NUANSA INFORMATIKA ***p-ISSN :1858-3911* , *e-ISSN : 2614-5405***
Volume 18 Nomor 01, Januari 2024 https://journal.fkom.uniku.ac.id/ilkom

Audit Keamanan Sistem Informasi Puskesmas Dengan Standar ISO/IEC 27001:2013 Dan Framework COBIT 5

Titan Parama Yoga*[1], Vani Maharani [2], Naufal Dwi Maulana [3]
[1]Sistem Informasi, Fakultas Teknologi dan Informatika
[2]Sistem Informasi, Fakultas Teknologi dan Informatika
[3]Sistem Informasi, Fakultas Teknologi dan Informatika
Universitas Informatika dan Bisnis Indonesia
E-mail: *[1]titanparamayoga@gmail.com, [2]vanimaharani@gmail.com, [3] NaufalDwi@gmail.com

Abstrak

Salah satu masalah suatu perusahaan adalah keamanan sistem informasi. Keamanan yang tinggi diperlukan untuk menjaga kerahasiaan dan penyalahgunaan informasi dalam organisasi. Untuk meningkatkan keamanan operasi bisnis dan kualitas sumber daya teknologi informasi, perlu dilakukan evaluasi keamanan aset teknologi informasi yang ada. Sama seperti salah satu sistem di PT Infokes Indonesia yaitu Sistem Informasi Puskesmas adalah aplikasi multi fungsi yang berbasis web base agar memungkinkan untuk digunakan oleh lebih dari satu orang pengguna pada saat yang bersamaan juga pencatatan pasien yang dilakukan secara elektronik.

Tujuan dari penelitian ini adalah untuk melakukan audit keamanan Sistem Informasi Puskesmas pada PT. Infokes Indonesia menggunakan ISO/IEC 27001:2013 dan *framework* COBIT 5 untuk mendokumentasikan temuan audit audit sistem informasi pada PT. Infokes Indonesia untuk membuat laporan audit.
Berdasarkan hasil penelitian yang telah dilakukan melalui wawancara dan kuesioner dengan menggunakan framework COBIT 5 dan menggunakan sub domain APO13, diperoleh hasil bahwa *Existing Capability* berada pada level 1 sedangkan *Capability Level* yang diharapkan berada pada level 3 sehingga Kesenjangan Kemampuan adalah 2

Kata kunci: ***Audit Keamanan Sistem Informasi, COBIT 5, APO13, ISO/IEC 27001:2013***

Abstract

One of the problems of a company is the security of information systems. High security is needed to maintain the confidentiality and misuse of information within the organization. To improve the security of business operations and the quality of information technology resources, it is necessary to evaluate the security of existing information technology assets. Just like one of the systems at PT Infokes Indonesia, namely the Health Center Information System, this is a multi-functional application based on a web base so that it can be used by more than one user at the same time as patient recording is done electronically. The purpose of this study was to conduct a security audit of the Health Center Information System at PT. Infokes Indonesia uses ISO/IEC 27001:2013 and the COBIT 5 framework to document audit findings of information system audits at PT. Infokes Indonesia to make an audit report. Based on the results of research that has been conducted through interviews and questionnaires using the COBIT 5 framework and using the APO13 sub domain, the results show that Existing Capability is at level 1 while the expected Capability Level is at level 3 so that the Capability Gap is 2.

Keywords: Information System Security Audit, COBIT 5, APO13, ISO/IEC 27001:2013

Diajukan: 15 Oktober 2023 *Disetujui: 12 Januari 2024* *Dipublikasi: 26 Januari 2024*

1 PENDAHULUAN

Dalam menjaga kondisi masyarakat untuk tetap sehat, pemerintah berkewajiban ikut andil dalam menjaga dan memenuhi kebutuhan pelayanan publik. Sesuai dengan UU No. 25 tahun 2009 tentang pelayanan publik, dijelaskan masyarakat berhak

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

mendapatkan pelayanan yang berkualitas sesuai dengan asas dan tujuan pelayanan publik. Pelayanan publik menjadi kegiatan atau rangkaian kegiatan dalam rangka pemenuhan kebutuhan pelayanan bagi setiap warga negara dan penduduk atas barang, jasa dan/atau pelayanan administratif yang disediakan oleh penyelenggara pelayanan publik.

Salah satu pelayanan publik yang memberikan pelayanan kesehatan pada masyarakat adalah Puskesmas. Pelayanan kesehatan yang dilakukan Puskesmas kepada masyarakat meliputi perencanaan, pelaksanaan, evaluasi, pendaftaran, pelaporan, dan sistematisasi. Puskesmas selalu berupaya memberikan pelayanan yang baik dalam segala kebutuhan pelayanan, meliputi pelayanan kuratif (pengobatan), preventif (upaya preventif), promotif (peningkatan kesehatan), dan rehabilitatif (memulihkan kesehatan), dengan harapan pasien yang menerima pelayanan kesehatan merasa puas.

Dalam pelaksanaan pelayanan kesehatan pada puskesmas tepat untuk memanfaatkan pelayanan teknologi yang sesuai dengan kebutuhan pelayanan disana, karena penggunaannya mudah dan tidak berdampak buruk bagi lingkungan sekitar. Dengan adanya pelaksanaan pelayanan kesehatan pada puskesmas ini sejalan dengan Instruksi Presiden No. 3 tahun 2003 tentang kebijakan dan strategi pengembangan e-Government. E-Government awalnya dipublikasi di Indonesia sejak tahun 2001 melalui Instruksi Presiden No.6 tahun 2001 tentang Telematika yang menyatakan bahwa aparat pemerintahan harus menggunakan teknologi telematika untuk mendukung good governance dan mempercepat proses demokrasi.

Tata kelola keamanan teknologi informasi memiliki banyak standar dalam melakukan evaluasi dan pengukuran, contoh yang paling sering digunakan adalah ISO 27001 dan COBIT. COBIT memiliki kelebihan sebagai framework tata kelola karena dapat mengintegrasikan sistem keamanan informasi ke dalam tata kelola TI yang lebih luas. Namun, keterbatasannya yaitu tidak memberikan petunjuk rinci bagi organisasi bagaimana melakukan sesuatu secara nyata dan lebih mengarahkan pada apa yang harus dilakukan. Sedangkan ISO 27001 merupakan salah satu standar yang telah berlaku secara internasional sebagai standar untuk membangun Sistem Manajemen Keamanan Informasi. Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis resiko, serta dirancang untuk menjamin kontrol keamanan yang dipilih perusahaan dapat melindungi aset informasi dari berbagai resiko serta memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan (Direktorat Keamanan Informasi, 2017).

PT. Infokes Indonesia (Infokes) adalah perusahaan Teknologi Informasi yang berfokus pada pengembangan produk dan solusi Teknologi Informasi Kesehatan secara online dan terintegrasi di Indonesia. Lebih dari 1 Dekade Infokes dipercaya membantu peningkatan kualitas pelayanan kesehatan di Indonesia dengan menerapkan lebih banyak sistem di 2500 titik (Puskesmas, Klinik, Pustu, Posyandu, Dinas Kesehatan Kota/Kabupaten) yang tersebar di seluruh Indonesia secara realtime. Produk-produk dari PT. Infokes Indonesia diantaranya yaitu e-Puskesmas, e-Clinic, e-Farmasi, e-Posyandu, e-Rujukan, e-Hospital, e-Dinkes dan e-Pustu.

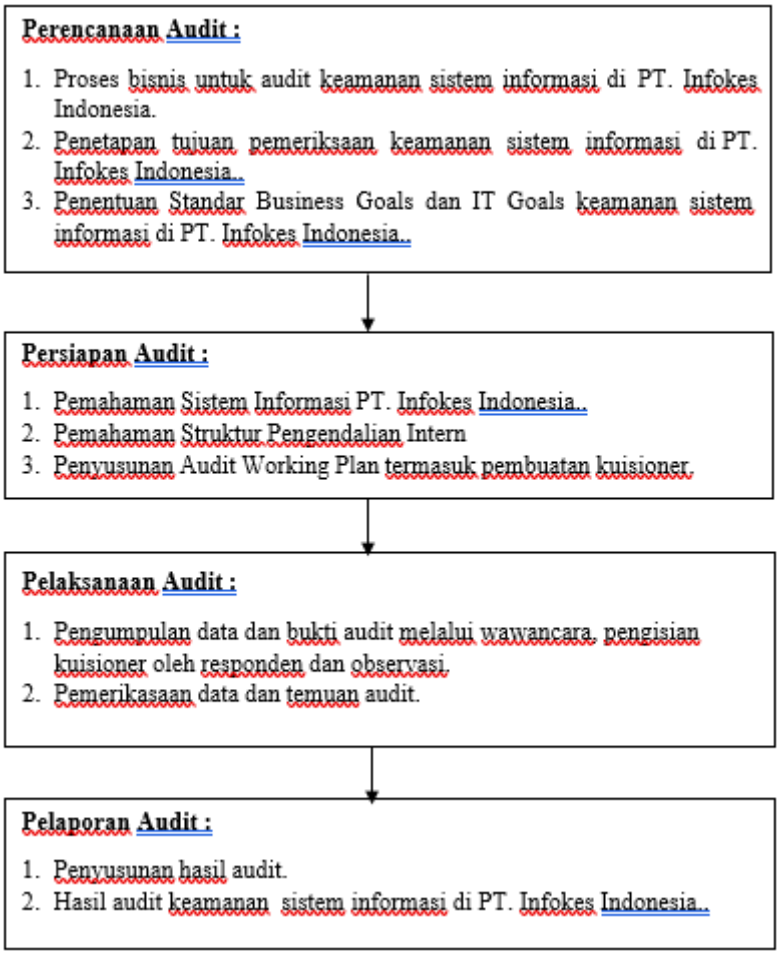
Dalam bisnisnya PT. Infokes Indonesia banyak klien dari pemerintahan Kabupaten/Kota di seluruh Indonesia. Untuk mendukung e-Government yang baik mulai menerapkan berstandar ISO terutama pada sistem informasi Puskesmas yang merupakan salah satu produk unggulan dari PT. Infokes Indonesia. Dalam pengembangan keamanan sistem informasi puskesmas, PT. Infokes Indonesia memilih standar ISO 27001:2013 dan *Framework* COBIT 5 sebagai acuan keamanan informasi.

2 METODE PENELITIAN

Dalam penelitian ini, metode penelitian yang digunakan adalah pendekatan deskriptif kualitatif. Pendekatan deskriptif kualitatif digunakan untuk mendapatkan gambaran yang jelas mengenai kondisi keamanan sistem informasi berdasarkan Standar ISO/IEC 27001 dan COBIT 5. Pengumpulan

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

data yang dilakukan dalam penelitian ini adalah data yang diperoleh dari hasil wawancara dan observasi mengenai tingkat kemampuan keamanan sistem informasi pada Sistem Informasi Puskesmas. Penelitian deskriptif kualitatif ini juga digunakan sebagai alat untuk menganalisis keterangan mengenai kinerja sistem yang sedang berjalan, yang kemudian dihubungkan dengan teori-teori yang ada pada Standar ISO/IEC 27001 dan *framework* COBIT 5. Tahap dalam penelitian ini dapat dilihat melalui skema penelitian berikut:



Gambar 1 Tahapan Penelitian

1. Perencanaan Audit

Pada tahapan ini peneliti melakukan pencarian informasi terkait proses bisnis pada PT Infokes Indonesia yang terkait keamanan sistem informasi. Selanjutnya menetapkan tujuan dan penentuan *standar business goals* dan *IT goals* dari pemeriksaan keamanan sistem informasi

2. Persiapan Audit

Setelah perencaan audit dilakukan, pada tahapan ini peneliti melakukan pemahaman sistem informasi, pemahaman struktur pengendalian intern dan penyusunan audit working plan di PT. Infokes Indonesia termasuk pembuatan kuesioner.

3. Pelaksanaan Audit

Pada tahapan ini peneliti melakukan pengumpulan data dan bukti audit melalui wawancara, pengisian kuesioner oleh responden dan observasi. Setelah terkumpul maka dilanjutkan dengan pemeriksaan data dan temuan audit

4. Pelaporan Audit

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Tahapan akhir dari rangkaian audit keamanan sistem informasi adalah dengan melakukan penyusunan hasil audit yang berupa rekomendasi apa saja yang harus dilakukan oleh PT. Infokes Indonesia agar keamanan sistem informasi nya memenuhi standar yang telah di tentukan oleh ISO-IEC 27001 dan COBIT 5.

A. Metode Pengumpulan dan Analisis Data

Dalam penelitian ini, peneliti membutuhkan data dan informasi lengkap sebagai bahan untuk mendukung teori-teori yang telah diuraikan pada bab sebelumnya, metode pengumpulan data yang digunakan meliputi studi kepustakaan, studi lapangan yang terdiri dari observasi, wawancara, dan juga kuesioner studi literatur serupa. Berikut adalah penjelasan dari masing-masing tahapan pengumpulan data dalam penelitian ini.

Studi Pustaka

Studi pustaka dilakukan oleh peneliti untuk mengumpulkan dan mempelajari berbagai perpustakaan berupa buku, *e-book*, hasil penelitian sebelumnya berupa jurnal, dan situs-situs di internet yang membahas tentang konsep pemerintahan teknologi informasi, konsep audit, tata kelola berbasis teknologi informasi COBIT 5, *security* audit berdasarkan ISO/IEC 27001:2013 dan referensi lainnya terkait dengan COBIT 5 dan ISO/IEC 27001:2013. Peneliti melakukan studi pustaka untuk memberikan gambaran bagaimana tahapan-tahapan tersebut COBIT 5, ISO/IEC 27001:2013 tahapan dan untuk memberikan gambaran umum ketika COBIT 5 dan ISO/IEC 27001:2013 digunakan bersama.

Sebelumnya pada beberapa penelitian terdahulu tentang hubungan antara kerangka kerja COBIT 5 dan ISO/IEC 27001. Oleh karena itu dalam penelitian ini peneliti melakukan audit dengan menggunakan *framework* COBIT 5 yaitu tahap *Initiation* yang ada di *Assessment Process Activities* untuk memetakan memiliki tujuan terkait informasi keamanan.

Studi Lapangan

Peneliti melakukan studi lapangan secara langsung di kantor PT. Infokes Indonesia yang beralamat Komp. Palm Bridge, No. 1E, Jalan Cukang Kawung - Cikutra, Cibeunying, Kec. Cimenyan, Kabupaten Bandung dan Jl. Rereng Barong No.40, Sukaluyu, Cibeunying Kaler, Kota Bandung. Studi lapangan ini mencakupsebagai berikut:

i. Observasi

Observasi dilakukan di Kantor 2 PT. Infokes Indonesia yang beralamat Jl. Rereng Perbandingan 2 Standar Keamanan Informasi Barong No.40, Sukaluyu, Cibeunying Kaler, Kota Bandung. Peneliti melakukan observasi selama 6 bulan, mulai pada awal tahun 2023 sampai bulan Juni. Pendataan melalui pengamatan yang dilakukan dengan melihat langsung bagaimana proses pengelolaannya keamanan informasi. Dari hasil observasi ini peneliti juga memperoleh data berupa visi, misi, tujuan organisasi, dan struktur organisasi yang berguna untuk tahap inisiasi

ii. Wawancara

Peneliti melakukan wawancara dengan tanya jawab langsung dengan para VP di PT. Infokes Indonesia. Orang-orang yang dilakukan wawancara yaitu:

Tabel 1. orang-orang yang dilakukan wawancara

No	Nama	Jabatan
1.	Viktor Tunggul	VP Application
2.	Aji Sulaeman	Tech Lead Backend Epuskesmas
3.	Arief	Tech Lead Frontend Epuskesmas
4.	Romi Arief Rachman	Tech Lead Eclinic
5.	Faisal Fasha	Tim Dev. Clinic

Secara garis besar hasil yang diperoleh dari wawancara adalah gambaran

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

umum dari tugas dari masing-masing VP. Selain itu dari hasil wawancara juga diketahui bagaimana penerapan manajemen keamanan informasi di sana, serta insiden apa saja yang pernah terjadi. Diketahui bahwa PT. Infokes Indonesia saat ini sedang melakukan penerapan standar ISO. Dari keterangan tersebut, para *top* manajemen menyarankan untuk melakukan audit keamanan sistem informasi pada seluruh divisi yang ada di PT. Infokes Indonesia. Dari hasil wawancara tersebut dapat dipetakan juga kebutuhan organisasi yang sesuai dengan proses yang ada pada COBIT 5 dan klausul ISO 27001:2013.

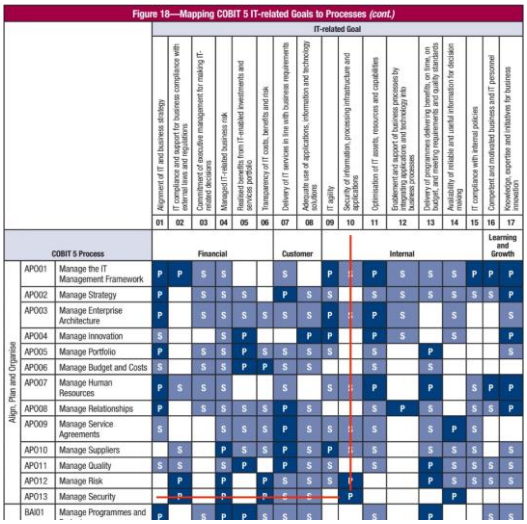
iii. Kuesioner

Kuesioner ini dilakukan setelah peneliti melakukan pemetaan.

Tabel 2. Pemetaan COBIT 5 dengan ISO 27001:2013 (NIST, 2014)

COBIT 5 *Process*		**ISO 27001:2013 *Control Objective***
APO13	**Mengelola Keamanan**	
APO13.01	*Establish and maintain an ISMS* (Menetapkan dan Mempertahankan Sistem Manajemen Keamanan Informasi)	A.6.1.5 Keamanan Informasi dalam Manajemen Proyek A.6.2.2 Teleworking A.8.2.2 Pemberian Label Informasi A.8.2.3 Penanganan aset A.8.3.1 Pengelolaan media yang dapat dilepas A.8.3.3 Transfer media fisik A.11.2.9 Hapus meja dan kebijakan layar jernih A.12.3.1 *Backup* Informasi A.13.1.1 Kontrol Jaringan A.13.2.1 Kebijakan dan prosedur pengalihan informasi
		A.14.1.1 Analisis dan spesifikasi kebutuhan keamanan informasi A.14.2.1 Kebijakan pengembangan yang aman A.14.2.5 Prinsip rekayasa sistem yang aman A.17.1.2 Menerapkan kontinuitas keamanan informasi A.17.1.3 Verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi A.18.1.3 Perlindungan catatan
APO13.02	Define and manage on information security risk treatment plan (Menetapkan dan mengelola rencana perawatan risiko keamanan informasi)	A.6.1.1 Peran dan Tanggung Jawab Keamanan Informasi A.7.2.1 Tanggung Jawab Manajemen A.14.2.8 Pengujian keamanan sistem
APO13.03	Monitor and review the ISMS (Pantau dan Tinjau Sistem Manajemen Keamanan Informasi)	

Berdasarkan tabel ini, peneliti mendapatkan hasil domain COBIT 5 yaitu APO13 (*Manage Security*). Domain APO13 ini berisi tentang Sistem Manajemen Keamanan Informasi yang berhubungan dengan ISO/IEC 27001:2013. Juga karena PT. Infokes Indonesia ingin melakukan sertifikasi ISO, maka peneliti menggunakan tahapan Initiation yang ada Assessment



Process Activities COBIT 5.

Pelaksanaan kuesioner ini berada pada tahap *Check* dan berdasarkan standar yang terdapat pada ISO/IEC 27001:2013 mengenai implementasi pada keamanan aset dan pendekatan pada penekanan manajemen risiko dan ISO/IEC 27002: 2013 mengenai petunjuk pelaksanaan sistem manajemen keamanan informasi dan klausul dipilih berdasarkan nilai dari risiko keamanan informasi Bagian *Infrastructure & Shared Services.*

3 HASIL DAN PEMBAHASAN

3.1 Pelaksanaan Audit

Assessment Process Activities COBIT 5

Dalam penelitian ini penulis menggunakan *Initiation* yang ada pada *Assessment Process Activities* COBIT 5. Hasil serta pembahasan dari *Initiation* dapat dilihat di bawah ini.

Initiation

Berikut ini merupakan pembahasan dari tiap *Initiation* yang hanya terdiri dari satu tahapan yaitu menjelaskan tentang focus area menurut COBIT 5.

Pada tahap ini akan ditentukan ruang lingkup audit dilakukan di PT. Infokes Indonesia khususnya pada produk Sistem

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Informasi Puskesmas berdasarkan identifikasi masalah ada sehingga dipetakan untuk mendapatkan domain proses COBIT 5 akan diaudit. Berdasarkan tujuan TI yaitu "Melindungi seluruh sistem keamanan untuk mempertahankan tingkatan dari keamanan informasi. Menetapkan, mengelola hak akses user dan melakukan pengawasan keamanan dengan tujuan meminimalisasikan dari kerentanan dan insiden dari keamanan informasi operasional." dan akan dilakukannya sertifikasi terdapat beberapa *enterprise goals* COBIT 5 yaitu:

Gambar 2. Cobit *Process (Mapping COBIT 5 IT-related Goals to Processes)*

Dari hasil pemetaan pada gambar di atas dengan lingkup yang sudah dikemukakan dapat diketahui bahwa *IT-related goals* tujuan TI menghasilkan 1 proses COBIT yang primary atau memiliki hubungan yaitu APO13 *Manage Security*.

Hasil pemetaan tersebut kemudian disesuaikan lagi dengan perencanaan sertifikasi ISO/IEC 27001:2013. ISO 27001:2013 ini memfokuskan diri pada keamanan sistem informasi suatu organisasi dan merupakan standar dalam Sistem Manajemen Keamanan Informasi (SMKI) yang menyediakan apa-apa saja yangharus dilakukan dalam upaya menerapkan konsep keamanan informasi di organisasi atau perusahaan.

Dari *mapping* COBIT berdasarkan *eBook* COBIT 5 Enabling Processes yang terpilih di atas, proses APO13 Manage Security di dalamnya berisi tentang Sistem Manajemen Keamanan Informasi. Pada Bab II terdapat penjabaran dari *sub-process* yang terdapat dari masing-masing. COBIT 5 process dan sub-process pada APO13 itu antara lain:

1. APO13.01 *Establish and maintain an ISMS* (Menetapkan dan Mempertahankan Sistem Manajemen Keamanan Informasi).
2. APO13.02 *Define and manage on information security risk treatment plan* (Menetapkan dan mengelola rencana perawatan risiko keamanan informasi).
3. APO13.03 *Monitor and review the ISMS* (Pantau dan tinjau Sistem Manajemen Keamanan Informasi).

Berdasarkan penjabaran tersebut penulis membatasi penelitian dengan proses COBIT 5 APO13 untuk melihat perkembangan apa saja yang sudah dilaksanakan PT. Infokes Indonesia dalam melaksanakan Sistem Manajemen Keamanan Informasi untuk produk mereka Sistem Informasi Puskesmas. Untuk pembahasan Sistem Manajemen Keamanan Informasi akan menggunakan Standar ISO/IEC 27001:2013 karena sesuai dengan kebutuhan PT. Infokes Indonesia pada produk Sistem Informasi Puskesmas.

Pengumpulan Data dan Bukti Audit

Proses pengumpulan data dari divisi-divisi dan pengguna yang berfokus pada wawancara dan evaluasi terhadap Sistem Informasi Puskesmas PT. Infokes Indonesia.

Pengumpulan Data dan Temuan Audit Menggunakan Standar ISO 27001:2013

Pemeriksaan data dan temuan audit menggunakan standar ISO 27001:2013 untuk Sistem Informasi Puskesmas dimulai dengan penentuan ruang lingkup yang dalam hal ini didapat sama halya ketika penentuan ruang lingkup untuk standar COBIT 5 yaitu dengan teknik wawancara terhadap VP yang ada di PT Infokes Indonesia. Dari hasil wawancara didapat ruang lingkup dengan menggunakan standar ISO 27001:2013 dengan klausul yang dapat dilihat dari tabel berikut.

Tabel 3. Klausul ISO 27001:2013 yang digunakan

Pada proses ini langkah yang dilakukan adalah menentukan klausul, objektif kontrol dan kontrol yang sesuai dengan permasalahan dan kebutuhan Sistem Informasi Puskesmas PT. Infokes Indonesia. Klausul, objektif kontrol dan kontrol yang ditentukan harus berdasarkan kesepakatan bersama pada proses wawancara sebelumnya.

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Kontrol keamanan menjadi acuan untuk pembuatan pernyataan yang terdapat pada setiap klausul yang telah ditetapkan berdasarkan standar ISO 27001:2013. Daftar pertanyaan ini digunakan untuk mempermudah dalam penyusunan daftar pertanyaan proses audit keamanan. Contoh pembuatan pertanyaan sebagai berikut.

Tabel 4. Contoh Pertanyaan berdasarkan ISO 27001:2013

A.7 Keamanan Sumber Daya Manusia

A.7.1 Sebelum Dipekerjakan

Tujuan Pengendalian (control objective):
Untuk memastikan bahwa karyawan memahami tanggung jawab mereka dan sesuai dengan peran yang ditetapkan bagi mereka.

Klausul	Deskripsi	Pertanyaan "Pengendalian Teknis (control)"	Y/N/P	Komentar
A.7.1.1	Penyaringan	Pengendalian Teknis (control): Apakah verifikasi latar belakang dari semua calon pegawai telah dilaksanakan berdasarkan peraturan perundangan (hukum, regulasi) dan etika terkait yang relevan serta telah proporsional terhadap persyaratan kerja (bisnis), klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan?		
A.7.1.2	Syarat dan Ketentuan Kepegawaian (Ketenagakerjaan)	Pengendalian Teknis (control): Apakah perjanjian tertulis dengan pegawai/ personil dan kontraktor telah menyatakan tanggung jawab keamanan informasi mereka dan organisasi?		

Pengumpulan Data dan Temuan Menggunakan COBIT 5

Pengumpulan data dan temuan audit menggunakan standar COBIT 5 dimulai dari pemeriksaan terhadap hasil dari pembuatan kuisioner yang berhubungan dengan keamanan sistem informasi yang diwakili oleh domain APO13. Setelah hasil terkumpul maka dilakukan validasi untuk menentukan apakah jawaban terhadap kuesioner yang disebar valid. Setiap pertanyaan yang akan dikategorikan secara terperinci sesuai dengan pertanyaan masing-masing domain, seperti berikut :

Tabel 5. Kategori dan *collection* domain APO13

Doman/Proses Number: APO13 (Manage Security)		
Data Collection	Description	Metode Pengumpulan
PA 1.1 - Process Performance	1. Pembangunan dan pemeliharaan sistem manajemen keamanan Performance informasi (SMKI). 2. Pemantauan dan peninjauan SMKI. 3. Pendefinisian dan pengelolaan rencana perlakuan risiko keamanan informasi.	Kuesioner
Doman/Proses Number: APO13 (Manage Security)		
Achievement	Result of Full Achievement of the Attribute	Metode Pengumpulan
PA 2.1 - Performance Management	1. Pendefinisian tujuan untuk kinerja proses. 2. Pemantauan dan perencanaan kinerja proses. 3. Penyesuaian kinerja proses untuk memenuhi rencana. 4. Pendefinisian, penugasan dan pengkomunikasian tanggungjawab dan wewenang untuk melakukan proses. 5. Pendefinisian, pengalokasian dan penggunaan sumber daya dan informasi yang diperlukan untuk melakukan proses. 6. Komunikasi antara pihak-pihak yang terlibat dikelola untuk memastikan komunikasi yang efektif dan keielasan penugasan tanggung jawab. 7. Pendefinisian tujuan untuk kinerja proses. 8. Pemantauan dan perencanaan kinerja proses. 9. Penyesuaian kinerja proses untuk memenuhi rencana. 10. Pendefinisian, penugasan dan pengkomunikasian tanggung jawab dan wewenang untuk melakukan proses. 11. Pendefinisian, pengalokasian dan penggunaan sumber daya dan informasi yang diperlukan untuk melakukan proses. 12. Komunikasi antara pihak-pihak yang terlibat dikelola untuk memastikan komunikasi yang efektif dan keielasan penugasan tanggung jawab.	Kuesioner
PA 2.2 - Work Product Management	1. Pendefinisian persyaratan untuk produk kerja dari proses. 2. Pendefinisian persyaratan untuk dokumentasi dan kontrol dari produk kerja. 3. Pengidentifikasian, pendokumentasian dan pengendalian produk kerja secara tepat. 4. Peninjauan produk kerja apakah sesuai dengan pengaturan yang direncanakan dan disesuaikan seperlunya untuk memenuhi persyaratan. 5. Pendefinisian persyaratan untuk produk kerja dari proses. 6. Pendefinisian persyaratan untuk dokumentasi dan kontrol dari produk kerja. 7. Pengidentifikasian, pendokumentasian dan pengendalian produk kerja secara tepat. 8. Peninjauan produk kerja apakah sesuai dengan pengaturan yang direncanakan dan disesuaikan seperlunya untuk memenuhi persyaratan.	Kuesioner
PA 3.1 - Process Definition	1. Pendefinisian proses standar yang dapat menggambarkan unsur-unsur mendasar yang harus dimasukkan ke dalam sebuah proses tersebut. 2. Penentuan Urutan dan interaksi dari proses standar dengan proses lainnya. 3. Pendefinisian kompetensi yang dibutuhkan dan peran untuk melakukan proses sebagai bagian dari proses standar. 4. Pengidentifikasian infrastruktur yang diperlukan dan lingkungan kerja untuk melakukan proses sebagai bagian dari proses standar. 5. Penetapan metode yang cocok untuk memantau efektivitas dan kesesuaian proses tersebut.	Kuesioner
PA 3.2 - Process Deployment	1. Pemilihan dan / atau penyesuaian proses yang didefinisikan Kuesioner ditempatkan didasarkan pada standar proses tepat. 2. Pendefinisian, penugasan dan pengkomunikasian peran, tanggung jawab dan kewenangan yang diperlukan untuk melakukan proses. 3. Pendefinisian kompetensi personel yang melaksanakan proses atas dasar pendidikan, pelatihan dan pengalaman. 4. Pendefinisian, pengalokasian dan penggunaan sumber daya yang diperlukan dan informasi yang diperlukan untuk melakukan proses. 5. Pendefinisian, pengelolaan dan pemeliharaan infrastruktur yang diperlukan dan lingkungan kerja untuk melakukan proses. 6. Data yang sesuai dikumpulkan dan dianalisis sebagai dasar untuk memahami perilaku dari proses untuk menunjukkan kesesuaian dan efektivitas, seta mengevaluasi perbaikan berkelanjutan dari proses dapat dibuat.	Kuesioner
PA 4.1 - Process Measurement	1. Informasi proses yang dibutuhkan mendukung tujuan bisnis relevan. 2. Tujuan pengukuran proses yang berasal dari kebutuhan informasi proses. 3. Tujuan kuantitatif untuk kinerja proses dalam mendukung tujuan bisnis yang relevan ditetapkan. 4. Tindakan dan frekuensi pengukuran didentifikasi dan didefinisikan sejalan dengan tujuan pengukuran proses dan tujuan kuantitatif untuk kinerja proses. 5. Pengumpulan, penganalisaan dan pelaporan hasil pengukuran untuk memantau sejauh mana tujuan kuantitatif untuk kinerja proses terpenuhi. 6. Hasil pengukuran yang digunakan menggambarkan kinerja proses.	Kuesioner
PA 4.2 - Process Measurement	1. Penentuan dan penerapan analisis dan kontrol teknik yang berlaku. 2. Penetapan batas kontrol variasi untuk kinerja proses normal. 3. Penganalisaan data pengukuran untuk penyebab khusus variasi. 4. Pengambilan tindakan korektif untuk mengatasi penyebab khusus variasi. 5. Pendirian kembali (jika diperlukan) batas kontrol berikut tindakan korektif.	Kuesioner
PA 5.1 - Process Innovation	1. Dampak dari semua perubahan yang diusulkan dinilai terhadap tujuan dari proses yang didefinisikan dan proses standar. 2. Pengelolaan persetujuan pelaksanaan semua perubahan untuk memastikan bahwa setiap gangguan terhadap kinerja proses dipahami dan diberi tindakan. 3. Berdasarkan kinerja aktual, efektivitas proses perubahan dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk penentuan hasil apakah dikarenakan sebab umum atau khusus.	Kuesioner
PA 5.2 - Optimisation	1. Dampak dari semua perubahan yang diusulkan dinilai terhadap	Kuesioner

No	Klausul	Deskripsi
1	A.7	Keamanan Sumber Daya Manusia
2	A.8	Manajemen Aset
3	A.9	Kontrol Akses
4	A.11	Keamanan Fisik dan Lingkungan
5	A.12	Keamanan Operasi
6	A.13	Keamanan Komunikasi
7	A.16	Pengelolaan Insiden Keamanan Informasi

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Process	Kuesioner tujuan dari proses yang didefinisikan dan proses standar. 2. Pengelolaan persetujuan pelaksanaan semua perubahan untuk memastikan bahwa setiap gangguan terhadap kinerja proses dipahami dan diberi tindakan. 3. Berdasarkan kinerja aktual, efektivitas proses perubahan dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk penentuan hasil apakah dikarenakan sebab umum atau khusus.	

Pemeriksaan Data dan Temuan Audit

Proses Number APO13 memiliki keturunan untuk penetapan hasil sebagai berikut:

Tabel 6. *Outcome* dari Process APO13

Outcome	***Description***
APO13.01	Sebuah sistem di tempatkan pada tempat yang dianggap efektifuntuk menangani persyaratan keamanan informasi perusahaan.
APO13.02	Sebuah rencana keamanan telah dibentuk, diterima dan dikomunikasikan di seluruh perusahaan.
APO13.03	Solusi keamanan informasi diimplementasikan dan dioperasikan secara konsisten di seluruh perusahaan.

Total dari persentase *achievement/outcome* menentukan nilai dari Total *Achievement* PA1.1 dan Rating by Criteria untuk APO13, namun persentase *achievement/outcome* masing-masing *outcome* ditentukan berdasarkan persentase *achievement / component*. Komponen dari masing-masing outcome yaitu sebagai berikut.

Tabel 7. Tabel Komponen dari masing-masing *outcome* pada *Process* APO13

Outcome	*Component*	*Number*	*Description*
APO13-O1	*Work Product Output*	APO13-WP1	Kebijakan SMKI
		APO13-WP2	Pernyataan ruang lingkup SMKI
		APO13-WP5	Laporan audit SMKI.
		APO13-WP6	Rekomendasi perbaikan/penggunaan SMKI.
	Base Practice + Work Product Input	APO13-BP1	Membangun dan memelihara sistem manajemen keamanan informasi (SMKI).
		APO13-BP3	Memantau dan meninjau SMKI.
APO13-O2	*Work Product Output*	APO13-WP3	Rencana penanganan risiko keamanan informasi.
		APO13-WP4	Kasus bisnis keamanan informasi.
	Base Practice + Work Product Input	APO13-BP2	Menentukan dan mengelola rencana penanganan risiko keamanan informasi.
APO13-O3	*Work Product Output*	APO13-WP5	Laporan audit SMKI.
		APO13-WP6	Rekomendasi perbaikan SMKI.
	Base Practice + Work Product Input	APO13-BP3	Memantau dan meninjau SMKI.

Proses c*omponent* yang didapatkan dari total semua jawaban "Y" dibagi dengan total jumlah pertanyaan dari setiap componentadalah sebagai berikut.

Tabel 8. Tabel Tabulasi penilaian *audit* terhadap proses *number* APO13

Number	*Description*	*Achievement / Component*	*Achievement / Component*	*Total Achievement PA 1.1 (APO13)*
APO13-WP1	Kebijakan SMKI	100%	96%	87%
APO13-WP2	Pernyataan ruang lingkup SMKI			
APO13-WP5	Laporan audit SMKI.			
APO13-WP6	Rekomendasi perbaikan/penggunaan SMKI.			
APO13-BP1	Membangun dan memelihara sistem manajemen keamanan informasi (SMKI).	92%		
APO13-BP3	Memantau dan meninjau SMKI.			
APO13-WP3	Rencana penanganan risiko keamanan informasi.	50%	75%	
APO13-WP4	Kasus bisnis keamanan informasi.			
APO13-BP2	Menentukan dan mengelola rencana penanganan risiko keamanan informasi.	100%		
APO13-WP5	Laporan audit SMKI.	100%	96%	
APO13-WP6	Rekomendasi perbaikan SMKI.			
APO13-BP3	Memantau dan meninjau SMKI.	92%		

Tabel diatas menunjukan tabulasi penilaian audit terhadap *process number* APO13, hasil dari *Achievement /Component* pertama didapatkan dari hasil perhitungan rekapitulasi dari hasil rata-rata perhitungan responden yang telah dihitung. Dari APO13-WP1, APO13-WP2, APO13-WPS dan APO13-WP6 dijumlahkan semua hasil responden dengan jumlah 100%. Selanjutnya perhitungan number APO13-BP1 dan APO13-BP5 menghasilkan perhitungan sebanyak 92% lalu diakumulasikan APO13-WP1 sampai APO13-WP6 dan APO13-BP1 dibagi 2 dengan APO13-BP5 maka menghasilkan hasil akhir dari APO13-01 sebesar 96%.

Perhitungan number APO13-WP1 dan APO13-WP4 menghasilkan jawaban responden sebesar 50% dari beberapa responden yang menjawab, sedangkan APO13-BP2 menghasilkan jawaban responden sebesar 86%. Dari kedua

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

perhitungan tersebut dijumlahkan lalu dibagi dua sehingga menghasilkan hasil akhir dari APO13-02 sebesar 68%.

Perhitungan terakhir yaitu APO13-WPS dan APO13-WP6 menghasilkan jawaban responden sebesar 100% dari 10 responden yang menjawab, sedangkan APO13-BP3 menghasilkan jawaban responden sebesar 80%. Dari kedua perhitungan tersebut dijumlahkan lalu dibagi dua sehingga menghasilkan hasil akhir dari APO13-03 sebesar 90%.

Total *Achievement* PA 1.1 (APO13) diatas dijumlahkan ((96%+68%+90%) : 3) menghasilkan hasil akhir sebesar 84,66%.

Setelah total *achievement* PA 1.1 dari masing-masing domain didapat dan dimasukkan ke dalam format yang disesuaikan dengan ISO/IEC maka didapat *rating*dari masing-masing domain yaitu:

Tabel 9. Rating untuk Domain APO13

Process Name	Level 1	Level 2		Level 3		Level 4		Level 5	
APO13	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Rating by Criteria	87%	88%	88%	45%	58%	83%	70%	70%	50%
Rating	F	F	F	P	L	L	L	L	P
Capability Level Achieved	1	1	2	2	Stop!	Stop!	Stop!	Stop!	Stop!

Tabel diatas menunjukan rating pada domain 13 menunjukan level 1 pada PA menghasilkan rating by criteria sebesar 87% dengan rating pada kategori Fdengan capability level *Fully Achieved(1)* pada level 1, lalu level 2 pada PA 2.1 menghasilkan *rating by criteria* sebesar 88% dengan rating pada kategori F dengan *capability level achieved* dengan keterangan *Fully Achieved(1)*, level 2 pada PA 2.2 menghasilkan *rating by criteria* sebesar 88% dengan *rating* pada kategori F dengan *capability level achieved* dengan keterangan *Fully Achieved(2)*, level 3 pada PA 3.1 menghasilkan rating by criteria sebesar 45% dengan rating pada kategori P dengan *capability level achieved* dengan keterangan *Fully Achieved(2)*, level 3 pada PA 3.2 menghasilkan *rating by criteria* sebesar 58% dengan rating pada kategori L dengan *capability level achieved* dengan keterangan STOP!, level 2 pada PA 4.1 menghasilkan *rating by criteria* sebesar 83% dengan *rating* pada kategori L dengan *capability level achieved* dengan keterangan STOP!, level 4 pada PA 4.2 menghasilkan *rating by criteria* sebesar 70% dengan *rating* pada kategori L dengan *capability level achieved* dengan keterangan STOP!, level 5 pada PA 5.1 menghasilkan *rating by criteria* sebesar 70% dengan rating pada kategori L dengan *capability level achieved* dengan keterangan STOP!, dan yang terakhir level 5 pada PA 5.2 menghasilkan menghasilkan *rating by criteria* sebesar 50% dengan *rating* pada kategori P dengan *capability level achieved* dengan keterangan STOP!.

Perolehan *rating by criteria* menjadi dasar penentuan rating yang diperoleh dari:

a. N (Not Achieved / Tidak Tercapai)
   Kategori ini terjadi apabila, *range* yang didapatkan dari rating by criteria berkisarantara 0%-15%.
b. P (Partially Achieved / Sebagian Tercapai)
   Kategori ini terjadi apabila, *range* yang didapatkan dari rating by criteria berkisarantara 15%-50%.
c. L (Large Achieved / Sebagian Besar Tercapai)
   Kategori ini terjadi apabila, *range* yang didapatkan dari rating by criteria berkisarantara 50%-85%.
d. F (Fully Achieved / Sepenuhnya Tercapai)
   Kategori ini terjadi apabila, *range* yang didapatkan dari rating by criteria berkisarantara 85%-100%.

Penilaian Hasil *Existing*

Perolehan rating dari masing-masing domain diperoleh, tahap selanjutnya yaitu penilaian terhadap hasil *existing* dari APO13, yaitu:

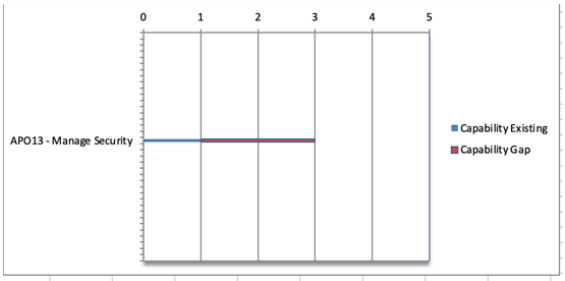
1. Sistem manajemen keamanan informasi berjalan dengan baik karenapenentuan ruang lingkup yang lebih rinci, terutama dalam hal karakteristik perusahaan, organisasi, lokasi, aset dan teknologi.
2. Sistem manajemen keamanan sistem informasi puskesmas di PT. Infokes Indonesia telah sesuai dengan organisasi, aset dan teknologi.

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

3. Sistem manajemen keamanan informasi di sistem informasi puskesmas di PT. Infokes Indonesia telah sejajar dengan keseluruhan manajemen keamanan.
4. Adanya komunikasi antara manajemen terkait peran dan tanggung jawab manajemen terhadap keamanan informasi.
5. Bahwa ada ulasan terhadap efektivitas SMKI meskipun tidak dilakukan secara regular.

GAP

Gap adalah selisih antara level target yang hendak dicapai dan *level capability* yang dicapai. Dari hasil existing terhadap domain diatas maka diperoleh grafik gap sebagai berikut.



Gambar 3. Gap antara level yang diinginkan perucahaan dengan *level capability*

Gap Grafik tersebut menunjukkan bahwa level yang diinginkan oleh perusahaan berada pada level 3, namun kenyataan level capability Sistem Informasi Puskesmas yang berada di PT. Infokes Indonesia berada pada level 1.

Rekomendasi

Maka pada berdasarkan hasil dari APO13 menghasilkan rekomendasi sebagai berikut:

a. Memberikan masukan untuk pemeliharaan rencana keamanan dengan mempertimbangkan temuan kegiatan pemantauan dan peninjauan jangka panjang.
b. Mempertimbangkan dan mendiskusikan kasus bisnis dengan keadaan keamanan informasi.
c. Pembuatan dokumen tata kelola dan dokumen manual keamanan informasi.
d. Melakukan tinjauan manajemen Sistem Manajemen Keamanan Informasi secara teratur untuk memastikan bahwa lingkup tetap memadai dan perbaikandalam proses Sistem Manajemen Keamanan Informasi dapat diidentifikasi.
e. Rencana perbaikan dan peningkatan keamanan sistem informasi.

Laporan Hasil Audit Keamanan

Hasil evaluasi dari pelaksanaan audit keamanan sistem informasi nantinyaakan berisi temuan berdasarkan uji kepatutan yang dilaksanakan serta rekomendasi yang berguna untuk memperbaiki keamanan sistem informasi puskesmas yang ada. Format dari laporan tersebut akan bermacam-macam di setiap divisi karena tidak ada format yang baku dalam penyusunannya. Laporan akhir dari audit akan mempresentasikan gambaran tingkat keamanan sistem informasi puskesmas saat ini kemudian memungkinkan pihak PT. Infokes Indonesia untuk mengambil langkah selanjutnya yang diperlukan.

Berdasarkan hasil penilaian dari audit keamanan sistem informasi puskesmasdi PT. Infokes Indonesia, *capability level* keamanan dapat dilihat dari tabel berikut.

Tabel 10. Laporan Hasil Audit Keamanan

Domain	Capability Level	Capability Existing	Kondisi Existing	Rekomendasi
APO13	3	1	1. Sistem manajemen keamanan informasi berjalan dengan baik karena penentuan ruang lingkup yang lebih rinci, terutama dalam hal karakteristik perusahaan, organisasi, lokasi, aset dan teknologi. 2. Sistem manajemen keamanan sistem informasi puskesmas di PT. Infokes Indonesia telah sesuai dengan organisasi, aset dan teknologi. 3. Sistem manajemen keamanan informasi di sistem informasi puskesmas di PT. Infokes Indonesia telah sejajar dengan keseluruhan manajemen keamanan. 4. Adanya komunikasi antara manajemen terkait peran dan tanggung jawab manajemen terhadap keamanan informasi 5. Bahwa ada ulasan terhadap efektivitas SMKI meskipun tidak dilakukan secara regular.	1. Memberikan masukan untuk pemeliharaan rencanakeamanan dengan mempertimbangkan temuan kegiatanpemantauan dan peninjauan jangka panjang. 2. Mempertimbangkan dan mendiskusikan kasus bisnis dengan keadaan keamanan informasi. 3. Pembuatan dokumen tata kelola dan dokumen manual keamanan informasi. 4. Melakukan tinjauan manajemen Sistem Manajemen Keamanan Informasi secara teratur untuk memastikan bahwa lingkup tetap memadai dan perbaikan dalam proses Sistem Manajemen Keamanan Informasi dapat diidentifikasi. 5. Rencana perbaikan dan peningkatan keamanan sistem informasi.

4 KESIMPULAN

Berdasarkan hasil audit keamanan Sistem Informasi Puskesmas di PT. Infokes Indonesia didapatkan kesimpulan sebagai berikut :

1. Melakukan audit keamanan sistem informasi menggunakan standar ISO/IEC

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

27001:2013 dan COBIT 5 melibatkan pendekatan deskriptif kualitatif untuk menilai kontrol dan proses keamanan dalam suatu organisasi. Kedua standar menyediakan kerangka kerja untuk memastikan keamanan dan tata kelola informasi yang efektif. Berikut adalah proses umum untuk melakukan audit semacam itu:

a. Persiapan
b. Pengenalan dengan Standar
c. Risk Assessment
d. Pelaksanaan Audit
e. Gap Analysis
f. Audit Reporting
g. Evaluasi

2. *Maturity level* yang dihasilkan audit dan evaluasi dari sistem manajemen keamanan informasi pada Sistem Informasi Puskesmas di PT. Infokes Indonesia yang didapatkan melalui kondisi existing domain APO13 memperoleh level 1 pada *Capability Existing* dengan *Capability Level* yang diharapkan oleh perusahaan berada pada level 3. Oleh karena itu, CapabilityGap pada kondisi tersebut yaitu 1 level.
   a. Pencapaian *Capability Existing* pada APO13 berada pada level 1.
   b. *Capability Level Achieved* pada domain yang didapat dari *rating by criteria* dimana domain APO13 dengan *rating by criteria* 87% - *Fully Achieved* (Sepenuhnya Tercapai) menempatkan keamanan sistem informasi Puskesmas di level 1 yaitu *Performed Process* - Proses yang diimplementasikan berhasil mencapai tujuannya.
3. Menghasilkan rekomendasi-rekomendasi untuk keamanan Sistem Informasi Puskesmas yang berada di PT. Infokes Indonesia seperti :
   a. Memberikan masukan untuk pemeliharaan rencana keamanan dengan mempertimbangkan temuan kegiatan pemantauan dan peninjauan jangka panjang.
   b. Mempertimbangkan dan mendiskusikan kasus bisnis dengan keadaan keamanan informasi.
   c. Pembuatan dokumen tata kelola dan dokumen manual keamanan informasi.
   d. Melakukan tinjauan manajemen Sistem Manajemen Keamanan Informasi secara teratur untuk memastikan bahwa lingkup tetap memadai dan perbaikan dalam proses Sistem Manajemen Keamanan Informasi dapat diidentifikasi.
   e. Rencana perbaikan dan peningkatan keamanan sistem informasi.

5 SARAN

Saran untuk penilaian terhadap Sistem Informasi Puskesmas di PT. Infokes Indonesia untuk kedepannya, lebih baik melakukan pembahasan keamanan sistem informasi dengan melibatkan semua domain yang ada pada COBIT 5 seperti domain EDM (*Evaluate, Direct and Monitor*) yang dapat mencapai tujuan perusahaan dengan mengevaluasi kebutuhan, kondisi dan pilihan pemangku kepentingan atau menggunakan domain BAI (*Build, Acquire and Implement*) yang dapat mencakup identifikasi persyaratan Teknologi Informasi.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada PT. Infokes Indonesia yang telah memberikan kesempatan untuk melaksanakan penelitian dengan skema Penelitian Dasar Pemula tahun pelaksanaan 2023 serta Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Informatika dan Bisnis Indonesia yang telah mendorong dan memfasilitasi dalam setiap pelaksanaan penelitian.

REFERENSI

[1] Ade Dwi Andayani, Obrina Candra Briliyant. 2021. Penilaian Kapabilitas Tata Kelola Keamanan Teknologi Informasi dan Rekomendasi Perbaikan

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Menggunakan COBIT 5. Politeknik Siber dan Sandi Negara.

[2] Boying Panjaitan, Lukman Abdurrahman, Rahmat Mulyana, 2021, Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis Iso 27001:2013 Menggunakan Kontrol Annex : Studi Kasus Data Center PT. XYZ; Telkom University.

[3] Darma Yanto Putra, Theresia Wati ,I Wayan Widi P, 2020, Audit Keamanan Sistem Informasi Berdasarkan Sni - Iso 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional "Veteran" Jakarta; Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

[4] Darmawansyah iwan, & Sismiati. (2021). *Pengembangan Dan Perancangan Perjalanan Pelanggan Dan Sistem Informasi Penjualan Pada Coffee Shop Frekuensi Kopi*..

[5] Direktorat Keamanan Informasi. 2017. Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI). Jakarta: Penerbit Kementerian Komunikasi dan Informatika.

[6] ISACA. 2012. COBIT 5 A Business Framework for the Governance and Management of Enterprise IT. USA: IT Governance Institute..

[7] ISACA. 2012. COBIT 5 Enabling Processes. USA: IT Governance Institute.

[8] ISACA. 2012. COBIT 5 Implementation. USA: IT Governance Institute.

[9] ISACA. 2012. COBIT 5 Process Assessment Model. USA: IT Governance Institute.

[10] ISACA, 2016. A Historical Timeline The COBIT® Framework. USA: IT Governance Institute.

[11] ISO, "International Standard ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements," IEC, vol. 27001, no. 27001, 2005.

[12] ISO, "International Standard ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements," IEC, vol. 27001, no. 27001, 2013.

[13] ISO, "International Standard ISO/IEC 27002 Information technology - Security techniques — Code of practice for information security controls," IEC, vol. 27002, no. 27002, 2013.

[14] ISO, "International Standard ISO/IEC 27005 Information Technology - Security techniques – Information security risk Management," vol. 27005, 2008..

[15] Kementerian Komunikasi dan Informatika Republik Indonesia. 2016. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 4 Tahun 2016: Sistem Manajemen Pengamanan Informasi.

[16] Mohamad Mirza Maulana. (2019), Audit Keamanan Sistem Informasi Pada Dinas Komunikasi Dan Informatika Kabupaten Bogor Menggunakan Standar ISO/IEC 27001:2013 dan Cobit 5; UIN JAKARTA.

[17] McLeod, Raymond & Schell, Jr. George. (2008). Sistem Informasi Manajemen, Edisi 10. Terjemahan oleh Hendra Teguh. Klaten: PT. Intan Sejati Klaten..

[18] Muhammad Nawir, Irfan AP dan Farid Wajidi. 2022. Integrasi Framework ISO 27001 Dan Cobit 2019 Pada Keamanan Informasi Smart Tourism Pt. YOY Manajemen Internasional. Universitas Sulawesi Barat.

[19] Putra Pamungkas Sukmana, Titan Parama Yoga, Chairul Habibi. (2023). Audit Manajemen Risiko Sistem Informasi pada Website Digo.id dengan Framework COBIT 5 dan ISO 31000. Jurnal Accounting Information System (AIMS). *Vol. 6 No. 2 (2023)*. Accounting Information Systems Study Program, Ma'soem University, Bandung

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

[20] Suci Fitriani Setiawan, Titan Parama Yoga, Budiman Budiman. (2023). Information System Security Audit SIMKA(Sistem Informasi Kearsipan) at Badan Pendapatan Daerah Jawa Barat Kota Bandung III Using COBIT 5 Framework and Standard IS0/IEC 27002. International Journal of Quantitative Research and Moadeling (IJQRM), V*ol 4, No 3 (2023)*. Copyright (c) 2023 International Journal of Quantitative Research and Modeling

[21] Titan Parama Yoga , R. Yadi Rakhman Alamsyah, Silca Silkillah Adwa, (2023). Audit Keamanan Sistem Informasi Menggunakan Cobit 5 di PT. Paramita Surya Makmur Plastika. Jurnal Accounting Information System (AIMS).VOL. 6 NO. 1 (2023). Accounting Information Systems Study Program, Ma'soem University, Bandung.

[22] Wibowo, Aldi S. et al. 2016. Kombinasi Framework COBIT 5, ITIL dan ISO/IEC 27002 Untuk Membangun Model Tata Kelola Teknologi Informasi Di Perguruan Tinggi. Seminar Nasional Teknologi Informasi dan Komunikasi 2016, pp. 122-128.