilakukan, namun belum optimal sehingga direkomendasikan perbaikan untuk mendorong peningkatan level kapabilitas yang lebih tinggi.

Kata Kunci— keamanan data *; framework Cobit 2019; DSS05*

Abstract— *Information technology is now growing rapidly in various sectors and even penetrates the world of education which continues to bring significant changes. Schools are now using information systems to support operational and academic activities, such as processing student data, grades, and managing attendance. However, the application of information systems in the school environment is inseparable from security risks that can threaten data integrity. Therefore, an information system audit is needed to determine the extent to which the system is managed safely and effectively. This research intends to measure the level of maturity of IT governance on existing academic systems using the Cobit 2019 framework, specifically the DSS05 (Manage Security Service) domain. After the research, it shows that the audit results are at level 1 (Performed Process) which means that the security process has been carried out, but it is not optimal so that improvements are recommended to encourage an increase in a higher level of capability.*

Keywords— *data security; framework Cobit 2019; DSS05*

I. PENDAHULUAN

Penggunaan teknologi (TI) informasi dalam bidang pendidikan menjadi kian meluas seiring tuntutan efiensi dalam megelola data dan layanan akademik. Sekolah yang merupakan lembaga pendidikan juga mengadopsi sistem informasi sebagai pendukung efektifitas administrasi, seperti absensi, nilai, dan data siswa. Apabila dirancang dengan baik tentunya dapat meningkatkan mutu layanan dan membantu pengambilan keputusan yang berbasis data[1].

Namun, tidak bisa dihindari dalam penerapannya akan menimbulkan tantangan tersendiri, terutama aspek keamanan informasi. Ancaman yang timbul terhadap sistem bisa datang dari luar maupun dalam institusi bisa berupa kesalahan manusia, serangan siber, atau bisa berasal dari kelemahan sistem itu sendiri[2]. Maka, perlu mekanisme yang memastikan sistem informasi yang diterapkan memiliki level keamanan yang memadai.

Audit sistem informasi menjadi salah satu cara menilai keamanan sistem informasi yang digunakan. Tujuannya adalah mengevaluasi apakah sistem telah dikelola sesuai standar dan prinsip tata kelola TI yang berlaku. Salah satu framework yang banyak digunakan adalah COBIT (Control Objectives for Information and Related Technologies) dikembangkan oleh ISACA. COBIT menyediakan panduan dan domain pengelolaan TI yang dapat membatu menilai kapabilitas proses TI dalam suatu instansi[3].

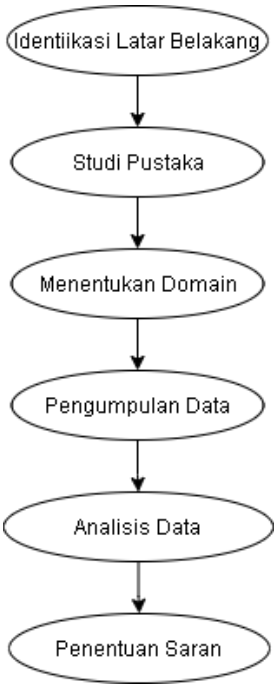
Studi kasus penelitian ini dilakukan di SMAN 1 Ponggok yang telah menerapkan sistem informasi dalam kegiatan akademiknya. Penelitian ini berfokus pada domain DSS05 (Manage Security Services) dalam COBIT 2019 yang mengatur pengelolaan layanan keamanan informasi[4]. Dengan memanfaatkan framework ini, bertujuan mengukur kapabilitas tata kelola keamanan TI serta memberikan rekomendasi perbaikan yang relevan[5].

Adapun penelitian seenis yang menggunakan COBIT. Penelitian oleh Ruri yang menggunakan kerangka kerja Cobit 2019 metode IT Audit Plan Development Process berokus pada management practice APO11, APO12, BA108, dan DSS05[6]. Sedangkan Indah melakukan audit menggunakan Cobit 5 dan mendapat hasil sistem informasi persediaan berada di level 2 yang berarti belum mencapai target karena masih ada GAP[7] . Penelitian yang dilakukan oleh Ridwan memilih domain APO03 karena design toolkit dapat nilai terbesar di Cobit 2019, hasilnya berada di level 3 berdasarkan domain tersebut[8].

Penelitian lainnya oleh Daffa menerapkan Cobit5 untuk mengukur tingkat keamanan dari sistem. Hasilnya sistem mencapai level 3 dengan nilai 3,89 dalam proses muturity level, sementara proses capability level berada di level 2. Maka perlunya perbaikan untuk mencapai level lebih tinggi[9]. Penelitian lainnya oleh Waruwu menggunakan Cobit 5 yang melakukan audit terhadap teknologi informasi jaringan transiber optic untuk mengukur kemamanannya[10].

II. METODE

Penelitian ini dilakukan sesuai dengan kerangka metode pada gambar 1 dibawah ini



Gambar 1. Kerangka Tahapan Penelitian

Berikut ini merupakan penjelasan dari tahapan penelitian pada gambar 1.

A. Identifikasi Latar Belakang

Langkah pertama yaitu mengidentifikasi latar belakang dan identifikasi masalah, tujuan penelitian, dan ruang lingkup penelitian yang akan dilakukan.

B. Studi Pustaka

Studi pustaka dilakukan untuk mencari landasan teori dalam melakukan pengumpulan data dan informasi. Studi pustaka dapat dilakukan dengan membaca dari berbagai jurnal, laporan, artikel, buku, dan data internet yang berhubungan dengan objek penelitian[11].

C. Menentukan Domain

Pada Cobit 2019 memiliki beberapa domain diantaranya adalah EDM, APO, BAI, DSS, dan MEA[12]. Setelah melakukan identifikasi latar belakang maka diimplementasikan domain DSS 05 *Manage Security Service.*

D. Pengumpulan Data

Pengumpulan data dilakukan dengan melakukan wawancara dan juga pengisian kuisioner pada pihak yang berkaitan dengan pengelolaan sistem informasi. Pemilihan responden berdasarkan pada pemetaan yang menggunakan diagram RACI yang menunjukkan bahwa responden dari penelitian adalah Staff IT.

E. Analisa Data

Analisis hasil dilakukan setelah responden mengisi kuisioner yang diberikan. Kuisioner yang diberikan berdasarkan panduan menggunakan Cobit 2019. Pertanyaan yang diberikan dimulai dari level 2 dan jika memenuhi kriteria akan dilanjut hingga level 5. Pengisian

jawaban akan bernilai 1 jika responden melilih jawaban Ya dan akan bernilai 0 jika memilih Tidak berdasarkan skala *guttman* [13].

Penghitungan capability level

Rumus perhitungan capability level = $\frac{Jumlah\ aktifitas\ yang\ telah\ dilakukan}{jumlah\ keseluruhan\ aktifitas}\ x\ 100\%$ *(1)*

Setelah perhitungan dilakukan maka terdapat skala level kapabilitas yaitu [15]:

1. Level 0 jika aktivitas tata kelola TI sama sekali tidak dilakukan.
2. Level 1 jika aktivitas tata kelola TI telah dilakukan namun belum konsisten atau belum lengkap.
3. Level 2 jika aktivitas tata kelola TI telah dijalankan mencapai tujuan dan terkelola dengan baik.
4. Level 3 jika ativitas tata kelola TI sudah berstandar.
5. Level 4 jika aktivitas tata kelola TI dapat diukur dan dikendalikan agar mencapai kinerja yang diinginkan
6. Level 5 jika aktivitas tata kelola TI telah mencapai tujuan dan diukur untuk meningkatkan perbaikan.

Rating proses dalam penilaian dijelaskan pada gambar dibawah :

Tabel 1. Skala Kapabilitas

Skala	Keterangan	Pencapaian
N	Not Achieved	0% - 15%
P	Partially Achieved	16% - 50%
L	Largely Achieved	51% - 85%
F	Fully Achieved	85% - 100%

Dalam melakukan pengukuran untuk melihat kesenjangan dapat dihitung dengan mengurangkan X dengan Y. Dimana X merupakan kapabilitas yang diharapkan dan Y kapabilitas yang dicapai.

F. Penentuan Saran

Penentuan saran dilakukan setelah mengetahui tingkat kapabilitas sistem dan bertujuan untuk perbaikan dan peningkatan sistem agar dapat mencapai level yang diharapkan[16].

III. HASIL DAN PEMBAHASAN

Setelah dilakukan pengukuran capability level DSS05 level 2 didapatkan hasil seperti pada gambar dibawah.

Tabel 2. Hasil Pengukuran Kuisioner DSS05.01 & DSS05.02

DSS05.01 Melindungi dari Perangkat Lunak Berbahaya		
No	***BP***	***Nilai***
1	Memasang dan mengaktifkan alat perlindungan perangkat lunak berbahaya sesuai kebutuhan	100%
2	Menyaring lalu lintas masuk, seperti email dan unduhan untuk melindungi informasi yang tidak diminta	100%

	Skala	100%

DSS05.02 Mengelola Jaringan dan Keamanan Konektivitas		
No	***BP***	***Nilai***
1	Hanya memberikan izin kepada perangkat yang memiliki akses dengan memasukkan kata sandi	100%
2	Menerapkan penyaringan jaringan dan kebijakan dalam	0%
3	Menerapkan protokol keamanan yang disetujui	100%
4	Mengkonfigurasi peralatan jaringan	100%
	Skala	75%

Pada tabel 2 hasil pengukuran kuisioner pada DSS05.01 Capaian 100% menunjukkan bahwa seluruh responden telah menerapkan praktik terbaik seperti penggunaan antivirus, pembaruan sistem keamanan, dan edukasi pengguna tentang risiko malware. Ini menjadi indikator positif bahwa sekolah sudah sadar akan bahaya serangan dari perangkat lunak berbahaya. Pada pengukuran DSS05.02, sebagian responden belum menerapkan kontrol keamanan jaringan secara menyeluruh. Hal ini bisa disebabkan oleh keterbatasan perangkat pendukung seperti firewall atau pengaturan router yang belum optimal. Jika tidak ditingkatkan, risiko akses jaringan yang tidak sah dapat terjadi.

Tabel 3. Hasil Pengukuran Kuisioner DSS05.03 & DSS05.04

DSS05.03 Mengelola Keamanan Endpoint		
No	***BP***	***Nilai***
1	Melakukan konfigurasi sistem operasi dengan cara yang aman	50%
2	Menerapkan mekanisme penguncian perangkat	50%
3	Mengelola dan mengontrol akses jarak jauh (perangkat seluler, kerja jarak jauh)	0%
4	Mengelola konfigurasi jaringan dengan cara yang aman	100%
5	Menerapkan fitur lalulintas jaringan pada perangkat *endpoint*	0%
6	Melindungi integritas sistem	100%
7	Memberikan perlindungan fisik pada perangkat *endpoint*	100%
8	Membuang perangkat endpoint dengan aman	0%
9	Mengelola akses berbahaya melalui email dan web browser	0%
	Skala	44%

DSS05.04 Mengelola Identitas Pengguna dan Akses		
No	***BP***	***Nilai***
1	Mengelola hak akses pengguna sesuai dengan persyaratan proses fungsi dan kebijakan keamanan yang telah ditetapkan	100%
	Skala	100%

Pada tabel 3, Menunjukkan hasil dari pengukuran DSS05.03 sebesar 44% hasil ini menunjukkan bahwa beberapa best practice tidak dilakukan oleh responden dan sebagian dilakukan. Pada DSS05.04 menunjukkan hasil 100% yang artinya seluruh best practice telah dilakukan.

Tabel 4. Hasil Pengukuran Kuisioner DSS05.05 & DSS05.06

DSS05.05 Mengelola Aset Fisik ke Aset TI		
No	***BP***	***Nilai***
1	Mencatat dan memantau semua titik masuk ke situs TI. Mendaftarkan semua pengunjung termasuk kontraktor dan vendor kedalam situs.	0%
2	Memasukkan semua anggota menampilkan tanda pengenal yang disetujui setiap saat	100%
3	Mengharuskan pengunjung untuk dikawal setiap waktu saat berada di lokasi	100%
4	Membatasi dan memantau akses ke situs TI yang sensitif dengan menetapkan batasan tertentu	100%
	Skala	75%

DSS05.06 Mengelola Dokumen Sensitif dan Perangkat Keluaran		
No	***BP***	***Nilai***
1	Menetapkan prosedur untuk mengatur penerimaan, penggunaan, pemindahan, dan penghapusan dokumen sensitif dan perangkat keluaran didalam dan diluar perusahaan	100%
2	Memastikan kontrol kriptografi diterapkan untuk melindungi informasi sensitif yang disimpan secara elektronik	50%
	Skala	75%

Pada tabel 4. Menunjukkan hasil dari pengukuran DSS05.05 sebesar 75% hasil ini menunjukkan bahwa terdapat satu best practice tidak dilakukan oleh seluruh responden dan pada hasil dari pengukuran DSS05.06 sebesar 75% hasil ini menunjukkan bahwa terdapat satu best practice yang tidak dilakukan oleh sebagian responden.

Tabel 5. Hasil Pengukuran Kuisioner DSS05.07

DSS05.07 Mengelola Kerentanan dan Memantau Infrastruktur Kejadian Melalui Keamanan		
No	***BP***	***Nilai***
1	Selalu menggunakan portofolio teknologi, layanan, dan aset yang didukung untuk mengidentifikasi kerentanan keamanan informasi	0%
2	Mendefinisikan dan mengkomunikasikan risiko, sehingga mudah dikenali, dan dapat memahami dampak yang terjadi	100%
3	Meninjau log peristiwa secara berkala untuk	100%

	mengetahui potensi insiden	
4	Pastikan tiket insiden yang berhubungan dengan keamanan dibuat tepat waktu saat pemantauan identifikasi potensi insiden	100%
	Skala	75%

Pada tabel 5. Menunjukkan hasil dari pengukuran DSS05.07 sebesar 75% hal ini menunjukkan bahwa mekanisme penanganan insiden belum terdokumentasi atau dilakukan secara formal. Belum ada tim tanggap insiden khusus atau prosedur standar saat terjadi pelanggaran keamanan. Dari hasil pengukuran diatas maka didapatkan hasil rekapitulasi sebagai berikut:

Tabel 6. Rekapitulasi Hasil Pengukuran Kuisioner

Rekapitulasi Hasil Kuisioner Penghitungan Capability Level DSS05				
Kode	***Proses***	***%***	***Pencapaian***	***Keterangan***
DSS05.01	Melindungi dari Perangkat Lunak Berbahaya	100%	F	Fully Achieved
DSS05.02	Mengelola Jaringan dan Keamanan Konektivitas	75%	L	Largely Achieved
DSS05.03	Mengelola Keamanan Endpoint	44%	P	Partially Achieved
DSS05.04	Mengelola Identitas Pengguna dan Akses	100%	F	Fully Achieved
DSS05.05	Mengelola Aset Fisik ke Aset TI	75%	L	Largely Achieved
DSS05.06	Mengelola Dokumen Sensitif dan Perangkat Keluaran	75%	L	Largely Achieved
DSS05.07	Mengelola Kerentanan dan Memantau Infrastruktur Kejadian Melalui Keamanan	75%	L	Largely Achieved
	Skala	78%	L	Largely Achieved

Pada hasil rekapitulasi tabel 6 dapat dilihat pencapaian dari masing-masing komponen proses yang menunjukkan hasil nilai rating kapabilitas sebesar 78%. Jika mengacu pada rating kapabilitas maka hasil dari penghitungan memiliki pencapaian L atau *Largely Achieved* level 1. Largely achieve yang didapat menyebabkan penilaian tidak dapat dilakukan kelevel berikutnya. Level ini menunjukkan bahwa proses yang dinilai dalam aktivitas sudah menunjukkan pencapaian yang substansial namun masih terdapat aktivitas yang dapat diperbaiki untuk mencapai level Fully Achieve yang kemudian dapat dilakukan pengukuran ke level berikutnya. Gap yang kesenjangan yang terjadi adalah 1 yang didapat dari penghitungan harapan dan kapabilitas yang dicapai yaitu 2-1.

Setelah penghitungan kapabilitas diatas saran / rekomendasi yang dapat diberikan adalah melakukan kontrol jarak jauh, lakukan kegiatan pengelolaan akses yang berbahaya melaui *email* dan *browser,* melakukan kegiatan penyaringan jaringan yang keluar masuk, melakukan pemantauan terhadap titik masuk situs TI.

IV. KESIMPULAN

Hal dapat disimpulkan sebagai hasil dari penelitian yang dilakukan pada SMAN 1 Ponggok berdasarkan audit sistem informasi berbasis web menggunakan COBIT 2019 adalah hasil penilaian terhadap capability di SMAN 1 Ponggok untuk DSS05. terlihat bahwa pencapaian pada level 1. artinya pihak sekolah telah melakukan aktivitas tata kelola TI khususnya pada pengelolaan layanan keamanan namun belum terdapat kekonsistenan atau belum lengkap sehingga penilain kapabilitas tidak dapat dilanjutkan pada level berikutnya dan perlu

dilakukannya perbaikan untuk mencapai tujuan kualitas yang diinginkan.

DAFTAR PUSTAKA

[1] Danianty Miranda Br. Bangun, Maida Andriani, and Risdiana Risdiana, "Audit Sistem Informasi Perpustakaan Sekolah Menggunakan Frame Work Cobit 5 Pada SMAN 1 Terbanggi Besar Lampung Tengah," *Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 2, no. 4, pp. 234–247, Jun. 2024, doi: 10.61132/merkurius.v2i4.173.

[2] Tiara Br Bangun, Amysa Putri Sitepu, Ayuri Nirvananda, and Adelia Revina Br PA, "Audit Sistem Informasi Perpustakaan Sekolah Menggunakan Frame Work Cobit 5 Pada SMK Negeri 1 Sirapit," *Jurnal Sistem Informasi dan Ilmu Komputer*, vol. 2, no. 3, pp. 105–114, Jul. 2024, doi: 10.59581/jusiik-widyakarya.v2i3.3788.

[3] ISACA, *COBIT 2019 Framework: Governance and Managemen Objectives*, 1st ed. Chicago: Information System Audit and Control Association (ISACA), 2019.

[4] W. W. A. Winarto, *Audit Sistem Informasi*, 1st ed., vol. 194 halaman. Pekalongan: PT. Natasya Expanding Management, 2022.

[5] U. Niswah and A. Purwinarko, "Audit Information Technology Using COBIT 5 in the Procurement Service Unit (Case Study: SIM UKPBJ Kabupaten XYZ)," *Journal of Advances in Information Systems and Technology*, vol. 4, no. 1, 2022, doi: https://doi.org/10.15294/jaist.v4i1.60793.

[6] R. Fadhilah, I. Santosa, and L. Abdurrahman, "RENCANA AUDIT TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 2019 PADA UNIT ISTI UNIVERSITAS TELKOM," *Jurnal Informatika dan Komputer) Akreditasi KEMENRISTEKDIKTI*, vol. 4, no. 3, 2021, doi: 10.33387/jiko.

[7] I. Fitria, L. Kurniawati, and T. Haryanti, "Audit Sistem Informasi Inventory Menggunakan Framework Cobit 5," *METIK JURNAL*, vol. 8, no. 2, pp. 99–106, Dec. 2024, doi: 10.47002/metik.v8i2.927.

[8] R. Dwi Irawan, E. Utami, and A. H. Muhammad, "EVALUASI MANAGED ENTERPRISE ARCHITECTURE PADA PENGADAAN ALAT PEMBELAJARAN TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 2019 (Studi Kasus: SMKN 1 Nglipar)."

[9] D. Iqbal Agselmora, A. Prasetyo Utomo, U. Stikubank Semarang, and J. Tri Lomba Juang Mugassari, "Audit Teknologi Informasi Menggunakan COBIT 5 Domain DSS Pada Universitas Stikubank Semarang," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 4, 2022, doi: https://doi.org/10.35957/jatisi.v9i4.2612.

[10] G. Waruwu and J. Sundari, "Audit Teknologi Informasi Menggunakan Cobit 5 Studi Kasus PT. Global Network Dharma Jaya," *Infomatek*, vol. 26, no. 1, pp. 69–74, May 2024, doi: 10.23969/infomatek.v26i1.13333.

[11] S. Safitri and N. Nurhayati, "Studi Pustaka: Pengaruh Perhatian Orang Tua Terhadap Prestasi Belajar Siswa Di Sekolah," *Journal of Educational Review and Research*, vol. 1, no. 2, pp. 64–67, 2018, doi: 10.26737/jerr.v1i2.1624.

[12] I. Bakti and M. Firdaus, "PENERAPAN FRAMEWORK COBIT 2019 PADA AUDIT TEKNOLOGI INFORMASI DI PT. LUM," *Jurnal Ilmiah Multidisiplin Ilmu*, vol. 1, no. 3, pp. 14–21, 2024, doi: 10.69714/p4eqa496.

[13] N. I. Atqiyak and D. B. Santoso, "Audit Sistem Informasi Aplikasi Gramedia Digital Menggunakan Framework COBIT 5," *Pixel: Jurnal Ilmiah Komputer Grafis*, vol. 15, no. 1, pp. 152–159, 2022, doi: 10.51903/pixel.v15i1.750.

[14] A. Hanifah, K. Kraugusteeliana, and S. Sarika, "PENGUKURAN CAPABILITY LEVEL PADA LAYANAN APLIKASI JAKI (JAKARTA KINI) MENGGUNAKAN FRAMEWORK COBIT 5 DOMAIN APO, DSS, & MEA," in *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya*, 2022, pp. 276–285.

[15] Y. Pratiwi and L. W. Widianti, "IMPLEMENTASI TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 PADA SALAH SATU BANK MILIK BUMN," *Jurnal Kecerdasan Buatan dan Teknologi Informasi*, vol. 4, no. 2, pp. 98–113, 2025, doi: 10.69916/jkbti.v4i2.281.

[16] A. P. Rabhani *et al.*, "Audit Sistem Informasi Absensi Pada Kejaksaan Negeri Kota Bandung Menggunakan Framework Cobit 5," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 9, no. 2, pp. 275–280, 2020, doi: 10.32736/sisfokom.v9i2.890.