TESIS

AUDIT TATA KELOLA TI MENGGUNAKAN COBIT 2019 PADA UPTD RSUD TARAKAN PROVINSI KALIMANTAN UTARA

Disusun oleh:

Nama : **Sophian**
NIM : **19.77.1226**
Konsentrasi : **Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

TESIS

AUDIT TATA KELOLA TI MENGGUNAKAN COBIT 2019 PADA UPTD RSUD TARAKAN PROVINSI KALIMANTAN UTARA

IT GOVERNANCE AUDIT USING COBIT 2019 AT UPTD RSUD TARAKAN PROVINCE KALIMANTAN UTARA

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Magister

Disusun oleh:

Nama : **Sophian**
NIM : **19.77.1226**
Konsentrasi : **Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA

PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2021

HALAMAN PENGESAHAN

AUDIT TATA KELOLA TI MENGGUNAKAN COBIT 2019
PADA UPTD RSUD TARAKAN
PROVINSI KALIMANTAN UTARA

IT GOVERNANCE AUDIT USING COBIT 2019 AT
UPTD RSUD TARAKAN
PROVINCE KALIMANTAN UTARA

Dipersiapkan dan Disusun oleh

Sophian

19.77.1226

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Rabu, 9 Februari 2022

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 9 Februari 2022
Rektor

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

HALAMAN PERSETUJUAN

AUDIT TATA KELOLA TI MENGGUNAKAN COBIT 2019 PADA UPTD RSUD TARAKAN PROVINSI KALIMANTAN UTARA

IT GOVERNANCE AUDIT USING COBIT 2019 AT UPTD RSUD TARAKAN PROVINCE KALIMANTAN UTARA

Dipersiapkan dan Disusun oleh

Sophian

19.77.1226

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Rabu, 9 Februari 2022

Pembimbing Utama

Prof. Dr. Kusrini, M.Kom
NIK. 190302106

Anggota Tim Penguji

Prof. Dr. Ema Utami, S.Si., M.Kom.
NIK. 190302037

Dhani Ariatmanto, M.Kom., Ph.D.
NIK. 190302197

Pembimbing Pendamping

M. Rudyanto Arief, M.T.
NIK. 190302098

Prof. Dr. Kusrini, M.Kom
NIK. 190302106

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, tanggal ujian tesis
Direktur Program Pascasarjana

Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Sophian
NIM : 19.77.1226
Konsentrasi : Informatics Technopreneurship

Menyatakan bahwa Tesis dengan judul berikut:
Audit Tata Kelola TI Menggunakan Cobit 2019 Pada UPTD RSUD Tarakan Provinsi Kalimantan Utara

Dosen Pembimbing Utama : Prof. Dr. Kusrini, M.Kom
Dosen Pembimbing Pendamping : M. Rudyanto Arief, M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 9 Februari 2022
Yang Menyatakan,

Sophian

HALAMAN PERSEMBAHAN

Penelitian Tesis ini Saya persembahkan kepada Allah SWT sebagai bentuk syukur Saya terhadap ilmu yang Saya dapatkan, Saya jabarkan pada laporan ini agar berguna dalam kontribusi ilmu bidang TI. Semoga dapat diterima sebagai suatu amal kebaikan. Selanjutnya karya ini Saya persembahkan kepada Ibunda tersayang dan Istri untuk segala bentuk dukungan, do'a dan kebaikan yang dilakukan sehingga memberikan Saya energi positif dan Saya dapat menyelesaikan studi serta penelitian ini dengan baik. Seluruh Dosen dan Karyawan Magister Teknik Informatika Universitas AMIKOM Yogyakarta. Seluruh Civitas Akademik PJJ Angkatan 2019 Magister Teknik Informatika Universitas AMIKOM Yogyakarta.

Penelitian ini juga Saya persembahkan untuk almamater Saya, Universitas AMIKOM Yogyakarta dan juga para pembaca semoga semua yang terdapat dalam naskah laporan penelitian Tesis ini dapat memberikan wawasan tambahan dan kontribusi keilmuan yang baik
dan bermanfaat.

HALAMAN MOTO

"Barang siapa yang menghendaki kehidupan dunia maka wajib baginya memiliki ilmu, dan barang siapa yang menghendaki kehidupan Akherat, maka wajib baginya memiliki ilmu, dan barang siapa menghendaki keduanya maka wajib baginya memiliki ilmu".

- HR. Turmudzi

"Pengetahuan yang baik adalah yang memberi manfaat, bukan yang hanya diingat."

- Imam Al-Safi'i

"Bila kamu tidak tahan lelahnya belajar, maka kamu harus menanggung perihnya kebodohan"

- Imam Al-Safi'i

KATA PENGANTAR

Puji serta syukur kehadirat Allah SWT, karena dengan rahmat, dan hidayah-Nya, sehingga Penulis dapat menyelesaikan penelitian yang berjudul "AUDIT TATA KELOLA TI MENGGUNAKAN COBIT 2019 PADA UPTD RSUD TARAKAN PROVINSI KALIMANTAN UTARA" dapat diselesaikan pada waktu yang telah direncanakan. Penulis menyadari bahwa dalam penyusunan Tesis ini masih banyak terdapat kekurangan. Oleh karena itu, kritik dan saran yang bersifat membangun serta pengembangan kepada penelitian, selanjutnya sangat Penulis harapkan demi perbaikan isi Tesis ini dikemudian hari. Terima kasih sebesar-besarnya juga tidak lupa Penulis ucapkan kepada :

1. Orang Tua Saya dan Istri serta keluarga besar atas do'a dan dukungannya yang tulus.
2. Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas AMIKOM Yogyakarta.
3. Prof. Dr. Kusrini, M.Kom., selaku Direktur Program Pascasarjana dan selaku Pembimbing Utama yang telah memberikan dukungan, dengan penuh kesabaran memberikan bimbingan kepada Penulis, menyediakan waktu, tenaga, serta pikiran demi mengarahkan Penulis dalam menyelesaikan Tesis ini secara maksimal kepada Penulis.
4. Bapak M. Rudyanto Arief, M.T, selaku Pembimbing Kedua yang telah memberikan bimbingan dan arahan dalam pemecahan masalah-masalah yang Penulis hadapi selama penelitian.

5. Bapak Dosen Penguji yang telah banyak mengarahkan secara teknis dan memberikan saran yang membangun pada penelitian ini serta memberikan rekomendasi perbaikan naskah penelitian
6. Bapak/Ibu Dosen Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang telah memberikan ilmunya kepada Penulis selama menempuh studi belajar di Magister Teknik Informatika Universitas AMIKOM Yogyakarta.
7. Rekan-rekan seperjuangan PJJ MTI Angkatan 2019 yang telah memberikan pengalaman baru dan waktu untuk bertukar pikiran dalam perkuliahan maupun penyelesaian Tesis ini.
8. Kepada seluruh sahabat, teman, keluarga, kenalan, sanak keluarga dekat maupun jauh, dan semuanya yang telah membantu Penulis namun tidak dapat Penulis sebutkan satu persatu sehingga penelitian ini dapat terselesaikan.

Yogyakarta, 20 Desember 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Telah diketahui bersama bahwa penyelenggaraan operasional UPTD RSUD dalam rangka pelayanan publik memerlukan Tata Kelola TI, di mana implementasinya akan menjamin transparansi, efisiensi, dan efektivitas penyelenggaraan RSUD. Penggunaan TI oleh RSUD Tarakan Prov. Kalimantan Utara menunjukkan intensitas yang meningkat, sehingga untuk memastikan penggunaan TI untuk mendukung tujuan RSUD diperlukan Tata Kelola TI.

UPTD RSUD Tarakan telah menjalankan tata kelola TI yang intinya memanfaatkan TI bersama dengan informasi dan pengetahuan untuk integrasi data, akan memudahkan proses administrasi serta pengelolaan data lainnya di Rumah Sakit menjadi lebih mudah dan efisien guna mencapai kondisi yang dicita-citakan. Tata kelola TI pada akhirnya akan mampu meningkatkan pelayanan Rumah Sakit menjadi lebih cepat. Namun demikian di dalam pengelolaan TI masih terdapat permasalahan yang dihadapi antara lain masalah TI dan Tim TI, masalah pengelolaan data dan informasi serta pengawalan perubahan. Berkaitan dengan hal tersebut, terdapat beberapa pertanyaan menarik : Bagaimana kondisi Tata Kelola TI di UPTD RSUD Tarakan saat ini? Kondisi ideal seperti apa yang diharapkan? Langkah apa yang mesti dilakukan oleh Pihak Manajemen untuk menutup gap yang ada?

Pada Tesis ini, peneliti mencoba melakukan audit untuk mengetahui kondisi Tata Kelola TI saat ini di RSUD Tarakan dan menentukan target yang diharapkan berdasarkan desain faktor yang berpengaruh, dengan mendasar kepada model kematangan pada Framework COBIT, sehingga didapatkan kesenjangan tingkat kematangan. Selain hal tersebut, pada penelitian ini dilakukan identifikasi terhadap faktor-faktor yang mempengaruhi pencapaian tingkat kematangan yang diharapkan serta memberi rekomendasi untuk mencapai target tingkat kematangan, untuk memberikan saran kepada UPTD RSUD Tarakan dalam melakukan pengelolaan TI.

Kata Kunci : COBIT, Tata Kelola TI, Analisis dan Perencanan Proses TI, Desain Faktor

ABSTRACT

It is well known that the operational implementation of the UPTD RSUD in the context of public services requires IT Governance, where its implementation will ensure transparency, efficiency, and effectiveness of the operation of the RSUD. The use of IT by RSUD Tarakan Prov. North Kalimantan is showing increasing intensity, so to ensure the use of IT to support the goals of the RSUD, IT Governance is needed.

UPTD Tarakan Hospital has implemented IT governance which essentially utilizes IT together with information and knowledge for data integration, will facilitate the administrative process and other data management in the Hospital to be easier and more efficient in order to achieve the desired conditions. IT governance will ultimately be able to improve hospital services to be faster. However, in IT management, there are still problems faced, including IT and IT Team problems, data and information management problems and change control. In this regard, there are several interesting questions: What is the current state of IT Governance at the UPTD of Tarakan Hospital? What ideal conditions are expected? What steps should be taken by the Management to close the existing gap?

In this thesis, the researcher tries to conduct an audit to find out the current condition of IT Governance at Tarakan Hospital and determine the expected target based on the design of the influencing factors, based on the model.
maturity level in the COBIT Framework, so that the maturity level gap is obtained. In addition to this, this study identifies the factors that influence the achievement of the expected maturity level and provides recommendations to achieve the maturity level target, to provide advice to UPTD Tarakan Hospital in managing IT.

Keywords: COBIT, IT Governance, IT Process Analysis and Planning, Factor Design

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Rumah Sakit merupakan sektor publik yang kompleks. Dengan tingkat kompleksitasnya, Rumah Sakit membutuhkan sebuah sistem agar proses bisnis dapat berjalan dengan efektif dan efisien. Salah satu alternatif yang dapat digunakan yaitu dengan mengimplementasikan TI. Dengan implementasi TI dapat membantu proses penyaluran informasi, pengolahan data menjadi lebih cepat dan membantu mengurangi terjadinya human error. Hal ini menjadikan Teknologi Informasi (TI) merupakan bagian yang sangat penting bagi perusahaan dan juga merupakan suatu nilai investasi untuk perusahaan menjadi lebih baik. Untuk mendukung penerapan TI yang baik perlu dilakukan analisis dan evaluasi terkait tata kelola TI yang baik agar sesuai dengan rencana strategis perusahaan. Rumah Sakit Umum Daerah Tarakan Provinsi Kalimantan Utara merupakan fasilitas di bidang kesehatan untuk menangani masalah kesehatan pada masyarakat. Menurut Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 bahwa setiap Rumah Sakit wajib menyelenggarakan Sistem Informasi Manajemen Rumah Sakit (SIMRS). Dalam kasus ini, RSUD Tarakan perlu menyelenggarakan SIMRS dengan menerapkan TI yang baik untuk menjadikan operasional yang efisien dan efektif. Oleh karena itu, perlu dilakukan analisis dan evaluasi terkait tata kelola yang baik agar penerapan TI bisa tepat sasaran sehingga kegiatan operasional bisa dikelola dengan baik sesuai standar yang sudah ditentukan.

Solusi yang tepat untuk menganalisis tata kelola TI adalah melakukan audit menggunakan kerangka kerja COBIT 2019.

Namun, seiring berjalannya waktu serta mengingat semakin penting dan besarnya investasi yang dianggarkan dalam bidang TI membuat organisasi/perusahaan semakin merasakan perlunya sebuah audit operasional terhadap fungsi TI itu sendiri. Konsep audit COBIT yang mana bertujuan untuk memperjelas peta (mapping) area audit Teknologi Informasi, maka secara umum audit Sistem Informasi itu sendiri dimaksudkan untuk mengevaluasi tingkat kesesuaian antara Sistem Informasi dengan prosedur bisnis (client) untuk mengetahui apakah suatu Sistem Informasi telah diimplementasikan secara efektif, efisien dan ekonomis, memiliki mekanisme pengamanan asset, serta menjamin integritas data yang memadai.

Penelitian sebelumnya oleh Ade Sukmawati (2020) dalam penelitiannya yang berjudul *"Evaluasi Tata Kelola Teknologi Informasi Pada Rumah Sakit Dr. H. Ibnu Sutowo Baturaja Berdasarkan Framework Cobit 5"* mengatakan pengendalian tata kelola Teknologi Informasi saat ini sangat berpengaruh bagi organisasi di mencapai tujuan strategisnya. Teknologi telah menjadi bagian penting dalam menunjang suatu layanan, termasuk di Rumah Sakit Dr. H. Ibnu Sutowo Baturaja. Rumah Sakit tersebut memiliki SIMRS dalam menunjang pelayanannya. Sehingga tata kelola harus direncanakan dengan baik. Penelitian ini dilakukan untuk mengevaluasi pengelolaan Teknologi Informasi yang mendukung SIMRS. Hasil dari penelitian ini adalah untuk mengetahui nilai tingkat kematangan di RSUD Dr. H. Ibnu Sutowo Baturaja. Evaluasi dilakukan dengan

menggunakan kerangka kerja pengukuran COBIT 5 standar. Fokus dari penelitian ini adalah domain Ensure Resource Optimization (EDM01), Manage The IT Management Framework (APO01) (APO07), Build, Acquire and Implement (BAI04) dan Monitoring, Evaluation and Access (MEA01).

Penelitian lain yang relevan yaitu penelitian oleh Muhammad Nur (2019) tentang *"Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Pada Rumah Sakit Umum Daerah Kalideres"* menjelaskan tentang audit dilakukan pada Rumah Sakit Umum Daerah Kalideres untuk mengetahui tata kelola Teknologi Informasi agar dapat diberikan gambaran penerapan TI yang baik pada pengoperasiannya. Berdasarkan hasil audit yang dilakukan dengan kerangka kerja COBIT 5 pada domain DSS (Deliver, Service, and Support), maka kesimpulan dari penelitian ini domain process yang akan dilakukan untuk audit adalah domain process DSS (Deliver, Service, and Support) yaitu DSS01 Manage Operations, DSS03 Manage Problems, dan DSS04 Manage Continuity. Sebagian besar aktifitas pada domain yang ditentukan yaitu DSS01, DSS03, dan DSS04 sudah dilakukan dengan baik dari penerapan dan pengelolaannya. Tetapi untuk memenuhi standar dan ketentuan yang ditetapkan masih cukup kurang. Terutama pada domain process DSS03 dan DSS04.

Pada penelitian lain yang dianggap relevan terhadap penelitian ini yaitu penelitian yang di lakukan oleh Angga Wijaya Narwa Putra (2020) yang berjudul *"Perencanaan Audit Tata Kelola Teknologi Informasi Laboratorium Kalibrasi Menggunakan Cobit 2019 (Studi Kasus : Laboratorium Kalibrasi BSML Regional II)"*. Dalam penelitian tersebut dilakukan untuk mengetahui ketidaksesuaian

pengelolaan, mengoptimalkan kinerja dan untuk mencapai visi dan misi perusahaan. COBIT 2019 sebagai framework edisi terbaru dari ISACA melakukan perbaikan dalam hal goal cascading menggunakan faktor desain. Selama ini sering terjadi permasalahan TI pada BSML Regional II sehingga diperlukan audit agar diperoleh solusi permasalahan. Kesimpulan yang dihasilkan sebuah perencanaan kegiatan audit tata kelola Teknologi Informasi pada laboratorium kalibrasi, dalam hal ini BSML Regional II menggunakan framework COBIT 2019 dengan identifikasi domain yang terpilih sebagai focus area adalah : EDM 03 Ensured Risk Optimization, APO 12 Managed Risk, DSS 02 Managed Service Request and Incidents, DSS 04 Managed Continuity, DSS 05 Managed Security Services.

Penelitian oleh Shahnilna F. Bayastura (2021) dengan judul "*Analisis Dan Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Pada PT. XYZ*", penelitian ini dilakukan karena belum pernah adanya penilaian rancangan tata kelola TI di PT. XYZ guna mengukur efektivitas dan efisiensi peningkatan proses bisnis perusahaan yang menggunakan Teknologi Informasi. Kesimpulan dari penelitian ini didapat hasil identifikasi level pengelolaan yang dilakukan, dapat disimpulkan bahwa terdapat 5 proses penting tersebut adalah DSS02 (managed service request and incidents), DSS03 (managed problems), DSS05 (managed security service), BAI09 (managed assets) dan MEA03 (managed compliance with external requirements).

1.2 Rumusan Masalah

Berdasarkan Latar Belakang yang dipaparkan diatas, maka didapat beberapa

masalah sebagai berikut :

1. Berapakah tingkat kapabilitas tata kelola teknologi informasi pada RSUD Tarakan saat ini (as is) menggunakan framework COBIT 2019 ?
2. Rekomendasi apa saja yang diusulkan berdasarkan hasil audit COBIT 2019 sebagai solusi permasalahan tata kelola teknologi informasi pada RSUD Tarakan untuk meningkatkan kualitas layanan Rumah Sakit ?

1.3 Batasan Penelitian

Berdasarkan Rumusan Masalah yang ada, maka Batasan Penelitian yang ingin dicapai adalah :

1. Data penelitian ini adalah studi dokumen bisnis perusahaan yang terdiri dari minimal Renstra, struktur organisasi, SOP Teknologi Informasi, RKA (Rencana Kinerja dan Anggaran) yang dibutuhkan dalam penelitian ini.
2. Kerangka kerja yang digunakan adalah kerangka kerja COBIT 2019.
3. Hasil dari penelitian ini berupa domain proses terpilih berdasarkan analisa kondisi Teknologi Informasi yang berjalan saat ini.
4. Hasil dari penelitian ini juga akan memberikan rekomendasi perbaikan berdasarkan domain proses terpilih.
5. Hasil identifkasi responden RACI chart terdiri dari pejabat struktural dan staff Instalasi TI.

1.4 Tujuan Penelitian

Tujuan Penelitian ini adalah :

1. Melakukan audit tata kelola teknologi informasi yang ada di RSUD Tarakan menggunakan COBIT 2019.
2. Memperoleh tingkat kapabilitas tata kelola TI saat ini dan yang diharapkan di RSUD Tarakan menggunakan COBIT 2019.
3. Menghasilkan rekomendasi tata kelola TI yang sesuai berdasarkan analisis domain proses terpilih untuk perencanaan tata kelola Teknologi Informasi di RSUD Tarakan.
4. Penelitian ini ditujukan sebagai salah satu syarat kelulusan Program Studi Magister Teknik Informatika pada Universitas AMIKOM Yogyakarta.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penelitian ini antara lain :

1. Audit tata kelola Teknologi Informasi Rumah Sakit menggunakan COBIT 2019 memberikan suatu pedoman baru yaitu pada tahap pemilihan domain.
2. Memberikan masukan kepada stakeholder RSUD Tarakan untuk dapat menyelaraskan antara kebutuhan dan tujuan dari sisi TI.
3. Sebagai kajian perencanaan pada program percepatan implementasi SPBE di RSUD Tarakan.

BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Ada beberapa penelitian sebelumnya yang dapat dijadikan sebagai acuan pustaka dalam penelitian ini diantaranya :

Penelitian sebelumnya oleh Ade Sukmawati (2020) dalam penelitiannya yang berjudul *"Evaluasi Tata Kelola Teknologi Informasi Pada Rumah Sakit Dr. H. Ibnu Sutowo Baturaja Berdasarkan Framework Cobit 5"* mengatakan pengendalian tata kelola Teknologi Informasi saat ini sangat berpengaruh bagi organisasi di mencapai tujuan strategisnya. Teknologi telah menjadi bagian penting dalam menunjang suatu layanan, termasuk di Dr. H. Ibnu Sutowo Baturaja. Rumah Sakit tersebut memiliki SIMRS dalam menunjang pelayanannya. Sehingga tata kelola harus direncanakan dengan baik. Penelitian ini dilakukan untuk mengevaluasi pengelolaan Teknologi Informasi yang mendukung SIMRS. Hasil dari penelitian ini adalah untuk mengetahui nilai tingkat kematangan di RSUD Dr. H. Ibnu Sutowo Baturaja. Evaluasi dilakukan dengan menggunakan kerangka kerja pengukuran COBIT 5 standar. Fokus dari penelitian ini adalah domain Ensure Resource Optimization (EDM01), Manage The IT Management Framework (APO01) (APO07), Build, Acquire and Implement (BAI04) dan Monitoring, Evaluation and Access (MEA01).

Penelitian lain yang relevan yaitu penelitian oleh Muhammad Nur (2019) tentang *"Audit Tata Kelola Teknologi Informasi Menggunakan Framework*

COBIT 5 Pada Rumah Sakit Umum Daerah Kalideres" menjelaskan tentang audit dilakukan pada Rumah Sakit Umum Daerah Kalideres untuk mengetahui tata kelola Teknologi Informasi agar dapat diberikan gambaran penerapan TI yang baik pada pengoperasiannya. Berdasarkan hasil audit yang dilakukan dengan kerangka kerja COBIT 5 pada domain DSS (Deliver, Service, and Support), maka kesimpulan dari penelitian ini domain process yang akan dilakukan untuk audit adalah domain process DSS (Deliver, Service, and Support) yaitu DSS01 Manage Operations, DSS03 Manage Problems, dan DSS04 Manage Continuity. Sebagian besar aktifitas pada domain yang ditentukan yaitu DSS01, DSS03, dan DSS04 sudah dilakukan dengan baik dari penerapan dan pengelolaannya. Tetapi untuk memenuhi standar dan ketentuan yang ditetapkan masih cukup kurang. Terutama pada domain process DSS03 dan DSS04.

Pada penelitian lain yang dianggap relevan terhadap penelitian ini yaitu penelitian yang di lakukan oleh Angga Wijaya Narwa Putra (2020) yang berjudul *"Perencanaan Audit Tata Kelola Teknologi Informasi Laboratorium Kalibrasi Menggunakan Cobit 2019 (Studi Kasus: Laboratorium Kalibrasi BSML Regional II)"* dalam penelitian tersebut dilakukan untuk mengetahui ketidaksesuaian pengelolaan, mengoptimalkan kinerja dan untuk mencapai visi dan misi perusahaan. COBIT 2019 sebagai framework edisi terbaru dari ISACA melakukan perbaikan dalam hal Goal Cascading menggunakan faktor desain. Selama ini sering terjadi permasalahan TI pada BSML Regional II sehingga diperlukan audit agar diperoleh solusi permasalahan. Kesimpulan yang dihasilkan sebuah perencanaan kegiatan audit tata kelola Teknologi Informasi pada laboratorium kalibrasi dalam

hal ini BSML Regional II menggunakan framework COBIT 2019 dengan identifikasi domain yang terpilih sebagai focus area adalah : EDM 03 Ensured Risk Optimization, APO 12 Managed Risk, DSS 02 Managed Service Request and Incidents, DSS 04 Managed Continuity, DSS 05 Managed Security Services.

Penelitian oleh Shahnilna F Bayastura (2021) dengan judul "*Analisis Dan Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Pada PT. XYZ*" penelitian ini dilakukan karena belum pernah adanya penilaian rancangan tata kelola TI di PT. XYZ guna mengukur efektivitas dan efisiensi peningkatan proses bisnis perusahaan yang menggunakan Teknologi Informasi. Kesimpulan dari penelitian ini didapat hasil identifikasi level pengelolaan yang dilakukan, dapat disimpulkan bahwa terdapat 5 proses penting tersebut adalah DSS02 (Managed Service Request and Incidents), DSS03 (Managed Problems), DSS05 (Managed Security Service), BAI09 (Managed Assets) dan MEA03 (Managed Compliance With External Requirements).

Dari semua penelitian yang disebutkan di atas, dapat disimpulkan bahwa COBIT selain dapat digunakan untuk menilai kondisi tata kelola TI (IT Governance tools) berdasar proses-proses TI yang dipilih, COBIT juga dapat digunakan untuk membantu perusahaan atau organisasi dalam mengoptimalkan investasi TI mereka, seperti melakukan audit pada suatu Sistem Informasi. COBIT dapat juga digunakan oleh manajemen sebagai jembatan antara risiko-risiko TI dengan pengendalian yang dibutuhkan (IT Risk Management) dan juga referensi utama yang sangat membantu dalam penerapan IT Governance di perusahaan atau organisasi (ITGI, 2007).

2.2 Keaslian Penelitian

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian

Audit Tata Kelola TI Menggunakan Cobit 2019 Pada UPTD RSUD Tarakan Provinsi Kalimantan Utara

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	Evaluasi Tata Kelola Teknologi Informasi Pada Rumah Sakit Dr. H. Ibnu Sutowo Baturaja Berdasarkan Framework Cobit 5	Ade Sukmawati, Widya Cholil, Syahril Rizal, 140 GEMA TEKNOLOGI Vol. 20 No. 4, 2020	Untuk mengevaluasi pengelolaan Teknologi Informasi yang mendukung SIMRS. Evaluasi dilakukan dengan menggunakan kerangka kerja pengukuran COBIT 5 standar. Fokus dari penelitian ini adalah domain Ensure Resource Optimization (EDM), Manage The IT Management Framework (APO), Build, Acquire and Implement (BAI),	Analisis tingkat kematangan SIMRS menggunakan framework COBIT 5, meliputi domain proses EDM04 memperoleh tingkat kematangan 3,22 berada pada level 3. Domain proses APO01 memperoleh tingkat kematangan 2,64 berada pada level 2 (Managed Process). Domain proses APO07 memperoleh tingkat kematangan 3,30 berada pada level 3 (Estabilished Process). Domain proses BAI04 memperoleh tingkat	Penelitian terdahulu batasannya hanya melakukan analisis tingkat kematangan dan tidak sampai menghasilkan rekomendasi perbaikan berdasarkan hasil analisis.	Penelitian ini membahas tentang melakukan Evaluasi tata kelola TI dengan framework COBIT 5, sedangkan pada penelitian yang akan dilakukan penggunaan COBIT 2019 ditujukan untuk mengetahui hasil kegiatan audit dan rekomendasi hasil audit tata kelola TI yang berjalan dengan menggunakan framework COBIT 2019.

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

			Monitoring, Evaluation and Access (MEA).	kematangan 3,2 berada pada level 3 (Estabilished Process). Domain proses MEA01 memperoleh tingkat kematangan 3,04 berada pada level 3 (Estabilished Process). Tingkat kematangan yang diperoleh tata kelola SIMRS adalah 3,30 berada pada level 3 (Estabilished Process) Sutowo Baturaja		
2	Evaluasi Sistem Informasi Rumah Sakit Ananda Purwokerto Menggunakan Domain EDM Dan APO Cobit 5	Ranggi Praharaningtyas Aji, Ito Setiawan, Yuliawan Adi Wibowo	Melakukan evaluasi atas tata kelola SI yang ada di Rumah Sakit Umum Ananda Purwokerto, menggunakan domain EDM dan APO pada COBIT 5	Selanjutnya nilai rata-rata pencapaian pada domain EDM dan APO adalah 3.12 dan pada kondisi Established. Tidak adanya SOP/aturan/peraturan yang terdokumentasi menjadi temuan masalah disemua domain. Dilanjutkan dengan kurangnya pelatihan serta tidak adanya perencanaan atas resiko	1. Melakukan pembagian tanggung jawab berdasarkan atas diagram RACI sesuai standar COBIT. 2. Selanjutnya organisasi perlu melakukan dan evaluasi atas SDM secara berkala minimal 2 kali setahun untuk menjamin kualitas SDM. 3. Peningkatan kualitas pengamanan data, baik berupa data	Hasil penelitian evaluasi ini memberikan saran yang harus dilakukan oleh pihak RSU untuk perbaikan SI kedepannya. Sedangkan pada penelitian yang dilakukan hasil audit dengan menggunakan desain faktor COBIT 2019 dan memberikan rekomendasi perbaikan hasil audit tata kelola TI

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

				yang mungkin terjadi dan keamanan yang kurang terjaga menjadi temuan lain pada RS Ananda	elektronik maupun data tertulis.	
3	Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 pada Rumah Sakit Umum Daerah Kalideres	Muhammad Nur, Eko Darwiyanto, Indra Lukmana Sardi. Jurnal SITECH : Sistem Informasi dan Teknologi, 2019	Analisis dan evaluasi terkait tata kelola penerapan TI dengan COBIT. Audit dilakukan sesuai dengan kondisi dan rencana strategis Rumah Sakit menggunakan domain DSS.	Hasil audit dapat menyimpulkan tingkat kematangan terkait standar domain process yang dipilih dan menghasilkan rekomendasi untuk tata kelola TI RSUD Kalideres	1. Untuk penilaian tingkat kapabilitas pada RSUD Kalideres dapat dilanjutkan lagi pada domain-domain yang ada pada kerangka kerja COBIT 5. 2. Dalam melakukan penelitian selanjutnya dapat dilanjutkan lagi pada tujuan perusahaan selain resource. Rekomendasi dapat dilakukan berupa teknologi yang tidak hanya berbentuk web application tetapi bisa dalam platform atau kerangka yang lain	Penelitian ini membahas tentang evaluasi tata kelola SI yang di sesuaikan dengan rencana strategis dan kondisi Rumah Sakit, sedangkan pada penelitian yang dilakukan oleh peneliti menyampaikan hasil audit tata kelola TI dengan COBIT 2019 dan memberikan rekomedasi berdasarkan hasil audit tata kelola TI.
4	Perancangan Tata Kelola Teknologi Informasi	Gelsi Isabel Belo, Yuyun Tri Wiranti, Lovinta	Menghasilkan rancangan tata kelola/manajemen	1. Perancangan dilakukan dimulai dari tahap	Telah dilakukan perencanaan audit dengan hasil audit	Penelitian ini membahas tentang hasil perencanaan Tata Kelola Teknologi

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

	Menggunakan Cobit 2019 Pada PT. Telekomunikasi Indonesia Regional VI Kalimantan	Happy Trinawati. JUSIKOM PRIMA (Jurnal Sistem Informasi Ilmu Komputer Prima), 2020	Teknologi Informasi, dan sebagai bahan evaluasi dalam meningkatkan kinerja perusahaan dalam memberikan layanan yang baik bagi customer maupun internal perusahaan PT. Telekomunikasi Regional VI Kalimantan	1. understand the enterprise context and strategy, determine the initial scope of the governance system dengan melakukan penilaian pada design factor 1 – design factor 4, refine the scope of the governance system dengan melakukan penilaian pada design factor 5 – design factor 11 dan conclude the governance system design. 2. Menghasilkan rancangan tata kelola/manajemen TI dengan 14 proses yang penting bagi PT. Telekomunikasi Indonesia Regional VI Kalimantan.	diketahui 14 proses penting bagi perusahaan namun sebaiknya dilanjutkan dengan memberikan rekomendasi perbaikan berdasarkan hasil audit yang dilakukan.	Informasi menggunakan Cobit 2019 sedangkan pada penelitian yang dilakukan membahas tentang hasil kegiatan audit tata kelola TI dan memberikan rekomendasi perbaikan hasil audit tersebut menggunakan COBIT 2019

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

5	Informasi Menggunakan Framework COBIT 2019 Pada PT. XYZ	Widodo, JIKO (Jurnal Informatika dan Komputer), 2021	yang digunakan dalam proses bisnisnya sehingga didapati rancangan tata kelola TI dan diketahui proses – proses penting di PT. XYZ	yang dilakukan di PT. XYZ, dapat disimpulkan bahwa terdapat 5 proses penting yang didapatkan dari analisis dan perancangan tata kelola TI di PT. XYZ. 5 proses penting tersebut adalah DSS02 (managed service request and incidents), DSS03 (managed problems), DSS05 (managed security service), BAI09 (managed assets) dan MEA03 (managed compliance with external requirements)	perusahaan namun sebaiknya dilanjutkan dengan memberikan rekomendasi perbaikan hasil audit 5 proses tersebut.	menggunakan framework COBIT 2019, sedangkan pada penelitian yang dilakukan disampaikan hasil kegiatan audit tata kelola TI serta rekomendasi perbaikan yang perlu dilakukan.
6	Perencanaan Audit Tata Kelola Teknologi Informasi Laboratorium Kalibrasi Menggunakan COBIT 2019 (Studi Kasus : Laboratorium Kalibrasi BSML Regional II)	Angga Wijaya Narwa Putra, Andi Sunyoto, Asro Nasiri, Jurnal Fasilkom			Sebaiknya dilanjutkan dengan rekomendasi rekomendasi perbaikan hasil audit tata kelola TI dari perusahaan tersebut.	Kajian pada penelitian ini melakukan Perencanaan Audit Tata Kelola Teknologi Informasi Laboratorium Kalibrasi Menggunakan COBIT 2019 sedangkan yang akan dilakukan dalam penelitian ini menyajikan hasil audit tata kelola TI dan

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

			kegiatan audit tata kelola Teknologi Informasi pada laboratorium kalibrasi dalam hal ini BSML Regional II menggunakan framework COBIT 2019.	pada tahap pemilihan domain. 2. Perencanaan lengkap kegiatan audit tata Kelola Teknologi Informasi BSML Regional II beserta tahapannya.		menambahkan rekomendasi perbaikan hasil audit tersebut.

2.3 Landasan Teori

2.3.1 Profil RSUD Tarakan

Rumah Sakit Umum Daerah Tarakan adalah salah satu Rumah Sakit yang berada di daerah bagian utara dari Propinsi Kalimantan Timur, tepatnya di Kota Tarakan Jl. Pulau Irian Skip yang berbatasan wilayah NKRI dengan negara tetangga serumpun Malaysia. Rumah Sakit Umum Daerah Tarakan Kalimantan Timur pada awalnya didirikan pada tahun 1947 dengan status milik pemerintah swasta Kabupaten Bulungan dengan kelas Rumah Sakit tipe D. Pendirian ini bertujuan untuk menyediakan fasilitas pelayanan yang memadai untuk masyarakat umum di lingkungan Pulau Tarakan. Pada awal keberadaan RSUD Tarakan masih menumpang pada Dinas Kesehatan Tentara (DKT) dengan menempati sebuah Rumah Sakit di Jl. Panglima Batur, Kelurahan Pamusian, Kecamatan Tarakan Tengah bersama dengan Dinas Kesehatan Tentara. Saat ini bekas rumah sakit tersebut telah beralih fungsi menjadi Asrama Tentara Angkatan Laut (TNI-AL). Mulai pertengahan tahun 1958, RSUD Tarakan secara bertahap pindah dari tempat lama di Jl. Panglima Batur ke tempat baru Rumah Sakit di Jl. Pulau Irian, Kelurahan Skip. Keberadaan Rumah Sakit di Jl. Pulau Irian, pada awalnya adalah milik perusahaan BPM (Bataysje Petroleum Maschavei) yang pada tahun 1959 mulai pindah lokasi kerja ke Pulau Bunyu. Pada awal perpindahan ke tempat baru tersebut, RSUD Tarakan hanya melayani rawat jalan. Untuk unit rawat inap masih dipakai oleh RS BPM tersebut. Setelah secara keseluruhan perusahaan BPM pindah ke Pulau Bunyu, maka baru pada saat itulah RSUD Tarakan pindah sepenuhnya secara permanen menempati yang ada saat ini.

Pada awalnya RSUD Tarakan adalah milik Pemerintah Kabupaten Bulungan, namun karena biaya operasional yang cukup tinggi RSUD Tarakan diserahkan kepemilikannya ke Propinsi Kalimantan Timur terhitung mulai tanggal 1 Januari 1964 berdasar Surat Keputusan Kepala Dinas Kesehatan Daerah Tingkat I Kalimantan Timur No. 64195/II-1/PA tanggal 31 Maret 1964. Perkembangan Rumah Sakit mulai pesat, pada tahun 1987 RSUD Tarakan berhasil ditingkatkan dari RS tipe D menjadi RS tipe C berdasarkan Surat Keputusan Menteri Kesehatan No. 303/MEN.KES/SK/IV/1987 tanggal 30 April 1987. Pada tahun 2003 RSUD Tarakan berhasil ditingkatkan dari RS tipe C menjadi RS tipe B non pendidikan berdasarkan Surat Keputusan Menteri Kesehatan No. 196/Men.Kes.SK/II/2003 serta Surat Keputusan Gubernur Kalimantan Timur No. 445/K.85/2003. Pada tahun 2009 ini RSUD Tarakan sedang dalam masa pembangunan tempat baru untuk meningkat kapasitas pelayanan sebesar 450 tempat tidur, sehingga kapasitas total meningkat dari 220 tempat tidur menjadi 670 tempat tidur. Gedung baru ini didesain dengan konsep modern dan atraktif untuk memberikan pelayanan yang berkualitas. RSUD Tarakan dalam pelayanannya mencakup beberapa wilayah di utara Kalimantan Timur antara lain :

1. Kota Tarakan
2. Kabupaten Berau
3. Kabupaten Bulungan
4. Kabupaten Nunukan
5. Kabupaten Malinau
6. Kabupaten Tana Tidung

RSUD Tarakan dalam pembangunannya berdasarkan dari komitmen kebijakan yang kuat antara Gubernur dan Jajaran Pemerintah Provinsi Kalimantan Timur dengan DPRD Provinsi Kalimantan Timur serta Pemerintah Kota Tarakan, pemerataan keadilan penyediaan sarana pelayanan yang lengkap bagi masyarakat di Wilayah Utara Kalimantan Timur.

2.3.1.1 Visi, Misi dan Motto RSUD Tarakan

Adapun Visi RSUD Tarakan yaitu "Menjadi Rumah Sakit Terdepan yang Bertumpu pada Teknologi, Sumber Daya Manusia dan Kemandirian".

Misi RSUD Tarakan meliputi :

1. Menyelenggarakan Pelayanan Kesehatan yang paripurna.
2. Meningkatkan program pelatihan, pendidikan dan penelitian.
3. Mewujudkan pengelolaan Rumah Sakit yang profesional.

Nilai pelayanan yang dianut "TRUST dengan arti Tertib, Ramah, Universal, Sehat dan Transparan".

Motto pelayanan yang dimiliki RSUD Tarakan yaitu " Melayani dengan sepenuh hati".

2.3.1.2 Struktur Organisasi RSUD Tarakan

Keberhasilan dan kelancaran kegiatan pelayanan di Rumah Sakit tidak terlepas dari peran dan kemampuan pengorganisasian sehingga program dan kegiatan yang dilaksanakan dapat berjalan dengan baik. Berkenaan dengan hal

tersebut perlu adanya struktur dan tata kerja organisasi Rumah Sakit sebagaimana digambarkan pada Gambar 2.1 berikut :

Gambar 2.1. Struktur Organisasi RSUD Tarakan

2.3.2 Sistem Informasi Manajemen Rumah Sakit

Peraturan Menteri Kesehatan Nomor 82 Tahun 2013 mendefinisikan Sistem Informasi Manajemen Rumah Sakit (SIMRS) sebagai suatu sistem teknologi informasi komunikasi yang memproses dan mengintegrasikan segala alur proses pelayanan yang terdapat di Rumah Sakit ke dalam suatu jaringan koordinasi, pelaporan dan prosedur administrasi guna memperoleh informasi yang akurat dan

tepat guna. Permenkes tersebut menyatakan bahwa setiap Rumah Sakit diwajibkan menyelenggarakan SIMRS.

Pada pasal 4 ayat 2 Peraturan Menteri Kesehatan Nomor 82 Tahun 2013, pelaksanaan pengelolaan dan pengembangan SIMRS harus memiliki kemampuan dalam peningkatan dan dukungan terhadap proses pelayanan kesehatan di Rumah Sakit yang meliputi:

1. Kecepatan, akurasi, integrasi, peningkatan pelayanan, peningkatan efisiensi, kemudahan pelaporan dalam pelaksanaan operasional
2. Kecepatan pengambilan keputusan, kecepatan identifikasi masalah, akurasi dan kemudahan dalam penyusunan strategi
3. Budaya kerja, transparansi, koordinasi antar unit, pemahaman sistem dan pengurangan biaya administrasi dalam pelaksanaan organisasi.

Pada pasal 5 Peraturan Menteri Kesehatan Nomor 82 Tahun 2013 mengatur tentang pengintegrasian SIMRS. SIMRS harus mampu diintegrasikan dengan program pemerintah dan Pemerintah Daerah dalam bentuk kemampuan komunikasi data yang disebut interoperabilitas. SIMRS harus memiliki kemampuan komunikasi data dengan :

1. Sistem Informasi Manajemen dan Akutansi Barang Milik Negara (SIMAK BMN).
2. Pelaporan Sistem Informasi Rumah Sakit (SIRS).

3. Indonesia Case Base Group's (INA CBG's).

4. Aplikasi lain yang dikembangkan oleh pemerintah.

5. Sistem Informasi Manajemen fasilitas pelayanan kesehatan lainnya.

2.3.3 Konsep Tata Kelola TI

2.3.3.1 Definisi Tata Kelola TI

Beberapa tahun belakangan ini, banyak definisi dari tata kelola TI dikemukakan oleh beberapa ahli. Beberapa diantaranya adalah Van Grembergen yang menyatakan bahwa tata kelola TI merupakan kapasitas organisasi yang dilakukan oleh dewan, manajemen eksekutif dan manajemen TI untuk mengontrol perumusan dan implementasi strategi TI dan berfungsi untuk memastikan perpaduan antara bisnis dan TI yang ada. Sedangkan IT Governance Institut (ITGI) menyatakan bahwa tata kelola TI merupakan tanggung jawab dari dewan direksi dan manajemen eksekutif. Tata kelola TI merupakan bagian integral dari pemerintahan pada perusahaan dan terdiri dari kepemimpinan, struktur organisasi serta proses yang memastikan bahwa organisasi TI mendukung dan memperluas strategi dan tujuan dari organisasi.

Meskipun terdapat perbedaan pandangan di beberapa aspek, keduanya memiliki fokus yang sama yaitu fokus terhadap isu-isu seperti pencapaian hubungan antara bisnis dan TI, dan juga tanggung jawab dari dewan direksi. Van Grambergen, melalui pernyataan definisinya menunjukkan bahwa manajemen TI juga adalah pemain penting dalam pengelolaan TI pada perusahaan. Namun terdapat perbedaan yang jelas antara tata kelola TI dan manajemen TI. Manajemen

TI berfokus pada penyediaan efektifitas layanan dan produk TI dan juga manajemen operasi TI. Sedangkan tata kelola TI memliki jangkauan yang lebih luas dan berkonsentrasi pada tindakan dan perubahan TI untuk memenuhi kebutuhan bisnis perusahaan saat ini dan masa depan. Definisi lainnya, seperti yang diutarakan oleh ITGI, juga menyatakan bahwa tata kelola TI merupakan bagian integral dari perusahaan atau corporate governance. ITGI's Board Briefing on IT Governance berpendapat bahwa tata kelola TI bertanggung jawab terhadap bagian dari kerangka kerja yang luas dari tata kelola perusahaan. ITGI's Board Briefing on IT Governance juga menyatakan bahwa tata kelola TI harus ditangani oleh dewan sama seperti agenda strategis lainnya (De Haes & Van Grembergen, 2005).

Terdapat empat objective yang menentukan arah atau bentuk dari tata kelola TI. Keempat objective tersebut terdiri dari Accountability (Bisa Dipertanggung Jawabkan), IT Value and Alignment (Nilai-Nilai TI), Risk Management (Manajemen Resiko), dan Performance Measurement (Pengukuran Kinerja). Tata kelola TI memiliki tujuan untuk mengelola informasi agar dapat dipertangungjawabkan, dan memberikan nilai tambah terhadap proses bisnis yang ada pada organisasi melalui informasi yang dihasilkan. Selain itu tata kelola TI bertujuan untuk meminimalkan resiko yang berhubungan dengan TI dan dapat digunakan untuk mengukur kinerja dari pengimplementasian TI tersebut (Yulhendri & Surendro, 2008).

Implementasi tata kelola TI yang tidak efektif dan efisien dapat menimbulkan efek yang buruk terhadap perusahaan seperti kerugian bisnis, berkurangnya reputasi, melemahnya posisi di dalam kompetisi, dan masih banyak lagi. Namun

sebaliknya jika tata kelola TI dapat diimplementasikan dengan efektif dan efisien di dalam sebuah perusahaan maka akan memberikan berbagai keuntungan-keuntungan antara lain (Ernala, 2009) :

1. The Wheel Exists, penggunaan standar yang sudah ada dan mature akan sangat efisien. Perusahaan tidak perlu mengembangkan sendiri framework dengan mengandalkan pengalamannya sendiri yang tentunya sangat terbatas.
2. Structured, standar-standar yang baik menyediakan suatu framework yang sangat terstruktur, yang dapat dengan mudah dipahami dan diikuti oleh manajemen.
3. Best Practices, standar-standar tersebut telah dikembangkan dalam jangka waktu yang relatif lama dan melibatkan ratusan orang dan organisasi di seluruh dunia. Pengalaman yang direfleksikan dalam model-model pengelolaan yang ada tidak dapat dibandingkan dengan suatu usaha dari satu perusahaan tertentu.
4. Knowledge Sharing, dengan mengikuti standar yang umum, manajemen akan dapat berbagi ide dan pengalaman antar organisasi melalui user groups, website, majalah, buku, dan media informasi lainnya.
5. Auditable, tanpa standar baku, akan sangat sulit bagi auditor, terutama auditor dari pihak ketiga untuk melakukan kontrol secara efektif. Dengan adanya standar, maka baik manajemen maupun auditor mempunyai dasar yang sama dalam melakukan pengelolaan TI dan pengukurannya.

2.3.3.2 Area Fokus Tata Kelola TI

Pada tata kelola Teknologi Informasi (TI), terdapat 5 area yang menjadi fokus seperti pada Gambar 2.2, yaitu Keselarasan Strategis (Strategic Alignment), Penyampaian Nilai (Value Delivery), Manajemen Resiko (Risk Management), Manajemen Sumber Daya (Resource Management), dan Pengukuran Kinerja (Performance Measurement).

Gambar 2.2. Fokus Area Tata Kelola TI

Berikut adalah penjelasan masing-masing area fokus dari tata kelola TI (Muthmainnah, 2015) :

1. Keselarasan Strategi (Strategic Alignment) berfokus pada menjalankan hubungan bisnis dan perencanaan TI seperti mendefinisikan, memelihara dan mengoptimalkan pemakaian biaya, dan menyelaraskan prosedur TI dengan perosedur perusahaan.

2. Penyampaian Nilai (Value Delivery) adalah tentang mengoptimalkan seluruh pemakaian biaya, memastikan bahwa TI memberikan manfaat yang sesuai

terhadap strategi, berkonsentrasi pada mengoptimalkan biaya dan membuktikan nilai yang sebenarnya dari TI.

3. Manajemen Resiko (Risk Management) untuk menjalankan pengelolaan terhadap resiko, diperlukan kesadaran staf organisasi dapat mengerti adanya resiko, keperluan organisasi, resiko-resiko signifikan yang mungkin terjadi, dan juga bertanggung jawab dalam mengelola resiko yang ada di organisasi.

4. Manajemen Sumber Daya (Resource Management) tentang mengoptimalkan investasi, dan pengelolaan sumber daya TI yang baik yang terdiri dari aplikasi, informasi, infrastruktur, dan sumberdaya. Ini merupakan kunci utama terkait dengan optimalisasi pengetahuan dan infrastruktur.

5. Pengukuran Kinerja (Performance Measurement) mengikuti dan mengawasi jalannya pelaksanaan rencana, pelaksanaan proyek, pemanfaatan sumber daya, sampai dengan pencapaian hasil TI.

Pelaksanaan kerangka kerja tata kelola TI apapun harus menyeimbangkan faktor internal maupun faktor eksternal yang relevan seperti (Setiawan & Mustofa, 2013) :

1. Fakta perkembangan teknologi : Perkembangan TI yang cepat mensyaratkan bahwa keputusan terkait dengan TI dilakukan secara tepat waktu, dengan pemahaman penuh resiko terkait dengan tantangan TI

2. Pengawasan fiskal : Bahwa proyek TI memerlukan belanja mahal yang kadang-kadang menyebabkan keraguan dan akuntabilitas penurunan sumber daya keuangan

3. Inovasi dan kontrol asas TI : Dalam kasus dimana inovasi (baru proyek TI) didukung oleh TI, mungkin bertentangan dengan kontrol atas lingkungan TI

4. Up to date infrastruktur : Infrastruktur teknologi menjadi ketinggalan zaman dari waktu ke waktu. Menjaga agar tetap up to date adalah suatu keharusan bagi setiap departemen

2.3.3.3 Definisi Audit TI

Sebelum mengetahui lebih jauh mengenai definisi dari audit TI, perlu dipahami mengenai pengertian dari audit dan Teknologi Informasi (TI) itu sendiri. Audit pada dasarnya merupakan sebuah proses yang sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti dari tindakan yang dilakukan. Bukti ini kemudian digunakan guna memberikan pernyataan dan menilai seberapa jauh tindakan yang dilakukan sudah sesuai dengan kriteria yang berlaku dan mengkomunikasikannya dengan pihak terkait (Wardani & Puspitasari, 2014).

Sedangkan pengertian Teknologi Informasi itu sendiri adalah merupakan segala hal yang terkait dengan Teknologi Komputer (Computing Technology) dan Teknologi Komunikasi (Communication Technology) yang digunakan untuk memproses dan menyebarkan informasi. Dengan kata lain, TI merupakan sebuah cara atau alat terintegrasi yang dapat digunakan untuk menjaring data, mengolah,

dan menyajikannya secara elektronik menjadi informasi dalam berbagai format yang bermaanfaat bagi penggunanya (Sarno, 2009).

Gambar 2.3. Siklus Hidup Audit TI

Jadi dengan demikian dapat diartikan bahwa audit TI merupakan aktivitas pengumpulan dan pengevaluasian bukti untuk menentukan apakah proses TI yang berlangsung di dalam perusahaan telah dikelola dengan standar yang ada. Bukti-bukti tersebut digunakan untuk menentukan apakah sistem informasi yang terkandung di dalam TI dapat melindungi aset, dan memelihara integritas data sehingga dapat diarahkan kepada pencapaian tujuan bisnis dengan memanfaatkan sumber daya secara efisien. Adapun tujuan dari dilakukannya audit TI terbagi menjadi empat tahap yaitu (Weber, 1999) :

1. Meningkatkan keamanan aset-aset perusahaan aset informasi suatu perusahaan seperti perangkat keras (hardware) dan perangkat lunak

(software), sumber daya manusia, file data harus dijaga oleh suatu sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset.

2. Meningkatkan Integritas Data (Data Integrity) adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti : kelengkapan, kebenaran dan keakuratan.

3. Meningkatkan efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan pengguna.

4. Meningkatkan efisiensi sistem menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai.

5. Ekonomis mencerminkan kalkulasi untuk rugi ekonomi (cost/benefit) yang lebih bersifat kuantifikasi nilai moneter (uang).

2.3.3.4 Peranan Audit dalam Tata Kelola TI

Perkembangan TI yang sangat pesat membuat perusahaan menjadikan TI sebagai salah satu instrumen penting dalam menjalankan kegiatan bisnis yang ada. Peran TI yang semakin vital dapat mempengaruhi seberapa jauh perusahaan telah mampu mencapai visi yang ada dan menjalankan misi dan tujuan strategisnya. Demi tercapainya kualitas yang baik dari implementasi TI, perusahaan perlu melakukan evaluasi terhadap pengelolaan TI agar tetap relevan. Besarnya resiko yang dapat muncul yang diakibatkan dari pengimplementasian TI di perusahaan

menjadikan audit semakin penting untuk dilakukan. Terdapat beberapa alasan penting mengapa audit TI perlu dilakukan antara lain (Sarno, 2009) :

1. Kerugian akibat kehilangan data merupakan aset penting yang dimiliki oleh sebuah perusahaan. TI memiliki peran untuk melakukan pengamanan terhadap data yang ada. Hal tersebut mengingat kehilangan data mungkin dapat berakibat terhentinya proses bisnis yang penting di dalam perusahaan atau aktivitas tetap dapat berjalan namun membutuhkan waktu yang lama karena dilakukan secara manual.

2. Kesalahan dalam pengambilan keputusan saat ini sudah banyak perusahaan melakukan pengambilan keputusan penting dengan menggunakan bantuan dari DSS (Decision Support System). Kesalahan sedikit saja dalam pengambilan keputusan dapat memiliki dampak yang buruk baik bagi perusahaan ataupun orang lain. Sebagai contoh, di dalam bidang kedokteran perangkat lunak berbasis DSS digunakan oleh dokter untuk melakukan pengambilan keputusan terkait tindakan operasi yang akan dilakukan terhadap pasien. Dapat dibayangkan terhadap perkembangan bisnis yang ada. Resiko yang ditimbulkan jika saja dokter salah melakukan penginputan data pasien ke dalam sistem TI yang tentu dapat membahayakan nyawa dari pasien tersebut.

3. Resiko kebocoran data merupakan salah satu sumber daya penting yang dimiliki oleh sebuah perusahaan. Salah satu contoh data penting tersebut adalah data pelanggan yang bisa digunakan untuk meningkatkan daya saing

perusahaan. Resiko yang ditimbulkan jika data tersebut bocor sangatlah buruk bagi perusahaan, seperti kehilangan pelanggan yang tentu dapat mengganggu aktivitas bisnis yang ada. Melalui proses audit TI, kebocoran data tersebut kemungkinan dapat diketahui sehingga perusahaan dapat melakukan antisipasi terkait dengan masalah tersebut.

4. Penyalahgunaan komputer pada perkembangan teknologi komputer saat ini yang kian pesat diikuti dengan meningkatnya kejahatan komputer yang terjadi. Kejahatan tersebut tidak hanya berasal dari pihak eksternal, namun juga berasal dari pihak internal perusahaan itu sendiri. Keberadaan audit TI khususnya dalam bidang manajemen keamanan informasi menjadi penting untuk mengetahui penyalahgunaan TI yang terjadi di dalam perusahaan.

5. Kerugian akibat kesalahan proses penghitungan salah satu alasan yang mendasari implementasi TI di dalam perusahaan adalah kemampuan mengolah data secara tepat dan akurat. Namun hal tersebut juga memiliki resiko. Resiko yang ditimbulkan akan semakin besar jika pengimplementasian TI tidak didukung dengan mekanisme pengembangan yang memadai serta evaluasi impelementasinya melalui kegiatan audit TI.

6. Tingginya nilai investasi perangkat keras dan perangkat lunak besarnya nilai investasi yang harus dikeluarkan dalam pengimplementasian TI terkadang tidak diikuti dengan pemanfaatan dan pengelolaan yang baik. Manfaat yang dimiliki oleh TI seringkali sulit untuk diukur karena melibatkan banyak faktor dan kepentingan. Keberadaan audit TI dapat membantu manajemen

perusahaan untuk memastikan TI sesuai dengan standar pengelolaan yang baik dan kebijakan perusahaan untuk mendukung pencapaian tujuan bisnis.

2.3.3.5 COBIT

COBIT dikembangkan.oleh IT Governance.Institute (ITGI), yang merupakan bagian dari Information. System Audit and Control Association. (ISACA). COBIT memberikan guidelines yang berorientasi pada bisnis, karena itu bussines process owners dan manajer, termasuk auditor dan pengguna, diharapkan dapat memanfaatkan guideline ini sebaik-baiknya. COBIT merupakan best practices yang membantu dalam mengoptimalkan investasi TI serta menyediakan suatu ukuran untuk menilai ketika terjadi berbagai hal yang tidak sesuai (ISACA, 2019).

Framework COBIT (Control Objective for Information and Related Technology) adalah suatu metodologi yang memberikan kerangka dasar dalam menciptakan sebuah teknologi informasi yang sesuai dengan kebutuhan organisasi. Sekumpulan dokumentasi best practices untuk IT Governance yang dapat membantu auditor, manajemen, dan pengguna untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol dan permasalahan teknis. COBIT adalah suatu framework untuk membangun suatu IT Governance. Dengan mengacu pada framework COBIT, suatu organisasi diharapkan mampu menerapkan IT Governance dalam pencapaian tujuannya IT Governance mengintegrasikan cara optimal dari proses perencanaan dan pengorganisasian, pengimplementasian, dukungan serta proses pemantauam kinerja teknologi informasi.

Selain itu COBIT adalah kerangka kontrol yang paling tepat untuk membantu

organisasi memastikan keselarasan antara penggunaan Teknologi Informasi dan tujuan bisnis. Dapat di simpulkan bahwa dari keseluruah teknologi informasi Framework yang paling sering digunakan dan mencakup keseluruhan tata kelola teknologi informasi adalah COBIT, karena COBIT Framework bergerak sebagai integrator dari praktik IT governance dan juga yang dipertimbangkan kepada petinggi manajemen atau manager, manajemen teknologi informasi dan bisnis para ahli governance, asuransi dan keamanan dan juga para ahli auditor teknologi informasi dan kontrol. COBIT Framework dibentuk agar dapat berjalan berdampingan dengan standar dan best practices yang lainnya (Setiawan, 2010).

Kerangka kerja ini dapat membantu optimalisasi investasi yang berkaitan dengan teknologi informasi, menjamin penyampaian layanan dan memberikan alat ukur atau standar yang efektif untuk kepentingan manajemen dalam mengambil keputusan dalam organisasi. Target pengguna dari framework COBIT adalah organisasi atau perusahaan dari berbagai latar belakang dan para professional external assurance. Secara manajerial target pengguna COBIT adalah manajer, pengguna dan profesional TI serta pengawas dan pengendali profesional. Fokus proses COBIT digambarkan oleh model proses yang membagi teknologi informasi menjadi empat domain dan puluhan proses sesuai dengan bidang yang bertanggung jawab terhadap perencanaan, membangun, menjalankan dan memonitor implementasi teknologi informasi, dan juga memberikan pandangan end-to-end teknologi informasi.

2.3.3.6 Information Technology and Infrastructure Librarry (ITIL)

Information Technology Infrastructure Library (ITIL) merupakan kerangka kerja yang berfokus kepada pengelolaan layanan TI, pengembangan dan operasi TI . ITIL memberikan deskripsi secara rinci dan memberikan panduan sehingga organisasi dapat menyesuaikan dengan kebutuhannya sendiri. ITIL diterbitkan dalam bentuk seri buku masing-masing mencakup topik manajemen TI (Jogiyanto, 2011). ITIL versi kedua dikeluarkan tahun 2000 yang memiliki bagian utama adalah layanan TI dan dua komponennya yaitu service delivery dan service support (Cartlidge, 2007). Pada pertengahan 2007, dikeluarkan ITIL versi 3 yang merupakan pengembangan proses dari ITIL versi 2 dalam sebuah siklus model. Dalam siklus model ini, layanan TI dirancang, dibuat dan memasuki tahap transisi menuju live environment, dukungan atas operasi dan peningkatan yang berkelanjutan. Banyak.organisasi melihat ITIL versi 3 merupakan evolusi dari ITIL versi 2 bukan menggantikan versi sebelumnya melainkan ITIL versi 3 sebagai keselarasan.dari proses manajemen layanan TI dalam mendukung proses bisnis. ITIL V3 memiliki lima komponen, masing-masing bagian dari siklus tersebut adalah service strategy, service design, service transition, service operation dan continual service improvement.

2.3.3.7 ISO 20000

Standar ISO 20000 adalah standar yang dipergunakan untuk sertifikasi manajemen teknologi informasi (TI). Standar ini dikembangkan untuk menggantikan sertifikasi British Standard (BS) 15000 yang ditetapkan oleh British

Standards International (BSI). Dikembangkan sebagai proyek bersama oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC), standar ini juga dikenal sebagai IEC 20000. Tujuannya adalah untuk memungkinkan semua organisasi yang berpondasi pada teknologi informasi agar mampu menerapkan praktik terbaik.

Standar ini secara spesifik menentukan persyaratan bagi institusi (merujuk kepada BUMN, Swasta dan Government) penyedia layanan TI untuk merencanakan, menetapkan, menerapkan, mengoperasikan, memantau, mereview, memelihara dan meningkatkan sistem manajemen layanan TI. Secara formal ISO 20000 terdiri dari :

1. ISO 20000-1:2011, berisi persyaratan sistem manajemen layanan TI yang harus dipenuhi oleh institusi agar layanan yang diberikan memiliki kualitas yang dapat diterima oleh pelanggan. Diantaranya terdiri desain, transisi, pengiriman dan peningkatan pelayanan yang memenuhi persyaratan layanan dan memberikan nilai bagi pelanggan dan penyedia layanan. Persyaratan tersebut wajib dipenuhi oleh institusi agar sesuai dengan standar. Bagian ini merupakan dasar bagi fihak ketiga untuk melakukan audit secara independen.
2. ISO 20000-2:2012, berisi petunjuk dalam penerapan sistem manajemen layanan TI. Bagian ini berisi saran untuk organisasi yang ingin melakukan sertifikasi. Bagian ini tidak terlalu wajib untuk diikuti.
3. ISO 20000-3:2009, berisi panduan tentang definisi ruang lingkup dan penerapan dari ISO 20000-1

4. ISO 20000-4:2010, berisi proses model referensi
5. ISO 20000-5:2010, berisi contoh implementasi rencana ISO 20000-1

2.3.3.8 ISO 27000

Sejak tahun 2005, International Organization for Standardization (ISO) atau Organisasi Internasional untuk Standarisasi telah mengembangkan sejumlah standar tentang *Information Security Management Systems* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan. Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

1. ISO/IEC 27000:2009 – ISMS Overview and Vocabulary
2. ISO/IEC 27001:2005 – ISMS Requirements
3. ISO/IEC 27002:2005– Code of Practice for ISMS
4. ISO/IEC 27003:2010 – ISMS Implementation Guidance
5. ISO/IEC 27004:2009 – ISMS Measurements
6. ISO/IEC 27005:2008 – Information Security Risk Management
7. ISO/IEC 27006: 2007 – ISMS Certification Body Requirements
8. ISO/IEC 27007 – Guidelines for ISMS Auditing

Dari standar seri ISO 27000 ini, hingga September 2011, baru ISO/IEC 27001:2005 yang telah diadopsi Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001:2009.

SNI ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

2.3.3.9 ISO 38500

ISO / IEC 38500 memberikan prinsip, definisi, dan model untuk membantu badan pemerintahan memahami pentingnya Teknologi Informasi (TI). Standar ini dimaksudkan untuk membantu semua jenis organisasi dalam mengevaluasi, mengarahkan, dan memantau penggunaan Teknologi Informasi (TI).), terlepas dari tingkat penggunaan TI. Ini terdiri dari praktik manajemen dan keputusan yang terkait dengan penggunaan TI saat ini dan di masa depan. Tujuan standar ini adalah untuk mempromosikan penggunaan TI yang efektif, efisien dan dapat diterima di semua organisasi dengan memberi informasi dan membimbing badan pengatur dalam mengatur penggunaan TI dan menetapkan kosa kata tata kelola TI.

Standar proses manajemen dan tata kelola layanan informasi dan komunikasi bagi sebuah organisasi ditujukan kepada :

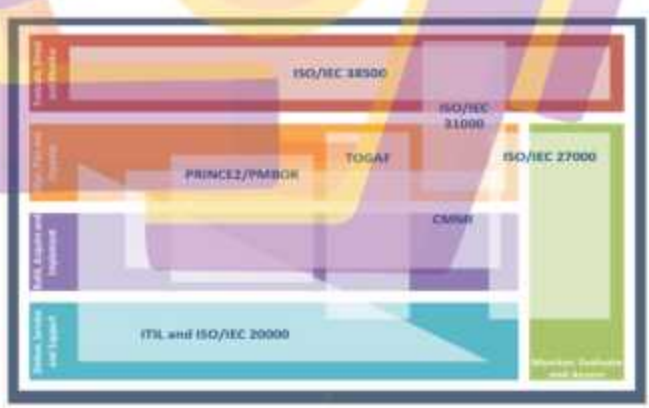
1. Manajer senior.
2. Anggota dari kelompok pengawasan sumber daya perusahaan.
3. Spesialis teknis atau eksternal bisnis.

4. Vendor perangkat keras, perangkat lunak dan komunikasi.
5. Penyedia layanan eksternal dan internal (misalnya konsultan).
6. Auditor Teknologi Informasi.

Tujuan dari penerapan ISO/IEC 38500 yaitu untuk menyediakan dukungan terhadap penggunaan TI secara efektif, efisien dan tepat pada organisasi dengan cara :

1. Memberi jaminan kepercayaan pada tata kelola TI organisasi kepada stakeholders (termasuk konsumen, shareholders dan karyawan perusahaan), ketika standar telah dipatuhi.
2. Menerangkan dan membimbing pimpinan dalam menata dan mengelola penggunaan TI pada organisasi.
3. Menyediakan dasar untuk mengevaluasi tujuan dari tata kelola TI perusahaan.

2.3.3.10 Perbandingan Framework COBIT, ITIL dan ISO



Gambar 2.4 IT Government Framework

Gambar 2.4 diatas adalam pemetaan (mapping) beberapa framework tata kelolal dan audit TI. Framework-framework tersebut merupakan framework yang paling banyak digunakan di Indonesia dalam penelitian tentang tata kelola TI. Telah diketahui bahwa tata kelola dan audit TI tidak jauh berbeda, termasuk juga framework yang digunakan. Maka pengunaan framework dalam penelitian tata kelola dan audit TI yang sering digunakan juga sama. Tidak sedikit penelitian tentang audit TI yang menggunakan COBIT sebagai framework. Meski framework lain juga digunakan, tetapi pasti tidak lebih banyak dari COBIT. Dari gambar di atas terlihat COBIT bisa dikatakan jadi rujukan atau rekomendasi dalam tata kelola dan audit TI hal ini terlihat dalam COBIT terdapat ruang lingkup dengan 5 domain. Dari gambar diatas terlihat garis-garis yang berbentuk kotak-kotak dan segitiga didalam dan beririsan setiap domain adalah beberapa framework yang beririsan antara setiap domain, contohnya penanganan masalah security ketika mengunakan framework ISO 27000 maka di dalam COBIT penanganan security juga telah tersedia dan diatur pada domain Align, Plan and Organize, domain Build, Acquire and Implement, Domain Deliver, Service and Support dan domain Monitor, Evaluate and Assess. Dilihat dari gambar diatas terlihat framework COBIT mencakup framework lainnya dengan cakupan area yang lebih luas dibandingkan dengan framework lainnya. Selain itu COBIT juga cocok digunakan untuk mengaudit atau mengevaluasi tata kelola TI suatu perusahaan atau instansi dikarenakan sifatnya yang fleksibel.

2.3.3.11 Hubungan Antara Audit TI dan COBIT

Audit tata kelola Teknologi Informasi (TI) merupakan sebuah proses yang memiliki dan melibatkan lingkup evaluasi yang luas dalam keseluruhan pengelolaan TI di dalam perusahaan. Dalam melakukan sebuah proses audit, auditor selaku pelaku proses membutuhkan sebuah tool atau alat bantu yang dapat digunakan sebagai alat ukur sebuah proses. Terdapat berbagai jenis tool atau alat bantu yang dapat digunakan, salah satunya adalah dengan menggunakan kerangka kerja atau best practice COBIT. COBIT merupakan sebuah panduan standar praktik dari manajemen Teknologi Informasi.

COBIT memiliki peran yang penting dalam mengawali proses audit terutama pada daerah-daerah yang relevan dan memiliki resiko yang tinggi. Analisa objektivitas audit tersebut dapat dimulai dengan melakukan identifikasi terhadap process goal TI yang terkandung dalam beberapa domain yang ada. Auditor juga dapat menggunakan COBIT sebagai materi tambahan untuk menentukan prosedur dari proses audit yang akan dilakukan. Dalam melakukan pemeriksaan, COBIT berfungsi untuk mengetahui apakah setiap process goal TI yang dipilih telah disusun/ditetapkan/dijalankan. Selain itu COBIT juga dapat digunakan oleh auditor untuk mengetahui apakah kriteria yang diinginkan dari sebuah proses telah ditentukan dan mengetahui apakah proses yang ada telah mencakup aspek-aspek yang terkait (Suhardi, 2011).

Gambar 2.5. Peran COBIT dalam Audit TI

Berdasarkan perannya seperti yang diperlihatkan pada Gambar 2.5, COBIT pada dasarnya merupakan sebuah panduan ataupun best practice dari proses audit TI yang cukup mudah digunakan dan dapat disesuaikan dengan keadaan pengelolaan Teknologi Informasi masing-masing perusahaan. COBIT bukan hanya berfungsi sebagai petunjuk audit tetapi juga memiliki fungsi sebagai pengendali informasi dan petunjuk model kematangan/kapabilitas yang akan menentukan arah pengendalian bagi proses Teknologi Informasi perusahaan. Berdasarkan penjelasan tersebut dapat disimpulkan bahwa hubungan antara proses audit TI dengan COBIT sangatlah erat. COBIT dapat membantu proses audit TI dimulai dari menjadi acuan awal dalam menentukan lingkup pelaksanaan kegiatan hingga menjadi pelengkap bagi proses audit TI itu sendiri. Dengan kombinasi tersebut diharapkan nantinya dapat menghasilkan sebuah hasil evaluasi dan rekomendasi yang baik dan mutakhir untuk meningkatkan kualitas TI perusahaan.

2.3.4 COBIT 2019 Framework

COBIT 2019 merupakan produk terbaru dari COBIT yang diciptakan dan dikembangkan lebih dari 25 tahun oleh ISACA. COBIT merupakan best practices yang dikembangkan oleh IT Governance Institute (ITGI) yang dapat diterima dan dijalankan secara internasional atas informasi TI, dan risiko terkait organisasi serta dapat digunakan dalam membantu penentuan TI yang digunakan dan memaksimalkan terhadap TI (ISACA, 2018).

COBIT 2019 yang merupakan evolusi dari versi sebelumnya yaitu COBIT 5. Dengan menggunakan framework COBIT 2019, dapat memberikan rekomendasi terhadap perusahaan dalam mengatur tata kelola TI serta memberikan fleksibilitas bisnis untuk menciptakan solusi tata kelola praktis yang dibuat khusus untuk tujuan dan sasaran organisasi mereka. COBIT 2019 mengalami peningkatkan versi dari COBIT 5 (Aldy Maulana Syuhada, 2021). Berikut perbedaan antara kedua framework COBIT :

Tabel 2.2. Perbandingan COBIT 5 dan COBIT 2019

No	Point Perbandingan	COBIT 5	COBIT 2019
1	Gambaran COBIT	Tidak memiliki *design factor*	Konsep *design factor* yang memungkinkan tata kelola dibangun lebih baik
			Konsep *Focus area* membuat lebih fleksibel
2	Prinsip	Memiliki 5 prinsip	Memiliki 9 prinsip
3	Detail Domain Proses	Disebut proses tata kelola TI	Disebut objective tata kelola TI
4	Goal Cascade	Pada tiap domain menjadi kata kerja, contoh : manage	Pada tiap domain menjadi kata yang lebih objectif, contoh : Managed
5	Perhitungan Tingkat Kematangan	Terdapat 37 domain	Terdapat 40 domain (3 domain tambahan)
6	Tata Kelola	Enabler	Komponen Sistem Tata Kelola

COBIT 2019 memiliki 5 (lima) model kapabilitas proses untuk mengukur tingkat kapabilitas proses tata kelola Teknologi Informasi yang dikelompokkan ke dalam 5 domain yang terdiri atas 1 domain tata kelola dan 4 domain manajemen dan terdiri atas kumpulan dari 40 proses tata kelolal dan manajemen TI.

1. Domain Evaluate, Direct and Monitor (EDM), merupakan domain yang menitikberatkan dalam mengevaluasi opsi-opsi strategis, mangarahkan dan memonitor kegiatan manajemen TI secara keseluruhan yang di lakukan oleh perusahaan atau organisasi.

2. Domain Align, Plan and Organize (APO), merupakan domain yang menitiberatkan kepada proses perencanaan penerapan TI dan keselarasannya dengan tujuan yang ingin dicapai oleh perusahaan secara umum. Domain ini meliputi taktik dan strategi, serta menyangkut masalah pengidentifikasian cara terbaik TI untuk memberikan kontribusi yang maksimal terhadap pencapaian tujuan bisnis perusahaan.

3. Domain Build, Acquire and Implement (BAI), merupakan domain yang menitikberatkan kepada proses pemilihan teknologi yang akan digunakan dan proses penerapannya. Untuk merealisasikan strategi TI yang telah ditetapkan harus disertai solusi-solusi yang sesuai, solusi TI kemudian diadakan dan diimplementasikan dan diintegrasikan ke dalam proses bisnis perusahaan.

4. Domain Deliver, Service and Support (DSS), merupakan domain yang menitikberatkan permasalahan pemenuhan layanan TI, keamanan sistem,

kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan.

5. Domain Monitor, Evaluate and Assess (MEA), domain yang menitikberatkan pada seluruh kendali-kendali yang diterapkan pada setiap proses TI harus diawasi dan dinilai kelayakannya secara berkala. Domain ini berfokus pada masalah kendali-kendali yang diterapkan dalam perusahaan, pemeriksaaan internal dan eksternal.

Gambar 2.6 di bawah ini menjelaskan beberapa proses yang terbagi dalam domain COBIT 2019.

Gambar 2.6. Proses TI Cobit 2019

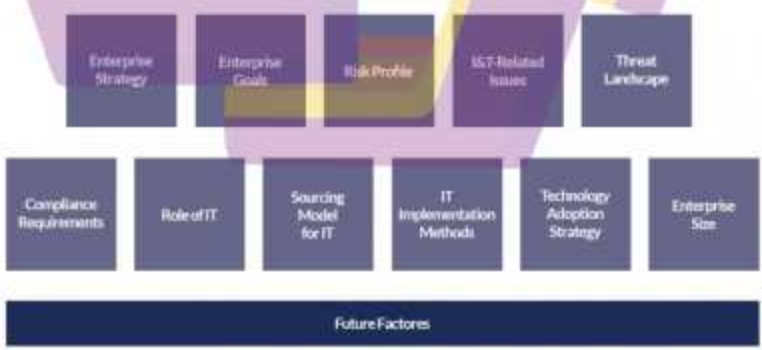
Area Fokus

Area Fokus menjelaskan topik, domain atau masalah tata kelola tertentu yang dapat ditangani oleh kumpulan tata kelola dan manajemen serta komponennya. Contoh area fokus meliputi : usaha kecil dan menengah, keamanan siber, transformasi digital, komputasi awan, privasi, dan devOps. Inilah kelebihan COBIT 2019.

2.3.4.1 Desain Faktor

COBIT 2019 yang merupakan evolusi dari versi sebelumnya, COBIT 5. COBIT 2019 dirilis dengan menambahkan perkembangan terbaru yang dapat mempengaruhi informasi dan teknologi pada sebuah organisasi. Dalam COBIT 2019, membantu perusahaan dalam merancang sistem tata kelola dengan menggunakan beberapa faktor desain yang telah disediakan.

Pada COBIT 2019 faktor inilah yang akan mempengaruhi pemilihan domain dalam rangka analisis maupun perancangan sistem tata kelola Teknologi Informasi seperti terlihat pada Gambar 2.7.



Gambar 2.7. Faktor Desain COBIT 2019

Pada proses perancangan sistem tata kelola terdapat 11 faktor desain yang dipertimbangkan diantaranya ialah [Anastasia, Priscilla Novita, Atrinawati, Lovinta Happy, 2020] :

1. Design Factor 1 – Enterprise Strategy

   Perusahaan memiliki strategi yang beragam sesuai dengan bidang bisnisnya. Dalam design factor ini terdapat beberapa jenis strategi perusahaan seperti fokus pada pertumbuhan perusahaannya, fokus pada produk dan layanan yang inovatif kepada klien, fokus pada minimalisasi biaya dalam jangka pendek, serta fokus pada penyediaan layanan yang stabil dan berorientasi kepada klien. Enterprise Strategy terlihat seperti Gambar 2.8 berikut ini :

Strategy Archetype	Explanation
Growth/Acquisition	The enterprise has a focus on growing (revenues).
Innovation/Differentiation	The enterprise has a focus on offering different and/or innovative products and services to their clients.
Cost Leadership	The enterprise has a focus on short-term cost minimization.
Client Service/Stability	The enterprise has a focus on providing stable and client-oriented service.

Gambar 2.8. Desain Faktor Enterprise Strategy

2. Design Factor 2 – Enterprise Goals

   COBIT 2019 menetapkan 13 tujuan umum perusahaan. Setiap perusahaan harus memprioritaskan sasaran perusahaannya sesuai dengan strategi perusahaan yang dipilih. Untuk menerjemahkan tujuan perusahaan ke dalam peringkat relatif pentingnya tata kelola dan tujuan manajemen, stakeholder harus membuat pilihan yang jelas ketika memilih tujuan perusahaan. Enterprise Goal terlihat seperti Gambar 2.9 berikut ini :

Reference	Balanced Scorecard (BSC) Dimension	Enterprise Goal
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business-service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Gambar 2.9. Desain Faktor Enterprise Goals

3. Design Factor 3 – IT Risk Profile

Memahami profil risiko perusahaan yaitu memahami skenario risiko mana yang dapat memengaruhi perusahaan, dan bagaimana menilai dampaknya dan kemungkinan terwujudnya. Untuk itu perlu dilakukannya analisis risiko tingkat tinggi pada perusahaan, seperti melakukan identifikasi risiko yang relevan. Dalam COBIT 2019, terdapat 19 kategori skenario risiko yang didefinisikan. IT Risk profile terlihat seperti Gambar 2.10 berikut ini :

Reference	Risk Category
1	IT investment decision making, portfolio definition and maintenance
2	Program and projects lifecycle management
3	IT cost and oversight
4	IT expertise, skills and behavior
5	Enterprise/IT architecture
6	IT operational infrastructure incidents
7	Unauthorized actions
8	Software adoption/usage problems
9	Hardware incidents
10	Software failures
11	Logical attacks (hacking, malware, etc.)
12	Third party/supplier incidents
13	Noncompliance
14	Geopolitical issues
15	Industrial action
16	Acts of nature
17	Technology-based innovation
18	Environmental
19	Data and information management

Gambar 2.10. Desain Faktor IT Risk Profile

4. Design Factor 4 – I&T Related Issues

Masalah TI dapat diidentifikasi atau dilaporkan melalui risiko manajemen, audit, manajemen senior atau pemangku kepentingan eksternal. Dalam COBIT 2019 terdapat beberapa 20 daftar masalah umum yang terkait TI. Perbedaan yang jelas harus dibuat dalam masalah peringkat I&T, untuk memberikan input yang diperlukan untuk menentukan prioritas desain tata kelola. I&T Related Issues terlihat seperti pada Gambar 2.11 berikut ini :

Reference	Description
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value
C	Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT-related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
G	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives, or other forms of wasted resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
K	Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT
L	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions
M	Excessively high cost of IT
N	Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems
O	Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages
P	Regular issues with data quality and integration of data across various sources
Q	High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation
R	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department[17]
S	Ignorance of and/or noncompliance with privacy regulations
T	Inability to exploit new technologies or innovate using I&T

Gambar 2.11. Desain Faktor I&T Related Issues

5. Design Factor 5 – Threat Landscape

Tipikal ancaman yang dihadapi oleh perusahaan juga menjadi salah satu faktor desain sistem tata kelola yang tepat. Terdapat 2 macam ancaman yaitu ancaman normal dan ancaman tinggi. Threat landscape terlihat seperti pada Gambar 2.12 berikut ini :

Threat Landscape	Explanation
Normal	The enterprise is operating under what are considered normal threat levels.
High	Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment.

Gambar 2.12. Desain Faktor Threat Landscape

6. Design Factor 6 – Compliance Requirement

Kebutuhan dan tuntutan kepatuhan yang harus dipenuhi oleh perusahaan merupakan salah satu faktor yang penting. Pada tahap ini terdapat 3 jenis kebutuhan/tuntutan kepatuhan yaitu rendah, normal, dan tinggi. Compliance Requirement terlihat seperti pada Gambar 2.13 berikut ini :

Regulatory Environment	Explanation
Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.
Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements that are common across different industries.
High compliance requirements	The enterprise is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions.

Gambar 2.13. Desain Faktor Compliance Requirement

7. Design Factor 7 – Role of IT

Peran TI dalam perusahaan juga menjaadi faktor yang penting. Dimana menilai apakah TI diposisikan sebagai strategic, support, maupun pabrik. Role of IT terlihat seperti pada Gambar 2.14 berikut ini :

Role of IT	Explanation
Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.
Factory	When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.
Turnaround	IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency on IT for the current running and continuity of the business processes and services.
Strategic	IT is critical for both running and innovating the organization's business processes and services.

Gambar 2.14. Desain Faktor Role of IT

8. Design Factor 8 – Sourcing Model of IT

Model pengalihan daya TI yang diterapkan dalam perusahaan biasanya menggunakan layanan TI dengan beberapa model seperti outsourcing, cloud, insourced, atau hybrid. Sourcing Model of IT terlihat seperti pada Gambar 2.15 berikut ini :

Sourcing Model	Explanation
Outsourcing	The enterprise calls upon the services of a third party to provide IT services.
Cloud	The enterprise maximizes the use of the cloud for providing IT services to its users.
Insourced	The enterprise provides for its own IT staff and services.
Hybrid	A mixed model is applied, combining the other three models in varying degrees.

Gambar 2.15. Desain Faktor Sourcing Model of IT

9. Design Factor 9 – IT Implementation Methods

Terdapat beberapa tipe metode implementasi TI seperti Agile, DevOps, Traditional, dan Hybird. IT Implementation Methods terlihat seperti pada Gambar 2.16 berikut ini :

IT Implementation Method	Explanation
Agile	The enterprise uses Agile development working methods for its software development.
DevOps	The enterprise uses DevOps working methods for software building, deployment and operations.
Traditional	The enterprise uses a more classic approach to software development (waterfall) and separates software development from operations.
Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as "bimodal IT."

Gambar 2.16. Desain Faktor IT Implementation Methods

10. Design Factor 10 – Technology Adoption Strategy

Strategi mengadopsi teknologi baru dalam perusahaan terdapat beberapa jenis sifatnya. Seperti first mover dimana perusahaan tersebut selalu ingin mengadopsi teknologi baru sesegera mungkin. Kemudia terdapat follower dimana perusahaan menunggu yang lain menerapkan teknologi tersebut baru dia ikuti, dan slow adopter dimana perusahaan sangat lambat dalam pengadopsian teknologi baru. Technology Adoption Strategy terlihat seperti pada Gambar 2.17 berikut ini :

Technology Adoption Strategy	Explanation
First mover	The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage.
Follower	The enterprise typically waits for new technologies to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with adoption of new technologies.

Gambar 2.17. Desain Faktor Technology Adoption Strategy

11. Design Factor 11 – Enterprise Size

Ukuran besar atau kecilnya suatu perusahaan yang umum digunakan antara lain adalah menggunakan ukuran jumlah karyawan tetap yang dipekerjakannya. Technology Adoption Strategy terlihat seperti pada Gambar 2.18 berikut ini :

Enterprise Size	Explanation
Large enterprise (Default)	Enterprise with more than 250 full-time employees (FTEs)
Small and medium enterprise	Enterprise with 50 to 250 FTEs

Gambar 2.18. Desain Faktor Enterprise Size

Goal Cascade

Saat membuat desain tata kelola maka hal yang harus dilakukan adalah mendetailkan target pada masing masing level. Kebutuhan stakeholder di turunkan menjadi target perusahaan, lalu di turunkan menjadi alignment goals, terakhir menjadi governance dan manajemen objectives seperti telihat pada Gambar 2.19 di bawah ini :

Gambar 2.19. Goal Cascading pada COBIT 2019

Enterprise Goals

Enterprise Goals merupakan target perusahaan yang diperoleh dari kebutuhan stakeholder. Target ini dapat dilihat dari visi dan misi suatu perusahaan atau organisasi. Berikut tampilan enterprise goals dalam Tabel 2.3 berikut :

Tabel 2.3. Enterprise Goals dalam COBIT 2019

Reference	BSC	Enterprise Goal
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Alignment Goals

Penyelarasan tujuan perusahaan agar dapat diperoleh tata kelola TI yang baik. Target penyelarasan ini diturunkan dari target perusahaan atau organisasi. Berikut tampilan Alignment Goals dalam Gambar 2.20 berikut :

Reference	IT BSC Dimension	Alignment Goal
AG01	Financial	I&T compliance and support for business compliance with external laws and regulations
AG02	Financial	Managed I&T-related risk
AG03	Financial	Realized benefits from I&T-enabled investments and services portfolio
AG04	Financial	Quality of technology-related financial information
AG05	Customer	Delivery of I&T services in line with business requirements
AG06	Customer	Agility to turn business requirements into operational solutions
AG07	Internal	Security of information, processing infrastructure and applications, and privacy
AG08	Internal	Enabling and supporting business processes by integrating applications and technology
AG09	Internal	Delivery of programs on time, on budget and meeting requirements and quality standards
AG10	Internal	Quality of I&T management information
AG11	Internal	I&T compliance with internal policies
AG12	Learning and Growth	Competent and motivated staff with mutual understanding of technology and business
AG13	Learning and Growth	Knowledge, expertise and initiatives for business innovation

Gambar 2.20. Alignment Goals dalam COBIT 2019

2.3.4.2 RACI Chart

RACI merupakan singkatan dari Responsible, Accountable, Consulted, dan Informed. Pada COBIT, RACI berfungsi untuk menunjukan peran dan tanggung jawab dari suatu fungsi dalam sebuah struktur organisasi terhadap sebuah aktivitas TI process goal tertentu. Penggunaan RACI memungkinkan manajer dari tingkat organisasi atau program yang sama atau berbeda untuk berpartisipasi aktif dalam diskusi yang terfokus dan sistematis mengenai deskripsi proses terkait dengan tindakan yang harus dilakukan dalam rangka untuk memberikan produk akhir atau jasa yang sukses.

Setiap process goal TI menerapkan RACI pada setiap aktivitas di dalamnya yang berfungsi untuk mendukung kesuksesan proses TI pada kelima domain yang ada. Adapun tujuan dari penerapan RACI adalah untuk memperjelas aktivitas sekaligus sebagai sarana untuk menentukan peran dari fungsi-fungsi lainnya terhadap suatu aktifitas tertentu. RACI chart mendefinisikan apa dan kepada siapa harus didelegasikan yang terdiri dari (Rozas & Effendy, 2012) :

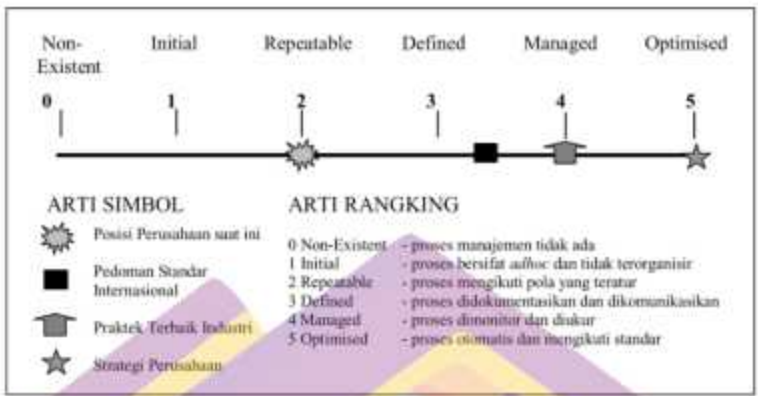
1. R = Responsible, artinya pihak yang harus memastikan aktivitas tersebut berhasil dilaksanakan.
2. A = Accountable, artinya pihak yang mempunyai kewenangan untuk menyetujui atau menerima pelaksanaan sebuah aktivitas.
3. C = Consulted, artinya pihak yang mana pendapatnya dibutuhkan dalam aktivitas (komunikasi arah).

4. I = Informed, artinya pihak yang selalu menjaga kemajuan informasi atas aktivitas yang dilakukan (komunikasi arah).

RACI Chart dapat membantu auditor untuk melakukan identifikasi terhadap orang-orang yang berkompeten untuk dilakukan proses wawancara. Terdapat role atau peran pada COBIT yang digunakan dalam RACI Chart. Semua role atau peran tersebut nantinya akan dipetakan sesuai dengan role atau peran yang ada pada Rumah Sakit.

2.3.4.3 Maturity Model

Untuk menggambarkan sejauh mana TI yang diterapkan telah dikelola dan dapat mendukung bisnis organisasi, penerapan TI membutuhkan pengembangan dan perbaikan agar mencapai tujuan organisasi (Nitrizal, 2007). Agar perbaikan proses pengelolaan TI dapat secara berkelanjutan dapat dilakukan, maka organisasi harus mampu mengevaluasi kondisi eksistingnya. COBIT menyediakan kerangka identifikasi sejauh mana organisasi telah memenuhi standar pengelolaan proses TI yang baik. Kerangka tersebut direpresentasikan dalam sebuah model kematangan COBIT yang memiliki level pengelompokan kapabilitas organisasi dalam pengelolaan proses TI dari level nol atau non exixtent (belum tersedia) hingga level lima atau opimised (teroptimasi). Secara grafis model kematangan COBIT ditunjukkan seperti pada Gambar 2.21.



Gambar 2.21. Representasi Grafis Model Kematangan COBIT (ITGI, 2007)

Model kematangan merupakan metode skoring yang memungkinkan oganisasi untuk memberi ranking bagi dirinya sendiri dengan memberikan penjelasan kepada manajer mengenai proses TI dengan menunjukkan kelemahan manajemen yang ada dan menetapkan target yang sesuai. Alat bantu pengukuran ini menawarkan kemudahan untuk memahami bagaimana menentukan posisi saat ini (as-is) dan posisi masa depan (to-be) serta memungkinkan organisasi untuk melakukan pembandingan pada dirinya sendiri berdasarkan praktik-praktik terbaik dan panduan strandar (Surendro, 2009). Deskripsi dari masing-masing level kematangan dari level nol (non existent) sampai dengan level lima (optimised) dapat ditunjukkan pada Tabel 2.4.

Tabel 2.4. Model Umum Kematangan COBIT (ITGI, 2007)

Model Kematangan secara umum	
Level 0 (incomplete)	Merupakan posisi kematangan terendah, yang merupakan suatu kondisi dimana organisasi merasa tidak membutuhkan adanya mekanisme proses tata kelola TI yang baku, sehingga tidak ada sama sekali pengawasan terhadap tata kelola TI yang dilakukan oleh organisasi.

Tabel 2.4. Model Umum Kematangan COBIT (ITGI, 2007) (Lanjutan)

Level 1 (performed)	Sudah ada beberapa inisiatif mekanisme perencanaan dan pengawasan sejumlah tata kelola TI yang dilakukan, namun tidak ada penilaian yang standar.
Level 2 (managed)	Kondisi dimana organisasi telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola tata kelola TI dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen formal.
Level 3 (established)	Pada tahapan ini organisasi telah memiliki mekanisme dan prosedur yang jelas mengenai tata cara dan manajemen tata kelola TI, dan telah terkomunikasikan dan tersosialisasikan dengan baik di seluruh jajaran manajemen.
Level 4 (predictable)	Merupakan kondisi dimana manajemen organisasi telah menerapkan sejumlah indikator pengukuran kinerja kuantitatif untuk memonitor efektivitas pelaksanaan manajemen tata kelola TI.
Level 5 (optimizing)	Level tertinggi ini diberikan kepada organisasi yang telah berhasil menerapkan prinsip-prinsip tata kelola TI secara utuh dan mengacu best practise. Penggunaan TI yang optimal untuk mendukung monitoring, pengukuran, analisa, pelatihan dan komunikasi.

Setiap atribut yang ada dinilai menggunakan standar skala penilaian yang ditetapkan dalam standar 15504 ISO/IEC. Adapun skala penilaian tersebut adalah (ISACA, 2013) :

a. N (*Not Achieved*) - Ketercapaian 0 sampai 15%

   Masih sedikit atau bahkan belum terdapat ketercapaian sama sekali pada proses yang dinilai pada atribut yang ditentukan.

b. P (*Partially Achieved*) - Ketercapaian > 15% sampai 50%

   Terdapat beberapa ketercapaian pada proses yang dinilai dari atribut yang ditentukan, namun belum signifikan.

c. L (*Largely Achieved*) - Ketercapaian > 50% sampai 85%

Terdapat ketercapaian yang signifikan pada proses yang dinilai dari atribut yang ditentukan.

d. F (*Fully Achieved*) - Ketercapaian > 85% sampai 100%

Terdapat ketercapaian secara penuh pada proses yang dinilai dari atribut yang ditentukan.

BAB III

METODELOGI PENELITIAN

3.1 Jenis, Sifat dan Pendekatan Penelitian

Jenis penelitian ini adalah penelitian studi kasus (case study), dimana peneliti melakukan analisis capability Teknologi Informasi yang diterapkan di UPTD RSUD Tarakan. Studi kasus lebih banyak berkutat pada atau berupaya menjawab pertanyaan-pertanyaan "how" (bagaimana) dan "why" (mengapa), serta pada tingkatan tertentu juga menjawab pertanyaan "what" (apa / apakah), dalam kegiatan penelitian [Bungin, B, 2005].

Sifat penelitian ini adalah penelitian deskriptif yang menggunakan pendekatan kualitatif, yaitu penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati [Bogdan, R., Taylor, S., 1992]. Data deskriptif dalam penelitian ini bertujuan untuk mendeskripsikan atau menjelaskan fenomena yang ada dengan menggunakan angka-angka dalam hal ini yaitu mendeskripsikan tingkat kematangan proses TI berdasarkan COBIT dalam bentuk analisis kondisi (saat ini dan harapan).

Pendekatan pada penelitian ini menggunakan metode kualitatif yang di proses menjadi kuantitatif. Konsepnya peningkatan pemahaman terhadap sesuatu dan bukan membangun penjelasan. Sifatnya subyektif, berorientasi ke observasi tanpa di kontrol, dan secara umum generalisasi dilakukan dengan mempertimbangkan pendekatan dan kesamaan objek.

3.2 Metode Pengumpulan Data

Dalam penelitian ini, metode pengumpulan data yang dilakukan oleh peneliti menggunakan metode wawancara dan kuisioner. Data yang di kumpulkan adalah data tingkat kapabilitas proses TI saat ini dan yang diharapkan. Kuisioner pada penelitian ini dilakukan pengumpulan dan pengolahan menggunakan beberapa metode agar mendapatkan hasil yang maksimal. Metode yang digunakan pada penelitian ini adalah RACI Chart. RACI chart merupakan sebuah metode dengan memanfaatkan tabel RACI pada COBIT 2019 untuk melakukan pengolahan data hasil kuisioner. Pengunaan metode ini bertujuan untuk melakukan pemilihan data praktek TI berdasarkan peran (role) yang ada pada kuisioner. Pemilihan data praktek TI dilakukan dikarenakan suatu praktek TI pada kuisioner dapat diisi lebih dari satu peran (role) dengan skala penilaian yang berbeda beda. Oleh karena itu untuk mendapatkan skala penilaian yang tepat dari satu praktek TI harus dilakukan dengan memilih data praktek TI yang ada. Proses pemilihan data praktek TI terpilih dilakukan dengan memilih peran (role) pada tabel RACI dengan tingkat tanggung jawab Responsible dan Accountable yang memiliki arti bahwa peran (role) tersebut lebih mengerti dan lebih menguasai praktek TI yang akan di teliti. Sehingga data yang diolah akan lebih valid. Sama halnya seperti pada proses sebelumnya, data dari reponden dengan tingkat tanggung jawab accountabnle hanya akan dipakai jika tidak ada data dari responden dengan tingkat tanggung jawab responsible yang dapat diolah atau dengan kata lain hanya bersifat opsional.

3.3 Metode Analisis Data

Setelah proses pengumpulan data dilakukan, proses selanjiutnya adalah melakukan pengolahan dan Analisa terhadap data yang ada. Data yang digunakan pada proses ini adalah data hasil wawancara dan survey kuisioner yang telah di berikan dan diisi oleh pihak pihak yang telah di tentukan.

3.3.1. Analisis Kondisi Tingkat Kapabilitas

Analisa kondisi tingkat kapabilitas merupakan proses yang dilakukan untuk mengetahuikondisi tingkat kapabilitas teknologi informasi saat ini (as-is) dan kondisi tingkat kapabilitas TI maksimal sesuai COBIT 2019. Hasil yang diperoleh dari proses ini akan digunakan untuk mengidentifikasi kesenjangan (gap) yang terjadi antara kondisi TI yang ada saat ini dengan kondisi TI yang diharapkan. Proses TI yang belum memenuhi harapan harus diberikan perhatian khusus agar dapat ditingkatkan dan sesuai dengan harapan. Analisa kondisi tingkat kapabilitas saat ini (as-is) merupakan sebuah proses untuk mengidentifikasi atau mendapatkan potret kondisi teraktual tingkat kapabilitas TI pada RSUD. Proses identifikasi pada penelitian ini dilakukan dengan melihat hasil kuisioner yang telah diisi sebelumnya oleh pihak yang telah ditentukan pada RSUD. Kuisioner yang dibagikan terdiri dari 6 level atau tingkat kapabilitas seperti yang dijelaskan pada bagian CMMI penelitian ini.

3.3.2. Analisis Kesenjangan (Gap)

Analisi kesenjangan (gap) dilakukandengan tujuan untuk memberikan kemudahan dalam perbaikan tata kelola yang ada. Analisis kesenjangan (gap) digunakan untuk melakukan perbandingan antara tingkat kapabilitas pengelolaan

TI maksimal. Jika hasil analisis kesenjangan (gap) menyatakan terdapat kesamaan antara keduanya, maka proses pengelolaan TI RSUD dinyatakan sudah berjalan dengai baik atau sesuai yang diharapkan. Sebaliknya, jika hasil analisis menyatakan adanya kesenjangan antara tingkat kapabilitas pengelolaan TI saat in (as-is) dengan yang diharapkan maka perlu dilakukan peningkatan terhadap pengelolaan TI saat ini agar dapat mencapai tingkat kapabilitas yang telahj di tentukan. Peningkatan tingkat kapabilitas pengelolaan TI saat ini (as-is) dapat dilakukan dengan perbaikan terhadap tata kelola TI RSUD secara menyel;uruh atau hanya pada bagian tertentu. Perbaikan tata kelola TI dilakukan berdasarkan informasi mengenai proses-proses mana saja yang memiliki kesenjangan dan membutuhkan perbaikan tata keloal TI dan manajemen pada RSUD.

3.3.3. Validasi Data Audit

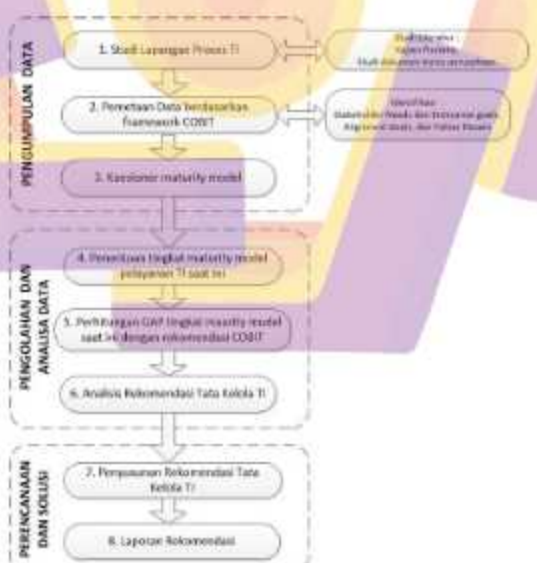
Audit merupakan kegiatan yang bersifat memotret kondisi suatu objek audit. Pada proses audit, seorang auditor akan menilai berdasarkan data dan fakta yang ada dilapangan. Agar hasil audit ini tepat dan dapat dipertangungjawabkan maka diperlukan proses validasi data. Proses validasi data audit dapat ditempuh menggunakan metode evaluasi dan cek data yang digunakan sebagai input audit oleh komite yang ditunjuk. Untuk itu pada penelitian ini akan dilakukan validasi data input audit oleh tim SPI RSUD dan di buktikan dengan persetujuan hasil audit.

3.3.4. Rekomendasi Perbaikan

Dalam proses evaluasi tata kelola TI, rekomendasi perbaikan diperlukan agar kekurangan ataupun kelemahan sumber data TI RSUD dapat diminimalisir atau bahkan dihilangkan. Rekomendasi perbaikan yang disusun bertujuan untuk

membuat sistem atau sumber daya TI yang ada dapat berjalan lebih efektif dan efisien. Rekomendasi yang diberikan merupakan hasil analisis kesenjangan (gap) yang terjadi antara tingkat kapabilitas proses TI saat ini (as-is) dengan tingkat kapabilitas proses TI yang diharapkan oleh perusahaan. Rekomendasi perbaikan pada penelitian ini disusun berdasarkan aktivitas serta praktek di setiap domain dan proses TI yang teridentifikasi pada masing masing level dari tingkat kapabilitas pada COBIT 2019. Pada COBIT 2019 terdapat beberapa pendefenisian dari aktifitas serta praktek yang dapat dijadikan acuan oleh RSUD untuk dapat mencapai goal dari sebuah proses TI serta meningkatkan tingkat kapabilitas pengelolaan TI yang ada. Rekomendasi yang diperoleh pada masing-masing domain akan disimpulkan menjadi rekomendasi umum bagi RSUD Tarakan.

3.4 Alur Penelitian



Gambar 3.1 Alur Penelitian

Bagian ini memuat penjelasan secara lengkap dan terinci tentang langkah-langkah yang dilakukan dalam melakukan penelitian dimulai dari perumusan permasalah hingga pengambilan kesimpulan. Penelitian ini dilakukan dalam beberapa tahap seperti terlihat pada gambar 3.1 diatas, yaitu :

Keterangan dari gambar diatas adalah sebagai berikut :

1. Melakukan studi pada proses IT yang sudah berjalan di layanan RSUD Tarakan melalui kajian pustaka dan studi dokumen bisnis perusahaan.

   Kajian pustaka merupakan sebuah proses dari penyusunan sebuah laporan penellitian yang diarahkan kepada pencarian dan pengumpulan informasi dan data melalui dokumen-dokumen yang ada.

   Studi dokumen bisnis perusahaan merupakan proses pancarian atau pengumpulan informasi dan data-datanmengenai perusahaan yang akan dijadikan objek penelitian. Proses ini dapat dilakukan dengan melakukan wawancara langsung kepada pihak terkait pada RSUD ataupun dengan mencari referensi dokumen melalui annual report dan melalui dokumen RSUD. Tujuan dilaksanakannya pada penelitian ini adalah untuk mengetahui dan memahami sejauh mana pengelolaan TI yanhg sudah berjalan dan penerapan manajemen tata kelola untuk aplikasi operasional RSUD. Adapun informasi dan data yang dibutuhkan meliputi visi dan misi, profil instalasi yang ada, standard operational procedure dan struktur organisasi perusahaan. Pelaksanaan studi dokumen ini diharapkan dapat menjadi landasan teori dalam penyusunan perumusan masalah pada penelitian ini.

2. Pemetaan data mengacu pada framework COBIT dengan melakukan identifikasi terhadap kebutuhan dari pemangku kepentingan dan tujuan bisnis perusahaan, yang pada COBIT 2019 dinyatakan sebagai Stakeholder Needs dan Enterprise Goals. Stakeholder Needs merupakan kebutuhan dari setiap pemangku kepentingan pada perusahaan. Hasil identifikasi kebutuhan stakeholder tersebut dapat digunakan untuk menjadi dasar untuk melakukan identifikasi terhadap enterprise goals atau tujuan bisnis yang dimiliki oleh perusahaan. Setelah kebutuhan stakeholder dan tujuan bisnis teridentifikasi, proses selanjutnya adalah melakukan identifikasi terhadap Alignment Goals dari perusahaan. Identifikasi Faktor Desain Identifikasi faktor desain merupakan tahap terakhir dalam proses pemilihan domain pada COBIT yaitu dengan melakukan pembobotan pada faktor desain berdasarkan kondisi riil dan aktual dari perusahaan. Adapun pada masing- masing faktor desain akan dipilih kriteria yang sesuai dengan kondisi pada objek penelitian.

   Setelah mengidentifikasi faktor desain, langkah selanjutnya adalah pembobotan berdasarkan tabel mapping yang menjadi metode baru COBIT 2019. Setiap pemilihan faktor desain memiliki nilai bobot pada masing- masing domain. Pada tahap akhir ini akan didapatkan domain mana saja yang prioritas dan bukan prioritas berdasarkan hasil pembobotan.

   Secara umum data penelitian terbagi menjadi dua jenis yaitu data primer dan data sekunder. Dalam melakukan pengumpulan data sekunder pada penelitian ini dengan menggunakan dokumen pendukung yang dimiliki perusahaan pada proses audit. Sedangkan untuk pengumpulan data primer yang dilakukan pada

penelitian ini menggunakan metode wawancara dan kuisioner. Yang paling perlu diperhatikan adalah bagaimana data primer ini menjadi tepat dan sesuai dengan fakta dilapangan dan tidak terjadi bias informasi. Untuk itu dalam pengelolaan data primer, framework COBIT 2019 telah memfasilitasi dengan RACI chart.

3. Kuesioner pengumpulan data dengan cara diskusi bersama penentuan nilai pernyataan dengan acuan domain hasil faktor desain dengan instalasi PDE dan Umum.
4. Pengolahan data untuk menentuan tingkat Maturity Model layanan TI yang berjalan saat ini.
5. Menentukan kondisi ideal yang diinginkan dan menentukan jarak (gap) antara level saat ini (existing) dan level rekomendasi dari COBIT (target).
6. Analisis dari hasil pengolahan data untuk menentukan rekomendasi tata kelola TI.
7. Penyusunan rekomendasi tata kelola TI berdasarkan analisis kesenjangan (gap analysis) yang muncul dengan menggunakan acuan famework COBIT. Usulan-usulan yang diberikan diharapkan dapat menjadi solusi agar target TI dimasa mendatangan dapat tercapai
8. Penyusunan laporan hasil rekomendasi tata kelola TI merupakan tahap akhir dari penelitian ini. Laporan ini diharapkan dapat mejelaskan kegiatan penelitian secara keseluruhan.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Gambaran Umum Tata Kelola TI

4.1.1 Kondisi Sistem Informasi

Sistem Informasi Manajemen Rumah Sakit di RSUD Tarakan sudah tersedia dan semua kegiatan input data untuk pelayanan sudah menggunakan fasilitas pada modul SIMRS, namun untuk pelayanan penunjang seperti Radiologi, Laboratorium, Farmasi dan Logistik mengunakan Sistem Informasi stand alone atau sistem terpisah dari SIMRS dan tidak terintegrasi dengan SIMRS yang ada sehingga kualitas layanan Rumah Sakit untuk SPM (Standar Pelayanan Minimal) masih menjadi temuan saat di lakukan audit. Human error juga menjadi masalah yang kedua yang harus diselesaikan manajemen sebagai akibat dari tidak terintegrasinya data antara sistem sistem yang berjalan dan digunalkan di RSUD Tarakan. Berikut tabel 4.1 daftar dari Sistem Informasi yang diimplementasikan di RSUD Tarakan yang saat ini sedang berjalan.

Tabel 4.1 Aplikasi Portofolio RSUD Tarakan

No	No. Aplikasi	Nama Aplikasi	Keterangan
1	Inova.1.1	Modul Pendaftaran	Transaksi pendaftaran offline pasien
2	Inova.1.2	Modul Rawat Jalan	Transaksi, Informasi, dan laporan Rawat Jalan Pasien
3	Inova.1.3	Modul Rawat Darurat	Transaksi, Informasi, dan laporan Rawat Darurat Pasien
4	Inova.1.4	Modul Rawat Inap	Transaksi, Informasi, dan laporan Rawat Inap Pasien

Tabel 4.1 Aplikasi Portofolio RSUD Tarakan (Lanjutan)

5	Inova.1.5	Modul Laboratorium	Pendaftaran dan Informasi pasien, output hasil pemeriksaan radiologi dari sistem yang berbeda dan di input ulang ke dalam modul ini.
6	Inova.1.6	Modul Radiologi	Transaksi, Informasi dan Laporan pasien, output hasil pemeriksaan radiologi dari sistem yang berbeda dan di input ulang ke dalam modul ini.
7	Inova.1.7	Modul Farmasi /Apotik	Modul tidak digunakan, Transaksi, Informasi dan Laporan obat/alkes menggunakan sistem stand alone yang berbeda dan belum terintegrasi dengan SIMRS.
8	Inova.1.8	Modul Rehab Medik	Transaksi, Informasi, dan Laporan Rehab medik
9	Inova.1.9	Modul Bedah Sentral	Transaksi, Informasi, dan Laporan Bedah pasien
10	Inova.1.10	Modul Persalinan	Transaksi, Informasi, dan Laporan Persalinan pasien
11	Inova.1.11	Modul Gizi	Transaksi, Informasi, dan Laporan Gizi pasien
12	Inova.1.12	Modul Ambulans	Transaksi, Informasi, dan Laporan fasilitas ambulans
13	Inova.1.13	Modul Pemulsaran Jenazah	Transaksi, Informasi, dan Laporan Pemulsaran Jenazah
14	Inova.1.14	Modul Billing Kasir	Transaksi dan Informasi Tagihan pasien
15	Inova.1.15	Modul Informasi	Informasi Ruangan dan Bed
16	Inova.1.16	Modul Antrian	Informasi antrian pendaftaran pasien
17	Inova.1.17	Modul Care Unit	Transaksi dan Informasi ICU, HCU, HCCU, ICCU, dan PICU
18	Inova.1.18	Modul MCU	Transaksi dan Informasi Medical checkup
19	Inova.1.19	Modul Mobile	Transaksi dan Informasi Pendaftaran online pasien
20	Inova.1.20	Modul Rekam Medis	Informasi Rekam medis pasien
21	Inova.1.21	Modul Sistem Admin	Konfigurasi dan Informasi SIMRS

Tabel 4.1 Aplikasi Portofolio RSUD Tarakan (Lanjutan)

22	Inova.1.22	Modul Gudang Farmasi	Modul tidak digunakan, Transaksi, Informasi dan Laporan obat/alkes menggunakan Agape.2.2 (DPI Farmasi) dan belum terintegrasi dengan SIMRS.
23	Inova.1.23	Modul Askep	Informasi Asuhan keperawatan
24	Inova.1.24	Modul Asuransi	Transaksi, Informasi dan laporan penjamin pasien
25	Inova.1.25	Modul Gudang Umum	Modul tidak digunakan, Transaksi, Informasi dan Laporan barang umum dan alkes menggunakan Agape.2.1 (DPI Logistik) dan belum terintegrasi dengan SIMRS.
26	Inova.1.26	Modul Kepegawaian	Informasi dan laporan data tenaga medis dan non medis
27	Inova.1.27	Modul Laundry	Transaksi, Informasi dan Laporan linen pasien
28	Inova.1.28	Modul CSSD	Informasi dan laporan sterilisasi alat medis
29	Agape.2.1	DPI Logistik	Transaksi, Informasi dan Laporan Barang umum. Sistem stand alone dan tidak terintegrasi dengan SIMRS
30	Agape.2.2	DPI Farmasi	Transaksi, Informasi dan Laporan Obat dan Alkes. Sistem stand alone dan tidak terintegrasi dengan SIMRS
31	RIS.3.1	GE PACS	Pemeriksaan Penunjang (Mengelola dan menyimpan data hasil pemeriksaan radiologi pasien), Sistem stand alone dan tidak terintegrasi dengan SIMRS
32	LIS.4.1	GE Laboratorium	Pemeriksaan Penunjang (Mengelola dan menyimpan data hasil pemeriksaan laboratorium pasien), Sistem stand alone dan tidak terintegrasi dengan SIMRS

4.1.2 Kondisi Teknologi Informasi

Secara umum kondisi infrastruktur TI di RSUD Tarakan sudah cukup memadai, di tahun 2019 dan 2020 telah diadakan peremajaan komputer di unit-unit, instalasi penunjang, poliklinik rawat jalan dan ruang rawat inap. Dengan adanya team hardware dan networking sangat membantu RSUD sehingga perawatan hardware dan infrastruktur TI sudah lebih baik. Team SIMRS bertugas untuk maintenance SIMRS dan seluruh transaksi yang terkait dengan SIMRS. Berikut tabel 4.2 infrastruktur SI/TI yang terdapat di RSUD Tarakan.

Tabel 4.2 Infrastruktur SI/TI di RSUD Tarakan

No	Infrastruktur	Keterangan
1.	Personal Computer	Setiap unit layanan memiliki pc dengan spesifikasi : - Processor Core i3 - Ram 4 Gb - Harddisk 500 gb - LCD 21,5" - UPS 600 va Total sebanyak 400 unit yang ada di RSUD Tarakan
2.	Server	Memiliki 7 unit server : 1. HP Proliant DL 380 Gen 9 sebanyak 2 unit 2. HP Proliant DL 380 Gen 10 sebanyak 2 unit 3. Synology DS1821+ sebanyak 1 unit 4. Dell PowerEdge T630 sebanyak 2 unit
3	Jaringan Komputer LAN	1. Kabel backbone LAN dari lantai 1 – lantai 6 menggunakna fiber optic 2. Setiap lantai menggunakan kabel UTP Cat 5e
4.	Jaringan Komputer Wifi	1. Menggunakan perangkat wifi Asus dan mikrotik type ceiling dengan total 30 titik accesspoint yang aktif
5.	Perangkat Jaringan	1. Menggunakan managed switch merek mikrotik dan netgear dengan total perangkat sebanyak 250 unit. 2. Perangkat firewall mengunakan Mikrotik CSS dengan total perangkat 6 unit
6.	Internet	1. Bandwidth 30 Mbps Astinet dengan 5 ip public 2. Bandwidth indihome 500 mbps

Tabel 4.2 Infrastruktur SI/TI di RSUD Tarakan (Lanjutan)

7.	Proses maintenance server dan backup Data	1. Proses backup data dilakukan otomatis dari server pada jam 12 malam.
8.	SOP	1. Belum ada SOP Tata kelola TI (maintenance server, hardware dan jaringan)
9.	UPS	1. Terdapat 3 unit UPS di ruang server 2. Genset RSUD sebanyak 4 unit dengan kapasitas 4 Megawatt untuk backup kebutuhan listrik di RSUD

4.2 Pemetaan Data berdasarkan Framework COBIT

4.2.1 Penentuan Responden

RACI chart dapat membantu untuk melakukan identifikasi terhadap orang-orang yang berkompeten untuk dilakukan proses wawancara. Terdapat 33 role atau peran pada COBIT 2019 yang digunakan dalam RACI chart. Semua role atau peran tersebut nantinya akan dipetakan sesuai dengan role atau peran yang ada pada RSUD.

Hasil penentuan responden berdasarkan RACI chart COBIT 2019 dan diimplementasikan pada RSUD Tarakan ditampilkan pada tabel 4.3 berikut ini.

Tabel 4.3. Hasil RACI chart secara keseluruhan

No	RACI Chart pada COBIT 2019	Struktur Organisasi RSUD Tarakan
1.	Chief Executive Officer	Direktur RSUD Tarakan
2.	Business Process Owner	Wadir Umum
3	Service Manager	Kepala Instalasi PDE
4.	Head IT Operations	Instalasi PDE Devisi Hardware
5.	Head Development	Instalasi PDE Devisi SIMRS
6.	Information Security Manager	Instalasi PDE Devisi Network

Setelah dilakukan identifikasi responden menggunakan RACI chart COBIT 2019, didapatkan 6 responden dalam audit tata kelola teknologi informasi pada RSUD Tarakan yaitu :

1. Direktur RSUD Tarakan
2. Wadir Umum RSUD Tarakan
3. Kepala Instalasi PDE
4. Staff Instalasi PDE devisi Hardware
5. Staff Instalasi PDE devisi Network
6. Staff Instalasi PDE devisi SIMRS/Software

4.2.2 Identifikasi Stakeholder Needs dan Enterprise Goals

Dalam menentukan domain yang akanm menjadi prioritas evaluasi maka dilakukan proses identifikasi stakeholder needs pada RSUD Tarakan. Proses ini dilakukan melalui wawancara dengan direktur dan wadir umum. Hasil identifikasi pada RSUD Tarakan dapat dilihat pada tabel 4.4.

Tabel 4.4. Kebutuhan Stakeholder

Kebutuhan Stakeholder	
Kebutuhan	Keterangan
Optimasi Resiko	RSUD Tarakan wajib menjalankan tupoksinya. Dalam menjalankan bisnisnya, optimasi resiko akan memperkecil kerugian dan hambatan.
Optimasi Sumber Daya	Dengan sumber daya yang dimiliki, diharapkan RSUD Tarakan dapat menjalankan tupoksi dengan optimal
Optimasi Pelayanan	Dengan sumber daya yang dimiliki, diharapkan RSUD Tarakan dapat mengoptimalkan pelayanan ke pelanggan.

Dilihat dari kebutuhan stakeholder pada tabel 4.4 diatas ada 3 pokok kebutuhan yang teridentifikasi. Selanjutnya dari hasil identifikasi kebutuhan

stakeholder kemudian dilanjutkan identifikasi enterprise goals. Dan hasilnya dapat dilihat pada tabel 4.5.

Tabel 4.5. Identifikasi Enterprise Goals

Referensi	BSC Dimension	Enterprise Goal
EG02	Financial	Resiko bisnis yang dikelola
EG05 EG06	Customer	Kontinuitas dan ketersediaan layanan bisnis
EG07	Internal	Kualitas informasi manajemen
EG13	Learning and Growth	Inovasi produk dan bisnis

4.2.3 Identifikasi Alignment Goals

Setelah melakukan identifikasi enterprise goals, dengan menggunakan tabel mapping yang telah di sediakan COBIT 2019 dilakukan alignment goals. Pada tabel mapping tersebut ada keterangan p (primary), S (secondary), dan tanpa keterangan. Yang dimaksud disini adalah Ketika P (primary) maka item tersebut berpengaruh besar sedangkan S (secondary) dan tanpa keterangan tidak memiliki pengaruh atau pengaruhnya kecil. Untuk itu dalam penelitian ini identifikasi alignment goals dipilih dengan kategori P (primary) saja seperti yang di tampilkan pada tabel 4.6 karena dimaksudkan agar nantinya rekomendasi yang berujung pada rencana strategis lebih fokus.

Tabel 4.6. Identifikasi Alignment Goals

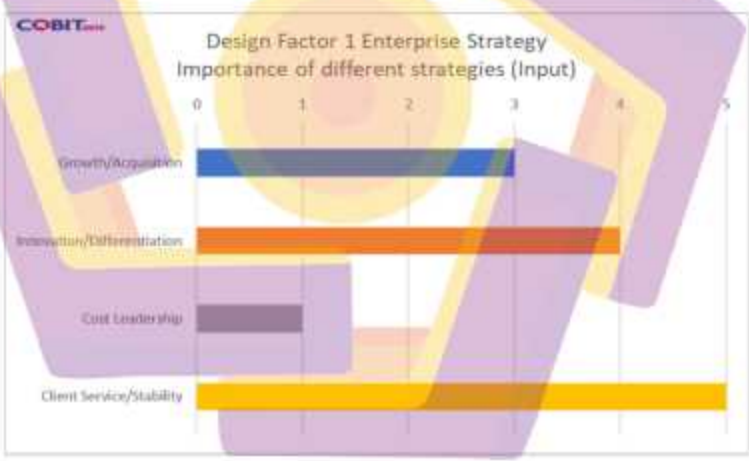
Referensi	Alignment Goal
AG02	Resiko IT terkelola
AG04	Kualitas terkait teknologi informasi keuangan
AG07	Keamanan informasi, infrastruktur, pengolahan dan aplikasi, serta privasi
AG08	Memungkinkan dan mendukung proses bisnis dengan mengintegrasikan aplikasi dan teknologi
AG13	Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis

4.2.4 Faktor Desain

Keunggulan dari COBIT 2019 dibandingkan dengan COBIT 5 adalah pada tahap dan metedologi penentuan objek manajemen dan tata kelola IT yang sering disebut domain atau fokus area. Berikut hasil identifikasi faktor desain yang sesuai dengan model bisnis RSUD Tarakan.

a. Faktor Desain 1 Strategi Organisasi

Faktor desain yang pertama adalah mengidentifikasi strategi perusahaan yang diterapkan RSUD Tarakan dari keempat strategi yang sudah disediakan oleh design toolkit COBIT 2019. Hasil dari identifikasi faktor desain 1 terdapat pada gambar 4.1



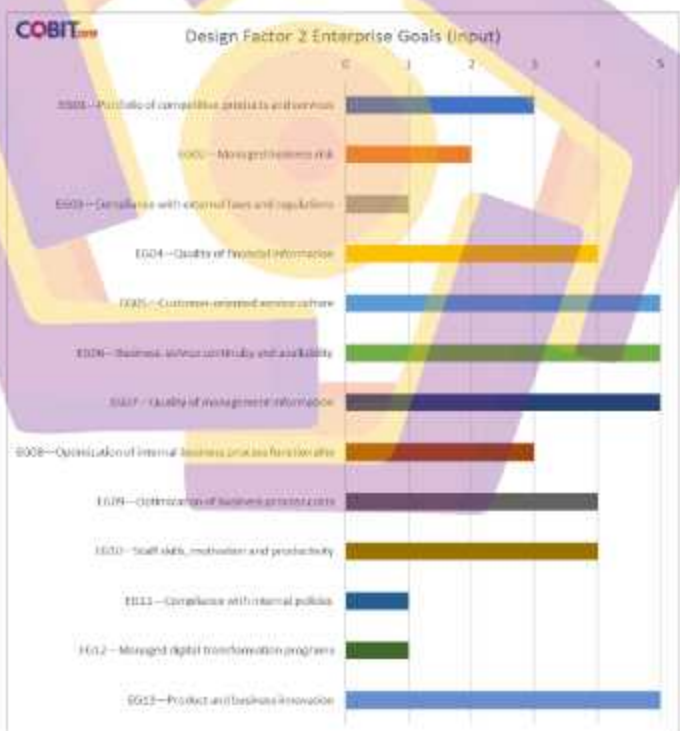
Gambar 4.1 Faktor Desain Strategi Organisasi

Gambar 4.1 menunjukan hasil pemetaan desain yang pertama yaitu adalah strategi rumah sakit, didapatkan satu strategi terpilih berdasarkan prioritas strategi pada RSUD Tarakan. Strategi orgnisasi keempat yaitu layanan, bersesuai dengan misi RSUD Tarakan yaitu adalah menyelenggarakan pelayanan kesehatan yang

paripurna dan mewujudkan pengelolaan rumah sakit yang professional. Berdasarkan misi tersebut maka RSUD Tarakan harus menyediakan layanan berbasis teknologi yang dapat diakses oleh pengguna yaitu masyarakat kota Tarakan.

b. Faktor Desain 2 Tujuan Organisasi

Faktor desain yang kedua yaitu tujuan organisasi, yaitu adalah tujuan atau target perusahaan yang mendukung strategi perusahaan yang sudah diidentifikasi pada tahap sebelumnya. Pada COBIT 2019 tujuan bisnis perusahaan dibagi menjadi 13 jenis. Hasil dari identifikasi faktor desain kedua terdapat pada gambar 4.2



Gambar 4.2 Faktor Desain Tujuan Organisasi

Gambar 4.2 menunjukan hasil faktor desain didapatkan 4 tujuan terpilih berdasarkan dengan tujuan RSUD Tarakan dan mendapat nilai 5, yaitu EG05 budaya layanan yang berorientasi pada pelanggan, EG06 keberlanjutan dan ketersediaan layanan bisnis, EG07 Kualitas informasi manajemen dan EG13 inovasi produk dan bisnis.

c. Faktor Desain 3 Profil Resiko

Faktor desain yang ketiga adalah profil resiko, yaitu mengidentifikasi profil resiko dari RSUD Tarakan. Hasil dari identifikasi faktor desain ketiga terdapat pada gambar 4.3

Gambar 4.3 Faktor Desain Profil Resiko

Gambar 4.3 menunjukan hasil faktor desain yang ketiga didapatkan 3 resiko terpilih yang memiliki resiko sangat tinggi. Resiko pertama yaitu adalah keahlian, keterampilan, dan perilaku TI. Kendala pertama yaitu kurangnya atau belumnya tercukupi sumber daya manusia seperti programmer sehingga pekerjaan tidak dapat berjalan dengan optimal khususnya dalam melakukan development bridging system antara modul ataupun antar aplikasi. Selanjutnya permasalahan dalam pemakaian atau penggunakan perangkat lunak. Dalam penggunaan perangkat lunak akan memiliki resiko yang tinggi dikarenakan sumber daya TI sangat kurang dalam upgrade skill dan kompetensi karena tidak adanya pelatihan TI dari RSUD. Pada kategori selanjutnya adalah serangan logis dikarenakan akan sangat berdampak pada operasional seperti sistem terkena hacking atau mallware.

d. Faktor Desain 4 Permasalahan yang Berkaitan dengan TI

Faktor desain yang keempat adalah permasalahan yang berkaitan dengan TI, yaitu adalah mengidentifikasi masalah yang akan dihadapi RSUD Tarakan dalam hal Teknologi Informasi. Hasil dari identifikasi faktor desain keempat terdapat pada gambar 4.4

Gambar 4.4 Faktor Desain Permasalahan yang Berkaitan dengan TI

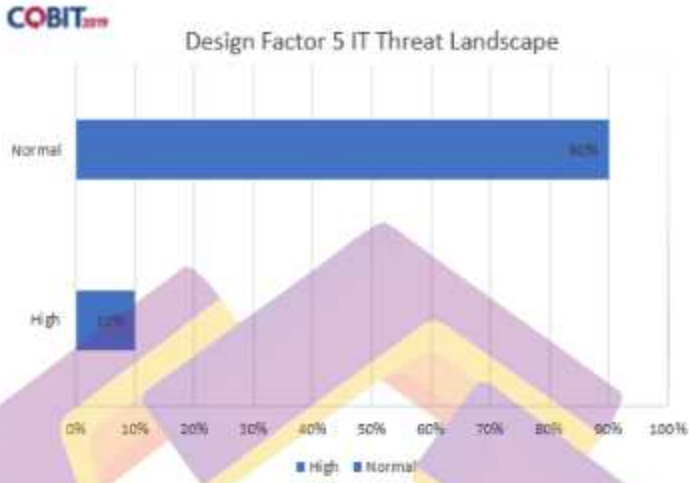
Gambar 4.4 menunjukan hasil faktor desain keempat, terdapat 3 penilaian yaitu nilai 1 untuk tidak ada masalah, nilai 2 untuk ada masalah, dan nilai 3 untuk masalah serius. Dari hasil pemetaan faktor desain ini terdapat 5 permasalahan yang sangat serius berkaitan dengan TI. Permasalahan yang pertama adalah masalah pengiriman layanan oleh agen outsourcing TI. Dalam pengembangan SIMRS ini masih menggunakan pihak ketiga dari luar sebab adanya keterbatasan pada ketersediaan sumber daya manusia bagian TI atau programmer.

Permasalahan selanjutnya adalah kegagalan dalam memenuhi persyaratan peraturan atau disebut dengan kontrak TI. Dibangunnya aplikasi SIMRS ini diharapkan menyediakan informasi yang akurat dan relevan. Jika tidak memenuhi kriteria tersebut dapat menyebabkan kegagalan dalam persyaratan pembangunan SIMRS. Permasalahan selanjutnya yaitu terdapat pada audit rutin atau laporan penilaian TI. Laporan penilaian terhadap SIMRS masih dinilai sangat kurang dikarenakan pengelolaan sistem yang belum terkendali dapat menyebabkan data tidak diperbarui dengan rutin.

Permasalahan selanjutnya yaitu sumber daya TI yang kurang mencukupi dan kompetensi yang kurang memadai pada bagian TI. Sehingga jika terjadi kesalahan pada sistem harus menghubungi pihak ketiga yang mengembangkan sistem yang sudah terikat kontrak sebelumnya.

e. Faktor Desain 5 Lanskap Ancaman

Faktor desain yang kelima adalah lanskap ancaman, yaitu mengidentifikasi ancaman TI di RSUD Tarakan. Hasil dari identifikasi faktor desain yang kelima dapat dilihat pada gambar 4.5



Gambar 4.5 Faktor Desain Lanskap Ancaman

Gambar 4.5 menunjukan hasil faktor desain kelima yaitu pada lanskap ancaman, DPKP Salatiga memiliki ancaman yang tinggi pada TI yaitu sebesar 70% dikarenakan tidak adanya pelaporan dan juga audit pada SIMRS. Serangan seperti peretasan (hacking dan mallware) pada SIMRS juga termasuk besar dikarenakan sumber daya manusia masih dinilai minim kompetensi dan skillset nya.

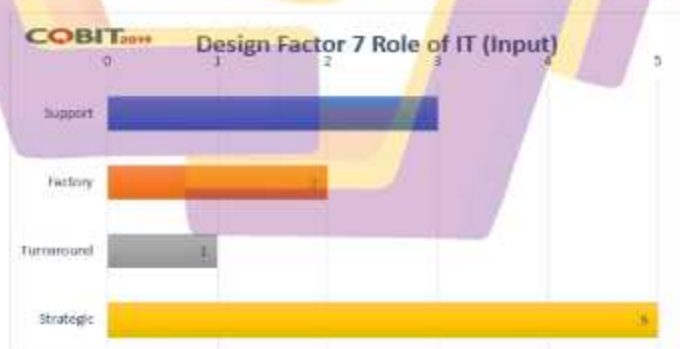
f. Faktor Desain 6 Persyaratan Kepatuhan

Faktor desain yang ke enam adalah persyaratan kepatuhan, yaitu dilakukan proses identifikasi kepatuhan RSUD Trakan terhadap peraturan. Ada tiga level kepatuhan, yaitu level tinggi, normal dan rendah. RSUD Tarakan memiliki kepatuhan pada level tinggi.

Gambar 4.6 Faktor Desain Persyaratan Kepatuhan

g. Faktor Desain 7 Peran dari TI

Faktor desain yang ketujuh adalah peran dari TI, domain ini dilakukan untuk menyesuaikan peran dari TI pada RSUD Tarakan dengan peran dari TI pada proses domain COBIT 2019. Ada empat jenis peran TI dalam perusahaan, yaitu support, factory, strategic dan turnaround. Hasil dari identifikasi faktor desain ketujuh terdapat pada gambar 4.7

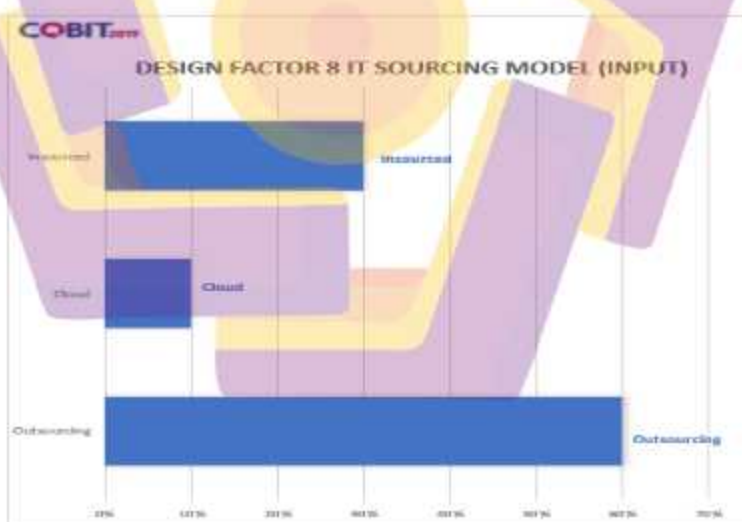


Gambar 4.7 Faktor Desain Peran dari TI

Gambar 4.7 menunjukan hasil dari pemetaan faktor desain yang ketujuh peran dari TI maka didapatkan satu peran dari TI terpilih berdasarkan kesesuaian peran dari TI dengan penilaian tertinggi adalah strategic atau strategi. Artinya TI memiliki peran sangat penting untuk menjalankan dan melakukan inovasi pada proses bisnis dan layanan dalam hal ini terkait SIMRS. Peran dari TI sudah sangat strategis dalam pelayanan yang diberikan pada masyarakat.

h. Faktor Desain 8 Model Sumber Daya TI

Faktor desain yang kedelapan model sumber daya TI, domain ini dilakukan untuk menyesuaikan model sumber daya TI pada RSUD Tarakan dengan model sumber daya TI pada proses domain COBIT 2019. Hasil dari identifikasi faktor desain kedelapan terdapat pada gambar 4.8

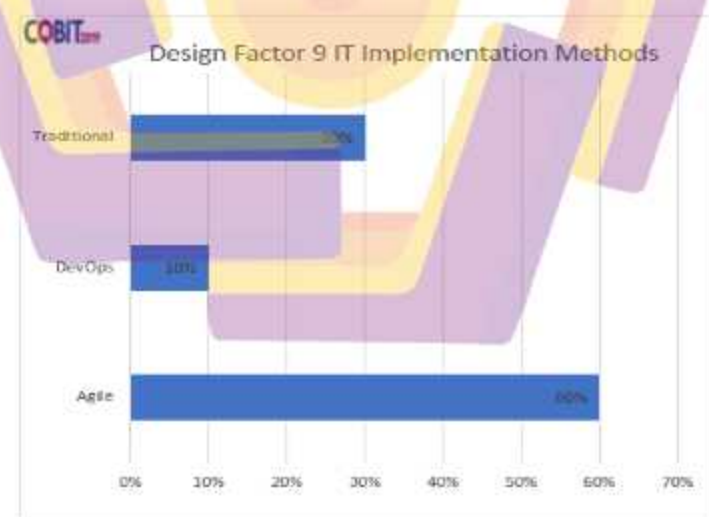


Gambar 4.8 Faktor Desain Model Sumber Daya TI

Gamabr 4.8 menunjukan hasil nilai 60% untuk model outsourcing RSUD Tarakan, karena ITK masih memerlukan sumber daya untuk mengembangkan atau menghasilkan produk layanan yang cenderung rumit, disisi lain terdapat instruksi pemerintah yang meminta untuk menggunakan produk yang sudah disediakan oleh pemerintah.

i. Faktor Desain 9 Metode Implementasi TI

Faktor desain yang kesembilan yaitu adalah metode implementasi TI, Ada tiga jenis metode implementasi TI yang digunakan dalam pengelolaan, yaitu agile dalam pengembangan perangkat lunaknya, DevOps dimana pengembangan perangkat lunak dan operasi TI digabungkan dan traditional dimana merupakan pengembangan yang lebih klasik (waterfall). Hasil dari identifikasi faktor desain kesembilan terdapat pada gambar 4.9

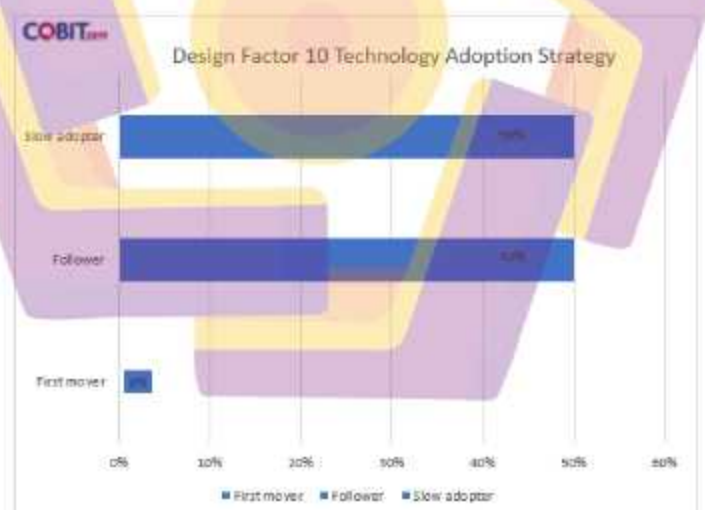


Gambar 4.9 Faktor Desain Implementasi TI

Gambar 4.9 menunjukan hasil dari implementasi TI yang digunakan RSUD Tarakan. Penerapan metode agile pada SIMRS memudahkan dalam proses pengembangan software, metode agile juga membutuhkan waktu yang relatif cepat dan juga tidak membutuhkan resources yang besar. Oleh karena itu metode pengembangan agile diimplementasikan sebelum layanan di rilis. Metode agile bernilai 50%, karena TI yang ada krusial untuk mendukung bisnis proses RSUD.

j. Faktor Desain 10 Strategi Adopsi Teknologi

Faktor desain yang kesepuluh adalah strategi adopsi teknologi, yaitu adalah mengadopsi teknologi pada strategi organisasi yang akan dilakukan dan Ada tiga jenis startegi, yaitu first mover, follower dan slow adaptor. Hasil dari identifikasi faktor desain kesepuluh terdapat pada gambar 4.10



Gambar 4.10 Faktor Desain Strategi Adopsi Teknologi

Gambar 4.10 menunjukan hasil dengan strategi follower karena RSUD Tarakan memiliki sumber daya yang mampu untuk mengimplementasikan perkembangan teknologi informasi dan memilih menjadi pengikut dikarenakan untuk menunggu teknologi baru tersebut digunakan oleh organisasi atau perusahaan lain terlebih dahulu. RSUD Tarakan juga termasuk slow adopter atau bukan orang yang cepat dalam mencoba hal-hal baru dikarenakan tidak semua sumber daya manusia yang yang ada dapat beradaptasi langsung dengan perubahan-perubahan dalam teknologi.

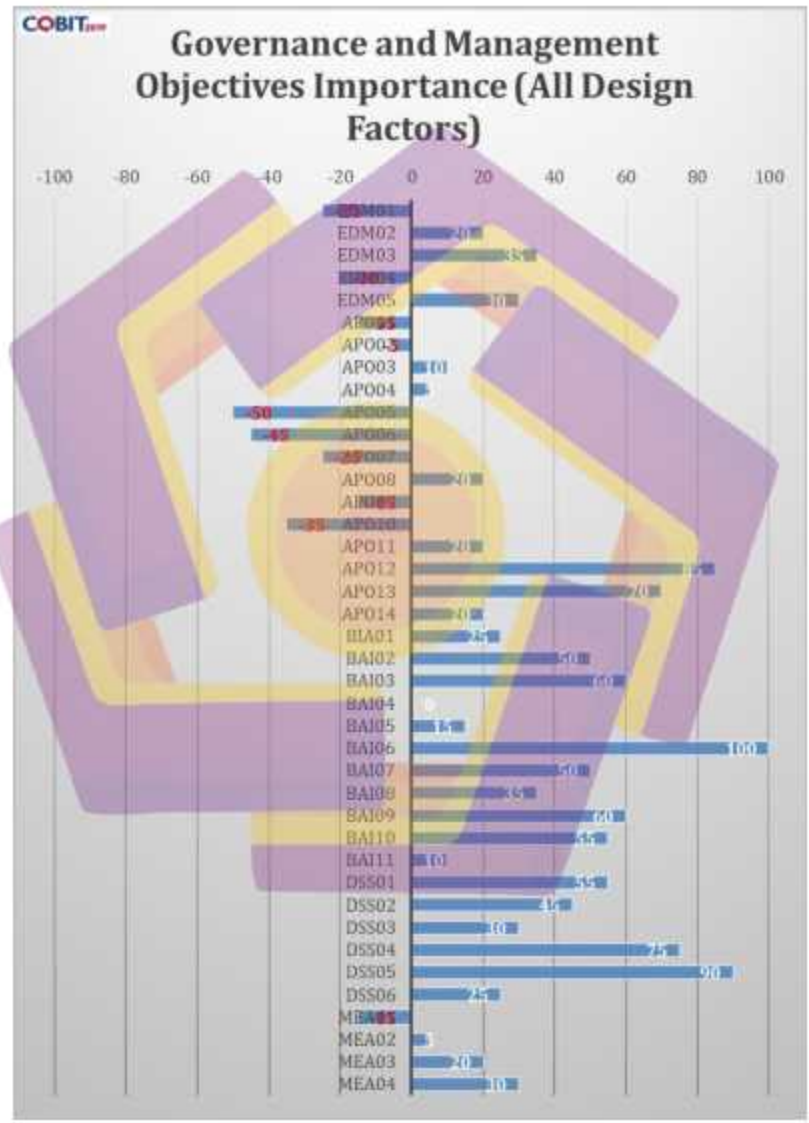
k. Faktor Desain 11 Ukuran Perusahaan

Faktor desain yang kesebelas adalah ukuran perusahaan, merupakan tahap unuk mengidentifikasi ukuran perusahaan dilihat dari jumlah karyawan yang dimiliki. Ada dua jenis ukuran perusahaan dilihat dari jumlah karyawan, yaitu large dan small & medium. RSUD Tarakan termasuk ke dalam ukuran perusahaan large karena memiliki lebih dari 250 karyawan. Hasil dari identifikasi faktor desain kesebelah terdapat pada tabel 4.7

Tabel 4.7. Faktor Desain Ukuran Perusahaan

Jenis Perusahaan	Pilihan Sesuai
Large (Perusahaan dengan lebih dari 250 karyawan tetap)	√
Small dan medium (Perusahaan dengan 50 hingga 250 karyawan tetap)	

Dari total 11 faktor desain, selanjutnya dilakukan identifikasi domain dengan pembobotan dan hasilnya dapat dilihat pada Gambar 4.11.



Gambar 4.11 Grafik hasil faktor desain

Hasil identifikasi tata kelola yang dihasilkan yaitu berupa proses dengan tingkat kemampuan yang disarankan. COBIT 2019 menjelaskan bahwa tingkat kemampuan yang diharapkan untuk skor lebih dari sama dengan 80 membutuhkan tingkat kemampuan 4. Jika skor kemampuan lebih dari sama dengan 50 membutuhkan tingkat kemampuan 3. Apabila skor lebih dari atau sama dengan 25 maka membutuhkan tingkat kemampuan 2, dan skor kurang dari 25 maka proses tersebut harus mencapai tingkat kemampuan 1. Dari hasil desain COBIT 2019 pada RSUD Tarakan didapatkan bahwa yang mendapatkan skor lebih dari atau sama dengan nilai 80 atau yang harus mencapai tingkat kemampuan 4 (Capability Level 4). Hasil identifikasi domain yang terpilih sebagai fokus area, yaitu :

a. APO12 Managed Risk dengan nilai 85
b. BAI06 Managed IT Changes dengan nilai 100
c. DSS05 Managed security services dengan nilai 90

4.2.5 Perencanaan Assesmen

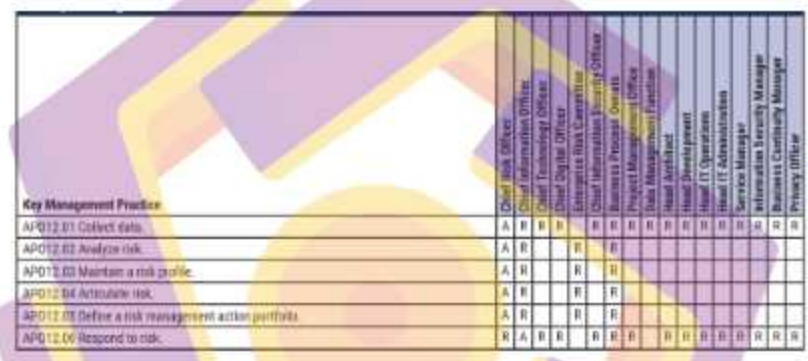
Pada tahap perencanaan asesmen, akan dijelaskan daftar responden untuk pelaksanaan audit sesuai dengan COBIT 2019. Dalam menentukan hasil responden, acuan yang digunakan adalah struktur organisasi RSUD Tarakan yang akan disesuaikan dengan RACI chart yang di anjurkan oleh COBIT 2019.

Dalam RACI chart, hanya yang memiliki peran responsible yang akan dijadikan responden evaluasi. Hal ini karena peran responsible merupakan orang yang bertangung jawab dalam mendapatkan tugas dan melaksanakan tugas tersebut dan juga memastikan aktifitass atau kegiatan operasional berjalan sukses. Berikut

daftar responden pada domain APO 12 Managed risk, DSS 05 Managed security services, dan BAI 06 Managed IT changes pada RSUD Tarakan.

4.2.5.1. Hasil responden pada objek APO 12 Managed risk

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang ikut serta dalam pelaksanaan evaluasi APO 12 managed risk adalah dapat di tunjukan pada gambar 4.12 di bawah ini.



Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Analyze risk.	A	R			R		R										
APO12.03 Maintain a risk profile.	A	R			R		R										
APO12.04 Articulate risk.	A	R			R		R										
APO12.05 Define a risk management action portfolio.	A	R			R		R										
APO12.06 Respond to risk.	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

Gambar 4.12 RACI chart APO 12 Managed risk

Jabatan-jabatan yang bertanda R memiliki arti responsible yaitu merupakan responden yang bertangung jawab pada aktivitas domain ini. Diharapkan responden yang memang melakukan aktivitas sesuai dengan area audit sehingga hasil audit tepat dan dapat dipertangungjawabkan. Untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar diats akan di jabarkan konversinya pada tabel 4.8 dibawah ini.

Tabel 4.8 Hasil identifikasi responden APO 12

No	RACI Chart APO 12 pada COBIT 2019	Struktur Organisasi RSUD Tarakan
1.	Chief Information Officer	-
2.	Chief Technology Officer	-

No	RACI Chart APO 12 pada COBIT 2019	Struktur Organisasi RSUD Tarakan
3	Chief Digital Officer	-
4.	Enterprise Risk Committee	-
5.	Chief Information Security Officer	-
6.	Business Process Owners	Wadir Umum
7.	Project Management Office	-
8.	Data Management Function	-
9.	Head Architect	-
10.	Head Development	Instalasi PDE Devisi SIMRS
11.	Head IT Operations	Instalasi PDE Devisi Hardware
12.	Head IT Administration	-
13.	Service Manager	Kepala Instalasi PDE
14.	Information Security Manager	Instalasi PDE Devisi Network
15.	Business Continuity Manager	-
16.	Privacy Officer	-

Berdasarkan RACI chart yang sudah disesuaikan pada jabatan fungsional pada RSUD Tarakan didapatkan 5 (lima) responden dari 16 (enam belas) peran yang di rekomendasikan COBIT 2019.

4.2.5.2. Hasil responden pada objek DSS 05 Managed security services

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang ikut serta dalam pelaksanaan evaluasi DSS 05 Managed security services adalah dapat di tunjukan pada gambar 4.13 di bawah ini.

Key Management Practice	Chief Information Officer	Chief Information Security Officer	Business Process Owners	Head Human Resources	Head Development	Head IT Operations	Information Security Manager	Privacy Officer
DSS05.01 Protect against malicious software.		A	R	R	R	R	R	
DSS05.02 Manage network and connectivity security.		A			R	R	R	
DSS05.03 Manage endpoint security.		A			R	R	R	
DSS05.04 Manage user identity and logical access.		A	R			R	R	R
DSS05.05 Manage physical access to I&T assets.		A				R	R	R
DSS05.06 Manage sensitive documents and output devices.	A					R		R
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.		A				R	R	R

Gambar 4.13 RACI chart DSS 05 Managed security services

Seperti pada domain APO 12, responden yang diikutsertakan dalam audit adalah yang bertanda R. Diharapkan responden yang memang melakukan aktivitas sesuai dengan area audit sehingga hasil audit tepat dan dapat dipertangungjawabkan. Untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar diats akan di jabarkan konversinya pada tabel 4.9 dibawah ini.

Tabel 4.9 Hasil identifikasi responden DSS 05

No	RACI Chart DSS 05 pada COBIT 2019	Struktur Organisasi RSUD Tarakan
1.	Business Process Owners	Wadir Umum
2.	Head Human Resources	-
3	Head Development	Instalasi PDE Devisi SIMRS
4.	Head IT Operations	Instalasi PDE Devisi Hardware
5.	Information Security Manager	Instalasi PDE Devisi Network
6.	Privacy Officer	-

Berdasarkan RACI chart yang sudah disesuaikan pada jabatan fungsional pada RSUD Tarakan didapatkan 4 (empat) responden dari 6 (enam) peran yang di rekomendasikan COBIT 2019.

4.2.5.3. Hasil responden pada objek BAI 06 Managed IT Changes

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang ikut serta dalam pelaksanaan evaluasi BAI 06 Managed IT Changes adalah dapat di tunjukan pada gambar 4.14 di bawah ini.

Key Management Practice	Chief Information Officer	Business Process Owners	Program Manager	Project Manager	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritize and authorize change requests.	A	R			R	R	R	R	R	R
BAI06.02 Manage emergency changes.	A				R	R	R	R		R
BAI06.03 Track and report change status.	A	R	R	R	R	R	R			
BAI06.04 Close and document the changes.	A	R	R	R	R	R	R		R	

Gambar 4.14 RACI chart BAI 06 Managed IT Changes

Seperti pada domain DSS 05, responden yang diikutsertakan dalam audit adalah yang bertanda R. Diharapkan responden yang memang melakukan aktivitas sesuai dengan area audit sehingga hasil audit tepat dan dapat dipertangungjawabkan. Untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar diats akan di jabarkan konversinya pada tabel 4.10 dibawah ini

Tabel 4.10 Hasil identifikasi responden BAI 06

No	RACI Chart BAI 06 pada COBIT 2019	Struktur Organisasi RSUD Tarakan
1.	Business Process Owners	Wadir Umum
2.	Program Manager	-
3.	Project Manager	-
4.	Head Development	Instalasi PDE Devisi SIMRS
5.	Head IT Operations	Instalasi PDE Devisi Hardware
6.	Services Manager	Kepala Instalasi PDE
7.	Information Security Manager	Instalasi PDE Devisi Network
8.	Business Continuity Manager	-
9.	Privacy Officer	-

Berdasarkan RACI chart yang sudah disesuaikan pada jabatan fungsional pada RSUD Tarakan didapatkan 5 (lima) responden dari 9 (sembilan) peran yang di rekomendasikan COBIT 2019.

4.3 Kuesioner Maturity Model

Pada audit ini, dengan memperhatikan kewajiban, kebutuhan dan kemampuan dan melalui tim mutu menertapkan target tingkat kapabilitas pada level 3 (tiga). Hasil audit tata kelola TI maka perlu dilakukan identifikasi hasil audit dan dikelola sehingga dapat dilakukan Analisa. Dengan menggunakan CMMI (capability maturity model integration) tingkat kapabilitas dapat di defenisikan menjadi 6 tingkatan/level, yaitu :

1. Incomplete – nilai 0, memiliki arti belum ada kegiatan/aktivitas yang berkaitan dengan proses.
2. Initial – nilai 1, memiliki arti kegiatan/aktivitas berkaitan proses sudah dilakukan namun belum ada manajemen dan perencanaan serta tidak berulang.
3. Managed – nilai 2, memiliki arti bahwa proses sudah dilakukan perencanaan dan manajemen walaupun belum terstandarrisasi, tidak tergantung pada orang.
4. Defined – nilai 3, memiliki arti bahwa setiap kegiatan/aktifitas sudah tercantum dalam instruksi kerja atau SOP, proses menjadi lebih stabil dan berulang , diharapkan hasilnya konsisten.
5. Quantitative – nilai 4, memillik arti bahwa setiap kegiatan sudah memiliki tujuan yang terukur untuk kualitas dan produktivitasnya, salah satu cirinya adalah sudah ada activity based costing.
6. Optimized – nilai 5, memiliki arti bahwa proses pengembangan system terstandarisasi secara continue dimonitor dan di tingkatkan berdasarkan Analisa atau evaluasi. Cirinya adalah adanya mekanisme pencegahan kegagalan, mekanisme evaluasi dan peningkatan kualitas proses.

Penilaian ini yang akan menjadi tolak ukur dalam melakukan Analisa tingkat kapabilitas tata kelola teknologi informasi pada RSUD Tarakan.

Berikut hasil audit pada masing masing domain yang terpilih.

4.3.1 Hasil Rekapitulasi Audit pada domain APO12 Managed Risk

a. APO 12.01 Collect data

Tabel 4.11. Hasil rekapitulasi kuesioner APO 12.01

No	Deskripsi	Skor Input As Is				
		R1	R2	R3	R4	R5
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait resiko TI	0	1	1	1	1
2	Catat data terkait resiko terkait TI yang relevan dan signifikan di lingkungan internal dan external RSUD	0	1	1	1	1
3	Mengadopsi atau mendefinisikan resiko untuk definisi yang konsisten dari skenario resiko dan dampak	0	1	1	1	1
4	Catat data tentang peristiwa resiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak	0	1	1	1	1
5	Survei dan analisis data resiko TI terkait kerugian dari data dan tren yang tersedia secara eksternal.	0	1	1	0	1
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan konstribusi umum faktor di berbagai peristiwa.	0	0	0	0	0
7	Tentukan kondisi spesifik yang dapat mempengaruhi resiko	1	1	1	1	1
8	Lakukan analisis faktor resiko secara berkala untuk mengidentifikasi masalah resiko barau atau yang muncul dan untuk mendapatkan pemahaman tentang faktor resiko internal dan eksternal terkait.	0	1	1	1	1
		0.13	0.88	0.88	0.75	0.88
rata – rata		0.70				

Berdasarkan hasil tabel 4.11 di atas, audit APO 12.01 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.70 atau tingkat 1. Fakta yang ditemukan adalah :

1. RSUD Tarakan telah merancang kegiatan pencatatan data sesuai kebutuhan RSUD.

2. Pencatatan data dan insiden dilakukan oleh pranata komputer sebagai bagian dari laporan kerja harian pegawai dan belum sebagai produk instansi/perusahaan.

b. APO 12.02 Analyze Risk

Tabel 4.12. Hasil rekapitulasi kuesioner APO 12.02

No	Deskripsi	Skor Input				
		As Is				
		R1	R2	R3	R4	R5
1	Menentukan cakupan yang tepat dari upaya analisis resiko, dengan mempertimbangkan semua faktor resiko.	1	1	1	0	0
2	Membangun dan memperbarui scenario resiko TI secara teratur, identifikasi kerugian terkait TI.	0	1	0	0	0
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario resiko TI. Mempertimbangkan semua faktor resiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	1	1	1	1	1
4	Bandingkan resiko saat ini (eksposur kerugian terkait TI) dengan toleransi resiko yang dapat diterima.	0	1	1	1	1
5	Mengusulkan respon resiko untuk resiko yang melebihi tingkat toleransi.	1	1	1	1	1
6	Identifikasi persyaratan dan target untuk respon mitigasi resiko yang optimal.	0	1	0	0	0
7	Validasi hasil analisis resiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	0	0	0	0	0
8	Menganalisis manfaat dari opsi respon resiko yang dipilih . konfirmasikan respon resiko yang optimal.	0	0	0	0	0
		0.38	0.75	0.50	0.38	0.38
rata – rata		0.48				

Berdasarkan hasil tabel 4.12 di atas, audit APO 12.02 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.48 atau tingkat 1. Fakta yang ditemukan adalah :

1. RSUD Tarakan sudah mencoba memetakan resiko namun belum dilakukan analisa, hal ini terlihat pada dokumen identifikasi resiko dan peluang.
2. Setiap indentifikasi resiko belum ada informasi respon sehingga belum dapat dapat dibuktikan perencanaan respon terhadap resiko yang ada.

c. APO 12.03 Maintain A Risk Profile

Tabel 4.13. Hasil rekapitulai kuesioner APO 12.03

No	Deskripsi	Skor Input As Is				
		R1	R2	R3	R4	R5
1	Menginventarisir proses layanan TI dan proses bisnis. Identifikasi pensonel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.	0	1	1	1	1
2	Menentukan dan menyetujui layanan TI dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.	1	1	0	0	0
3	Mengumpulkan skenario resiko saat ini menurut kategori, lini bisnis, dan area fungsional	0	1	1	1	1
4	Secara teratur mendata semua informasi profil resiko dan menggabungkannya ke dalam profil resiko gabungan.	0	0	0	0	0
5	Mendata informasi tentang status rencana tindakan resiko untuk dimasukkan dalam profil resiko TI RSUD.	0	0	0	0	0
6	Berdasarkan semua data profil resiko, tentukan seperangkat indikator resiko yang memungkinkan	0	0	0	0	0

Tabel 4.13. Hasil rekapitulai kuesioner APO 12.03 (Lanjutan)

	Identifikasi dan monitoring resiko saat ini secara tepat					
7	Mendata informasi tentang peristiwa resiko TI yang telah terwujud untuk dimasukkan dalam profil resiko TI RSUD.					
		0	0	0	0	0
		0.14	0.43	0.29	0.29	0.29
Rata - Rata		0.29				

Berdasarkan hasil Tabel 4.13 diatas, audit APO 12.03 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.29 atau tingkat 1. Fakta yang ditemukan adalah :

1. Penentuan layanan TI dan manajemennya merupakan bagian dari kegiatan layanan dalam operasional, namun belum ditemukan dokumen proses yang tertuang;
2. Belum ditemukan proses adopsi atau analisis dari contoh manajemen TI hasil benchmarking atau interkomparasi.

d. APO 12.04 Articulate Risk

Tabel 4.14. Hasil Rekapitulasi Kuesioner APO 12.04

No	Deskripsi	Skor Input				
		As Is				
		R1	R2	R3	R4	R5
1	Laporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam format tertentu yang berguna untuk mendukung keputusan RSUD Tarakan.	1	1	0	0	0
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait TI.	0	1	1	1	1

Tabel 4.14. Hasil Rekapitulasi Kuesioner APO 12.04 (Lanjutan)

3	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, dan gap.	1	1	0	0	0
4	Secara berkala, identifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan.	0	1	1	1	1
5	Meninjau hasil penilaian pihak ketiga yang obyektif dan audit internal. Sertakan mereka di profil risiko.	0	1	1	1	1
		0.40	1	0.60	0.60	0.60
Rata – Rata		0.64				

Berdasarkan hasil Tabel 4.14 diatas, audit APO 12.04 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.64 atau tingkat 1. Fakta yang ditemukan adalah :

1. Proses identifikasi risiko dan peluang dalam proses bisnis telah dilakukan dan terdokumentasi, pelaporan kepada stakeholder belum disampaikan dalam kegiatan audit internal;
2. Belum ditemukan format pelaporan profil dan manajemen risiko TI pada RSUD Tarakan.

e. APO 12.05 Define a risk management action portfolio

Tabel 4.15 Hasil Rekapitulasi Kuesioner APO 12.05

No	Deskripsi	Skor Input				
		As Is				
		R1	R2	R3	R4	R5
1	Klasifikasikan aktivitas pengendalian dan petakan pada skenario risiko TI.	0	1	1	1	1
2	Tentukan apakah setiap entitas organisasi memantau risiko dan memiliki peran.	1	1	1	1	1

Tabel 4.15 Hasil Rekapitulasi Kuesioner APO 12.05 (Lanjutan)

3	Buat proposal proyek yang dirancang untuk mengurangi risiko dan / atau proyek yang memiliki peluang dengan mempertimbangkan risiko TI.	1	1	1	1	1
		0.67	1	1	1	1
Rata – Rata		0.93				

Berdasarkan hasil Tabel 4.15 diatas, audit APO 12.05 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.93 atau tingkat 1. Hal ini dapat diartikan bahwa kegiatan mendefinisikan profil manajemen risiko sudah dilakukan melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif. Fakta yang ditemukan adalah :

1. Pada proses audit internal, pembahasan identifikasi risiko dan peluang telah dilakukan dengan harapan dapat diketahui oleh seluruh pegawai, namun pegawai yang terlibat dalam audit internal terbatas;
2. Identifikasi risiko dan peluang sudah ada PIC pada masing-masing topik namun belum ditemukan distribusi ke pegawai sehingga belum jelas tanggung jawabnya.

f. APO 12.06 Respon to Risk

Tabel 4.16 Hasil Rekapitulasi Kuesioner APO 12.06

No	Deskripsi	Skor Input				
		As Is				
		R1	R2	R3	R4	R5
1	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika	0	1	1	1	1

Tabel 4.16 Hasil Rekapitulasi Kuesioner APO 12.06 (Lanjutan)

	peristiwa risiko dapat menyebabkan terhentinya operasional bisnis.					
2	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.	1	1	1	1	1
3	Komunikasikan respon risiko kepada pengambil keputusan sebagai bagian dari pelaporan dan pembaharuan profil risiko.	0	1	1	1	1
4	Memeriksa kerugian masa lalu dan peluang yang hilang dan menentukan akar penyebabnya.	1	0	1	1	1
5	Komunikasikan akar masalah, respons risiko dan perbaikan proses kepada pengambil keputusan yang tepat.	1	1	1	1	1
		0.60	0.80	1	1	1
Rata – Rata		0.88				

Berdasarkan hasil Tabel 4.16 diatas, audit APO 12.06 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.88 atau tingkat 1. Hal ini dapat diartikan bahwa kegiatan respon terhadap risiko sudah dilakukan melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif. Fakta yang ditemukan adalah :

1. Belum ada bukti penerapan perencanaan risiko pada saat terjadi insiden.
2. Perencanaan risiko dibuktikan dengan adanya proses kegiatan identifikasi risiko dan peluang, namun belum adanya evaluasi dan standardisasi.

g. Hasil keseluruhan audit domain APO 12 managed risk

Berdasarkan diagram representasi pada gambar 4.15 dibawah diperoleh kesimpulan bahwa tingkat kapabilitas pada domain APO 12 Managed Risk sebesar 0.65 satau pada level 1 artinya proses APO 12 sudah dilakukan namun belum

terencana dan belum terdokumentasikan dengan baik. Adapun target yang ingin dicapai yaitu tingkaty kapabilitas pada level 3, sehingga terdapat gap. Rekomendasi pada domain APO 12 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

Gambar 4.15 Diagram Representasi Hasil Audit APO 12

4.3.2. Hasil Rekapitulasi Audit pada Domain DSS 05 Managed Security Services

a. DSS 05.01 Protect against malicious software

Tabel 4.17 Hasil Rekapitulasi Kuesioner DSS 05.01

No	Deskripsi	Skor Input As Is			
		R1	R2	R3	R4
1	Instal dan aktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas pemrosesan.	1	1	1	1
2	Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (misalnya, spyware, email phishing).	1	1	0	1
3	Komunikasikan kesadaran akan ancaman malware. Lakukan pelatihan berkala tentang malware dalam email dan penggunaan internet.	1	1	1	1

Tabel 4.17 Hasil Rekapitulasi Kuesioner DSS 05.01 (Lanjutan)

4	Mendistribusikan anti virus secara terpusat.	0	1	0	1
5	Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau keamanan produk dan layanan vendor).	0	0	0	1
		0.80	0.80	0.40	1
Rata – Rata		0.75			

Berdasarkan hasil Tabel 4.17 diatas, audit DSS 05.01 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.75 atau tingkat 1. Fakta yang ditemukan adalah :

1. Belum ditemukan kegiatan atau perencanaan pelatihan khusus mengenai bahaya malware, penggunaan email dan internet yang baik pada user RSUD Tarakan.
2. Evaluasi terhadap potensi ancaman security belum dilakukan.

b. DSS 05.02 Manage network and connectivity security

Tabel 4.18 Hasil Rekapitulasi Kuesioner DSS 05.02

No	Deskripsi	Skor Input			
		As Is			
		R1	R2	R3	R4
1	Izinkan hanya perangkat resmi yang memiliki akses ke informasi RSUD dan jaringan RSUD. Konfigurasi perangkat ini untuk entri kata sandi.	1	1	1	1
2	Menerapkan mekanisme penyaringan jaringan, seperti firewall.	1	1	1	1
3	Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.	1	1	1	1
4	Konfigurasi peralatan jaringan dengan cara yang aman.	1	1	1	1

Tabel 4.18 Hasil Rekapitulasi Kuesioner DSS 05.02 (Lanjutan)

5	Berdasarkan penilaian risiko dan kebutuhan bisnis, menetapkan dan memelihara kebijakan keamanan konektivitas.	0	0	0	0
6	Menetapkan mekanisme terpercaya untuk transformasi informasi yang aman.	0	1	1	1
7	Melakukan pengujian keamanan sistem secara berkala untuk menentukan kecukupan perlindungan sistem.	0	0	0	0
		0.57	0.71	0.71	0.71
Rata – Rata		0.68			

Berdasarkan hasil Tabel 4.18 diatas, audit DSS 05.02 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.68 atau tingkat 1. Fakta yang ditemukan adalah :

1. Belum ada bukti pelaksanaan pengujian keamanan sistem pada RSUD Tarakan.
2. Penggunaan akun tertentu untuk mengakses jaringan dan server sudah diterapkan namun belum ditemukan manajemen akun.

c. DSS 05.03 Manage endpoint security

Tabel 4.19 Hasil Rekapitulasi Kuesioner DSS 05.03

No	Deskripsi	Skor Input			
		As Is			
		R1	R2	R3	R4
1	Konfigurasi sistem operasi dengan cara yang aman.	1	1	1	1
2	Menerapkan mekanisme penguncian perangkat.	0	1	1	1
3	Kelola akses dan kontrol jarak jauh (mis., perangkat seluler, teleworking).	0	1	1	1
4	Kelola konfigurasi jaringan dengan cara yang aman.	0	1	1	1

Tabel 4.19 Hasil Rekapitulasi Kuesioner DSS 05.03 (Lanjutan)

5	Menerapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.	1	1	1	1
6	Lindungi integritas sistem.	1	1	1	1
7	Memberikan perlindungan fisik perangkat titik akhir.	1	1	1	1
8	Kelola akses jahat melalui email dan browser web. Misalnya, blokir situs web tertentu.	0	1	0	1
		0.50	1	0.88	1
Rata – Rata		0.84			

Berdasarkan hasil Tabel 4.19 diatas, audit DSS 05.03 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.84 atau tingkat 1. Fakta yang ditemukan adalah :

1. Seluruh perangkat komputer terutama pada bagian layanan menggunakan password, dan penetapan user sudah dilakukan pada masing-masing unit atau instalasi.
2. Situs web tertentu telah diblokir pada saat menggunakan jaringan kantor namun belum dilakukan evaluasi dan pengujian secara berkala. RSUD Tarakan telah mengklaim bahwa aktivitas blok telah dilakukan.

d. DSS 05.04 Manage user identity and logical access

Tabel 4.20 Hasil Rekapitulasi Kuesioner DSS 05.04

No	Deskripsi	Skor Input			
		As Is			
		R1	R2	R3	R4
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan.	1	1	1	1
2	Mengelola semua perubahan pada hak akses (pembuatan, modifikasi dan penghapusan) secara tepat waktu hanya berdasarkan	0	1	1	0

Tabel 4.20 Hasil Rekapitulasi Kuesioner DSS 05.04 (Lanjutan)

	persetujuan dan transaksi terdokumentasi yang disahkan oleh personel yang berwewenang.				
3	Pastikan pemantauan pada akun yang memiliki hak istimewa.	0	1	1	1
4	Berkoordinasi dengan unit bisnis untuk memastikan bahwa semua peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam aplikasi proses bisnis.	0	1	1	0
5	Lakukan analisis pasca latihan untuk evaluasi.	0	0	0	0
6	Mengautentikasi semua akses ke aset informasi berdasarkan peran individu atau aturan bisnis. Berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan.	0	0	1	1
7	Menjaga jejak akses ke informasi tergantung pada tingkat kerahasiaan.	0	0	1	0
8	Lakukan tinjauan manajemen secara rutin pada semua akun dan hak istimewa terkait.	0	0	0	0
		0.13	0.50	0.75	0.38
Rata – Rata		0.44			

Berdasarkan hasil Tabel 4.20 diatas, audit DSS 05.04 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.44 atau tingkat 1. Fakta yang ditemukan adalah :

1. Evaluasi pasca pelatihan belum dilakukan;
2. Pemberian hak akses SIMRS sesuai peran individu dan unit bisnisnya, namun belum dilakukan monitoring dan evaluasi secara berkala untuk akun dengan hak akses intimewa.

e. DSS 05.05 Manage physical access to IT assets

Tabel 4.21 Hasil Rekapitulasi Kuesioner DSS 05.05

No	Deskripsi	Skor Input As Is			
		R1	R2	R3	R4
1	Daftarkan semua pengunjung, termasuk kontraktor dan vendor.	1	1	1	1
2	Pastikan semua personel menampilkan identifikasi yang disetujui dengan benar setiap saat.	1	1	1	1
3	Mengharuskan pengunjung untuk didampingi setiap saat berada di lokasi.	1	1	1	1
4	Batasi dan pantau akses ke situs TI yang sensitif dengan menetapkan batasan perimeter, seperti pagar, dinding, dan keamanan perangkat di pintu interior dan eksterior.	1	1	1	1
5	Kelola permintaan untuk mengizinkan akses resmi yang sesuai ke fasilitas komputasi.	1	1	1	1
6	Pastikan profil akses tetap terkini. Akses dasar ke situs TI (ruang server, gedung, area atau zona) pada fungsi pekerjaan dan tanggung jawab.	1	1	1	1
7	Lakukan pelatihan kesadaran keamanan informasi fisik secara teratur. Panduan Terkait (Standar, Kerangka Kerja, Persyaratan Kepatuhan).	0	0	0	0
		0.86	0.86	0.86	0.86
Rata – Rata		0.86			

Berdasarkan hasil Tabel 4.21 diatas, audit DSS 05.05 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.86 atau tingkat 1. Fakta yang ditemukan adalah :

1. Setiap pengunjung telah dipersyaratkan mengisi form kunjungan dan mengenakan tanda pengenal di pos satpam sebelum memasuki area situs TI.
2. Pengunjung akan ditemani oleh pegawai TI, namun belum ada penerapan daerah terlarang pada ruang server dan control room CCTV.

3. Belum ditemukan agenda pelatihan tentang kesadaran keamanan informasi fisik, termasuk server.

f. DSS 05.06 Manage sensitive documents and output devices

Tabel 4.22 Hasil Rekapitulasi Kuesioner DSS 05.06

No	Deskripsi	Skor Input			
		As Is			
		R1	R2	R3	R4
1	Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif perusahaan.	0	0	0	0
2	Tetapkan hak akses istimewa kepada jabatan tertentu berdasarkan keputusan manajemen.	1	0	0	0
3	Buat inventarisasi dokumen sensitif perusahaan.	0	0	0	0
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.	0	1	1	0
		0.25	0.25	0.25	0
Rata – Rata		0.19			

Berdasarkan hasil Tabel 4.22 diatas, audit DSS 05.06 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,19 atau tingkat 1. Fakta yang ditemukan adalah :

1. Setiap dokumen yang bersifat confidential dikelola oleh personel tertentu namun masih belum ada prosedur secara legal atas penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif tersebut.
2. Belum ditemukan bukti kegiatan penanganan khusus terhadap dokumen penting RSUD Tarakan.

g. DSS 05.07 Manage vulnerabilities and monitor the infrastructure for security-related events

Tabel 4.23 Hasil Rekapitulasi Kuesioner DSS 05.07

No	Deskripsi	Skor Input As Is			
		R1	R2	R3	R4
1	Terus gunakan tools untuk mengidentifikasi kerentanan keamanan informasi.	0	0	0	0
2	Tentukan dan komunikasikan skenario risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.	1	1	1	1
3	Tinjau data peristiwa secara teratur untuk mengetahui potensi insiden.	0	0	0	0
4	Pastikan kejadian terkait keamanan dikelola tepat waktu untuk identifikasi potensi risiko.	0	0	0	0
5	Catat kejadian terkait keamanan dan simpan catatan untuk periode yang sesuai.	0	0	0	1
		0.6	0.4	0.6	0.6
Rata – Rata		0.25			

Berdasarkan hasil Tabel 4.23 diatas, audit DSS 05.07 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,25 atau tingkat 1. Fakta yang ditemukan adalah :

1. Belum ditemukan kejadian keamanan, namun aktivitas tersebut telah menjadi tupoksi dari pranata komputer pada RSUD Tarakan yang harus dicatat dalam laporan kerja harian;
2. Belum ada mekanisme peninjauan ulang terhadap kejadian atau aktivitas terkait keamanan.

h. Hasil keseluruhan audit domain DSS 05 Managed security services

Berdasarkan diagram representasi pada gambar 4.16 di bawah diperoleh kesimpulan bahwa tingkat kapabilitas pada domain DSS 05 Managed security services sebesar 0,57 atau pada level 1 artinya proses DSS 05 sudah dilakukan namun belum terencana dan belum terdokumentasi dengan baik. Adapun target

yang ingin dicapai yaitu tingkat kapabilitas level 3, sehingga terdapat gap rekomendasi pada domain DSS 05 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

Gambar 4.16 Diagram Representasi Hasil Audit DSS 05

4.3.3. Hasil Rekapitulasi Audit pada Domain BAI06 Build, Acquire, and Implement

a. BAI 06.01 Evaluate, prioritize and authorize change request

Tabel 4.24 Hasil Rekapitulasi Kuesioner BAI 06.01

No	Deskripsi	Skor Input As Is				
		R1	R2	R3	R4	R5
1	Permintaan perubahan pada proses bisnis dan TI termasuk infrastruktur, sistem, dan aplikasi harus dilakukan secara formal dan disetujui oleh manajemen	0	0	0	0	0
2	Kategorikan semua perubahan yang diminta (misalnya, proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, perangkat lunak aplikasi yang dibeli/dikemas) dan menghubungkan item konfigurasi yang terpengaruh terhadap perubahan	1	1	1	1	1
3	Memprioritaskan semua perubahan yang diminta berdasarkan persyaratan bisnis dan teknis, sumber daya yang.	1	1	1	1	1

Tabel 4.24 Hasil Rekapitulasi Kuesioner BAI 06.01 (Lanjutan)

	dibutuhkan, dan alasan hukum, peraturan dan secara kontraktual.					
4	Perubahan resmi disetujui oleh pemilik proses bisnis, manajer layanan dan pemangku kepentingan teknis TI serta perubahan dengan resiko rendah yang relatif sering harus di setujui sebelumnya sebagai perubahan standar.	0	0	0	0	0
5	Rencana dan jadwalkan semua perubahan yang disetujui.	0	0	0	0	0
6	Merencanakan, mengevaluasi dan menilai semua permintaan perubahan TI secara terstruktur dengan melibatkan manajemen RSUD.	1	1	1	1	1
7	Pada proses manajemen perubahan pertimbangkan dampak penyedia layanan yang dikontrak (misalnya, pemrosesan bisnis yang dialihdayakan, infrastruktur, pengembangan aplikasi, dan layanan bersama). Sertakan integrasi proses manajemen perubahan RSUD dengan proses manajemen perubahan penyedia layanan dan dampaknya terhadap persyaratan kontrak dan SLA.	0	0	0	0	0
		0.43	0.43	0.43	0.43	0.43
Rata – Rata		0.43				

Berdasarkan hasil Tabel 4.24 diatas, audit BAI 06.01 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.43 atau tingkat 1. Fakta yang ditemukan adalah :

1. Permintaan perubahan pada sistem dan aplikasi disetujui oleh manajemen namun tidak dilakukan secara formal dan terdokumentasi.

2. Perubahan dilakukan tanpa mempertimbangkan dampak terhadap layanan, integrasi data, dan penyedia layanan SLA sehingga akan berdampak pada business continuity plans (BCP).

b. BAI 06.02 Manage emergency changes

Tabel 4.25 Hasil Rekapitulasi Kuesioner BAI 06.02

No	Deskripsi	Skor Input				
		As Is				
		R1	R2	R3	R4	R5
1	Menentukan mana yang merupakan perubahan darurat	1	1	1	1	1
2	Prosedur perubahan darurat terdokumentasi dan meliputi untuk menyatakan, menilai, menyetujui awal, mengotorisasi, dan mencatat setelah perubahan darurat.	0	0	0	0	0
3	Setelah perubahan darurat diterapkan lakukan verifikasi pengaturan akses darurat untuk diotorisasi, didokumentasikan dan di cabut.	0	0	0	0	0
4	Melakukan monitoring semua perubahan darurat dan melakukan tinjauan pasca implementasi yang melibatkan semua pihak terkait. Tinjauan harus mempertimbangkan dan memulai Tindakan korektif berdasarkan akar penyebab seperti masalah dengan proses bisnis, pengembangkan dan pemeliharaan sistem aplikasi, lingkungan pengembangan dan pangujian, dokumentasi dan manual, serta integritas data.	0	0	0	0	0
		0.25	0.25	0.25	0.25	0.25
Rata – Rata		0.25				

Berdasarkan hasil Tabel 4.25 diatas, audit BAI 06.02 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.25 atau tingkat 1. Fakta yang ditemukan adalah :

1. Telah di tentukan mana yang menjadi perubahan dan direalisasikan namun secara prosedur belum terdokumentasi, belum di verifikasi dan tidak dilakukan monitoring terhadap hasil dari perubahan darurat tersebut.

c. BAI 06.03 Track and report change status

Tabel 4.26 Hasil Rekapitulasi Kuesioner BAI 06.03

No	Deskripsi	Skor Input As Is				
		R1	R2	R3	R4	R5
1	Mengkategorikan permintaan perubahan dalam proses klasifikasi (misalnya dengan status ditolak, disetujui tetapi belum di mulai, disetujui dan dalam proses, dan selesai)	1	1	1	1	1
2	Menerapkan laporan status perubahan sehingga perubahan selanjutnya dapat dilacak dari awal hingga disposisi akhir	0	0	0	0	0
3	Monitoring akan prioritas dari perubahan yang berlangsung dan pastikan bahwa semua perubahan yang disetujui diselesaikan tepat waktu.	1	1	0	1	0
4	Berlakukan sistem pelacakan dan pelaporan untuk semua permintaan perubahan	0	0	0	0	0
		0.50	0.50	0.25	0.50	0.25
Rata – Rata		0.40				

Berdasarkan hasil Tabel 4.26 diatas, audit BAI 06.03 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.40 atau tingkat 1. Fakta yang ditemukan adalah :

1. RSUD Tarakan telah melakukan proses klasifikasi dengan mengkategorikan permintaan perubahan dan monitoring juga telah di lakukan namun untuk pelaporannya belum dilakukan secara detail dan belum terdokumentasi.

d. BAI 06.04 Close and document the changes

Tabel 4.27 Hasil Rekapitulasi Kuesioner BAI 06.04

No	Deskripsi	Skor Input				
		As Is				
		R1	R2	R3	R4	R5
1	Menyertakan perubahan di dokumentasi dalam prosedur manajemen. Contoh dokumentasi prosedur operasional bisnis dan TI, kontinuitas bisnis dan dokumentasi	0	1	0	1	0
2	Menetapkan periode penyimpanan untuk dokumentasi baik sebelum dan sesudah dilakukan perubahan, serta dokumentasi pengguna.	0	1	0	1	0
3	Melakukan dokumentasi subjek perubahan ke tingkat tinjauan yang sama dengan perubahan yang sebenarnya.	0	0	0	0	0
		0	0.67	0	0.67	0
Rata – Rata		0.44				

Berdasarkan hasil Tabel 4.27 diatas, audit BAI 06.04 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.44 atau tingkat 1. Fakta yang ditemukan adalah :

1. Aktifitas perubahan yang terjadi hingga selesai peru bahan tidak dilakukan proses dokumentasi baik dokumentasi prosedur operasional bisnis dan TI, dokumentasi user, dokumentasi subjek, serta penyimpanan dokumentasi.

Berdasarkan diagram representasi pada gambar 4.17 di bawah diperoleh kesimpulan bahwat ingkat kapabilitas pada domain BAI 06 Build, Acquire and Implement sebesar 0,38 atau pada level 1 artinya proses BAI 06 sudah dilakukan namun belum terencana dan belum terdokumentasi dengan baik. Adapun target yang ingin dicapai yaitu tingkat kapabilitas level 3, sehingga terdapat gap

rekomendasi pada domain BAI 06 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

Gambar 4.17 Diagram Representasi Hasil Audit BAI 06

4.3.4 Rekapitulasi Hasil Audit

Adapun rekapitulasi hasil audit tata kelola teknologi informasi RSUD Tarakan menggunakan framework COBIT 2019 dapat ditunjukan pada tabel 4.27. Dan secara rata-rata menunjukan angka 0.53 atau pada tingkat kapabilitas level 1. Sedangkan gap atau kesenjangan pada tiap domain dapat tunjukan pada gambar tabel 4.28 dan gambar 4.18.

Tabel 4.28 Hasil Rekapitulasi Audit

No	Domain	Tingkat Kapabilitas Saat ini	Tingkat Kapabilitas Target	Gap
1	APO 12	0.65	3	2
2	DSS 05	0.57	3	2
3	BAI 06	0.38	3	2
Rata – Rata		0.53	3	2

Gambar 4.18. Tingkat kapabilitas tata kelola TI RSUD Tarakan

Berikut gap analysis SIMRS / aplikasi yang berjalan di RSUD Tarakan terlihat pada tabel 4.29 berikut.

Tabel 4.29 Analisis Gap Aplikasi Portofolio RSUD Tarakan

No	No. Aplikasi	Temuan	Rencana	Pengembangan
1	Inova.1.1 Modul Pendaftaran	Registrasi pasien BPJS dilakukan 2 kali, dengan SIMRS dan dengan sstem dari BPJS	Registrasi hanya dilakukan sekali saja	Membuat bridging sistem antara aplikasi BPJS dengan SIMRS
2	Agape.2.1 DPI Logistik	Agape.2.1. merupakan sistem tersendiri (stand alone)	Integrasi data antara Agape.2.1 dengan SIMRS	Membuat bridging sistem antara Agape.2.1 dengan Inova.1.25, Inova.1.22, Inova.1.14
3	Agape.2.2 DPI Farmasi	Agape.2.2. merupakan sistem tersendiri (stand alone)	Integrasi data antara Agape.2.1 dengan SIMRS	Membuat bridging sistem antara Agape.2.1 dengan Inova.1.7, Inova.1.22, Inova.1.14
4	RIS.3.1	RIS.3.1 merupakan sistem tersendiri (stand alone)	Integrasi data hasil radiologi antara SIMRS dengan RIS.3.1	Membuat bridging sistem antara RIS.3.1 dengan Inova.1.6

Tabel 4.29 Analisis Gap Aplikasi Portofolio RSUD Tarakan (Lanjutan)

5	LIS.4.1	LIS.4.1 merupakan sistem tersendiri (stand alone)	Integrasi data ahasil laboratorium antara SIMRS dengan LIS.4.1	Membuat bridging sistem antara LIS.4.1 dengan Inova.1.5
6	Laporan SIMRS	Beberapa laporan masih belum sesuai dengan standar SIRS online V6	Laporan sudah sesuai dengan standar SIRS online V6	Standarisasi data dan format laporan sesuai dengan SIRS online V6
7	Tata keloal SI-TI	Belum memiliki standar dan tata kelola yang baik	Tata kelola SI-TI sesuai dengan permenkes tentang SIMRS dan standar akreditasi SNARS 1.1	Standarisasi tata kelola SI-TI sesuai dengan aturan dan standar yang ada

4.4. Rekomendasi Perbaikan

Dalam proses audit teknologi informasi, rekomendasi perbaikan diperlukan agar kekurangan ataupun kelemahan sumber daya teknologi informasi (TI) perusahaan dapat diminimalisir atau bahkan dihilangkan. Dalam upaya untuk meningkatkan tingkat kapabilitas pengelolaan TI saat ini agar selaras dengan tingkat kapabilitas pengelolaan TI yang telah diharapkan oleh RSUD Tarakan tersebut, diperlukannya perbaikan dari proses TI yang ada secara bertahap sesuai dengan prioritas. Berikut rekomendasi perbaikan untuk peningkatan tingkat kapabilitas proses TI dapat dilihat pada tabel 4.30 di bawah ini :

Tabel 4.30. Rekomendasi Hasil Audit

No.	Rekomendasi	Temuan	Domain Diperbaiki
1	1. Menetapkan template formal untuk laporan catatan data insiden, maka pelaporan dilakukan	1. RSUD Tarakan telah merancang kegiatan pencatatan data sesuai kebutuhan RSUD.	APO 12.01

Tabel 4.30. Rekomendasi Hasil Audit (Lanjutan)

	melalui sistem informasi berbasis web agar data tersebut mudah diolah dan diakses. 2. Direkomendasikan untuk pengembangan aplikasi ERM (enterprise risk manajemen)	2. RSUD Tarakan telah merancang kegiatan pencatatan data sesuai kebutuhan RSUD. 3. Pencatatan data dan insiden dilakukan oleh pranata komputer sebagai bagian dari laporan kerja harian pegawai dan belum sebagai produk instansi/perusahaan.	APO 12.01
2	1. RSUD Tarakan diharapkan melakukan analisa pada kegiatan identifikasi risiko TI dengan dibuktikan adanya penggunaan data pendukung pada saat identifikasi setiap risiko TI 2. Pengolahan data dari sistem informasi insiden yang dibangun salah satunya adalah mengumpulkan respon pada setiap potensi risiko diambil dari data pelaporan insiden yang diolah dan melakukan perencanaan respon berdasarkan evaluasi.	1. RSUD Tarakan sudah mencoba memetakan resiko namun belum dilakukan analisa, hal ini terlihat pada dokumen identifikasi resiko dan peluang. 2. Setiap indentifikasi resiko belum ada informasi respon sehingga belum dapat dapat dibuktikan perencanaan respon terhadap resiko yang ada.	APO 12.02
3	1. Setiap kegiatan pelayanan TI dicatat dengan format yang telah ditentukan oleh personel yang ditunjuk dengan menggunakan sistem informasi yang dibangun, sehingga dapat dipastikan formatnya sama dan dapat diolah dengan mudah. 2. RSUD Tarakan direkomendasikan melakukan interkomparasi dengan organisasi/perusahaan	1. Penentuan layanan TI dan manajemennya merupakan bagian dari kegiatan layanan dalam operasional, namun belum ditemukan dokumen proses yang tertuang. 2. Belum ditemukan proses adopsi atau analisis dari contoh manajemen TI hasil benchmarking atau interkomparasi.	APO 12.03

Tabel 4.30. Rekomendasi Hasil Audit (Lanjutan)

	dengan proses bisnis serupa, kemudian adopsi manajemen yang TI dapat diaplikasikan pada RSUD Tarakan.	3. Penentuan layanan TI dan manajemennya merupakan bagian dari kegiatan layanan dalam operasional, namun belum ditemukan dokumen proses yang tertuang. 4. Belum ditemukan proses adopsi atau analisis dari contoh manajemen TI hasil benchmarking atau interkomparasi.	APO 12.03
4	1. RSUD Tarakan perlu melakukan penjadwalan pelaporan insiden kepada stakeholder dan menetapkan format yang dituangkan pada sistem informasi yang dibangun, dan tertuang dalam SK Direktur tentang pelaporan.	1. Proses identifikasi risiko dan peluang dalam proses bisnis telah dilakukan dan terdokumentasi, pelaporan kepada stakeholder belum disampaikan dalam kegiatan audit internal. 2. Belum ditemukan format pelaporan profil dan manajemen risiko TI pada RSUD Tarakan.	APO 12.04
5	1. Memperbaiki mekanisme disposisi pekerjaan terutama dalam hal risiko TI menggunakan ERM (Enterprise Risk Manajemen) dan mewajibkan seluruh pegawai menggunakan aplikasi tersebut.	1. Pada proses audit internal, pembahasan identifikasi risiko dan peluang telah dilakukan dengan harapan dapat diketahui oleh seluruh pegawai, namun pegawai yang terlibat dalam audit internal terbatas 2. Identifikasi risiko dan peluang sudah ada PIC pada masing-masing topik namun belum ditemukan distribusi ke pegawai sehingga belum jelas tanggung jawabnya.	APO 12.05

Tabel 4.30. Rekomendasi Hasil Audit (Lanjutan)

6	1. Melakukan pencatatan data insiden menggunakan sistem informasi kemudian diolah, lakukan analisa korelasi antara insiden dengan respon. 2. Setelah itu, RSUD Tarakan dapat melakukan evaluasi hasil analisa tersebut.	1. Belum ada bukti penerapan perencanaan risiko pada saat terjadi insiden. 2. Perencanaan risiko dibuktikan dengan adanya proses kegiatan identifikasi risiko dan peluang, namun belum adanya evaluasi dan standardisasi.	APO 12.06
7	1. RSUD Tarakan perlu melakukan mitigasi risiko terkait serangan malware dan dilakukan simulasi serta mengadakan pelatihan bagi seluruh karyawan terutama pengguna layanan TI. 2. Merencanakan kegiatan identifikasi potensi ancaman security dan lakukan evaluasi. 3. Melakukan pengolahan data laporan harian terkait insiden menggunakan sistem informasi insiden TI.	1. Belum ditemukan kegiatan atau perencanaan pelatihan khusus mengenai bahaya malware, penggunaan email dan internet yang baik pada user RSUD Tarakan. 2. Evaluasi terhadap potensi ancaman security belum dilakukan.	DSS 05.01
8	1. RSUD Tarakan direkomendasikan untuk merencanakan penjadwalan pengujian keamanan sistem terutama server, lakukan pengujian, kemudian evaluasi hasilnya. 2. Mengontrol akun dengan melakukan manajemen dan hirarki akun, terutama pada hak akses data server dan hak akses jaringan.	1. Belum ada bukti pelaksanaan pengujian keamanan sistem pada RSUD Tarakan. 2. Penggunaan akun tertentu untuk mengakses jaringan dan server sudah diterapkan namun belum ditemukan manajemen akun	DSS 05.02
9	1. Melakukan evaluasi penggunaan perangkat komputer, melakukan back up data terdistribusi pada masing-masing komputer	1. Seluruh perangkat komputer terutama pada bagian layanan menggunakan password, dan penetapan user	DSS 05.03

Tabel 4.30. Rekomendasi Hasil Audit (Lanjutan)

	layanan, dan menetapkan penanggung jawab masing-masing PC/Laptop beserta akunnya. 2. Melakukan manajemen pengaturan situs yang diblokir, sosialisasi dan menetapkan PIC yang bertugas untuk melakukan evaluasi.	sudah dilakukan pada masing-masing unit atau instalasi. 2. Situs web tertentu telah diblokir pada saat menggunakan jaringan kantor namun belum dilakukan evaluasi dan pengujian secara berkala. RSUD Tarakan telah mengklaim bahwa aktivitas blok telah dilakukan.	DSS 05.03
10	1. RSUD Tarakan perlu melakukan perencanaan pelatihan penggunaan SIMRS dan komputer serta manajemen akun, kemudian lakukan dan evaluasi. 2. Menjadwalkan meeting dengan pimpinan untuk membahas hirarki user menggunakan SIMRS dan dijabarkan dengan jelas stakeholder yang terlibat.	1. Evaluasi pasca pelatihan belum dilakukan; 2. Pemberian hak akses SIMRS sesuai peran individu dan unit bisnisnya, namun belum dilakukan monitoring dan evaluasi secara berkala untuk akun dengan hak akses intimewa	DSS 05.04
11	1. Membuat mekanisme penerimaan tamu, menggunakan google form sebagai DSS (Decision Support System), sehingga penerimaan tamu menjadi semi otomatis. 2. Menetapkan daerah-daerah yang terlarang dan menetapkan PIC tiap ruangan terutama server dan control room. Pada daerah tersebut perlu diberikan pengamanan ganda seperti pemasangan kunci finger print dan pemasangan CCTV pada ruangan tersebut.	1. Setiap pengunjung telah dipersyaratkan mengisi form kunjungan dan mengenakan tanda pengenal di pos satpam sebelum memasuki area situs TI. 2. Pengunjung akan ditemani oleh pegawai TI, namun belum ada penerapan daerah terlarang pada ruang server dan control room CCTV. 3. Belum ditemukan agenda pelatihan tentang kesadaran keamanan informasi fisik, termasuk server.	DSS 05.05

Tabel 4.30. Rekomendasi Hasil Audit (Lanjutan)

	3. Merencanakan pelatihan, lakukan dan evaluasi.		
12	1. RSUD Tarakan direkomendasikan menggunakan aplikasi Sinology Document Manajemen System dengan melakukan manajemen pada user dan dokumen untuk pengelolaan akses folder data. 2. Membuat jadwal meeting untuk agenda penanganan khusus terhadap dokumen penting RSUD Tarakan menggunakan Synology Document Manajemen system.	1. Setiap dokumen yang bersifat confidential dikelola oleh personel tertentu namun masih belum ada prosedur secara legal atas penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif tersebut. 2. Belum ditemukan bukti kegiatan penanganan khusus terhadap dokumen penting RSUD Tarakan	DSS 05.06
13	1. Mempertegas tugas pada jabatan Pranata Komputer berikut kewenangan dan kewajibannya melalui SK Direktur. 2. Dengan menetapkan PIC, maka pencatatan data insiden terkait keamanan dapat diolah dan digunakan dalam membuat kebijakan	1. Belum ditemukan kejadian keamanan, namun aktivitas tersebut telah menjadi tupoksi dari pranata komputer pada RSUD Tarakan yang harus dicatat dalam laporan kerja harian. 2. Belum ada mekanisme peninjauan ulang terhadap kejadian atau aktivitas terkait keamanan	DSS 05.07
14	1. Mengembangkan metode pengelolaan perubahan dengan baik dan secara konsisten untuk semua perubahan, dan Pihak Manajemen memastikan tidak ada pengecualian terhadap penerapan proses pengelolaan perubahan. 2. Memastikan perubahan sesuai dengan perencanaan menyeluruh dan melakukan kegiatan penilaian terhadap	1. Permintaan perubahan pada sistem dan aplikasi disetujui oleh manajemen namun tidak dilakukan secara formal dan terdokumentasi. 2. Perubahan dilakukan tanpa mempertimbangkan dampak terhadap layanan, integrasi data, dan penyedia layanan SLA sehingga akan	BAI 06.01

Tabel 4.30. Rekomendasi Hasil Audit (Lanjutan)

	dampak menggunakan tools untuk meminimalkan kemungkinan masalah-masalah pasca penerapan perubahan	berdampak pada business continuity plans (BCP).	BAI 06.01
15	1. Mendukung kegiatan mengelola perubahan dalam bentuk regulasi yang mengatur proses pengelolaan perubahan, dokumentasi tersebut aktual dan sesuai, dilengkapi dengan detil langkah-langkah yang tepat, cermat dan teliti menuju perubahan untuk memastikan pencapaian tujuan.	1. Telah di tentukan mana yang menjadi perubahan dan direalisasikan namun secara prosedur belum terdokumentasi, belum di verifikasi dan tidak dilakukan monitoring terhadap hasil dari perubahan darurat tersebut.	BAI 06.02
16	1. Mengintegrasikan perencanaan mengelola perubahan TI serta pelaksanaannya dengan perubahan operasional kegiatan, untuk memastikan pelatihan penanganan, hal yang terkait dengan perubahan organisasi dan penyelesaian masalah bisnis yang berkelanjutan.	1. RSUD Tarakan telah melakukan proses klasifikasi dengan mengkategorikan permintaan perubahan dan monitoring juga telah di lakukan namun untuk pelaporannya belum dilakukan secara detail dan belum terdokumentasi.	BAI 06.03
17	1. Melakukan metode pengelolaan perubahan secara konsisten untuk memantau kualitas dan mengawasi kinerja proses manajemen perubahan	1. Aktifitas perubahan yang terjadi hingga selesai peru bahan tidak dilakukan proses dokumentasi baik dokumentasi prosedur operasional bisnis dan TI, dokumentasi user, dokumentasi subjek, serta penyimpanan dokumentasi.	BAI 06.04

Berdasarkan audit tata Kelola teknologi informasi pada 3 domain yang terpilih menggunakan COBIT 2019 dan rekomendasi pada setiap subdomain

tersebut di atas, maka dapat disusun rekomendasi umum dibagi atas tiga bagian, yaitu sebagai berikut :

1. Rekomendasi Personel

   Rekomendasi personel merupakan rekomendasi mengenai struktur organisasi yang ada pada RSUD Tarakan dimana rekomendasi ini disusun dengan mengacu pada analisis resiko yang dilakukan sebelumnya. Penyusunan rekomendasi personel dapat menghasilkan perubahan pada struktur organisasi, tangung jawab, kompetensi dan kualifikasi. Perubahan tersebut perlu dilakukan untuk dapat meminimalkan resiko-resiko keamanan informasi yang tidak dapat diterima dan meningkatkan kualitas dan kemampuan dalam mengelola tata kelola TI. Adapun rekomendasi personil terlihat pada tabel 4.31.

Tabel 4.31. Rekomendasi Personil

No	Rekomendasi	Pertimbangan
1	Perekrutan / PIC Sandiman	Belum terdapat pelaksana yang bertangung jawab langsung dalam penyelenggaraan sistem manajemen keamanan informasi
2	Pelatihan / PIC Pengelola Sistem Informasi	Dilakukan pelatihan / upgrade kompetensi SDM yang bertangung jawab dalam operasional sistem dan backup aplikasi.
3	Pelatihan / PIC Hardware	Dilakukan pelatihan / upgrade kompetensi SDM yang bertangung jawab dalam pengelolaan dan perawatan infrastruktur secara berkala.
4	Perekrutan / PIC Programer, Sistem Analyst, Database Desainer.	Belum terdapat pelaksana / SDM yang bertangung jawab terhadap mpengembangan yang lebih banyak di bidang ini melakukan pengembangan, pengujian aplikasi, desain database aplikasi

2. Rekomendasi Proses

Tugas tiap tiap personil telah dibagi pada bagian sebelumnya untuk menentukan partisipasinya masing-masing dalam penyelenggaraan tata kelola TI. Tentunya dalam melakukan tugas tugas tersebut diperlukan adanya pedoman dalam pelaksanaan, sehingga tata kelola TI bisa dilakukan dengan efektif. Pedoman tersebut bisa dalam bentuk paying hukum maupun pedoman teknis berupa standard operating procedure (SOP).

2.1 Kebijakan Pelaksanaan Tata Kelola TI

Kebijakan merupakan salah satu bentuk pedoman untuk melaksanakan suatu proses yang ada pada sebuah organisasi. Begitu pula dalam pelaksanaan proses tata kelola TI, perlu ada kebijakan yang ada digunakan sebagai dasar dalam mengamankan informasi. Kebijakan tata kelola TI perlu disusun sebagai pedoman pelaksanaan yang bersifat memaksa dan mengikat. Hal ini diperlukan dengan alasan agar tata kelola TI dapat dilaksanakan dengan seksama.

1. Penangung Jawab Pelaksanaan Tata Kelola TI

   Padsa bagian ini terdapat penangung jawab pelaksanaan tata kelola TI, penangung jawab merupakan pejabat eselon 2 pada RSUD Tarakan.

2. Pelaksana Tata Kelola TI

   Pelaksana tata kelola TI adalah Instalasi PDE. Oleh karena itu, PDE memiliki kewenangan untuk mengeluarkan kebijakan terkait tata kelola TI. Kebijakan terkait tata kelola TI yang dikeluarkan wajib diikuti oleh partisipan tata kelola TI yang terdiri atas pegawai, kontraktor, atau pihak ketiga lainnya.

Partisipan tata kelola TI wajib mengikuti pelatihan, prosedur, dan kebijakan yang berkaitan dengan tata kelola TI.

3. Pengelolaan Informasi yang dikecualikan

   Informasi yang dikecualikan selanjutnya akan dipilah lagi menjadi dua jenis informasi, yaitu informasi rahasia dan informasi umum. Pengklasifikasian dan pengelompokan ini merupakan tangung jawab dari seksi persandian. Informasi rahasia adalah informasi yang mendapat perlindungan maksimal dan penggunaannya wajib dengan fasilitas berupa tanda tangan elektronik dan sertifikat elektronik. Informasi

4. Hak Ases

   Hak akses merupakan hak yang dimiliki oleh pengguna untuk dapat membuat, membaca, memperbarui, dan menghapus informasi, mengakses system, dan mengakses fasilitas pengolah informasi. Hak akses dipisahkan berdasarkan kebutuhan pengguna terhadap akses kepada informasi, system, dan fasilitas pengolah informasi. Peninjauan terhadap hak akses perlu dilakukan secara berkala untuk dapat mengetahui perubahan kebutuhan hak akses yang ada. Hak akses membutuhkan kredensial berupa password atau kunci kriptografi. Password yang digunakan haruslah rumit dan memiliki kadaluwarsa. Sementara, penggunaan kriptografi diatur dengan peraturan Gubernur terkait tanda tangan elektronik dan sertifikat elektronik. Password tidak diperbolehkan untuk dibagi kepada pihak lain.

5. Pengembangan Aplikasi

RSUD Tarakan memiliki kewenangan untuk melakukan pengembangan aplikasi. Setelah aplikasi di kembangkan terdapat pengujian aplikasi yang dilakukan secara internal dan eksternal. Secara internal dilakukan pengujian aplikasi yang dilakukan oleh pelaksana yang berbeda dengan pelaksana pengembang aplikasi untuk mencari celah keamanan. Pengujian secara eksternal adalah pemohon pengembangan aplikasi wajib melakukan user acceptance test (UAT) dengan tujuan untuk memastikan bahwa aplikasi sesuai dengan kebutuhan yang sudah disepakati. Pra operasional aplikasi harus terpisah baik secara pelaksanaan maupun secara lingkungan dari pengembang dan penguji aplikasi.

6. Fasilitas Pengolahan Informasi

Area aman meruapa area yang dilindunggi oleh perimeter pengamanan untuk melindungi tempat informasi kritis dan fasilitas pengolah informasi. Area aman hanya dapat hanya dapat dimasuki oleh orang dengan ha akses terhadapnya. Bentuk perimeter dapat berupa pintu, kunci, pemindai sidik jari, dan pengenal wajah. Pengamanan area aman bertujuan mengamankan dari akses yang tidaK diperkenankan, pencurian perangkat, dan peruskaan perangkat. Fasilitas pengolah ionformasi perlu dapat terus berjalan untuk menjamin ketersediaan layanan. Ketersediaan layanan berhubungan dengan keberlangsungan fasilitas pengolah informasi. Oleh karena itu, diperlukan adanya pencadangan (backup) informasi dan sistem dengan tujuan pencadangan ke pusat data yang berbeda. Aplikasi yang diinstall pada

system perlu diperhatikan bahwasannya aplikasi tersebut tidak berbahaya bagi system dan informasi yang ada pada fasilitas. Insiden keamanan informasi perlu didentifikasi, dikalsifikasikan, ditangani, didokumentasikan dan selanjutnya dilakukan peninjauan secara berkala.

2.2 Perancangan standar operational procedure (SOP)

Kebijakan merupakan pedoam umum dalam melaksanakan suatu tugas atau kegiatan. Sementara pada tataran teknis, tetap diperlukan adanya petunjuk pelaksanaan agar proses atau aktifitasyang dilaksanakan dapat dipastikan berjalan dengan baik, efektif, dan terstruktur. Berikut ada beberapa rekomendasi SOP yang perlu disusun untuk memastikan kesesuaiapn dengan standar keamanan informasi.

a. SOP bekerja di dalam area aman

Bekerja di area aman memerlukan petunjuk agar pengguna yang sedang mengakses area aman terjaga keselamatannya dan fasilitas pengolah informasi dapat terjaga dari kerusakan yang disebabkan oleh keteledoran pengguna yang memasuki area aman.

b. SOP pengawalan untuk pengunjung

Akses yang tidak diizinkan terhadap informasi atau fasilitas pengolah informasi dapat memberikan ancaman kepada keamanan informasi. Oleh karena itu, ketika terdapat pengunjung yang memiliki kepentingan dengan RSUD Tarakan perlu dilakukan mekanisme pengawalan. Hal ini dilakukan untuk dapat memastikan bahwa pengunjung tidak melakukan pelanggaran hak akses.

c. SOP Klasifikasi, Dokumentasi, dan Peninjauan insiden keamanan informasi.

Terjadinya insidn keamanan informasi merupakan bukti bahwa terdapat upaya baik secara sengaja maupun tidak untuk meretas keamanan informasi yang ada. Oleh karena itu, diperlukan adanya identifikasi, dokumentasi, klasifikasi, dan peninjauan insiden keamanan informasi agar tidak terulang kembali.

d. SOP pengamanan diri ketika terjadi bencana alam kebakaran.

Bencana alam atau kebakaran dapat menyebabkan korban jiwa. Oleh karena itu untuk mengantisipasi dan meminimalkan kemungkinan jatuhnya korban jiwa, perlu ada panduan teknis mengenai apa yang perlu dilakukan Ketika terjadi bencana alam atau kebakaran.

3. Rekomendasi Sistem Informasi dan Teknologi Informasi

Perancangan rekomendasi sistem informasi dan teknologi informasi dilakukan berdasarkan analisis resiko yang telah dilakukan pada tahap sebelumnya. Penggunaan teknologi dapat mempermudah pelaksanaan suatu proses atau bahkan melakukan otomasi terhadap proses tersebut. Adapun rekomendasi sistem informasi dan teknologi informasi antara lain :

a. Penggunaan Aplikasi Pengelola Kebijakan Password

Mengacu pada standar ISO 27001:2013 dan rancangan proses mengenai kebijakan password, perlu di terapkan penggunaan password yang rumit dan memiliki masa kadaluarsa. Aplikasi pengelola kebijakan password dapat melakukan pengaturan kebijakan password termasuk pengaturan masa kadaluarsa dari suatu password. Beberapa aplikasi pengelola kebijakan

password yang dapat digunakan antara lain : google password manager, IPassword, LastPass, dan Dashlane.

b. Pengunaan Aplikasi Pemantauan Kondisi Server

Pusat data merupakan bagian penting yang bekerja selaku fasilitas pengolah informasi. Salah satu bagian yang penting dari pusat data adalah server. Server perlu dikelola dengan baik demi menjaga kontinuitas bisnis dan stabilitas layanan yang diberikan. Oleh karena itu, diperlukan aplikasi yang berguna untuk memantau kondisi server. Beberapa aplikasi yang dapat digunakan untuk melakukan pemantauan kondisi server antara lain : cacti dan nagios.

c. Pengembangan Aplikasi Enterprise Risk Manajemen Sistem (ERM)

Lingkungan bisnis yang saat ini sangat dinamis tentunya banyak juga risiko baik dari internal maupun eksternal. Pada kondisi ini mitigasi risiko telah menjadi salah satu elemen kunci dalam mendorong pertumbuhan suatu bisnis. Praktik manajemen risiko yang baik akan menjadi pilar utama dalam setiap proses pengambilan keputusan.

Dalam menghadapi risiko-risiko yang ada, saat ini lazimnya RSUD dapat beradaptasi dengan mengoptimalisasikan penggunaan teknologi aplikasi *Enterprise Risk Management* (ERM). Kombinasi teknologi dan bisnis dalam melakukan mitigasi risiko ini tentunya akan memberikan dampak yang signifikan pada jalannya bisnis proses RSUD Tarakan. Mitigasi risiko melalui penerapan aplikasi Enterprise Risk Management yang terpadu akan memungkinkan RSUD secara efektif mengelola dampak risiko, sehingga

dapat memperkirakan dan melakukan tindakan preventif untuk mengantisipasi risiko terhadap RSUD dan tujuan RSUD tetap dapat diraih. Pengelolaan risiko juga tidak hanya terbatas pada risiko kecil yang biasa terjadi, tetapi juga pada seluruh proses yang melekat pada fungsi-fungsi yang kritikal untuk memastikan kelangsungan operasional bisnis berjalan secara efisien dan efektif. Dalam pengembangan aplikasi harus terdapat fitur-fitur seperti, pencatatan dan pelaporan data kritikal RSUD akan lebih transparan. Pencatatan ini melibatkan beberapa lini approval sehingga dapat memastikan keterlibatan seluruhnya hingga level operasional. Selain itu ada fitur reminder untuk memastikan kegiatan mitigasi dapat dilakukan dengan baik.

d. Penggunaan Aplikasi WAF (Web Application Firewall)

RSUD Tarakan perlu mempertimbangkan pengunaan aplikasi WAF dalam implementasi tata kelola TI mengingat perkembangan TI yang begitu pesat. WAF memiliki banyak kelebihan daripada firewall tradisional lainnya karena menawarkan visibilitas lebih baik terhadap data sensitif dari layer HTTP. WAF bisa mencegah serangan di layer aplikasi yang normalnya melewati firewall tradisional. Adapun serangan yang sering terjadi dan serangan yang dapat di tangulanggi oleh WAF seperti berikut :

- Serangan cross-site scripting (XSS) memungkinkan penyerang menginjeksi dan mengeksekusi skrip berbahaya di browser pengguna lain.

- Serangan structured query language (SQL) bisa mengakibatkan aplikasi mana pun yang menggunakan database SQL dan bisa membuat penyerang mengakses dan berpotensi mengubah data-data yang sensitif.
- Web session hacking bisa membuat penyerang membajak sesi ID dan menyamar sebagai authorized user. ID sesi biasanya disimpan dalam cookie atau Uniform Resource Locator (URL).
- Serangan distributed denial-of-service (DDoS) bisa membuat sebuah jaringan dipenuhi oleh traffic sehingga tidak bisa melayani user. Baik jaringan firewall dan WAF sejatinya bisa mengandalikan serangan seperti ini, tapi mereka melakukannya dengan cara berbeda.

e. Pengembangan Aplikasi Bridging Sistem

Banyaknya sistem informasi yang dikembangkan pada platform yang berbeda2 membuat interoperabilitas dan konsistensi data menjadi semakin sulit untuk disinkronisasi secara realtime. Dalam pelayanan kesehatan untuk meningkatkan mutu layanan yang lebih baik kepada peserta maupun terhadap provider layanan kesehatan (rumah sakit/RS) maka dikembangkanlah suatu metode handshake antar sistem yang biasa disebut dengan bridging system.

Bridging system merupakan penggunaan fasilitas teknologi informasi web service yang memungkinkan dua sistem yang berbeda pada saat yang sama mampu melakukan dua proses tanpa adanya intervensi satu sistem pada

sistem lainnya secara langsung, sehingga tingkat keamanan dan kerahasiaan masing-masing sistem tetap terjaga.

Modul / aplikasi bridging system yang akan di rekomendasikan untuk dikembangkan pada sistem informasi RSUD Tarakan terlihat pada tabel 4.32 di bawah ini :

Tabel 4.32 Rekomendasi Analisis Gap Aplikasi Portofolio RSUD Tarakan

No	Rencana Aplikasi	Temuan	Rencana Hasil
1	Modul bridging sistem SIMRS-BPJS (Inova.1.1 Modul Pendaftaran)	Registrasi pasien BPJS dilakukan 2 kali, dengan SIMRS dan dengan sistem dari BPJS	Registrasi pasien hanya melalui SIMRS yang telah terintegrasi dengan sistem BPJS.
2	Modul bridging sistem SIMRS- Agape.2.1 DPI Logistik	Agape.2.1. merupakan sistem tersendiri (stand alone)	Integrasi data khususnya data logistik antara Agape.2.1 dengan SIMRS (modul Inova.1.25, Inova.1.22,dan Inova.1.14)
3	Modul bridging sistem SIMRS- Agape.2.2 DPI Farmasi	Agape.2.2. merupakan sistem tersendiri (stand alone)	Integrasi data khususnya data farmasi antara Agape.2.2 dengan SIMRS (modul Inova.1.7, Inova.1.22, dan Inova.1.14)
4	Modul bridging sistem SIMRS- RIS.3.1	RIS.3.1 merupakan sistem tersendiri (stand alone)	Integrasi data khususnya data hasil radiologi antara RIS.3.1 dengan SIMRS modul Inova.1.6
5	Modul bridging sistem SIMRS- LIS.4.1	LIS.4.1 merupakan sistem tersendiri (stand alone)	Integrasi data hasil laboratorium antara LIS.4.1 dengan SIMRS modul Inova.1.5

Tujuan bridging system ini untuk meningkatkan efektivitas entry data processing, efisiensi penggunaan sumber daya, serta lebih cepat dalam proses pengelolaan, baik klaim, piutang, verifikasi, dan sebagainya. Dengan

sistem ini, proses antrean peserta BPJS Kesehatan jadi lebih cepat karena registrasi peserta hanya pada sistem RS. Dengan begitu, peserta jadi lebih cepat mendapatkan pelayanan kesehatan.

Bagi rumah sakit, sistem ini dapat meningkatkan layanan administrasi peserta, menghemat SDM dan sarana-prasarana, perekaman data pelayanan kesehatan dan proses pengajuan klaim menjadi lebih cepat, serta penyelesaian insentif pelayanan berdasarkan beban kerja juga lebih cepat diselesaikan.

BAB V

KESIMPULAN DAN SARAN

Bab ini menjelaskan mengenai kesimpulan yang diperoleh dari hasil pembahasan serta saran yang diperlukan untuk pengembangan penelitian dengan judul "Audit Tata Kelola TI Menggunakan COBIT 2019 Pada UPTD RSUD Tarakan Provinsi Kalimantan Utara".

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan di RSUD Tarakan, adapun kesimpulan yang dihasilkan adalah sebagai berikut :

1. Berdasarkan hasil audit tata kelola TI menggunakan COBIT 2019, tingkat kapabilitas tata kelola TI RSUD Tarakan berada pada level 1 atau dapat diartikan bahwa kegiatan sudah dilakukan melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif. RSUD Tarakan masih berada pada level 1 sehingga tata kelola TI bagi Lembaga pemerintahan bidang pelayanan kesehatan harus menjadi prioritas demi percepatan implementasi SPBE.
2. Rekomendasi yang dapat dilakukan guna percepatan implementasi SPBE pada RSUD Tarakan berdasarkan hasil audit COBIT 2019 secara umum terdiri dari tiga bagian, pertama adalah rekomendasi proses yaitu rekomendasi pada sisi peraturan/kebijakan yaitu penurunan petunjuk pelaksanaan, sisi organisasi RSUD Tarakan yaitu menambahkan tupoksi tata kelola IT pada organisasi RSUD Tarakan, kedua adalah rekomendasi personil yakni rekomendasi pada sisi SDM yaitu pengembangan kompetensi SDM dan rekruitment pranata komputer

dan ketiga adalah rekomendasi teknologi informasi dimana di sisi teknologi dilakukan pengembangan aplikasi agar terjadi integrasi data pada semua sistem informasi yang berjalan di RSUD Tarakan dan implementasi pengunaan hardware atau teknologi terbaru dan terupdate sesuai dengan perkembangan kemajuan teknologi saat ini.

5.2 Saran

Sesuai dengan hasil dari penelitian ini, saran yang dapat diberikan kepada RSUD Tarakan adalah sebagai berikut :

1. Bagi RSUD Tarakan hendaknya menerapkan suatu framework tata kelola TI sebagai acuan dalam mengelola implementasi tata kelola TI sehingga dapat dijadikan salah satu motor yang mendorong tercapainya tujuan RS.
2. RSUD Tarakan di sarankan agar pihak dapat menerapkan rekomendasi-rekomendasi guna mencapai tata kelola TI yang terstandarisasi. Dan secara kontinyu dan berkesinambungan melakukan audit tata kelola TI guna kontrol dan pengawasan proses-proses TI sehingga dapat menjadi acuan untuk mengambil keputusan.

Beberapa saran yang dapat penulis sampaikan berkaitan dengan penyempurnaan penelitian serupa dan penelitian lebih lanjut adalah sebagai berikut:

1. Penelitian mengenai Audit Tata Kelola TI dengan mempersempit cakupan dan lebih fokus pada proses- proses tertentu, sehingga menghasilkan data pengujian yang lebih tajam dan semakin mendalam.
2. Penelitian dengan menggunakan tools atau peralatan ukur lain selain COBIT 2019 Framework dalam melakukan evaluasi tata kelola TI, untuk mendapatkan

perbandingan baik cara pelaksanaan audit ataupun hasil dari pelaksanaan audit tata kelola TI.

3. Perlunya memperluas responden audit namun tetap mempertimbangkan RACI chart.

DAFTAR PUSTAKA

Ade Sukmawati, Widya Cholil, Syahril Rizal, 2020, Evaluasi Tata Kelola Teknologi Informasi Pada Rumah Sakit Dr. H. Ibnu Sutowo Baturaja Berdasarkan Framework COBIT 5. GEMA TEKNOLOGI Vol. 20 No. 4 Periode Oktober 2019

Alreemy, Z., Chang, V., Walters, R., & Wills, G., 2016, Critical Success Factors (CSFs) for Information Technology Governance (ITG). International Journal of Information Management

Aldy Maulana Syuhada, 2021, Kajian Perbandingan COBIT 5 Dengan COBIT 2019 Sebagai Framework Audit Tata Kelola Teknologi Informasi. Jurnal Ilmiah Indonesia. Vol. 6, No. 1, Januari 2021.

Anastasia, Priscilla Novita, Atrinawati, Lovinta Happy, 2020, Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Hotel Xyz. JSI : Jurnal Sistem Informasi (E-Journal), VOL.12, NO.2, Oktober 2020

Angga Wijaya Narwa Putra, Andi Sunyoto, Asro Nasiri, 2020, Perencanaan Audit Tata Kelola Teknologi Informasi Laboratorium Kalibrasi Menggunakan COBIT 2019 (Studi Kasus: Laboratorium Kalibrasi BSML Regional II), JURNAL FASILKOM Volume 10 No. 3

Atmoko, T. 2008. Standar Operasional Prosedur (SOP) dan Akuntabilitas Kinerja Instansi Pemerintah, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran, Bandung.

Belo, G. I., Wiranti, Y. T., & Atrinawati, L. H. (2020). Perancangan Tata Kelola Teknologi Informasi Menggunakan Cobit 2019 Pada PT Telekomunikasi Indonesia Regional VI Kalimantan. JUSIKOM PRIMA (Jurnal Sistem Informasi Ilmu Komputer Prima), 4(1), 23–30.

Bogdan, R., Taylor, S., 1992, Pengantar Metode Kualitatif, Usaha Nasional, Surabaya

Bungin, B., 2005, Metodologi Penelitian Kualitatif, Prenada Media Group, Jakarta

De Haes, S., & Van Grembergen, W. (2005), IT Governance Structures, Processes and Relational Mechanisms Achieving IT/Business Alignment in A Major Belgian Financial Group, ITAG Research Institute, Belgium.

Ernala, I. (2009), Tata Kelola Teknologi Informasi (IT Governance), Universitas Bina Nusantara, Jakarta.

Fikri, Ahmad Maulana Priastika, Hesti Shofia Octaraisya, Nadine Sadriansyah, Sadriansyah Trinawati, Lovinta Happy, 2020, Rancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: PT XYZ). Journal of Information Management, Vol. 5, No. 1, Desember 2020, 1 – 14

Gelsi Isabel Belo, Yuyun Tri Wiranti, Lovinta Happy Atrinawati, 2019, Perancangan Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 Pada PT Telekomunikasi Indonesia Regional VI Kalimantan. JUSIKOM PRIMA (Junal Sistem Informasi Ilmu Komputer Prima) Vol. 4 No. 1, Agustus 2020

Grembergen, W. V. 2002. Introduction to the Minitrack: IT Governance and its mechanisms. Prosiding Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS).

Grembergen, W. V. 2004. Strategies for Information Technology Governance. United States of America: Idea Group Publishing.

Hanafi, I. 2011. Bagaimana Organisasi Mengelola Kompetensi SDM 2008. http://www.ptpn3.co.id/ptb.pdf. Diakses 24 Januari 2011.

Hartanto, I. D., dan A. Tjahyanto. 2009. Analisis Kesenjangan Tata Kelola Teknologi Informasi untuk Proses Pengelolaan Data Menggunakan COBIT (Studi Kasus Badan Pemeriksa Keuangan Republik Indonesia), Magister Manajemen Teknologi, Institut Teknologi Sepuluh November, Surabaya.

Hasbi, M. 2005. Audit Sistem Informasi Kepegawaian pada Kementerian Kebudayaan dan Pariwisata, Magister Teknologi dan Informasi, Universitas Gadjah Mada, Yogyakarta.

HM, Jogiyanto. dan Willy Abdillah. 2011. Sistem Tatakelola Teknologi Informasi. Andi, Yogyakarta.

ISACA, 2018, COBIT 2019 Framework : Governance And Management Objectives, USA

ISACA, 2018, COBIT 2019 Design Guide : Designing an Information and Technology Governance Solution, USA

ISACA, Introducing COBIT 2019, USA: ISACA, 2018.

ISACA, 2018, COBIT 2019 Framework: Introduction and Methodology, USA

ISO 27001 dan Tata Kelola IT di Indonesia, 2016. https://isoindonesiacenter.com/iso-27001-dan-tata-kelola-it-di-indonesia/ (accessed Feb. 13, 2022).

ITGI. 2003. Board Briefing on IT Governance, 2nd Edition. United States of America: The IT Governance Institute

Joshi, A., Bollen, L., Hassink, H., Haes, S. D., & Grembergen, W. V., 2018, Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. Information & Management

Konsultasi ISO 38500:2015, 2022. https://delta.id/index.php/article/iso/11 (accessed Feb. 13, 2022).

Lanter, D. (2019). COBIT 2019 Framework Introduction and methodology. In www.icasa.org/COBITuse. https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019- Framework-Introduction-and-Methodology_res_eng_1118.pdf

Muhammad Nur, Eko Darwiyanto, Indra Lukmana Sardi, 2019, Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 pada Rumah Sakit Umum Daerah Kalideres. e-Proceeding of Engineering : Vol.6, No.3

Muthmainnah. (2015), Model Perancangan Tata Kelola Teknologi Informasi (IT Governance) Pada Proses Pengelolaan Data di Universitas Malikussaleh Lhokseumawe, Techsi, 6(1).

Nachrowi, E., Nurhadryani, Y., Sukoco, H., 2020, Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4, Resti Journal Vol. 4 No. 4 (2020) 764 – 774

Pederiva, A. 2003. The Cobit Maturity Model in a Vendor Evaluation Case. Information Systems Control Journal Volume 3 (www.isaca.org).

Peraturan Menteri Kesehatan Republik Indonesia Nomer 82 Tahun 2013. Sistem Informasi Manajemen Rumah Sakit. 10 Desember 2013. Berita Negara Republik Indonesia Tahun 2014 Nomor 87. Jakarta. https://staff.blog.ui.ac.id/r-suti/files/2016/11/PMK-No.-82-ttg-Sistem-Informasi-Manajemen-RS.pdf.

Ranggi Praharaningtyas Aji, Ito Setiawan,Yuliawan Adi Wibowo, 2019, Evaluasi Sistem Informasi Rumah Sakit Ananda Purwokerto Menggunakan Domain Edm Dan Apo Cobit 5. JTIM : Jurnal Teknologi Informasi dan Multimedia Vol. 1, No. 2, Agustus 2019

Rozas, I. S., & Effendy, D. A. (2012), Mengukur Efektifitas Hasil Audit Teknologi Informasi COBIT 4.1 Berdasarkan Perspektif End User, Universitas Narotama, Surabaya.

Sarno, R. (2009), Audit Sistem dan Teknologi Informasi, ITS Press, Surabaya.

Selengkapnya tentang ISO 20000, 2016. https://isoindonesiacenter.com/selengkapnya-tentang-iso-20000/ (accessed Feb. 13, 2022).

Setiawan, H. (2010). IT Governance & Penggunaan COBIT Framework.

Setiawan, H., & Mustofa, K. (2013), Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia, Universitas Gadjah Mada, Yogyakarta.

Shahnilna F Bayastura, Shinta Krisdina, Aris P Widodo, Analisis Dan Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 Pada PT. XYZ. JIKO (Jurnal Informatika dan Komputer) Vol. 4, No. 1, April 2021

Suhardi. S. N. (2011), Evaluasi Kematangan Pengelolaan Teknologi Informasi Pada PT. Multi Garmenjaya Surabaya Dengan Pendekatan COBIT, Insitut Teknologi Sepuluh Nopember, Surabaya.

Surendro, K. 2009. Implementasi Tata Kelola Teknologi Informasi. Bandung: Informatika.

Surwi, F. 2008. Evaluasi Penerapan Sistem Informasi Akademik pada Universitas Muhammadiyah Surakarta Menggunakan COBIT Framework, Magister Teknologi Informasi, Universitas Gadjah Mada, Yogyakarta.

Wardani, S., & Puspitasari, M. (2014, Juni), Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT dengan Model Maturity (Studi Kasus Fakultas ABC), Jurnal Teknologi, 7(1).

Weber, Ron. (1999). Information Systems Control and Audit. Prentice-Hall, Inc. New Jersey, Amerika Serikat.

Yulhendri, & Surendro, K. (2008), Pengembangan Tata Kelola TI untuk Pengelolaan Sistem Informasi Terintegrasi di Perguruan Tinggi Melalui Penentuan Kebijakan, Aturan, Pedoman dan Prosedur, Sekolah Teknik Elektro dan Informatika (STEI), Purwokerto.

KUESIONER SURVEY

APO 12 – Managed Risk

KUESIONER SURVEY

Penilaian Capability Level APO 12 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **APO 12 – Managed Risk**. Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Drs. Prijono Pancasila Apt. Sp.frs
Email	–
Unit Kerja	Wadir Umum
Organisasi / Perusahaan	RSUD Tarakan
Paraf	[signature]

1

Domain	:	Align, Plan, Organize
Objek Manajemen	:	APO 12 - Managed Risk

Deskripsi :
Identifikasi, nilai, dan kurangi resiko terkait TI secara berkelanjutan dalam tingkat toleransi yang di tetapkan oleh manajemen eksekutif organisasi / RSUD

Tujuan :
Mengintegrasikan manajemen resiko organisasi / RSUD terkait IT dengan manajemen resiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola resiko perusahaan terkait TI.

APO 12.01 – Collect Data
Identifikasi, dan kumpulkan data yang relevan untuk mengaktifkan resiko terkait TI yang efektifitas identifikasi, analisis dan pelaporan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait resiko TI	✓									✓		
2	Catat data terkait resiko terkait TI yang relevan dan signifikan di lingkungan internal dan external RSUD	✓									✓		
3	Mengadopsi atau mendefinisikan resiko untuk definisi yang konsisten dari skenario resiko dan dampak	✓									✓		
4	Catat data tentang peristiwa resiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak	✓									✓		
5	Survei dan analisis data resiko TI terkait kerugian dari data dan tren yang tersedia secara eksternal.	✓									✓		
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan konstribusi umum faktor di berbagai peristiwa.		✓								✓		
7	Tentukan kondisi spesifik yang dapat mempengaruhi resiko	✓									✓		
8	Lakukan analisis faktor resiko secara berkala untuk mengidentifikasi masalah resiko barau atau yang muncul dan untuk mendapatkan pemahaman tentang faktor resiko internal dan eksternal terkait.	✓									✓		

APO 12.02 – Analyze Risk
Kembangkan pandangan yang dibuktikan tentang resiko TI actual, untuk mendukung kkeputusan resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan cakupan yang tepat dari upaya analisis resiko, dengan mempertimbangkan semua faktor resiko.		✓								✓		
2	Membangun dan memperbarui scenario resiko TI secara teratur, identifikasi kerugian terkait TI.	✓									✓		
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario resiko TI. Mempertimbangkan semua faktor resiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓								✓		
4	Bandingkan resiko saat ini (eksposur kerugian terkait TI) dengan toleransi resiko yang dapat diterima.	✓									✓		
5	Mengusulkan respon resiko untuk resiko yang melebihi tingkat toleransi.		✓								✓		
6	Identifikasi persyaratan dan target untuk respon mitigasi resiko yang optimal.	✓									✓		
7	Validasi hasil analisis resiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	✓									✓		
8	Menganalisis manfaat dari opsi respon resiko yang dipilih , konfirmasikan respon resiko yang optimal.	✓									✓		

APO 12.03 – Maintain A Risk Profile
Menjaga inventaris resiko yang diketahui dan atribut resiko, termasuk frekuensi yang diharapkan, potensi dampak dan tanggapan. Dokumen terkait sumber daya, kapabilitas dan aktivitas pengendalian saat ini yang berkaitan dengan item resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menginventarisir proses layanan TI dan proses bisnis. Identifikasi pensonel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.	✓									✓		
2	Menentukan dan menyetujui layanan TI dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.		✓								✓		
3	Mengumpulkan skenario resiko saat ini menurut kategori, lini bisnis, dan area fungsional	✓									✓		
4	Secara teratur mendata semua informasi profil resiko dan menggabungkannya ke dalam profil resiko gabungan.	✓									✓		
5	Mendata informasi tentang status rencana tindakan resiko untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		
6	Berdasarkan semua data profil resiko, tentukan seperangkat indikator resiko yang memungkinkan identifikasi dan monitoring resiko saat ini secara tepat.	✓									✓		
7	Mendata informasi tentang peristiwa resiko TI yang telah terwujud untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		

APO 12.04 – Articulate Risk
Komunikasikan informasi tentang status saat ini dari eksposur terkait TI dan peluan secara tepat waktu untuk semua pemangku kepentingan yang dibutuhkan respon yang tepat.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Laporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam format tertentu yang berguna untuk mendukung keputusan RSUD Tarakan.		✓								✓		
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait TI.	✓									✓		
3	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, dan gap.		✓								✓		
4	Secara berkala, identifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan.	✓									✓		
5	Meninjau hasil penilaian pihak ketiga yang obyektif dan audit internal. Sertakan mereka di profil risiko.	✓									✓		

APO 12.05 – Define A Risk Management Action Portofolio
Kelola peluang untuk menguranggi resiko ke tingkat yang dapat di terima sebagai portofolio.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Klasifikasikan aktivitas pengendalian dan petakan pada skenario risiko TI.	✓									✓		
2	Tentukan apakah setiap entitas organisasi memantau risiko dan memiliki peran.		✓								✓		
3	Buat proposal proyek yang dirancang untuk mengurangi risiko dan / atau proyek yang memiliki peluang dengan mempertimbangkan risiko TI.		✓								✓		

APO 12.05 – Respon To Risk
Menanggapi secara tepat waktu kejadian resiko yang terwujud dengan efektif Langkah-langkah untuk membatasi besarnya kerugian

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan terhentinya operasional bisnis.		✓								✓		
2	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi		✓								✓		
3	Komunikasikan respon risiko kepada pengambil keputusan sebagai bagian dari pelaporan dan pembaharuan profil risiko.	✓									✓		
4	Memeriksa kerugian masa lalu dan peluang yang hilang dan menentukan akar penyebabnya.		✓								✓		
5	Komunikasikan akar masalah, respons risiko dan perbaikan proses kepada pengambil keputusan yang tepat.		✓								✓		

KUESIONER SURVEY

Penilaian Capability Level APO 12 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **APO 12 – Managed Risk.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Irma Ulfa, S.Kom
Email	irmaulfa@gmail.com
Unit Kerja	Instalasi PDE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Align, Plan, Organize
Objek Manajemen	:	APO 12 - Managed Risk

Deskripsi :
Identifikasi, nilai, dan kurangi resiko terkait TI secara berkelanjutan dalam tingkat toleransi yang di tetapkan oleh manajemen eksekutif organisasi / RSUD

Tujuan :
Mengintegrasikan manajemen resiko organisasi / RSUD terkait IT dengan manajemen resiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola resiko perusahaan terkait TI.

APO 12.01 – Collect Data

Identifikasi, dan kumpulkan data yang relevan untuk mengaktifkan resiko terkait TI yang efektifitas identifikasi, analisis dan pelaporan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait resiko TI		✓								✓		
2	Catat data terkait resiko terkait TI yang relevan dan signifikan di lingkungan internal dan external RSUD		✓								✓		
3	Mengadopsi atau mendefinisikan resiko untuk definisi yang konsisten dari skenario resiko dan dampak		✓								✓		
4	Catat data tentang peristiwa resiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak		✓								✓		
5	Survei dan analisis data resiko TI terkait kerugian dari data dan tren yang tersedia secara eksternal.		✓								✓		
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan konstribusi umum faktor di berbagai peristiwa.	✓									✓		
7	Tentukan kondisi spesifik yang dapat mempengaruhi resiko		✓								✓		
8	Lakukan analisis faktor resiko secara berkala untuk mengidentifikasi masalah resiko barau atau yang muncul dan untuk mendapatkan pemahaman tentang faktor resiko internal dan eksternal terkait.		✓								✓		

APO 12.02 – Analyze Risk

Kembangkan pandangan yang dibuktikan tentang resiko TI actual, untuk mendukung kkeputusan resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan cakupan yang tepat dari upaya analisis resiko, dengan mempertimbangkan semua faktor resiko.		✓								✓		
2	Membangun dan memperbarui scenario resiko TI secara teratur, identifikasi kerugian terkait TI.		✓								✓		
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario resiko TI. Mempertimbangkan semua faktor resiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓								✓		
4	Bandingkan resiko saat ini (eksposur kerugian terkait TI) dengan toleransi resiko yang dapat diterima.		✓								✓		
5	Mengusulkan respon resiko untuk resiko yang melebihi tingkat toleransi.		✓								✓		
6	Identifikasi persyaratan dan target untuk respon mitigasi resiko yang optimal.		✓								✓		
7	Validasi hasil analisis resiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	✓									✓		
8	Menganalisis manfaat dari opsi respon resiko yang dipilih . konfirmasikan respon resiko yang optimal.	✓									✓		

APO 12.03 – Maintain A Risk Profile

Menjaga inventaris resiko yang diketahui dan atribut resiko, termasuk frekuensi yang diharapkan, potensi dampak dan tanggapan. Dokumen terkait sumber daya, kapabilitas dan aktivitas pengendalian saat ini yang berkaitan dengan item resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menginventarisir proses layanan TI dan proses bisnis. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		✓								✓		
2	Menentukan dan menyetujui layanan TI dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.		✓								✓		
3	Mengumpulkan skenario resiko saat ini menurut kategori, lini bisnis, dan area fungsional		✓								✓		
4	Secara teratur mendata semua informasi profil resiko dan menggabungkannya ke dalam profil resiko gabungan.	✓									✓		
5	Mendata informasi tentang status rencana tindakan resiko untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		
6	Berdasarkan semua data profil resiko, tentukan seperangkat indikator resiko yang memungkinkan identifikasi dan monitoring resiko saat ini secara tepat.	✓									✓		
7	Mendata informasi tentang peristiwa resiko TI yang telah terwujud untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		

APO 12.04 – Articulate Risk

Komunikasikan informasi tentang status saat ini dari eksposur terkait TI dan peluan secara tepat waktu untuk semua pemangku kepentingan yang dibutuhkan respon yang tepat.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Laporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam format tertentu yang berguna untuk mendukung keputusan RSUD Tarakan.		✓								✓		
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait TI.		✓								✓		
3	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, dan gap.		✓								✓		
4	Secara berkala, identifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan.		✓								✓		
5	Meninjau hasil penilaian pihak ketiga yang obyektif dan audit internal. Sertakan mereka di profil risiko.		✓								✓		

APO 12.05 – Define A Risk Management Action Portofolio
Kelola peluang untuk menguranggi resiko ke tingkat yang dapat di terima sebagai portofolio.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Klasifikasikan aktivitas pengendalian dan petakan pada skenario risiko TI.		✓								✓		
2	Tentukan apakah setiap entitas organisasi memantau risiko dan memiliki peran.		✓								✓		
3	Buat proposal proyek yang dirancang untuk mengurangi risiko dan / atau proyek yang memiliki peluang dengan mempertimbangkan risiko TI.		✓								✓		

APO 12.06 – Respon To Risk

Menanggapi secara tepat waktu kejadian resiko yang terwujud dengan efektif Langkah-langkah untuk membatasi besarnya kerugian

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan terhentinya operasional bisnis.		✓								✓		
2	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.		✓								✓		
3	Komunikasikan respon risiko kepada pengambil keputusan sebagai bagian dari pelaporan dan pembaharuan profil risiko.		✓								✓		
4	Memeriksa kerugian masa lalu dan peluang yang hilang dan menentukan akar penyebabnya.	✓									✓		
5	Komunikasikan akar masalah, respons risiko dan perbaikan proses kepada pengambil keputusan yang tepat.		✓								✓		

KUESIONER SURVEY

Penilaian Capability Level APO 12 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **APO 12 – Managed Risk**. Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Swandhi Prabowo
Email	Swandhi prabowoshakti@gmail.com
Unit Kerja	P.D. E
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Align, Plan, Organize
Objek Manajemen	:	APO 12 - Managed Risk

Deskripsi :
Identifikasi, nilai, dan kurangi resiko terkait TI secara berkelanjutan dalam tingkat toleransi yang di tetapkan oleh manajemen eksekutif organisasi / RSUD

Tujuan :
Mengintegrasikan manajemen resiko organisasi / RSUD terkait IT dengan manajemen resiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola resiko perusahaan terkait TI.

APO 12.01 – Collect Data

Identifikasi, dan kumpulkan data yang relevan untuk mengaktifkan resiko terkait TI yang efektifitas identifikasi, analisis dan pelaporan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait resiko TI		✓								✓		
2	Catat data terkait resiko terkait TI yang relevan dan signifikan di lingkungan internal dan external RSUD		✓								✓		
3	Mengadopsi atau mendefinisikan resiko untuk definisi yang konsisten dari skenario resiko dan dampak		✓								✓		
4	Catat data tentang peristiwa resiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak		✓								✓		
5	Survei dan analisis data resiko TI terkait kerugian dari data dan tren yang tersedia secara eksternal.		✓								✓		
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan konstribusi umum faktor di berbagai peristiwa.	✓									✓		
7	Tentukan kondisi spesifik yang dapat mempengaruhi resiko		✓								✓		
8	Lakukan analisis faktor resiko secara berkala untuk mengidentifikasi masalah resiko barau atau yang muncul dan untuk mendapatkan pemahaman tentang faktor resiko internal dan eksternal terkait.		✓								✓		

APO 12.02 – Analyze Risk
Kembangkan pandangan yang dibuktikan tentang resiko TI actual, untuk mendukung kkeputusan resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan cakupan yang tepat dari upaya analisis resiko, dengan mempertimbangkan semua faktor resiko.		✓								✓		
2	Membangun dan memperbarui scenario resiko TI secara teratur, identifikasi kerugian terkait TI.	✓									✓		
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario realko TI. Mempertimbangkan semua faktor resiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓								✓		
4	Bandingkan resiko saat ini (eksposur kerugian terkait TI) dengan toleransi resiko yang dapat diterima.		✓								✓		
5	Mengusulkan respon resiko untuk resiko yang melebihi tingkat toleransi.		✓								✓		
6	Identifikasi persyaratan dan target untuk respon mitigasi resiko yang optimal.	✓									✓		
7	Validasi hasil analisis resiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	✓									✓		
8	Menganalisis manfaat dari opsi respon resiko yang dipilih , konfirmasikan respon resiko yang optimal.	✓									✓		

APO 12.03 – Maintain A Risk Profile
Menjaga inventaris resiko yang diketahui dan atribut resiko, termasuk frekuensi yang diharapkan, potensi dampak dan tanggapan. Dokumen terkait sumber daya, kapabilitas dan aktivitas pengendalian saat ini yang berkaitan dengan item resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menginventarisir proses layanan TI dan proses bisnis. Identifikasi pensonel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		✓								✓		
2	Menentukan dan menyetujui layanan TI dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.	✓									✓		
3	Mengumpulkan skenario resiko saat ini menurut kategori, lini bisnis, dan area fungsional		✓								✓		
4	Secara teratur mendata semua informasi profil resiko dan menggabungkannya ke dalam profil resiko gabungan.	✓									✓		
5	Mendata informasi tentang status rencana tindakan resiko untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		
6	Berdasarkan semua data profil resiko, tentukan seperangkat indikator resiko yang memungkinkan identifikasi dan monitoring resiko saat ini secara tepat.	✓									✓		
7	Mendata informasi tentang peristiwa resiko TI yang telah terwujud untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		

APO 12.04 – Articulate Risk
Komunikasikan informasi tentang status saat ini dari eksposur terkait TI dan peluan secara tepat waktu untuk semua pemangku kepentingan yang dibutuhkan respon yang tepat.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Laporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam format tertentu yang berguna untuk mendukung keputusan RSUD Tarakan.	✓									✓		
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait TI.		✓								✓		
3	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, dan gap.	✓									✓		
4	Secara berkala, identifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan.		✓								✓		
5	Meninjau hasil penilaian pihak ketiga yang obyektif dan audit internal. Sertakan mereka di profil risiko.		✓								✓		

APO 12.05 – Define A Risk Management Action Portofolio
Kelola peluang untuk menguranggi resiko ke tingkat yang dapat di terima sebagai portofolio.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Klasifikasikan aktivitas pengendalian dan petakan pada skenario risiko TI.		✓								✓		
2	Tentukan apakah setiap entitas organisasi memantau risiko dan memiliki peran.		✓								✓		
3	Buat proposal proyek yang dirancang untuk mengurangi risiko dan / atau proyek yang memiliki peluang dengan mempertimbangkan risiko TI.		✓								✓		

APO 12.06 – Respon To Risk
Menanggapi secara tepat waktu kejadian resiko yang terwujud dengan efektif Langkah-langkah untuk membatasi besarnya kerugian

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan terhentinya operasional bisnis.		✓								✓		
2	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.		✓								✓		
3	Komunikasikan respon risiko kepada pengambil keputusan sebagai bagian dari pelaporan dan pembaharuan profil risiko.		✓								✓		
4	Memeriksa kerugian masa lalu dan peluang yang hilang dan menentukan akar penyebabnya.		✓								✓		
5	Komunikasikan akar masalah, respons risiko dan perbaikan proses kepada pengambil keputusan yang tepat.		✓								✓		

KUESIONER SURVEY

Penilaian Capability Level APO 12 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **APO 12 – Managed Risk**. Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	ERICK SEPTIA.H
Email	erik.sephi@gmail.com
Unit Kerja	PDE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Align, Plan, Organize
Objek Manajemen	:	APO 12 - Managed Risk

Deskripsi :
Identifikasi, nilai, dan kurangi resiko terkait TI secara berkelanjutan dalam tingkat toleransi yang di tetapkan oleh manajemen eksekutif organisasi / RSUD

Tujuan :
Mengintegrasikan manajemen resiko organisasi / RSUD terkait IT dengan manajemen resiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola resiko perusahaan terkait TI.

APO 12.01 – Collect Data

Identifikasi, dan kumpulkan data yang relevan untuk mengaktifkan resiko terkait TI yang efektifitas identifikasi, analisis dan pelaporan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait resiko TI		✓								✓		
2	Catat data terkait resiko terkait TI yang relevan dan signifikan di lingkungan internal dan external RSUD		✓								✓		
3	Mengadopsi atau mendefinisikan resiko untuk definisi yang konsisten dari skenario resiko dan dampak		✓								✓		
4	Catat data tentang peristiwa resiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak		✓								✓		
5	Survei dan analisis data resiko TI terkait kerugian dari data dan tren yang tersedia secara eksternal.	✓									✓		
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan konstribusi umum faktor di berbagai peristiwa.	✓									✓		
7	Tentukan kondisi spesifik yang dapat mempengaruhi resiko		✓								✓		
8	Lakukan analisis faktor resiko secara berkala untuk mengidentifikasi masalah resiko barau atau yang muncul dan untuk mendapatkan pemahaman tentang faktor resiko internal dan eksternal terkait.		✓								✓		

APO 12.02 – Analyze Risk
Kembangkan pandangan yang dibuktikan tentang resiko TI actual, untuk mendukung kkeputusan resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan cakupan yang tepat dari upaya analisis resiko, dengan mempertimbangkan semua faktor resiko.	✓									✓		
2	Membangun dan memperbarui scenario resiko TI secara teratur, identifikasi kerugian terkait TI.	✓									✓		
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario resiko TI. Mempertimbangkan semua faktor resiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓								✓		
4	Bandingkan resiko saat ini (eksposur kerugian terkait TI) dengan toleransi resiko yang dapat diterima.		✓								✓		
5	Mengusulkan respon resiko untuk resiko yang melebihi tingkat toleransi.		✓								✓		
6	Identifikasi persyaratan dan target untuk respon mitigasi resiko yang optimal.	✓									✓		
7	Validasi hasil analisis resiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	✓									✓		
8	Menganalisis manfaat dari opsi respon resiko yang dipilih . konfirmasikan respon resiko yang optimal.	✓									✓		

APO 12.03 – Maintain A Risk Profile

Menjaga inventaris resiko yang diketahui dan atribut resiko, termasuk frekuensi yang diharapkan, potensi dampak dan tanggapan. Dokumen terkait sumber daya, kapabilitas dan aktivitas pengendalian saat ini yang berkaitan dengan item resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menginventarisir proses layanan TI dan proses bisnis. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		✓								✓		
2	Menentukan dan menyetujui layanan TI dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.	✓									✓		
3	Mengumpulkan skenario resiko saat ini menurut kategori, ini bisnis, dan area fungsional		✓								✓		
4	Secara teratur mendata semua informasi profil resiko dan menggabungkannya ke dalam profil resiko gabungan.	✓									✓		
5	Mendata informasi tentang status rencana tindakan resiko untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		
6	Berdasarkan semua data profil resiko, tentukan seperangkat indikator resiko yang memungkinkan identifikasi dan monitoring resiko saat ini secara tepat.	✓									✓		
7	Mendata informasi tentang peristiwa resiko TI yang telah terwujud untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		

APO 12.04 – Articulate Risk
Komunikasikan informasi tentang status saat ini dari eksposur terkait TI dan peluan secara tepat waktu untuk semua pemangku kepentingan yang dibutuhkan respon yang tepat.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Laporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam format tertentu yang berguna untuk mendukung keputusan RSUD Tarakan.		✓								✓		
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait TI.			✓							✓		
3	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, dan gap.		✓								✓		
4	Secara berkala, identifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan.			✓							✓		
5	Meninjau hasil penilaian pihak ketiga yang obyektif dan audit internal. Sertakan mereka di profil risiko.			✓							✓		

APO 12.05 – Define A Risk Management Action Portofolio
Kelola peluang untuk menguranggi resiko ke tingkat yang dapat di terima sebagai portofolio.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Klasifikasikan aktivitas pengendalian dan petakan pada skenario risiko TI.		✓								✓		
2	Tentukan apakah setiap entitas organisasi memantau risiko dan memiliki peran.		✓								✓		
3	Buat proposal proyek yang dirancang untuk mengurangi risiko dan / atau proyek yang memiliki peluang dengan mempertimbangkan risiko TI.		✓								✓		

APO 12.06 – Respon To Risk

Menanggapi secara tepat waktu kejadian resiko yang terwujud dengan efektif Langkah-langkah untuk membatasi besarnya kerugian

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan terhentinya operasional bisnis.		✓								✓		
2	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.		✓								✓		
3	Komunikasikan respon risiko kepada pengambil keputusan sebagai bagian dari pelaporan dan pembaharuan profil risiko.		✓								✓		
4	Memeriksa kerugian masa lalu dan peluang yang hilang dan menentukan akar penyebabnya.		✓								✓		
5	Komunikasikan akar masalah, respons risiko dan perbaikan proses kepada pengambil keputusan yang tepat.		✓								✓		

KUESIONER SURVEY

Penilaian Capability Level APO 12 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **APO 12 – Managed Risk.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Tyo
Email	wasedamas5@gmail
Unit Kerja	PDE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Align, Plan, Organize
Objek Manajemen	:	APO 12 - Managed Risk

Deskripsi :
Identifikasi, nilai, dan kurangi resiko terkait TI secara berkelanjutan dalam tingkat toleransi yang di tetapkan oleh manajemen eksekutif organisasi / RSUD

Tujuan :
Mengintegrasikan manajemen resiko organisasi / RSUD terkait IT dengan manajemen resiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola resiko perusahaan terkait TI.

APO 12.01 – Collect Data

Identifikasi, dan kumpulkan data yang relevan untuk mengaktifkan resiko terkait TI yang efektifitas identifikasi, analisis dan pelaporan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait resiko TI		✓								✓		
2	Catat data terkait resiko terkait TI yang relevan dan signifikan di lingkungan internal dan external RSUD		✓								✓		
3	Mengadopsi atau mendefinisikan resiko untuk definisi yang konsisten dari skenario resiko dan dampak		✓								✓		
4	Catat data tentang peristiwa resiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak		✓								✓		
5	Survei dan analisis data resiko TI terkait kerugian dan data dan tren yang tersedia secara eksternal.		✓								✓		
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan konstribusi umum faktor di berbagai peristiwa.	✓									✓		
7	Tentukan kondisi spesifik yang dapat mempengaruhi resiko		✓								✓		
8	Lakukan analisis faktor resiko secara berkala untuk mengidentifikasi masalah resiko barau atau yang muncul dan untuk mendapatkan pemahaman tentang faktor resiko internal dan eksternal terkait.		✓								✓		

APO 12.02 – Analyze Risk
Kembangkan pandangan yang dibuktikan tentang resiko TI actual, untuk mendukung kkeputusan resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan cakupan yang tepat dari upaya analisis resiko, dengan mempertimbangkan semua faktor resiko.	✓									✓		
2	Membangun dan memperbarui scenario resiko TI secara teratur, identifikasi kerugian terkait TI.	✓									✓		
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario resiko TI. Mempertimbangkan semua faktor resiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓								✓		
4	Bandingkan resiko saat ini (eksposur kerugian terkait TI) dengan toleransi resiko yang dapat diterima.		✓								✓		
5	Mengusulkan respon resiko untuk resiko yang melebihi tingkat toleransi.		✓								✓		
6	Identifikasi persyaratan dan target untuk respon mitigasi resiko yang optimal.	✓									✓		
7	Validasi hasil analisis resiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	✓									✓		
8	Menganalisis manfaat dari opsi respon resiko yang dipilih . konfirmasikan respon resiko yang optimal.	✓									✓		

APO 12.03 – Maintain A Risk Profile
Menjaga inventaris resiko yang diketahui dan atribut resiko, termasuk frekuensi yang diharapkan, potensi dampak dan tanggapan. Dokumen terkait sumber daya, kapabilitas dan aktivitas pengendalian saat ini yang berkaitan dengan item resiko.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menginventarisir proses layanan TI dan proses bisnis. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		✓								✓		
2	Menentukan dan menyetujui layanan TI dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.	✓									✓		
3	Mengumpulkan skenario resiko saat ini menurut kategori, lini bisnis, dan area fungsional		✓								✓		
4	Secara teratur mendata semua informasi profil resiko dan menggabungkannya ke dalam profil resiko gabungan.	✓									✓		
5	Mendata informasi tentang status rencana tindakan resiko untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		
6	Berdasarkan semua data profil resiko, tentukan seperangkat indikator resiko yang memungkinkan identifikasi dan monitoring resiko saat ini secara tepat.	✓									✓		
7	Mendata informasi tentang peristiwa resiko TI yang telah terwujud untuk dimasukkan dalam profil resiko TI RSUD.	✓									✓		

APO 12.04 – Articulate Risk

Komunikasikan informasi tentang status saat ini dari eksposur terkait TI dan peluan secara tepat waktu untuk semua pemangku kepentingan yang dibutuhkan respon yang tepat.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Laporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam format tertentu yang berguna untuk mendukung keputusan RSUD Tarakan.	✓									✓		
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait TI.		✓								✓		
3	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, dan gap.	✓									✓		
4	Secara berkala, identifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan.		✓								✓		
5	Meninjau hasil penilaian pihak ketiga yang obyektif dan audit internal. Sertakan mereka di profil risiko.		✓								✓		

APO 12.05 – Define A Risk Management Action Portofolio
Kelola peluang untuk menguranggi resiko ke tingkat yang dapat di terima sebagai portofolio.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Klasifikasikan aktivitas pengendalian dan petakan pada skenario risiko TI.		✓								✓		
2	Tentukan apakah setiap entitas organisasi memantau risiko dan memiliki peran.		✓								✓		
3	Buat proposal proyek yang dirancang untuk mengurangi risiko dan / atau proyek yang memiliki peluang dengan mempertimbangkan risiko TI.		✓								✓		

APO 12.06 – Respon To Risk
Menanggapi secara tepat waktu kejadian resiko yang terwujud dengan efektif Langkah-langkah untuk membatasi besarnya kerugian

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan terhentinya operasional bisnis.		✓								✓		
2	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.		✓								✓		
3	Komunikasikan respon risiko kepada pengambil keputusan sebagai bagian dari pelaporan dan pembaharuan profil risiko.		✓								✓		
4	Memeriksa kerugian masa lalu dan peluang yang hilang dan menentukan akar penyebabnya.		✓								✓		
5	Komunikasikan akar masalah, respons risiko dan perbaikan proses kepada pengambil keputusan yang tepat.		✓								✓		

KUESIONER SURVEY

DSS 05
Managed Security Services

KUESIONER SURVEY

Penilaian Capability Level DSS 05 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **DSS05 – Managed Security Services**. Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Dr. Heryono Puncasila Apt. Sp.FRS
Email	–
Unit Kerja	Wadir Umum
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Delivery, Service, and Support
Objek Manajeman	:	DSS05 Managed Security Services

Deskripsi :
Lindungi informasi perusahaan untuk menjaga tingkat resiko keamanan informasi yang dapat diterima oleh perusahaan / RSUD sesuai dengan kebijakan keamanan. Tetapkan dan pertahankan peran keamanan informasi dan hak akses. Lakukan pemantauan keamanan.

Tujuan :
Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional

DSS 05.01 – Protect Against Malicious Software

Menetapkan dan memelihara Tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan control virus) di file perusahaan/ / RSUD untuk melindunggi sistem informasi dan teknologi dari kejahatan perangkat linak (mis, ransomware, malware, virus, word, soyware, dan spam)

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Instal dan aktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas pemrosesan		✓								✓		
2	Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (misalnya, spyware, email phishing).		✓								✓		
3	Komunikasikan kesadaran akan ancaman malware. Lakukan pelatihan berkala tentang malware dalam email dan penggunaan internet.		✓								✓		
4	Mendistribusikan anti virus secara terpusat.		✓								✓		
5	Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau keamanan produk dan layanan vendor)	✓									✓		

DSS05.02 – Manage Network and Connectivity Security

Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi atas semua metode konektivitas.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Izinkan hanya perangkat resmi yang memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasi perangkat ini untuk entri kata sandi.		✓								✓		
2	Menerapkan mekanisme penyaringan jaringan, seperti firewall.		✓								✓		
3	Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.		✓								✓		
4	Konfigurasi peralatan jaringan dengan cara yang aman.		✓								✓		
5	Berdasarkan penilaian risiko dan kebutuhan bisnis, menetapkan dan memelihara kebijakan keamanan konektivitas.	✓									✓		
6	Menetapkan mekanisme terpercaya untuk transformasi informasi yang aman.	✓									✓		
7	Melakukan pengujian keamanan sistem secara berkala untuk menentukan kecukupan perlindungan sistem.	✓									✓		

DSS 05.03 – Manage Endpoint Scunty
Pastikan titik akhir (misalnya laptop, desktop, server dan handphone lainnya serta perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi, disimpan atau dikirim.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman.		✓								✓		
2	Menerapkan mekanisme penguncian perangkat.	✓									✓		
3	Kelola akses dan kontrol jarak jauh (mis., perangkat seluler, teleworking).	✓									✓		
4	Kelola konfigurasi jaringan dengan cara yang aman.	✓									✓		
5	Menerapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.		✓								✓		
6	Lindungi integritas sistem.		✓								✓		
7	Memberikan perlindungan fisik perangkat titik akhir.		✓								✓		
8	Kelola akses jahat melalui email dan browser web. Misalnya, blokir situs web tertentu.	✓									✓		

DSS 05.04 – Manage User Identity and Logical Access

Memastikan bahwa semua pengguna memiliki hak akases informasi yang sesuai dengan persyaratan bisnis. Berkoordinasi dengan unit bisnis yang mengelolanya memiliki hak akses dalam proses bisnis solusi inovatif untuk dikembangkan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan.		✓								✓		
2	Mengelola semua perubahan pada hak akses (pembuatan, modifikasi dan penghapusan) secara tepat waktu hanya berdasarkan persetujuan dan transaksi terdokumentasi yang disahkan oleh personel yang berwewenang.	✓									✓		
3	Pastikan pemantauan pada akun yang memiliki hak istimewa.	✓									✓		
4	Berkoordinasi dengan unit bisnis untuk memastikan bahwa semua peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam aplikasi proses bisnis.	✓									✓		
5	Lakukan analisis pasca latihan untuk evaluasi.	✓									✓		
6	Mengautentikasi semua akses ke aset informasi berdasarkan peran individu atau aturan bisnis. Berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan.	✓									✓		
7	Menjaga jejak akses ke informasi tergantung pada tingkat kerahasiaan.	✓									✓		
8	Lakukan tinjauan manajemen secara rutin pada semua akun dan hak istimewa terkait.	✓									✓		

DSS 05.05 – Manage Physical Access to I&T Assets

Tentukan dan terapkan prosedur (termasuk prosedur darurat) untuk memberikan, membatasi dan mencabut akses ke tempat, bangunan dan area, sesuai dengan kebutuhan bisnis. Akses ke gedung, Gedung, dan area harus di benarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, smeentara staf, client, vendor, pengunjung, atau pihak ketiga lainnya.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Daftarkan semua pengunjung, termasuk kontraktor dan vendor.		✓								✓		
2	Pastikan semua personel menampilkan identifikasi yang disetujui dengan benar setiap saat.		✓								✓		
3	Mengharuskan pengunjung untuk didampingi setiap saat berada di lokasi.		✓								✓		
4	Batasi dan pantau akses ke situs TI yang sensitif dengan menetapkan batasan perimeter, seperti pagar, dinding, dan keamanan perangkat di pintu interior dan eksterior.		✓								✓		
5	Kelola permintaan untuk mengizinkan akses resmi yang sesuai ke fasilitas komputasi.		✓								✓		
6	Pastikan profil akses tetap terkini. Akses dasar ke situs TI (ruang server, gedung, area atau zona) pada fungsi pekerjaan dan tanggung jawab.		✓								✓		
7	Lakukan pelatihan kesadaran keamanan informasi fisik secara teratur. Panduan Terkait (Standar, Kerangka Kerja, Persyaratan Kepatuhan).	✓									✓		

DSS 05.06 – Manage Sensitive Documents and Outout Devices

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset TI sensitive, seperti formular khusus, instrument yang dapat di negosiasikan, printer tujuan khusus dan token keamanan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif perusahaan.	✓									✓		
2	Tetapkan hak akses istimewa kepada jabatan tertentu berdasarkan keputusan manajemen.		✓								✓		
3	Buat inventarisasi dokumen sensitif perusahaan.	✓									✓		
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.	✓									✓		

DSS 05.07 – Manage Vulnerabilities and Monitor the Infrastructure for Security – Related Events
Menggunakan portofolio alat dan teknologi (misalnya , Deteksi instruksi alat), mengelola kerentanan dan memantau infrastruktur akses tidak sah. Pastikan bahwa alat keamanan, teknologi dan deteksi terintegrasi dengan pemantauan dan insiden peristiwa umum pengelolaan.

No	Aktivitas Tata Kelola	As – Is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Terus gunakan tools untuk mengidentifikasi kerentanan keamanan informasi.	✓									✓		
2	Tentukan dan komunikasikan skenario risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.		✓								✓		
3	Tinjau data peristiwa secara teratur untuk mengetahui potensi insiden.	✓									✓		
4	Pastikan kejadian terkait keamanan dikelola tepat waktu untuk identifikasi potensi risiko.	✓									✓		
5	Catat kejadian terkait keamanan dan simpan catatan untuk periode yang sesuai.	✓									✓		

KUESIONER SURVEY

Penilaian Capability Level DSS 05 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **DSS05 – Managed Security Services.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Irma Ulfa, S.Kom
Email	irmaulfa@gmail.com
Unit Kerja	Instalasi PDE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Delivery, Service, and Support
Objek Manajemen	:	DSS05 Managed Security Services

Deskripsi :
Lindungi informasi perusahaan untuk menjaga tingkat resiko keamanan informasi yang dapat diterima oleh perusahaan / RSUD sesuai dengan kebijakan keamanan. Tetapkan dan pertahankan peran keamanan informasi dan hak akses. Lakukan pemantauan keamanan.

Tujuan :
Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional

DSS 05.01 – Protect Against Malicious Software

Menetapkan dan memelihara Tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan control virus) di file perusahaan/ / RSUD untuk melindunggi sistem informasi dan teknologi dari kejahatan perangkat linak (mis, ransomware, malware, virus, word, soyware, dan spam)

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Instal dan aktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas pemrosesan.		✓								✓		
2	Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (misalnya, spyware, email phishing).		✓								✓		
3	Komunikasikan kesadaran akan ancaman malware. Lakukan pelatihan berkala tentang malware dalam email dan penggunaan internet.		✓								✓		
4	Mendistribusikan anti virus secara terpusat.		✓								✓		
5	Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau keamanan produk dan layanan vendor).	✓									✓		

DSS05.02 – Manage Network and Connectivity Security

Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindunggi informasi atas semua metode konektivitas.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Izinkan hanya perangkat resmi yang memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasi perangkat ini untuk entri kata sandi.		✓								✓		
2	Menerapkan mekanisme penyaringan jaringan, seperti firewall.		✓								✓		
3	Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.		✓								✓		
4	Konfigurasi peralatan jaringan dengan cara yang aman.		✓								✓		
5	Berdasarkan penilaian risiko dan kebutuhan bisnis, menetapkan dan memelihara kebijakan keamanan konektivitas.	✓									✓		
6	Menetapkan mekanisme terpercaya untuk transformasi informasi yang aman.		✓								✓		
7	Melakukan pengujian keamanan sistem secara berkala untuk menentukan kecukupan perlindungan sistem.	✓									✓		

DSS 05.03 – Manage Endpoint Scurity
Pastikan titik akhir (misalnya laptop, desktop, server dan handphone lainnya serta perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi, disimpan atau dikirim.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman.		✓								✓		
2	Menerapkan mekanisme penguncian perangkat.		✓								✓		
3	Kelola akses dan kontrol jarak jauh (mis., perangkat seluler, teleworking).		✓								✓		
4	Kelola konfigurasi jaringan dengan cara yang aman.		✓								✓		
5	Menerapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.		✓								✓		
6	Lindungi integritas sistem.		✓								✓		
7	Memberikan perlindungan fisik perangkat titik akhir.		✓								✓		
8	Kelola akses jahat melalui email dan browser web. Misalnya, blokir situs web tertentu.		✓								✓		

DSS 05.04 – Manage User Identity and Logical Access

Memastikan bahwa semua pengguna memiliki hak akases informasi yang sesuai dengan persyaratan bisnis. Berkoordinasi dengan unit bisnis yang mengelolanya memiliki hak akses dalam proses bisnis solusi inovatif untuk dikembangkan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan.		✓								✓		
2	Mengelola semua perubahan pada hak akses (pembuatan, modifikasi dan penghapusan) secara tepat waktu hanya berdasarkan persetujuan dan transaksi terdokumentasi yang disahkan oleh personel yang berwewenang.		✓								✓		
3	Pastikan pemantauan pada akun yang memiliki hak istimewa.		✓								✓		
4	Berkoordinasi dengan unit bisnis untuk memastikan bahwa semua peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam aplikasi proses bisnis.		✓								✓		
5	Lakukan analisis pasca latihan untuk evaluasi.	✓									✓		
6	Mengautentikasi semua akses ke aset informasi berdasarkan peran individu atau aturan bisnis. Berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan.	✓									✓		
7	Menjaga jejak akses ke informasi tergantung pada tingkat kerahasiaan.	✓									✓		
8	Lakukan tinjauan manajemen secara rutin pada semua akun dan hak istimewa terkait.	✓									✓		

DSS 05.05 – Manage Physical Access to I&T Assets

Tentukan dan terapkan prosedur (termasuk prosedur darurat) untuk memberikan, membatasi dan mencabut akses ke tempat, bangunan dan area, sesuai dengan kebutuhan bisnis. Akses ke gedung, Gedung, dan area harus di benarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, smeentara staf, client, vendor, pengunjung, atau pihak ketiga lainnya.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Daftarkan semua pengunjung, termasuk kontraktor dan vendor.		✓								✓		
2	Pastikan semua personel menampilkan identifikasi yang disetujui dengan benar setiap saat.		✓								✓		
3	Mengharuskan pengunjung untuk didampingi setiap saat berada di lokasi.		✓								✓		
4	Batasi dan pantau akses ke situs TI yang sensitif dengan menetapkan batasan perimeter, seperti pagar, dinding, dan keamanan perangkat di pintu interior dan eksterior.		✓								✓		
5	Kelola permintaan untuk mengizinkan akses resmi yang sesuai ke fasilitas komputasi.		✓								✓		
6	Pastikan profil akses tetap terkini. Akses dasar ke situs TI (ruang server, gedung, area atau zona) pada fungsi pekerjaan dan tanggung jawab.		✓								✓		
7	Lakukan pelatihan kesadaran keamanan informasi fisik secara teratur. Panduan Terkait (Standar, Kerangka Kerja, Persyaratan Kepatuhan).	✓									✓		

DSS 05.05 – Manage Sensitive Documents and Outout Devices

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset TI sensitive, seperti formular khusus, instrument yang dapat di negosiasikan, printer tujuan khusus dan token keamanan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif perusahaan.	✓									✓		
2	Tetapkan hak akses istimewa kepada jabatan tertentu berdasarkan keputusan manajemen.	✓									✓		
3	Buat inventarisasi dokumen sensitif perusahaan.	✓									✓		
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.		✓								✓		

DSS 05.07 – Manage Vulnerabilities and Monitor the Infrastructure for Security – Related Events
Menggunakan portofolio alat dan teknologi (misalnya , Deteksi instruksi alat), mengelola kerentanan dan memantau infrastruktur akses tidak sah. Pastikan bahwa alat keamanan, teknologi dan deteksi terintegrasi dengan pemantauan dan insiden peristiwa umum pengelolaan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Terus gunakan tools untuk mengidentifikasi kerentanan keamanan informasi.		✓								✓		
2	Tentukan dan komunikasikan skenario risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.			✓							✓		
3	Tinjau data peristiwa secara teratur untuk mengetahui potensi insiden.		✓								✓		
4	Pastikan kejadian terkait keamanan dikelola tepat waktu untuk identifikasi potensi risiko.		✓								✓		
5	Catat kejadian terkait keamanan dan simpan catatan untuk periode yang sesuai.		✓								✓		

KUESIONER SURVEY

Penilaian Capability Level DSS 05 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **DSS05 – Managed Security Services.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktifitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	SWANDHI PRABOWO
Email	Swandiprabowo81rsbt@gmail.com
Unit Kerja	P.O.E
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Delivery, Service, and Support
Objek Manajemen	:	DSS05 Managed Security Services

Deskripsi :
Lindungi informasi perusahaan untuk menjaga tingkat resiko keamanan informasi yang dapat diterima oleh perusahaan / RSUD sesuai dengan kebijakan keamanan. Tetapkan dan pertahankan peran keamanan informasi dan hak akses. Lakukan pemantauan keamanan.

Tujuan :
Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional

DSS 05.01 – Protect Against Malicious Software

Menetapkan dan memelihara Tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan control virus) di file perusahaan/ / RSUD untuk melindunggi sistem informasi dan teknologi dari kejahatan perangkat lunak (mis, ransomware, malware, virus, word, soyware, dan spam)

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Instal dan aktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas pemrosesan.		✓								✓		
2	Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (misalnya, spyware, email phishing).	✓									✓		
3	Komunikasikan kesadaran akan ancaman malware. Lakukan pelatihan berkala tentang malware dalam email dan penggunaan internet.		✓								✓		
4	Mendistribusikan anti virus secara terpusat.	✓									✓		
5	Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau keamanan produk dan layanan vendor).	✓									✓		

DSS05.02 – Manage Network and Connectivity Security

Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindunggi informasi atas semua metode konektivitas.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Izinkan hanya perangkat resmi yang memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasi perangkat ini untuk entri kata sandi.		✓								✓		
2	Menerapkan mekanisme penyaringan jaringan, seperti firewall.		✓								✓		
3	Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.		✓								✓		
4	Konfigurasi peralatan jaringan dengan cara yang aman.		✓								✓		
5	Berdasarkan penilaian risiko dan kebutuhan bisnis, menetapkan dan memelihara kebijakan keamanan konektivitas.	✓									✓		
6	Menetapkan mekanisme terpercaya untuk transformasi informasi yang aman.		✓								✓		
7	Melakukan pengujian keamanan sistem secara berkala untuk menentukan kecukupan perlindungan sistem.	✓									✓		

DSS 05.03 – Manage Endpoint Scurity

Pastikan titik akhir (misalnya laptop, desktop, server dan handphone lainnya serta perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi, disimpan atau dikirim.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman.		✓								✓		
2	Menerapkan mekanisme penguncian perangkat.		✓								✓		
3	Kelola akses dan kontrol jarak jauh (mis., perangkat seluler, teleworking).		✓								✓		
4	Kelola konfigurasi jaringan dengan cara yang aman.		✓								✓		
5	Menerapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.		✓								✓		
6	Lindungi integritas sistem.		✓								✓		
7	Memberikan perlindungan fisik perangkat titik akhir.		✓								✓		
8	Kelola akses jahat melalui email dan browser web. Misalnya, blokir situs web tertentu.	✓									✓		

DSS 05.04 – Manage User Identity and Logical Access

Memastikan bahwa semua pengguna memiliki hak akases informasi yang sesuai dengan persyaratan bisnis. Berkoordinasi dengan unit bisnis yang mengelolanya memiliki hak akses dalam proses bisnis solusi inovatif untuk dikembangkan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan.		✓								✓		
2	Mengelola semua perubahan pada hak akses (pembuatan, modifikasi dan penghapusan) secara tepat waktu hanya berdasarkan persetujuan dan transaksi terdokumentasi yang disahkan oleh personel yang berwewenang.		✓								✓		
3	Pastikan pemantauan pada akun yang memiliki hak istimewa.		✓								✓		
4	Berkoordinasi dengan unit bisnis untuk memastikan bahwa semua peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam aplikasi proses bisnis.		✓								✓		
5	Lakukan analisis pasca latihan untuk evaluasi.	✓									✓		
6	Mengautentikasi semua akses ke aset informasi berdasarkan peran individu atau aturan bisnis. Berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan.		✓								✓		
7	Menjaga jejak akses ke informasi tergantung pada tingkat kerahasiaan.		✓								✓		
8	Lakukan tinjauan manajemen secara rutin pada semua akun dan hak istimewa terkait.	✓									✓		

DSS 05.05 – Manage Physical Access to I&T Assets

Tentukan dan terapkan prosedur (termasuk prosedur darurat) untuk memberikan, membatasi dan mencabut akses ke tempat, bangunan dan area, sesuai dengan kebutuhan bisnis. Akses ke gedung, Gedung, dan area harus di benarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, smeentara staf, client, vendor, pengunjung, atau pihak ketiga lainnya.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Daftarkan semua pengunjung, termasuk kontraktor dan vendor.		✓								✓		
2	Pastikan semua personel menampilkan identifikasi yang disetujui dengan benar setiap saat.		✓								✓		
3	Mengharuskan pengunjung untuk didampingi setiap saat berada di lokasi.		✓								✓		
4	Batasi dan pantau akses ke situs TI yang sensitif dengan menetapkan batasan perimeter, seperti pagar, dinding, dan keamanan perangkat di pintu interior dan eksterior.		✓								✓		
5	Kelola permintaan untuk mengizinkan akses resmi yang sesuai ke fasilitas komputasi.		✓								✓		
6	Pastikan profil akses tetap terkini. Akses dasar ke situs TI (ruang server, gedung, area atau zona) pada fungsi pekerjaan dan tanggung jawab.		✓								✓		
7	Lakukan pelatihan kesadaran keamanan informasi fisik secara teratur. Panduan Terkait (Standar, Kerangka Kerja, Persyaratan Kepatuhan).	✓									✓		

DSS 05.06 – Manage Sensitive Documents and Outout Devices

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset TI sensitive, seperti formular khusus, instrument yang dapat di negosiasikan, printer tujuan khusus dan token keamanan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif perusahaan.	✓									✓		
2	Tetapkan hak akses istimewa kepada jabatan tertentu berdasarkan keputusan manajemen.	✓									✓		
3	Buat inventarisasi dokumen sensitif perusahaan.	✓									✓		
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.		✓								✓		

DSS 05.07 – Manage Vulnerabilities and Monitor the Infrastructure for Security – Related Events
Menggunakan portofolio alat dan teknologi (misalnya , Deteksi instruksi alat), mengelola kerentanan dan memantau infrastruktur akses tidak sah. Pastikan bahwa alat keamanan, teknologi dan deteksi terintegrasi dengan pemantauan dan insiden peristiwa umum pengelolaan.

No	Aktivitas Tata Keloia	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Terus gunakan tools untuk mengidentifikasi kerentanan keamanan informasi.	✓									✓		
2	Tentukan dan komunikasikan skenario risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.		✓								✓		
3	Tinjau data peristiwa secara teratur untuk mengetahui potensi insiden.	✓									✓		
4	Pastikan kejadian terkait keamanan dikelola tepat waktu untuk identifikasi potensi risiko.	✓									✓		
5	Catat kejadian terkait keamanan dan simpan catatan untuk periode yang sesuai.	✓									✓		

KUESIONER SURVEY

Penilaian Capability Level DSS 05 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **DSS05 – Managed Security Services.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktifitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	ERICK SEPTIA - H
Email	erik . seph@gmail . com
Unit Kerja	POE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Delivery, Service, and Support
Objek Manajemen	:	DSS05 Managed Security Services

Deskripsi :
Lindungi informasi perusahaan untuk menjaga tingkat resiko keamanan informasi yang dapat diterima oleh perusahaan / RSUD sesuai dengan kebijakan keamanan. Tetapkan dan pertahankan peran keamanan informasi dan hak akses. Lakukan pemantauan keamanan.

Tujuan :
Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional

DSS 05.01 – Protect Against Malicious Software

Menetapkan dan memelihara Tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan control virus) di file perusahaan/ / RSUD untuk melindungi sistem informasi dan teknologi dari kejahatan perangkat linak (mis, ransomware, malware, virus, word, soyware, dan spam)

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Instal dan aktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas pemrosesan.		✓								✓		
2	Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (misalnya, spyware, email phishing).		✓								✓		
3	Komunikasikan kesadaran akan ancaman malware. Lakukan pelatihan berkala tentang malware dalam email dan penggunaan internet.		✓								✓		
4	Mendistribusikan anti virus secara terpusat.		✓								✓		
5	Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau keamanan produk dan layanan vendor).		✓								✓		

DSS05.02 – Manage Network and Connectivity Security

Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindunggi informasi atas semua metode konektivitas.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Izinkan hanya perangkat resmi yang memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasi perangkat ini untuk entri kata sandi.		✓								✓		
2	Menerapkan mekanisme penyaringan jaringan, seperti firewall.		✓								✓		
3	Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.		✓								✓		
4	Konfigurasi peralatan jaringan dengan cara yang aman.		✓								✓		
5	Berdasarkan penilaian risiko dan kebutuhan bisnis, menetapkan dan memelihara kebijakan keamanan konektivitas.		✓								✓		
6	Menetapkan mekanisme terpercaya untuk transformasi informasi yang aman.			✓							✓		
7	Melakukan pengujian keamanan sistem secara berkala untuk menentukan kecukupan perlindungan sistem.	✓									✓		

DSS 05.03 – Manage Endpoint Scurity

Pastikan titik akhir (misalnya laptop, desktop, server dan handphone lainnya serta perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi, disimpan atau dikirim.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman.		✓								✓		
2	Menerapkan mekanisme penguncian perangkat.		✓								✓		
3	Kelola akses dan kontrol jarak jauh (mis., perangkat seluler, teleworking).		✓								✓		
4	Kelola konfigurasi jaringan dengan cara yang aman.		✓								✓		
5	Menerapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.		✓								✓		
6	Lindungi integritas sistem.		✓								✓		
7	Memberikan perlindungan fisik perangkat titik akhir.		✓								✓		
8	Kelola akses jahat melalui email dan browser web. Misalnya, blokir situs web tertentu.		✓								✓		

DSS 05.04 – Manage User Identity and Logical Access

Memastikan bahwa semua pengguna memiliki hak akases informasi yang sesuai dengan persyaratan bisnis. Berkoordinasi dengan unit bisnis yang mengelolanya memiliki hak akses dalam proses bisnis solusi inovatif untuk dikembangkan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan.		✓								✓		
2	Mengelola semua perubahan pada hak akses (pembuatan, modifikasi dan penghapusan) secara tepat waktu hanya berdasarkan persetujuan dan transaksi terdokumentasi yang disahkan oleh personel yang berwewenang.	✓									✓		
3	Pastikan pemantauan pada akun yang memiliki hak istimewa.		✓								✓		
4	Berkoordinasi dengan unit bisnis untuk memastikan bahwa semua peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam aplikasi proses bisnis.	✓									✓		
5	Lakukan analisis pasca latihan untuk evaluasi.	✓									✓		
6	Mengautentikasi semua akses ke aset informasi berdasarkan peran individu atau aturan bisnis. Berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan.		✓								✓		
7	Menjaga jejak akses ke informasi tergantung pada tingkat kerahasiaan.	✓									✓		
8	Lakukan tinjauan manajemen secara rutin pada semua akun dan hak istimewa terkait.	✓									✓		

DSS 05.05 – Manage Physical Access to I&T Assets

Tentukan dan terapkan prosedur (termasuk prosedur darurat) untuk memberikan, membatasi dan mencabut akses ke tempat, bangunan dan area, sesuai dengan kebutuhan bisnis. Akses ke gedung, Gedung, dan area harus di benarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, smeentara staf, client, vendor, pengunjung, atau pihak ketiga lainnya.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Daftarkan semua pengunjung, termasuk kontraktor dan vendor.		✓								✓		
2	Pastikan semua personel menampilkan identifikasi yang disetujui dengan benar setiap saat.		✓								✓		
3	Mengharuskan pengunjung untuk didampingi setiap saat berada di lokasi.		✓								✓		
4	Batasi dan pantau akses ke situs TI yang sensitif dengan menetapkan batasan perimeter, seperti pagar, dinding, dan keamanan perangkat di pintu interior dan eksterior.			✓							✓		
5	Kelola permintaan untuk mengizinkan akses resmi yang sesuai ke fasilitas komputasi.			✓							✓		
6	Pastikan profil akses tetap terkini. Akses dasar ke situs TI (ruang server, gedung, area atau zona) pada fungsi pekerjaan dan tanggung jawab.			✓							✓		
7	Lakukan pelatihan kesadaran keamanan informasi fisik secara teratur. Panduan Terkait (Standar, Kerangka Kerja, Persyaratan Kepatuhan).	✓									✓		

DSS 05.06 – Manage Sensitive Documents and Outout Devices

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset TI sensitive, seperti formular khusus, instrument yang dapat di negosiasikan, printer tujuan khusus dan token keamanan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif perusahaan.		✓								✓		
2	Tetapkan hak akses istimewa kepada jabatan tertentu berdasarkan keputusan manajemen.		✓								✓		
3	Buat inventarisasi dokumen sensitif perusahaan.		✓								✓		
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.		✓								✓		

DSS 05.07 – Manage Vulnerabilities and Monitor the Infrastructure for Security – Related Events
Menggunakan portofolio alat dan teknologi (misalnya , Deteksi instruksi alat), mengelola kerentanan dan memantau infrastruktur akses tidak sah. Pastikan bahwa alat keamanan, teknologi dan deteksi terintegrasi dengan pemantauan dan insiden peristiwa umum pengelolaan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Terus gunakan tools untuk mengidentifikasi kerentanan keamanan informasi.	✓									✓		
2	Tentukan dan komunikasikan skenario risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.		✓								✓		
3	Tinjau data peristiwa secara teratur untuk mengetahui potensi insiden.	✓									✓		
4	Pastikan kejadian terkait keamanan dikelola tepat waktu untuk identifikasi potensi risiko.	✓									✓		
5	Catat kejadian terkait keamanan dan simpan catatan untuk periode yang sesuai.		✓								✓		

KUESIONER SURVEY

BAI 06

Build, Acquire, and Implement

KUESIONER SURVEY

Penilaian Capability Level BAI 06 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **BAI06 – Build, Acquire, and Implement.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Drs. Prijono Pancasilan Apt, Sp. FRS
Email	-
Unit Kerja	Wadir Umum
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Build, Acquire, and Implement
Objek Manajemen	:	BAI06 Managed it Changes

Deskripsi :
Mengeloia semua perubahan dengan cara yang terkendali, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi dan infrastruktur. Ini termasuk perubahan standar dan prosedur, penilaian dampak, prioritas dan otorisasi, perubahan darurat, pelacakan, pelaporan, penutupan, dan dokumentasi.

Tujuan :
Memungkinkan realisasi perubahan yang cepat dan andal ke bisnis proses perusahaan dan menguranggi resiko berdampak negatif terhadap stabilitas pada perubahan lingkungan tersebut.

BAI 06.01 – Evaluate, prioritize and authorize change requests.

Mengevaluasi semua permintaan perubahan untuk menentukan dampak pada proses bisnis dan layanan TI, dan untuk menilai apakah perubahan akan berdampak buruh pada lingkungan operasional dan menimbulkan resiko yang tidak dapat diterima. Pastikan bahwa perubahan dicatat, diprioritaskan, dikategorikan, dinilai, disahkan, direncanakan, dan di jadwalkan.

No	Aktivitas Tata Kelola	As – Is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Permintaan perubahan pasa proses bisnis dan TI termasuk infrastruktur, sistem, dan aplikasi harus dilakukan secara formal dan disetujui oleh manajemen.	✓									✓		
2	Kategorikan semua perubahan yang diminta (misalnya, proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, perangkat lunak aplikasi yang dibeli/dikemas) dan menghubungkan item konfigurasi yang terpengaruh terhadap perubahan		✓								✓		
3	Memprioritaskan semua perubahan yang diminta berdasarkan persyaratan bisnis dan teknis, sumber daya yang dibutuhkan, dan alasan hukum, peraturan dan secara kontraktual.		✓								✓		
4	Perubahan resmi disetujui oleh pemilik proses bisnis, manajer layanan dan pemangku kepentingan teknis TI serta perubahan dengan resiko rendah yang relatif sering harus di setujui sebelumnya sebagai perubahan standar.	✓									✓		
5	Rencana dan jadwalkan semua perubahan yang disetujui.	✓									✓		
6	Merencanakan, mengevaluasi dan menilai semua permintaan perubahan TI secara terstruktur dengan melibatkan manajemen RSUD. Sertakan analisis dampak pada proses bisnis, infrastruktur, sistem dan aplikasi, rencana kelangsungan bisnis (BCP) dan penyedia layanan untuk memastikan bahwa semua komponen yang		✓								✓		

	terpengaruh telah diidentifikasi. Menilai kemungkinan dampak negative terhadap lingkungan operasional dan resiko penerapan perubahan. Pertimbangkan implikasi keamanan, privasi, hukum, kontrak dan kepatuhan dari perubahan yang diminta. Pertimbangkan juga saling ketergantungan antar perubahan yang diinginkan.													
7	Pada proses manajemen perubahan pertimbangkan dampak penyedia layanan yang dikontrak (misalnya, pemrosesan bisnis yang dialihdayakan, infrastruktur, pengembangan aplikasi, dan layanan bersama). Sertakan integrasi proses manajemen perubahan RSUD dengan proses manajemen perubahan penyedia layanan dan dampaknya terhadap persyaratan kontrak dan SLA.	✓									✓			

BAI06 06.02 – Manage emergency changes

Pastikan perubahan tata Kelola TI terkendali dan berlangsung dengan aman guna meminimalkan insiden lebih lanjut. Verifikasi perubahan untuk di nilai dan disahkan oleh manajemen.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan mana yang merupakan perubahan darurat		✓								✓		
2	Prosedur perubahan darurat terdokumentasi dan meliputi untuk menyatakan, menilai, menyetujui awal, mengotorisasi, dan mencatat setelah perubahan darurat.	✓									✓		
3	Setelah perubahan darurat diterapkan lakukan verifikasi pengaturan akses darurat untuk diotorisasi, didokumentasikan dan di cabut.	✓									✓		
4	Melakukan monitoring semua perubahan darurat dan melakukan tinjauan pasca implementasi yang melibatkan semua pihak terkait. Tinjauan harus mempertimbangkan dan memulai Tindakan korektif berdasarkan akar penyebab seperti masalah dengan proses bisnis, pengembangkan dan pemeliharaan sistem aplikasi, lingkungan pengembangan dan pangujian, dokumentasi dan manual, serta integritas data.	✓									✓		

BAI06.06.03 – Track and report change status
Lakukan pemeliharaan sistem pelacakan dan pelaporan untuk mendokumentasikan perubahan yang tidak disetujui dan mengkomunikasikan status perubahan yang disetujui ke dalam proses lengkap. Pastikan bahwa perubahan yang disetujui diimplementasikan sesuai rencana.

No	Aktivitas Tata Kelola	As – Is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengkategorikan permintaan perubahan dalam proses klasifikasi (misalnya dengan status ditolak, disetujui tetapi belum di mulai, disetujui dan dalam proses, dan selesai)		✓								✓		
2	Menerapkan laporan status perubahan sehingga perubahan selanjutnya dapat dilacak dari awal hingga disposisi akhir	✓									✓		
3	Monitoring akan prioritas dari perubahan yang berlangsung dan pastikan bahwa semua perubahan yang disetujui diselesaikan tepat waktu.		✓								✓		
4	Berlakukan sistem pelacakan dan pelaporan untuk semua permintaan perubahan	✓									✓		

BAI06 06.04 – Close and document the changes
Setiap kali perubahan diterapkan, perbarui solusi, dokumentasi pengguna, dan prosedur yang terpengaruh oleh perubahan tersebut

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menyertakan perubahan di dokumentasi dalam prosedur manajemen. Contoh dokumentasi prosedur operasional bisnis dan TI, kontinuitas bisnis dan dokumentasi	✓									✓		
2	Menetapkan periode penyimpanan untuk dokumentasi baik sebelum dan sesudah dilakukan perubahan, serta dokumentasu pengguna.	✓									✓		
3	Melakukan dokumentasi subjek perubahan ke tingkat tinjauan yang sama dengan perubahan yang sebenarnya.	✓									✓		

KUESIONER SURVEY

Penilaian Capability Level BAI 06 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **BAI06 – Build, Acquire, and Implement.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Irma Ulfa, S.Kom
Email	Irmaulfa@email.com
Unit Kerja	Instalasi PDE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Build, Acquire, and Implement
Objek Manajemen	:	BAI06 Managed it Changes

Deskripsi :
Mengelola semua perubahan dengan cara yang terkendali, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi dan infrastruktur. Ini termasuk perubahan standar dan prosedur, penilaian dampak, prioritas dan otorisasi, perubahan darurat, pelacakan, pelaporan, penutupan, dan dokumentasi.

Tujuan :
Memungkinkan realisasi perubahan yang cepat dan andal ke bisnis proses perusahaan dan menguranggi resiko berdampak negatif terhadap stabilitas pada perubahan lingkungan tersebut.

BAI 06.01 – Evaluate, prioritize and authorize change requests.

Mengevaluasi semua permintaan perubahan untuk menentukan dampak pada proses bisnis dan layanan TI, dan untuk menilai apakah perubahan akan berdampak buruh pada lingkungan operasional dan menimbulkan resiko yang tidak dapat diterima. Pastikan bahwa perubahan dicatat, diprioritaskan, dikategorikan, dinilai, disahkan, direncanakan, dan di jadwalkan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Permintaan perubahan pasa proses bisnis dan TI termasuk infrastruktur, sistem, dan aplikasi harus dilakukan secara formal dan disetujui oleh manajemen.	✓									✓		
2	Kategorikan semua perubahan yang diminta (misalnya, proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, perangkat lunak aplikasi yang dibeli/dikemas) dan menghubungkan item konfigurasi yang terpengaruh terhadap perubahan		✓								✓		
3	Memprioritaskan semua perubahan yang diminta berdasarkan persyaratan bisnis dan teknis, sumber daya yang dibutuhkan, dan alasan hukum, peraturan dan secara kontraktual.		✓								✓		
4	Perubahan resmi disetujui oleh pemilik proses bisnis, manajer layanan dan pemangku kepentingan teknis TI serta perubahan dengan resiko rendah yang relatif sering harus di setujui sebelumnya sebagai perubahan standar.	✓									✓		
5	Rencana dan jadwalkan semua perubahan yang disetujui.	✓									✓		
6	Merencanakan, mengevaluasi dan menilai semua permintaan perubahan TI secara terstruktur dengan melibatkan manajemen RSUD. Sertakan analisis dampak pada proses bisnis, infrastruktur, sistem dan aplikasi, rencana kelangsungan bisnis (BCP) dan penyedia layanan untuk memastikan bahwa semua komponen yang		✓								✓		

	terpengaruh telah diidentifikasi. Menilai kemungkinan dampak negative terhadap lingkungan operasional dan resiko penerapan perubahan. Pertimbangkan implikasi keamanan, privasi, hukum, kontrak dan kepatuhan dari perubahan yang diminta. Pertimbangkan juga saling ketergantungan antar perubahan yang diinginkan.												
7	Pada proses manajemen perubahan pertimbangkan dampak penyedia layanan yang dikontrak (misalnya, pemrosesan bisnis yang dialihdayakan, infrastruktur, pengembangan aplikasi, dan layanan bersama). Sertakan integrasi proses manajemen perubahan RSUD dengan proses manajemen perubahan penyedia layanan dan dampaknya terhadap persyaratan kontrak dan SLA.	✓									✓		

BAI06 06.02 – Manage emergency changes

Pastikan perubahan tata Kelola TI terkendali dan berlangsung dengan aman guna meminimalkan insiden lebih lanjut. Verifikasi perubahan untuk di nilai dan disahkan oleh manajemen.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan mana yang merupakan perubahan darurat		✓								✓		
2	Prosedur perubahan darurat terdokumentasi dan meliputi untuk menyatakan, menilai, menyetujui awal, mengotorisasi, dan mencatat setelah perubahan darurat	✓									✓		
3	Setelah perubahan darurat diterapkan lakukan verifikasi pengaturan akses darurat untuk diotorisasi, didokumentasikan dan di cabut.	✓									✓		
4	Melakukan monitoring semua perubahan darurat dan melakukan tinjauan pasca implementasi yang melibatkan semua pihak terkait. Tinjauan harus mempertimbangkan dan memulai Tindakan korektif berdasarkan akar penyebab seperti masalah dengan proses bisnis, pengembangkan dan pemeliharaan sistem aplikasi, lingkungan pengembangan dan pangujian, dokumentasi dan manual, serta integritas data.	✓									✓		

BAI06 06.03 – Track and report change status

Lakukan pemeliharaan sistem pelacakan dan pelaporan untuk mendokumentasikan perubahan yang tidak disetujui dan mengkomunikasikan status perubahan yang disetujui ke dalam proses lengkap. Pastikan bahwa perubahan yang disetujui diimplementasikan sesuai rencana.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengkategorikan permintaan perubahan dalam proses klasifikasi (misalnya dengan status ditolak, disetujui tetapi belum di mulai, disetujui dan dalam proses, dan selesai)		✓								✓		
2	Menerapkan laporan status perubahan sehingga perubahan selanjutnya dapat dilacak dari awal hingga disposisi akhir	✓									✓		
3	Monitoring akan prioritas dari perubahan yang berlangsung dan pastikan bahwa semua perubahan yang disetujui diselesaikan tepat waktu.		✓								✓		
4	Berlakukan sistem pelacakan dan pelaporan untuk semua permintaan perubahan	✓									✓		

BAI06 06.04 – Close and document the changes
Setiap kali perubahan diterapkan, perbarui solusi, dokumentasi pengguna, dan prosedur yang terpengaruh oleh perubahan tersebut

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menyertakan perubahan di dokumentasi dalam prosedur manajemen. Contoh dokumentasi prosedur operasional bisnis dan TI, kontinuitas bisnis dan dokumentasi		✓								✓		
2	Menetapkan periode penyimpanan untuk dokumentasi baik sebelum dan sesudah dilakukan perubahan, serta dokumentasu pengguna.		✓								✓		
3	Melakukan dokumentasi subjek perubahan ke tingkat tinjauan yang sama dengan perubahan yang sebenarnya.	✓									✓		

KUESIONER SURVEY

Penilaian Capability Level BAI 06 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **BAI06 – Build, Acquire, and Implement**. Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Swandi prabowo
Email	swandiprabowoshakti@gmail.com
Unit Kerja	P.D.E
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Build, Acquire, and Implement
Objek Manajemen	:	BAI06 Managed it Changes

Deskripsi :
Mengelola semua perubahan dengan cara yang terkendali, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi dan infrastruktur. Ini termasuk perubahan standar dan prosedur, penilaian dampak, prioritas dan otorisasi, perubahan darurat, pelacakan, pelaporan, penutupan, dan dokumentasi.

Tujuan :
Memungkinkan realisasi perubahan yang cepat dan andal ke bisnis proses perusahaan dan menguranggi resiko berdampak negatif terhadap stabilitas pada perubahan lingkungan tersebut.

BAI 06.01 – Evaluate, prioritize and authorize change requests.

Mengevaluasi semua permintaan perubahan untuk menentukan dampak pada proses bisnis dan layanan TI, dan untuk menilai apakah perubahan akan berdampak buruh pada lingkungan operasional dan menimbulkan resiko yang tidak dapat diterima. Pastikan bahwa perubahan dicatat, diprioritaskan, dikategorikan, dinilai, disahkan, direncanakan, dan di jadwalkan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Permintaan perubahan pasa proses bisnis dan TI termasuk infrastruktur, sistem, dan aplikasi harus dilakukan secara formal dan disetujui oleh manajemen.	✓									✓		
2	Kategorikan semua perubahan yang diminta (misalnya, proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, perangkat lunak aplikasi yang dibeli/dikemas) dan menghubungkan item konfigurasi yang terpengaruh terhadap perubahan		✓								✓		
3	Memprioritaskan semua perubahan yang diminta berdasarkan persyaratan bisnis dan teknis, sumber daya yang dibutuhkan, dan alasan hukum, peraturan dan secara kontraktual.		✓								✓		
4	Perubahan resmi disetujui oleh pemilik proses bisnis, manajer layanan dan pemangku kepentingan teknis TI serta perubahan dengan resiko rendah yang relatif sering harus di setujui sebelumnya sebagai perubahan standar.	✓									✓		
5	Rencana dan jadwalkan semua perubahan yang disetujui.	✓									✓		
6	Merencanakan, mengevaluasi dan menilai semua permintaan perubahan TI secara terstruktur dengan melibatkan manajemen RSUD. Sertakan analisis dampak pada proses bisnis, infrastruktur, sistem dan aplikasi, rencana kelangsungan bisnis (BCP) dan penyedia layanan untuk memastikan bahwa semua komponen yang		✓								✓		

	terpengaruh telah diidentifikasi. Menilai kemungkinan dampak negative terhadap lingkungan operasional dan resiko penerapan perubahan. Pertimbangkan implikasi keamanan, privasi, hukum, kontrak dan kepatuhan dari perubahan yang diminta. Pertimbangkan juga saling ketergantungan antar perubahan yang diinginkan.															
7	Pada proses manajemen perubahan pertimbangkan dampak penyedia layanan yang dikontrak (misalnya, pemrosesan bisnis yang dialihdayakan, infrastruktur, pengembangan aplikasi, dan layanan bersama). Sertakan integrasi proses manajemen perubahan RSUD dengan proses manajemen perubahan penyedia layanan dan dampaknya terhadap persyaratan kontrak dan SLA.				✓								✓			

BAI06 06.02 – Manage emergency changes

Pastikan perubahan tata Kelola TI terkendali dan berlangsung dengan aman guna meminimalkan insiden lebih lanjut. Verifikasi perubahan untuk di nilai dan disahkan oleh manajemen.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan mana yang merupakan perubahan darurat		✓								✓		
2	Prosedur perubahan darurat terdokumentasi dan meliputi untuk menyatakan, menilai, menyetujui awal, mengotorisasi, dan mencatat setelah perubahan darurat.	✓									✓		
3	Setelah perubahan darurat diterapkan lakukan verifikasi pengaturan akses darurat untuk diotorisasi, didokumentasikan dan di cabut.	✓									✓		
4	Melakukan monitoring semua perubahan darurat dan melakukan tinjauan pasca implementasi yang melibatkan semua pihak terkait. Tinjauan harus mempertimbangkan dan memulai Tindakan korektif berdasarkan akar penyebab seperti masalah dengan proses bisnis, pengembangkan dan pemeliharaan sistem aplikasi, lingkungan pengembangan dan pangujian, dokumentasi dan manual, serta integritas data.	✓									✓		

BAI06 06.03 – Track and report change status

Lakukan pemeliharaan sistem pelacakan dan pelaporan untuk mendokumentasikan perubahan yang tidak disetujui dan mengkomunikasikan status perubahan yang disetujui ke dalam proses lengkap. Pastikan bahwa perubahan yang disetujui diimplementasikan sesuai rencana.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengkategorikan permintaan perubahan dalam proses klasifikasi (misalnya dengan status ditolak, disetujui tetapi belum di mulai, disetujui dan dalam proses, dan selesai)		✓								✓		
2	Menerapkan laporan status perubahan sehingga perubahan selanjutnya dapat dilacak dari awal hingga disposisi akhir	✓									✓		
3	Monitoring akan prioritas dari perubahan yang berlangsung dan pastikan bahwa semua perubahan yang disetujui diselesaikan tepat waktu.	✓									✓		
4	Berlakukan sistem pelacakan dan pelaporan untuk semua permintaan perubahan	✓									✓		

BAI06 06.04 – Close and document the changes

Setiap kali perubahan diterapkan, perbarui solusi, dokumentasi pengguna, dan prosedur yang terpengaruh oleh perubahan tersebut

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menyertakan perubahan di dokumentasi dalam prosedur manajemen. Contoh dokumentasi prosedur operasional bisnis dan TI, kontinuitas bisnis dan dokumentasi	✓									✓		
2	Menetapkan periode penyimpanan untuk dokumentasi baik sebelum dan sesudah dilakukan perubahan, serta dokumentasu pengguna.	✓									✓		
3	Melakukan dokumentasi subjek perubahan ke tingkat tinjauan yang sama dengan perubahan yang sebenarnya.	✓									✓		

KUESIONER SURVEY

Penilaian Capability Level BAI 06 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **BAI06 – Build, Acquire, and Implement.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	ERICK SEPTIA H
Email	e.rik.sophi@gmail.com
Unit Kerja	PDE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Build, Acquire, and Implement
Objek Manajemen	:	BAI06 Managed it Changes

Deskripsi :
Mengelola semua perubahan dengan cara yang terkendali, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi dan infrastruktur. Ini termasuk perubahan standar dan prosedur, penilaian dampak, prioritas dan otorisasi, perubahan darurat, pelacakan, pelaporan, penutupan, dan dokumentasi.

Tujuan :
Memungkinkan realisasi perubahan yang cepat dan andal ke bisnis proses perusahaan dan menguranggi resiko berdampak negatif terhadap stabilitas pada perubahan lingkungan tersebut.

BAI 06.01 – Evaluate, prioritize and authorize change requests.

Mengevaluasi semua permintaan perubahan untuk menentukan dampak pada proses bisnis dan layanan TI, dan untuk menilai apakah perubahan akan berdampak buruh pada lingkungan operasional dan menimbulkan resiko yang tidak dapat diterima. Pastikan bahwa perubahan dicatat, diprioritaskan, dikategorikan, dinilai, disahkan, direncanakan, dan di jadwalkan.

No	Aktivitas Tata Kelola	As – Is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Permintaan perubahan pasa proses bisnis dan TI termasuk infrastruktur, sistem, dan aplikasi harus dilakukan secara formal dan disetujui oleh manajemen.	✓									✓		
2	Kategorikan semua perubahan yang diminta (misalnya, proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, perangkat lunak aplikasi yang dibeli/dikemas) dan menghubungkan item konfigurasi yang terpengaruh terhadap perubahan		✓								✓		
3	Memprioritaskan semua perubahan yang diminta berdasarkan persyaratan bisnis dan teknis, sumber daya yang dibutuhkan, dan alasan hukum, peraturan dan secara kontraktual.		✓								✓		
4	Perubahan resmi disetujui oleh pemilik proses bisnis, manajer layanan dan pemangku kepentingan teknis TI serta perubahan dengan resiko rendah yang relatif sering harus di setujui sebelumnya sebagai perubahan standar.	✓									✓		
5	Rencana dan jadwalkan semua perubahan yang disetujui.	✓									✓		
6	Merencanakan, mengevaluasi dan menilai semua permintaan perubahan TI secara terstruktur dengan melibatkan manajemen RSUD. Sertakan analisis dampak pada proses bisnis, infrastruktur, sistem dan aplikasi, rencana kelangsungan bisnis (BCP) dan penyedia layanan untuk memastikan bahwa semua komponen yang		✓								✓		

	terpengaruh telah diidentifikasi. Menilai kemungkinan dampak negative terhadap lingkungan operasional dan resiko penerapan perubahan. Pertimbangkan implikasi keamanan, privasi, hukum, kontrak dan kepatuhan dari perubahan yang diminta. Pertimbangkan juga saling ketergantungan antar perubahan yang diinginkan.																
7	Pada proses manajemen perubahan pertimbangkan dampak penyedia layanan yang dikontrak (misalnya, pemrosesan bisnis yang dialihdayakan, infrastruktur, pengembangan aplikasi, dan layanan bersama). Sertakan integrasi proses manajemen perubahan RSUD dengan proses manajemen perubahan penyedia layanan dan dampaknya terhadap persyaratan kontrak dan SLA	✓										✓					

BAI06 06.02 – Manage emergency changes

Pastikan perubahan tata Kelola TI terkendali dan berlangsung dengan aman guna meminimalkan insiden lebih lanjut. Verifikasi perubahan untuk di nilai dan disahkan oleh manajemen.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan mana yang merupakan perubahan darurat		✓								✓		
2	Prosedur perubahan darurat terdokumentasi dan meliputi untuk menyatakan, menilai, menyetujui awal, mengotorisasi, dan mencatat setelah perubahan darurat.	✓									✓		
3	Setelah perubahan darurat diterapkan lakukan verifikasi pengaturan akses darurat untuk diotorisasi, didokumentasikan dan di cabut.	✓									✓		
4	Melakukan monitoring semua perubahan darurat dan melakukan tinjauan pasca implementasi yang melibatkan semua pihak terkait. Tinjauan harus mempertimbangkan dan memulai Tindakan korektif berdasarkan akar penyebab seperti masalah dengan proses bisnis, pengembangkan dan pemeliharaan sistem aplikasi, lingkungan pengembangan dan pangujian, dokumentasi dan manual, serta integritas data.	✓									✓		

BAI06 06.03 – Track and report change status

Lakukan pemeliharaan sistem pelacakan dan pelaporan untuk mendokumentasikan perubahan yang tidak disetujui dan mengkomunikasikan status perubahan yang disetujui ke dalam proses lengkap. Pastikan bahwa perubahan yang disetujui diimplementasikan sesuai rencana.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengkategorikan permintaan perubahan dalam proses klasifikasi (misalnya dengan status ditolak, disetujui tetapi belum di mulai, disetujui dan dalam proses, dan selesai)		✓								✓		
2	Menerapkan laporan status perubahan sehingga perubahan selanjutnya dapat dilacak dari awal hingga disposisi akhir	✓									✓		
3	Monitoring akan prioritas dari perubahan yang berlangsung dan pastikan bahwa semua perubahan yang disetujui diselesaikan tepat waktu.		✓								✓		
4	Berlakukan sistem pelacakan dan pelaporan untuk semua permintaan perubahan	✓									✓		

BAI06 06.04 – Close and document the changes

Setiap kali perubahan diterapkan, perbarui solusi, dokumentasi pengguna, dan prosedur yang terpengaruh oleh perubahan tersebut

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menyertakan perubahan di dokumentasi dalam prosedur manajemen. Contoh dokumentasi prosedur operasional bisnis dan TI, kontinuitas bisnis dan dokumentasi		✓								✓		
2	Menetapkan periode penyimpanan untuk dokumentasi baik sebelum dan sesudah dilakukan perubahan, serta dokumentasu pengguna.			✓							✓		
3	Melakukan dokumentasi subjek perubahan ke tingkat tinjauan yang sama dengan perubahan yang sebenarnya.	✓									✓		

KUESIONER SURVEY

Penilaian Capability Level BAI 06 COBIT 2019

Perkenalkan nama saya Sophian mahasiswa Magister Teknik Informatika Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Audit Tata Kelola Teknologi Informasi menggunakan framework Cobit 2019.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **BAI06 – Build, Acquire, and Implement.** Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut :

0 Tidak adanya kemampuan dasar, pendekatan yang tidak sempurna untuk menangani tata Kelola dan manajemen, tidak ada perhatian atau konsen terhadap permasalahan.

1 Aktvitas yang dilakukan kurang lebih telah mencapai tujuannya melalu penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif – tidak terlalu terorganisir.

2 Aktifitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.

3 Aktfitas yang dilakukan terlah mencapai tujuannya dengan cara yang jauh lebnih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefenisikan dengan baik.

4 Aktifitas yang dilakukan telah mencapai tujuannya, didefenisikan dengan baik dan kinerjanya dapat diukur secara kuantitatif.

5 Proses telah mencapai tujuan, terdefenisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan.

Di dalam kuesioner ini ada 2 isian, yaitu tingkat kapabilitas saat ini (as-is) dan tingkat kapabilitas yang diinginkan (to-be)

Identitas Responden	
Nama Responden	Tyo
Email	wongedan455@gmail.com
Unit Kerja	PDE
Organisasi / Perusahaan	RSUD Tarakan
Paraf	

Domain	:	Build, Acquire, and Implement
Objek Manajemen	:	BAI06 Managed it Changes

Deskripsi :
Mengelola semua perubahan dengan cara yang terkendali, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi dan infrastruktur. Ini termasuk perubahan standar dan prosedur, penilaian dampak, prioritas dan otorisasi, perubahan darurat, pelacakan, pelaporan, penutupan, dan dokumentasi.

Tujuan :
Memungkinkan realisasi perubahan yang cepat dan andal ke bisnis proses perusahaan dan menguranggi resiko berdampak negatif terhadap stabilitas pada perubahan lingkungan tersebut.

BAI 06.01 – Evaluate, prioritize and authorize change requests.

Mengevaluasi semua permintaan perubahan untuk menentukan dampak pada proses bisnis dan layanan TI, dan untuk menilai apakah perubahan akan berdampak buruh pada lingkungan operasional dan menimbulkan resiko yang tidak dapat diterima. Pastikan bahwa perubahan dicatat, diprioritaskan, dikategorikan, dinilai, disahkan, direncanakan, dan di jadwalkan.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Permintaan perubahan pasa proses bisnis dan TI termasuk infrastruktur, sistem, dan aplikasi harus dilakukan secara formal dan disetujui oleh manajemen.	✓									✓		
2	Kategorikan semua perubahan yang diminta (misalnya, proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, perangkat lunak aplikasi yang dibeli/dikemas) dan menghubungkan item konfigurasi yang terpengaruh terhadap perubahan		✓								✓		
3	Memprioritaskan semua perubahan yang diminta berdasarkan persyaratan bisnis dan teknis, sumber daya yang dibutuhkan, dan alasan hukum, peraturan dan secara kontraktual.		✓									✓	
4	Perubahan resmi disetujui oleh pemilik proses bisnis, manajer layanan dan pemangku kepentingan teknis TI serta perubahan dengan resiko rendah yang relatif sering harus di setujui sebelumnya sebagai perubahan standar.	✓										✓	
5	Rencana dan jadwalkan semua perubahan yang disetujui.	✓										✓	
6	Merencanakan, mengevaluasi dan menilai semua permintaan perubahan TI secara terstruktur dengan melibatkan manajemen RSUD. Sertakan analisis dampak pada proses bisnis, infrastruktur, sistem dan aplikasi, rencana kelangsungan bisnis (BCP) dan penyedia layanan untuk memastikan bahwa semua komponen yang		✓									✓	

	terpengaruh telah diidentifikasi. Menilai kemungkinan dampak negative terhadap lingkungan operasional dan resiko penerapan perubahan. Pertimbangkan implikasi keamanan, privasi, hukum, kontrak dan kepatuhan dari perubahan yang diminta. Pertimbangkan juga saling ketergantungan antar perubahan yang diinginkan.															
7	Pada proses manajemen perubahan pertimbangkan dampak penyedia layanan yang dikontrak (misalnya, pemrosesan bisnis yang dialihdayakan, infrastruktur, pengembangan aplikasi, dan layanan bersama). Sertakan integrasi proses manajemen perubahan RSUD dengan proses manajemen perubahan penyedia layanan dan dampaknya terhadap persyaratan kontrak dan SLA.														✓	

BAI06 06.02 – Manage emergency changes

Pastikan perubahan tata Kelola TI terkendali dan berlangsung dengan aman guna meminimalkan insiden lebih lanjut. Verifikasi perubahan untuk di nilai dan disahkan oleh manajemen.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menentukan mana yang merupakan perubahan darurat		✓								✓		
2	Prosedur perubahan darurat terdokumentasi dan meliputi untuk menyatakan, menilai, menyetujui awal, mengotorisasi, dan mencatat setelah perubahan darurat.	✓									✓		
3	Setelah perubahan darurat diterapkan lakukan verifikasi pengaturan akses darurat untuk diotorisasi, didokumentasikan dan di cabut.	✓									✓		
4	Melakukan monitoring semua perubahan darurat dan melakukan tinjauan pasca implementasi yang melibatkan semua pihak terkait. Tinjauan harus mempertimbangkan dan memulai Tindakan korektif berdasarkan akar penyebab seperti masalah dengan proses bisnis, pengembangkan dan pemeliharaan sistem aplikasi, lingkungan pengembangan dan pangujian, dokumentasi dan manual, serta integritas data.	✓									✓		

BAI06 06.03 – Track and report change status

Lakukan pemeliharaan sistem pelacakan dan pelaporan untuk mendokumentasikan perubahan yang tidak disetujui dan mengkomunikasikan status perubahan yang disetujui ke dalam proses lengkap. Pastikan bahwa perubahan yang disetujui diimplementasikan sesuai rencana.

No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengkategorikan permintaan perubahan dalam proses klasifikasi (misalnya dengan status ditolak, disetujui tetapi belum di mulai, disetujui dan dalam proses, dan selesai)		✓								✓		
2	Menerapkan laporan status perubahan sehingga perubahan selanjutnya dapat dilacak dari awal hingga disposisi akhir	✓									✓		
3	Monitoring akan prioritas dari perubahan yang berlangsung dan pastikan bahwa semua perubahan yang disetujui diselesaikan tepat waktu.	✓									✓		
4	Berlakukan sistem pelacakan dan pelaporan untuk semua permintaan perubahan	✓									✓		

BAI06 06.04 – Close and document the changes
Setiap kali perubahan diterapkan, perbarui solusi, dokumentasi pengguna, dan prosedur yang terpengaruh oleh perubahan tersebut

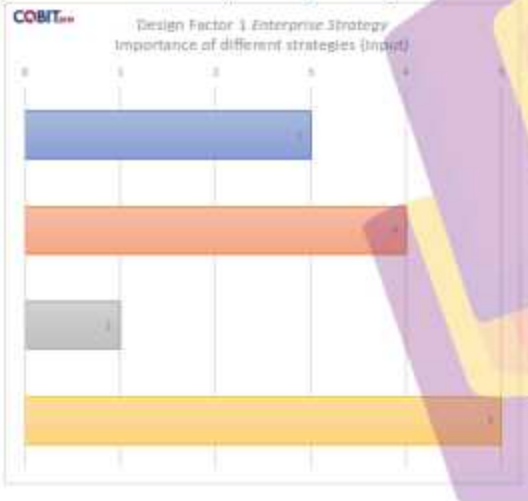
No	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Menyertakan perubahan di dokumentasi dalam prosedur manajemen. Contoh dokumentasi prosedur operasional bisnis dan TI, kontinuitas bisnis dan dokumentasi	✓									✓		
2	Menetapkan periode penyimpanan untuk dokumentasi baik sebelum dan sesudah dilakukan perubahan, serta dokumentasu pengguna.	✓									✓		
3	Melakukan dokumentasi subjek perubahan ke tingkat tinjauan yang sama dengan perubahan yang sebenarnya.	✓									✓		

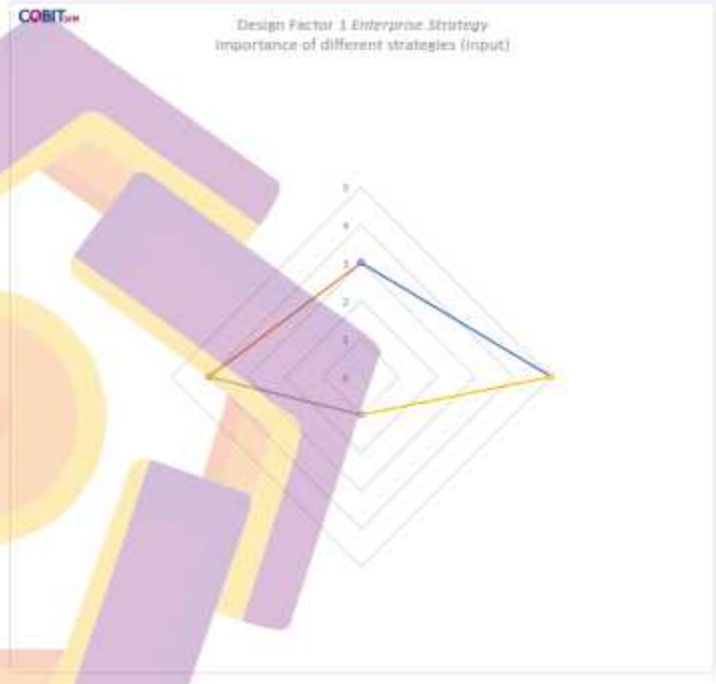
Design Factor
&
Mapping Table Design Factor

COBIT 2019 Information & Technology Governance System Design
Design Factor 1 *Enterprise Strategy*

Input Section—Importance of Each Enterprise Strategy Archetype

Value	Importance (1-5)	Baseline
Growth/Acquisition	3	
Innovation/Differentiation	4	
Cost Leadership	1	
Client Service/Stability	5	





COBIT 2019 Information & Technology Governance System Design
Design Factor 1 *Enterprise Strategy*

Input Section—Importance of Each Enterprise Strategy Archetype

Tabel Mapping Design Factor 1 Enterprise Strategy

DF1	Growth / Acquisition	Innovation / Differentiation	Cost Leadership	Client Service / Stability
EDM01	1,0	1,0	1,5	1,5
EDM02	1,5	1,0	2,0	3,5
EDM03	1,0	1,0	1,0	2,0
EDM04	1,5	1,0	4,0	1,0
EDM05	1,5	1,5	1,0	2,0
APO01	1,0	1,0	1,0	1,0
APO02	3,5	3,5	1,5	1,0
APO03	4,0	2,0	1,0	1,0
APO04	1,0	4,0	1,0	1,0
APO05	3,5	4,0	2,5	1,0
APO06	1,5	1,0	4,0	1,0
APO07	2,0	1,0	1,0	1,0
APO08	1,0	1,5	1,0	3,5
APO09	1,0	1,0	1,5	4,0
APO10	1,0	1,0	3,5	1,5
APO11	1,0	1,0	1,0	4,0
APO12	1,0	1,5	1,0	2,5
APO13	1,0	1,0	1,0	2,5
APO14	1,0	1,0	1,0	1,0
BAI01	4,0	2,0	1,5	1,5
BAI02	1,0	1,0	1,5	1,0
BAI03	1,0	1,0	1,5	1,0
BAI04	1,0	1,0	1,0	3,0
BAI05	4,0	2,0	1,0	1,5
BAI06	2,0	2,0	1,0	1,5
BAI07	1,5	2,0	1,0	1,5
BAI08	1,0	3,5	1,0	1,0
BAI09	1,0	1,0	1,0	1,0
BAI10	1,0	1,0	1,0	1,0
BAI11	3,5	3,0	1,5	1,0
DSS01	1,0	1,0	1,0	1,5
DSS02	1,0	1,0	1,0	4,0
DSS03	1,0	1,0	1,0	3,0
DSS04	1,0	1,0	1,0	4,0
DSS05	1,0	1,0	1,0	2,5
DSS06	1,0	1,0	1,0	1,5
MEA01	1,0	1,0	1,0	1,0
MEA02	1,0	1,0	1,0	1,0
MEA03	1,0	1,0	1,0	1,0
MEA04	1,0	1,0	1,0	1,0

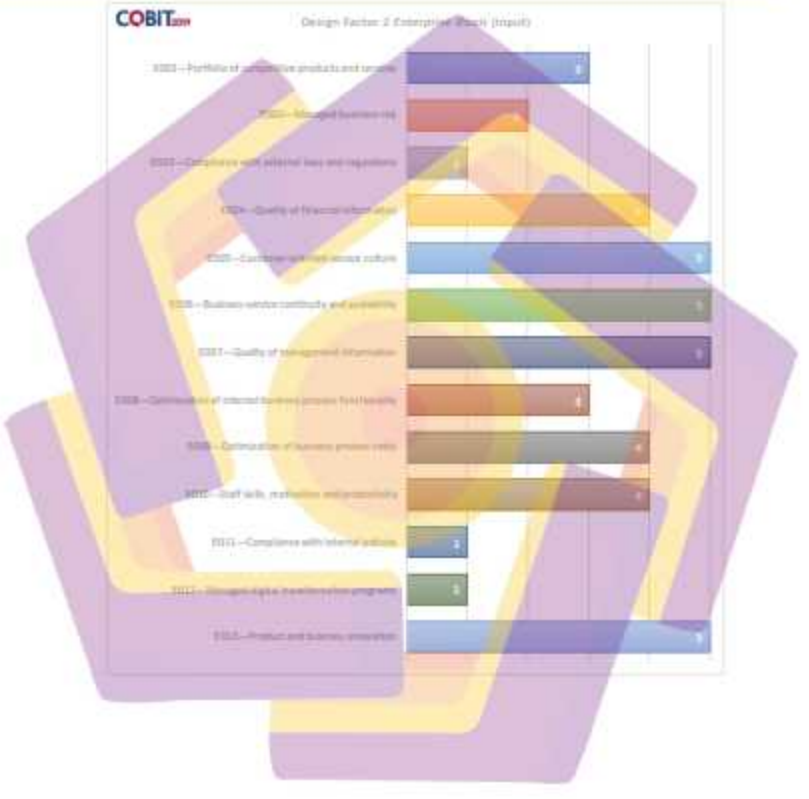
COBIT 2019 Information & Technology Governance System Design
Design Factor 2 *Enterprise Goals*

COBIT 2019 Information & Technology Governance System Design
Design Factor 2 *Enterprise Goals*

Input Section—Importance of Each Enterprise Goal

Input Section—Importance of Each Enterprise Goal

Value	Importance (1-5)	Baseline
EG01—Portfolio of competitive products and services	3	
EG02—Managed business risk	2	
EG03—Compliance with external laws and regulations	1	
EG04—Quality of financial information	4	
EG05—Customer oriented service culture	5	
EG06—Business service continuity and availability	5	
EG07—Quality of management information	5	
EG08—Optimization of internal business process functionality	3	
EG09—Optimization of business process costs	4	
EG10—Staff skills, motivation and productivity	4	
EG11—Compliance with internal policies	1	
EG12—Managed digital transformation programs	1	
EG13—Product and business innovation	5	



Compliance of external policies and laws	Managed business risk	Compliance with external laws and regulations	Quality of IT-related services to internal users	Internal transparency about IT	Optimization of service delivery costs	Quality of management information	Optimization of business process functionality	Optimization of business process costs	IT compliance and support for business compliance with external laws and regulations	Managed business transformation programs	Client-oriented service culture
0	0	0	0	0	0	0	0	0	0	0	0

Mapping table (EG-GG)		EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
		IT compliance and support for business compliance with external laws and regulations	Managed business risk	Compliance with external laws and regulations	Quality of IT-related services to internal users	Internal transparency about IT	Optimization of service delivery costs	Quality of management information	Optimization of business process functionality	Optimization of business process costs	IT compliance and support for business compliance with external laws and regulations	Managed business transformation programs	Client-oriented service culture
GG01	Portfolio of right-sized investment, service and assets	0	0	1	0	0	1	0	0	0	0	0	0	1
GG02	Managed enterprise risk	0	0	0	0	0	0	1	0	0	0	0	0	0
GG03	Compliance with external laws and regulations	0	0	0	0	0	0	0	0	0	0	0	0	0
GG04	Quality, cost and delivery of digital innovation	0	0	0	0	0	0	0	0	0	0	1	0	0
GG05	Customer-oriented service culture	0	0	1	0	1	1	0	0	1	0	0	1	0
GG06	Business service continuity and availability	0	1	0	0	1	0	0	0	0	0	0	0	0
GG07	Quality-driven IT solution development	0	0	0	0	0	0	0	0	0	0	0	0	0
GG08	Optimization of business process functionality	0	0	0	0	0	0	0	0	0	0	0	0	0
GG09	Optimization of business process costs	0	0	0	0	0	0	0	0	0	0	0	0	0
GG10	Staff skills, motivation and productivity	0	0	0	0	0	0	0	1	0	0	1	0	0
GG11	Compliance with internal policies	1	0	0	0	0	0	0	0	0	1	0	0	0
GG12	Managed business transformation programs	0	0	0	0	0	0	0	0	0	0	0	0	0
GG13	Agile responses to change	0	0	0	0	0	0	0	0	0	0	0	0	0

	EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
	IT compliance and support for business compliance with external laws and regulations	Managed business risk	Compliance with external laws and regulations	Quality of IT-related services to internal users	Internal transparency about IT	Optimization of service delivery costs	Quality of management information	Optimization of business process functionality	Optimization of business process costs	IT compliance and support for business compliance with external laws and regulations	Managed business transformation programs	Client-oriented service culture
	0	0	17	10	10	10	10	10	0	0	0	10	0

Mapping Table (EG-AMG)		AMG01	AMG02	AMG03	AMG04	AMG05	AMG06	AMG07	AMG08	AMG09	AMG10	AMG11	AMG12	AMG13	AMG14
		I&T Governance Board (IGB)	I&T Risk Office	I&T Compliance and Audit	Chief Information Officer (CIO)	Chief Technology Officer (CTO)	Chief Digital Officer (CDO)	I&T Engineering Function	I&T Service Management Function	I&T Security Management Function	Business Process Owners	Head Human Resources	Head Architect	Head Development	Head IT Operations
AMG01	Portfolio of right-sized investment, service and assets (EG01)	1	0	1	0	0	1	0	0	0	0	0	0	0	0
AMG02	Managed enterprise risk (EG02)	1	0	1	0	0	1	0	0	0	0	0	0	0	0
AMG03	Compliance with external laws and regulations (EG03)	1	0	1	0	0	1	0	0	0	0	0	0	0	0
AMG04	Quality, cost and delivery of digital innovation (EG04)	0	0	0	1	0	1	1	0	0	1	0	0	0	0
AMG05	Customer-oriented service culture (EG05)	0	0	0	1	0	1	1	0	0	1	0	0	0	0
AMG06	Business service continuity and availability (EG06)	0	1	0	1	0	1	1	0	0	1	0	0	0	0
AMG07	Quality-driven IT solution development (EG07)	0	0	0	0	0	1	0	0	0	0	0	0	0	0
AMG08	Optimization of business process functionality (EG08)	0	0	0	0	0	1	0	0	0	0	0	0	0	0
AMG09	Optimization of business process costs (EG09)	0	0	0	0	0	1	0	0	0	0	0	0	0	0
AMG10	Staff skills, motivation and productivity (EG10)	0	0	0	0	0	1	0	0	0	0	1	0	0	0
AMG11	Compliance with internal policies (EG11)	0	0	0	0	0	1	0	0	0	0	0	0	0	0
AMG12	Managed business transformation programs (EG12)	0	0	0	0	0	1	0	0	0	0	0	0	0	0
AMG13	Agile responses to change (EG13)	0	0	0	0	0	1	0	0	0	0	0	0	0	0

	AMG01	AMG02	AMG03	AMG04	AMG05	AMG06	AMG07	AMG08	AMG09	AMG10	AMG11	AMG12	AMG13	AMG14
	I&T Governance Board (IGB)	I&T Risk Office	I&T Compliance and Audit	Chief Information Officer (CIO)	Chief Technology Officer (CTO)	Chief Digital Officer (CDO)	I&T Engineering Function	I&T Service Management Function	I&T Security Management Function	Business Process Owners	Head Human Resources	Head Architect	Head Development	Head IT Operations
Maximum	24	1	23	10	10	23	10	10	0	0	0	10	0	0
Max*	1	1	1	1	1	1	1	1	0	0	0	1	0	0

COBIT2019 Information & Technology Governance System Design
Design Factor 3 *Risk Profile*

COBIT2019 Information & Technology Governance System Design
Design Factor 3 *Risk Profile*

Input Section—Importance of Each Generic IT Risk Category

Input Section—Importance of Each Generic IT Risk Category

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating	Baseline
IT investment decision making, portfolio definition & maintenance	3	2		
Program & projects life cycle management	3	2		
IT cost & oversight	2	2		
IT expertise, skills & behavior	3	2		
Enterprise/IT architecture	5	3		
IT operational infrastructure incidents	4	3		
Unauthorized actions	4	2		
Software adoption/usage problems	2	2		
Hardware incidents	2	2		
Software failures	3	1		
Logical attacks (hacking, malware, etc.)	5	3		
Third-party/supplier incidents	2	2		
Noncompliance	3	2		
Geopolitical issues	3	1		
Industrial action	2	1		
Acts of nature	3	2		
Technology-based innovation	3	2		
Environmental	2	3		
Data & information management	5	3		

	Very High Risk
	High Risk
	Normal Risk
	Low Risk

Tabel Mapping Design Factor 3 Risk Profile

DF3	RISKCAT01 IT Investment Decision Making, Portfolio Definition & Maintenance	RISKCAT02 Program & Projects Life Cycle Management	RISKCAT03 IT Cost & Oversight	RISKCAT04 IT Expertise, Skills & Behavior	RISKCAT05 Enterprise/ IT Architecture	RISKCAT06 IT Operational Infrastructure Incidents	RISKCAT07 Unauthorized Actions	RISKCAT08 Software Adoption/ Usage Problems	RISKCAT09 Hardware Incidents	RISKCAT10 Software Failures	RISKCAT11 Logical Attacks (Hacking, Malware, etc.)	RISKCAT12 Third-Party/ Supplier Incidents	RISKCAT13 Noncompliance	RISKCAT14 Geopolitical Issues	RISKCAT15 Industrial Action	RISKCAT16 Acts of Nature	RISKCAT17 Technology-Based Innovation	RISKCAT18 Environmental	RISKCAT19 Data & Information Management
EDM01	3,0	2,0	3,0	0,0	0,0	0,0	2,0	0,0	0,0	0,0	0,0	0,0	3,0	2,0	0,0	0,0	2,0	2,0	2,0
EDM02	3,0	2,0	0,0	0,0	2,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	1,0	0,0	0,0	0,0	3,0	1,0	3,0
EDM03	2,0	2,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	1,0	2,0	0,0	3,0	3,0	0,0	0,0	0,0	2,0	3,0
EDM04	3,0	0,0	4,0	3,0	2,0	0,0	0,0	0,0	0,0	0,0	0,0	2,0	1,0	0,0	2,0	0,0	0,0	2,0	3,0
EDM05	3,0	1,0	3,0	0,0	0,0	0,0	2,0	0,0	0,0	1,0	0,0	1,0	3,0	3,0	0,0	0,0	0,0	2,0	2,0
APO01	2,0	3,0	2,0	0,0	2,0	2,0	4,0	2,0	0,0	2,0	3,0	3,0	3,0	0,0	0,0	0,0	3,0	2,0	3,0
APO02	2,0	0,0	0,0	0,0	3,0	0,0	0,0	2,0	1,0	0,0	1,0	2,0	0,0	0,0	0,0	0,0	2,0	2,0	1,0
APO03	2,0	0,0	0,0	0,0	4,0	0,0	0,0	2,0	0,0	2,0	2,0	2,0	0,0	0,0	0,0	0,0	2,0	0,0	3,0
APO04	0,0	0,0	0,0	0,0	1,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	4,0	0,0	0,0
APO05	4,0	2,0	2,0	0,0	2,0	0,0	0,0	2,0	2,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	2,0	0,0	0,0
APO06	2,0	3,0	4,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	2,0	0,0	2,0	0,0	0,0	2,0	2,0	0,0
APO07	0,0	0,0	0,0	4,0	0,0	2,0	3,0	3,0	0,0	0,0	2,0	0,0	0,0	2,0	4,0	0,0	2,0	2,0	0,0
APO08	0,0	0,0	0,0	2,0	2,0	0,0	0,0	4,0	0,0	0,0	2,0	2,0	0,0	0,0	0,0	0,0	2,0	0,0	2,0
APO09	0,0	0,0	2,0	0,0	0,0	0,0	2,0	3,0	0,0	1,0	2,0	3,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
APO10	0,0	2,0	3,0	0,0	0,0	0,0	2,0	2,0	3,0	2,0	2,0	4,0	2,0	2,0	0,0	0,0	0,0	0,0	0,0
APO11	0,0	3,0	0,0	0,0	0,0	0,0	0,0	2,0	0,0	4,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	2,0
APO12	0,0	0,0	0,0	0,0	0,0	0,0	3,0	0,0	0,0	2,0	3,0	0,0	0,0	0,0	0,0	2,0	0,0	0,0	0,0
APO13	0,0	0,0	0,0	0,0	0,0	0,0	4,0	0,0	0,0	0,0	4,0	0,0	3,0	0,0	0,0	0,0	0,0	0,0	0,0
APO14	0,0	0,0	0,0	0,0	0,0	0,0	3,0	2,0	0,0	0,0	2,0	0,0	3,0	0,0	2,0	4,0	2,0	0,0	4,0
BAI01	0,0	4,0	0,0	0,0	2,0	0,0	0,0	3,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI02	2,0	2,0	0,0	0,0	2,0	0,0	0,0	2,0	0,0	2,0	2,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI03	0,0	3,0	0,0	0,0	2,0	0,0	0,0	2,0	0,0	3,0	3,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI04	0,0	1,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI05	0,0	2,0	0,0	2,0	0,0	0,0	0,0	4,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI06	0,0	0,0	0,0	0,0	0,0	3,0	4,0	0,0	0,0	2,0	3,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	3,0
BAI07	0,0	0,0	0,0	0,0	0,0	2,0	3,0	2,0	0,0	4,0	2,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI08	0,0	0,0	0,0	2,0	0,0	3,0	0,0	3,0	0,0	3,0	0,0	0,0	0,0	0,0	2,0	0,0	0,0	0,0	2,0
BAI09	0,0	0,0	0,0	0,0	0,0	1,0	3,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI10	0,0	0,0	0,0	0,0	0,0	2,0	4,0	0,0	0,0	2,0	3,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
BAI11	0,0	4,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
DSS01	0,0	0,0	0,0	0,0	0,0	4,0	3,0	0,0	4,0	0,0	2,0	0,0	0,0	0,0	0,0	0,0	0,0	2,0	0,0
DSS02	0,0	0,0	0,0	0,0	0,0	3,0	2,0	3,0	2,0	2,0	4,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
DSS03	0,0	0,0	0,0	0,0	0,0	3,0	1,0	4,0	0,0	3,0	1,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
DSS04	0,0	0,0	0,0	0,0	0,0	3,0	3,0	0,0	3,0	0,0	4,0	0,0	2,0	0,0	3,0	4,0	0,0	0,0	2,0
DSS05	0,0	0,0	0,0	0,0	0,0	3,0	4,0	0,0	2,0	0,0	4,0	0,0	3,0	0,0	3,0	2,0	0,0	0,0	3,0
DSS06	0,0	0,0	0,0	0,0	0,0	3,0	4,0	2,0	0,0	0,0	2,0	0,0	2,0	0,0	0,0	0,0	0,0	0,0	3,0
MEA01	1,0	2,0	2,0	0,0	0,0	2,0	2,0	0,0	0,0	2,0	3,0	2,0	2,0	2,0	0,0	2,0	0,0	0,0	2,0
MEA02	1,0	2,0	2,0	0,0	0,0	3,0	3,0	0,0	0,0	2,0	3,0	2,0	2,0	3,0	0,0	2,0	0,0	0,0	2,0
MEA03	0,0	1,0	0,0	0,0	0,0	1,0	2,0	0,0	0,0	0,0	3,0	2,0	4,0	2,0	0,0	0,0	0,0	0,0	2,0
MEA04	1,0	2,0	0,0	0,0	0,0	0,0	2,0	0,0	0,0	2,0	2,0	2,0	2,0	4,0	0,0	2,0	2,0	0,0	2,0

COBIT 2019 — Information & Technology Governance System Design
Design Factor 4 *IT-Related Issues*

Input Section—Importance of Each Generic IT-Related Issue

IT-Related Issue	Importance (1-3)	Baseline
Frustration between different IT entities across the organisation because of a perception of low contribution to business value	2	
Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value	2	
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	3	
Service delivery problems by the IT outsourcer(s)	1	
Failures to meet IT-related regulatory or contractual requirements	2	
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	1	
Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets	2	
Duplications or overlaps between various initiatives, or other forms of wasted resources	2	
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	3	
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	1	
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	2	
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	1	
Excessively high cost of IT	1	
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	1	
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	1	
Regular issues with data quality and integration of data across various sources	3	
High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	2	
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department (related to end-user computing, which often stems from dissatisfaction with IT solutions and services)	1	
Ignorance of and/or noncompliance with privacy regulations	2	
Inability to exploit new technologies or innovate using I&T	1	

2	No Issue
1	Issue
3	Serious Issue

Input Section—Importance of Each Generic IT-Related Issue

2026	Organization becomes difficult for IT outside across the organization because of a perception of low contribution to business value	Organization becomes inactive in departments (i.e., the IT operations Council for IT Organization) because of failed initiatives or a perception of low contribution to business value	Significant IT outages (stability, such as downtime causing lost orders, project delays and significant revenue losses) in an IT	Access delivery problems (cycle, IT environments)	Failure to ensure IT-related regulatory or contractual requirements	Regular audit findings or other issues concern raised about poor IT performance or supervisor IT quality or service problems	Substantial hidden and rogue IT spending (that is, IT spending by other departments outside the control of the core service division mechanisms and approved budgets)	Duplications or overlaps between various solutions or other forms of wasted resources	Insufficient IT resources with valid concerns (i.e., skills or staff turnover / dissatisfaction)	IT-enabled changes or projects frequently failing to meet business needs and be delivered on time and budget	Reluctance by board members, executives or senior management to engage with IT as a lack of concern or ignorance in sponsorship for IT	Complex IT operating model and/or unclear decision-mechanisms for IT-related decisions	Excessively high costs of IT	Observations or failed implementations of new solutions or re-assessments cause delays for successful IT solutions and systems	Cyber-security decisions and technical knowledge, which leads to excessive, cross-level deliberations and/or marketing your skills & speaking different languages	Regular issues with data quality and integrations or data errors, errors or issues	High level of credit card compromise, resulting primarily within a problem of a loss of non-sight and quality or total poor-like applications that are being developed and put in operation	Chronic or disproportionate negative impact on user satisfaction or adverse public links or an incidence rate of the categories, IT departments	Ignorance of analysis case compliance with privacy regulations	Inability to exploit new technologies or networks using .NET	
[illegible]	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	10
[illegible]	0.5	0.0	0.0	0.0	0.5	0.5	0.0	0.0	0.5	0.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	11
[illegible]	1.0	1.0	0.5	1.0	0.5	0.5	1.0	1.0	0.0	0.5	1.0	0.5	1.0	1.0	1.0	1.0	1.0	0.5	0.5	1.0	12
[illegible]	1.0	1.0	1.0	1.0	1.0	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	13
[illegible]	1.5	1.0	1.0	1.5	1.5	0.5	1.0	1.0	0.0	0.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	14
[illegible]	0.5	1.0	0.5	1.0	0.5	0.5	1.0	1.0	0.0	0.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	15
[illegible]	1.5	1.5	1.0	1.0	1.0	1.5	1.0	1.0	1.0	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	16
[illegible]	1.0	1.0	1.0	1.0	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	17
[illegible]	1.5	1.5	1.0	1.0	1.5	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	18
[illegible]	1.5	1.5	1.0	1.0	1.5	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	19
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	20
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	21
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	22
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	23
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	24
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	25
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	26
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	27
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	28
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	29
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	30
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	31
[illegible]	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	32

Copyright CIO.S, 2026

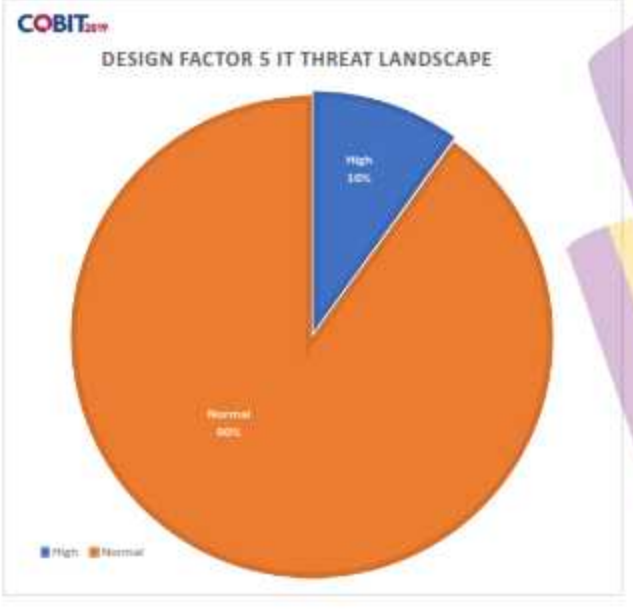
COBIT2019 Information & Technology Governance System Design
Design Factor 5 *Threat Landscape*

COBIT2019 Information & Technology Governance System Design
Design Factor 5 *Threat Landscape*

Input Section—Importance of Threat Landscape

Input Section—Importance of Threat Landscape

Value	Importance (100%)	Baseline
High	10%	
Normal	90%	



Page intentionally left blank

DF5	High	Normal
EDM01	3,0	1,0
EDM02	1,0	1,0
EDM03	4,0	1,0
EDM04	1,0	1,0
EDM05	2,0	1,0
APO01	3,0	1,0
APO02	1,0	1,0
APO03	3,0	1,0
APO04	1,0	1,0
APO05	1,0	1,0
APO06	1,0	1,0
APO07	2,0	1,0
APO08	1,0	1,0
APO09	2,0	1,0
APO10	3,0	1,0
APO11	2,0	1,0
APO12	4,0	1,0
APO13	4,0	1,0
APO14	3,0	1,0
BAI01	1,0	1,0
BAI02	1,0	1,0
BAI03	1,0	1,0
BAI04	2,0	1,0
BAI05	1,0	1,0
BAI06	3,0	1,0
BAI07	1,0	1,0
BAI08	1,0	1,0
BAI09	1,0	1,0
BAI10	3,0	1,0
BAI11	1,0	1,0
DSS01	1,0	1,0
DSS02	3,0	1,0
DSS03	2,0	1,0
DSS04	4,0	1,0
DSS05	3,0	1,0
DSS06	3,0	1,0
MEA01	3,0	1,0
MEA02	2,0	1,0
MEA03	3,0	1,0
MEA04	3,0	1,0

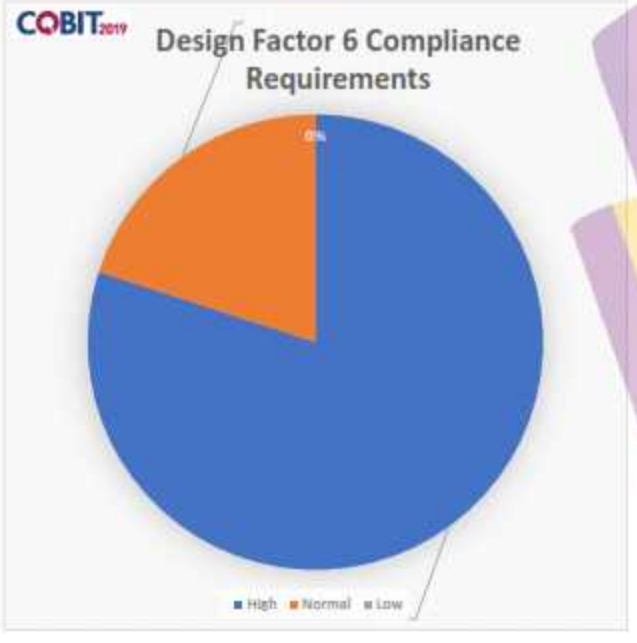
COBIT 2019 Information & Technology Governance System Design
Design Factor 6 *Compliance Requirements*

COBIT 2019 Information & Technology Governance System Design
Design Factor 6 *Compliance Requirements*

Input Section—Importance of Compliance Requirements

Input Section—Importance of Compliance Requirements

Value	Importance (100%)	Baseline
High	80%	
Normal	20%	
Low	0%	



Page intentionally left blank

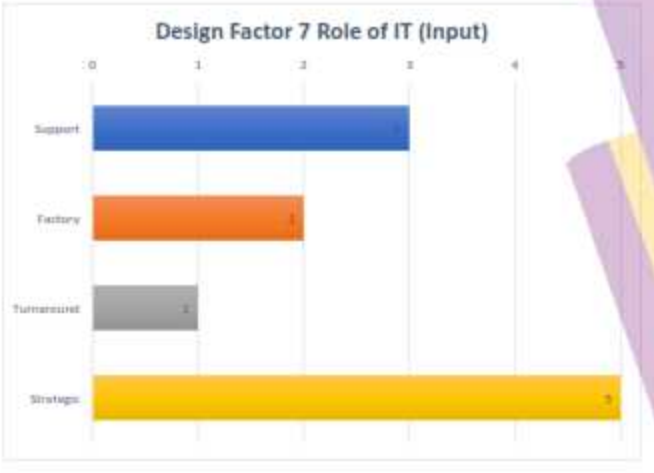
Tabel mapping Design Factor 6 Compliance Requirements

DF6	High	Normal	Low
EDM01	3,0	2,0	1,0
EDM02	1,0	1,0	1,0
EDM03	4,0	2,0	1,0
EDM04	1,0	1,0	1,0
EDM05	1,5	1,0	1,0
APO01	2,0	1,5	1,0
APO02	1,0	1,0	1,0
APO03	1,0	1,0	1,0
APO04	1,0	1,0	1,0
APO05	1,0	1,0	1,0
APO06	1,0	1,0	1,0
APO07	1,0	1,0	1,0
APO08	1,0	1,0	1,0
APO09	1,0	1,0	1,0
APO10	1,5	1,0	1,0
APO11	1,0	1,0	1,0
APO12	4,0	2,0	1,0
APO13	1,5	1,0	1,0
APO14	2,0	1,5	1,0
BAI01	1,0	1,0	1,0
BAI02	1,0	1,0	1,0
BAI03	1,0	1,0	1,0
BAI04	1,0	1,0	1,0
BAI05	1,0	1,0	1,0
BAI06	1,0	1,0	1,0
BAI07	1,0	1,0	1,0
BAI08	1,0	1,0	1,0
BAI09	1,0	1,0	1,0
BAI10	1,0	1,0	1,0
BAI11	1,0	1,0	1,0
DSS01	1,0	1,0	1,0
DSS02	1,0	1,0	1,0
DSS03	1,0	1,0	1,0
DSS04	1,5	1,0	1,0
DSS05	2,0	1,0	1,0
DSS06	1,0	1,0	1,0
MEA01	1,0	1,0	1,0
MEA02	1,0	1,0	1,0
MEA03	4,0	2,0	1,0
MEA04	3,5	2,0	1,0

COBIT 2019 Information & Technology Governance System Design
Design Factor 7 *Role of IT*

Input Section—Importance of Role of IT

Value	Importance (1-5)	Baseline
Support	3	
Factory	2	
Turnaround	1	
Strategic	5	



COBIT 2019 Information & Technology Governance System Design
Design Factor 7 *Role of IT*

Input Section—Importance of Role of IT

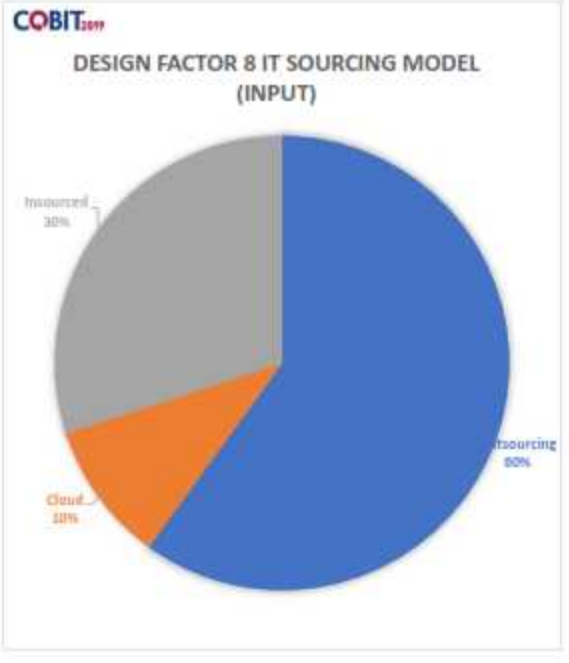
Page intentionally left blank

DF7	Support	Factory	Turnaround	Strategic
EDM01	1,0	2,0	1,5	4,0
EDM02	1,0	1,0	2,5	3,0
EDM03	1,0	3,0	1,0	3,0
EDM04	1,0	1,0	1,0	2,0
EDM05	1,0	1,0	1,0	2,0
APO01	1,0	1,5	1,5	2,5
APO02	1,0	1,0	3,0	3,0
APO03	1,0	1,0	2,0	2,0
APO04	0,5	1,0	3,5	4,0
APO05	1,0	1,0	2,5	3,0
APO06	1,0	1,0	1,0	2,0
APO07	1,0	1,0	1,0	1,5
APO08	1,0	1,0	2,0	2,5
APO09	1,0	2,0	1,5	2,0
APO10	1,0	2,5	1,5	2,0
APO11	1,0	1,5	1,5	2,0
APO12	1,0	2,5	1,0	3,0
APO13	1,0	2,0	1,5	3,0
APO14	1,0	1,5	1,5	2,5
BAI01	1,0	1,0	2,0	2,5
BAI02	1,0	1,0	3,0	3,0
BAI03	1,0	1,0	3,0	3,0
BAI04	1,0	2,5	1,5	2,0
BAI05	1,0	1,0	1,0	2,0
BAI06	1,0	2,5	1,0	2,0
BAI07	1,0	1,0	2,0	2,0
BAI08	1,0	1,0	1,0	2,0
BAI09	1,0	1,0	1,0	2,0
BAI10	1,0	1,5	1,0	2,0
BAI11	1,0	1,0	2,0	2,0
DSS01	1,0	3,5	1,0	3,0
DSS02	1,0	3,0	1,5	3,0
DSS03	1,0	3,0	1,5	3,5
DSS04	1,0	3,0	1,5	3,5
DSS05	1,5	2,5	1,5	3,5
DSS06	1,0	1,0	1,0	2,5
MEA01	1,0	1,0	1,0	2,0
MEA02	1,0	1,0	1,0	2,0
MEA03	1,0	1,0	1,0	1,5
MEA04	1,0	1,0	1,0	2,0

COBIT 2019 Information & Technology Governance System Design
Design Factor 8 *Sourcing Model for IT*

Input Section—Importance of Sourcing Model for IT

Value	Importance (100%)	Baseline
Outsourcing	60%	
Cloud	10%	
Insourced	30%	



COBIT 2019 Information & Technology Governance System Design
Design Factor 8 *Sourcing Model for IT*

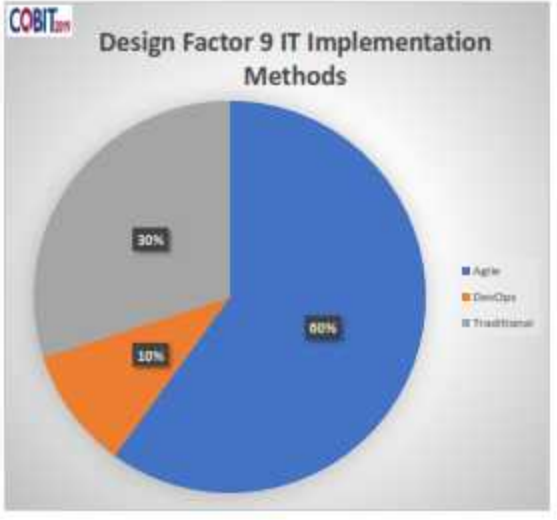
Input Section—Importance of Sourcing Model for IT

Page intentionally left blank

DF8	Outsourcing	Cloud	Insourcing
EDM01	1,0	1,0	1,0
EDM02	1,0	1,0	1,0
EDM03	1,0	2,0	1,0
EDM04	1,0	1,0	1,0
EDM05	1,0	1,0	1,0
APO01	1,0	1,0	1,0
APO02	1,0	1,0	1,0
APO03	1,0	1,0	1,0
APO04	1,0	1,0	1,0
APO05	1,0	1,0	1,0
APO06	1,0	1,0	1,0
APO07	1,0	1,0	1,0
APO08	1,0	1,0	1,0
APO09	4,0	4,0	1,0
APO10	4,0	4,0	1,0
APO11	1,0	1,0	1,0
APO12	2,0	2,0	1,0
APO13	1,0	1,0	1,0
APO14	1,0	1,0	1,0
BAI01	1,0	1,0	1,0
BAI02	1,0	1,0	1,0
BAI03	1,0	1,0	1,0
BAI04	1,0	1,0	1,0
BAI05	1,0	1,0	1,0
BAI06	1,0	1,0	1,0
BAI07	1,0	1,0	1,0
BAI08	1,0	1,0	1,0
BAI09	1,0	1,0	1,0
BAI10	1,0	1,0	1,0
BAI11	1,0	1,0	1,0
DSS01	1,0	1,0	1,0
DSS02	1,0	1,0	1,0
DSS03	1,0	1,0	1,0
DSS04	1,0	1,0	1,0
DSS05	1,0	1,0	1,0
DSS06	1,0	1,0	1,0
MEA01	1,0	3,0	1,0
MEA02	1,0	1,0	1,0
MEA03	1,0	1,0	1,0
MEA04	1,0	1,0	1,0

Input Section—Importance of IT Implementation Methods

Value	Importance (100%)	Baseline
Agile	60%	
DevOps	10%	
Traditional	30%	



Page intentionally left blank

COBIT 2019 Information & Technology Governance System Design
Design Factor 9 *IT Implementation Methods*
Input Section—Importance of IT Implementation Methods

DF9	Agile	DevOps	Traditional
EDM01	1,0	1,0	1,0
EDM02	1,0	1,0	1,0
EDM03	1,0	1,0	1,0
EDM04	1,0	1,0	1,0
EDM05	1,0	1,0	1,0
APO01	1,0	1,0	1,0
APO02	1,0	1,0	1,0
APO03	1,0	2,0	1,0
APO04	1,0	1,0	1,0
APO05	1,0	1,0	1,0
APO06	1,0	1,0	1,0
APO07	1,0	1,5	1,0
APO08	1,0	1,0	1,0
APO09	1,0	1,0	1,0
APO10	1,0	1,0	1,0
APO11	1,0	1,0	1,0
APO12	1,0	1,5	1,0
APO13	1,0	1,0	1,0
APO14	1,0	1,0	1,0
BAI01	2,0	1,5	1,0
BAI02	3,5	2,0	1,0
BAI03	4,0	3,0	1,0
BAI04	1,0	1,0	1,0
BAI05	2,5	1,5	1,0
BAI06	3,5	2,0	1,0
BAI07	2,5	2,5	1,0
BAI08	1,0	1,0	1,0
BAI09	1,0	1,0	1,0
BAI10	1,5	2,0	1,0
BAI11	2,5	1,0	1,0
DSS01	1,0	2,5	1,0
DSS02	1,0	1,5	1,0
DSS03	1,0	1,5	1,0
DSS04	1,0	1,0	1,0
DSS05	1,0	1,0	1,0
DSS06	1,0	1,0	1,0
MEA01	1,5	1,5	1,0
MEA02	1,0	1,0	1,0
MEA03	1,0	1,0	1,0
MEA04	1,0	1,0	1,0

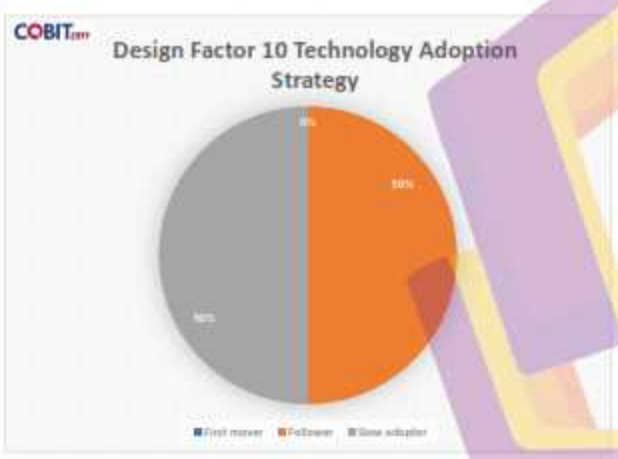
COBIT 2019 Information & Technology Governance System Design
Design Factor 10 *Technology Adoption Strategy*

COBIT 2019 Information & Technology Governance System Design
Design Factor 10 *Technology Adoption Strategy*

Input Section—Importance of Technology Adoption Strategy

Input Section—Importance of Technology Adoption Strategy

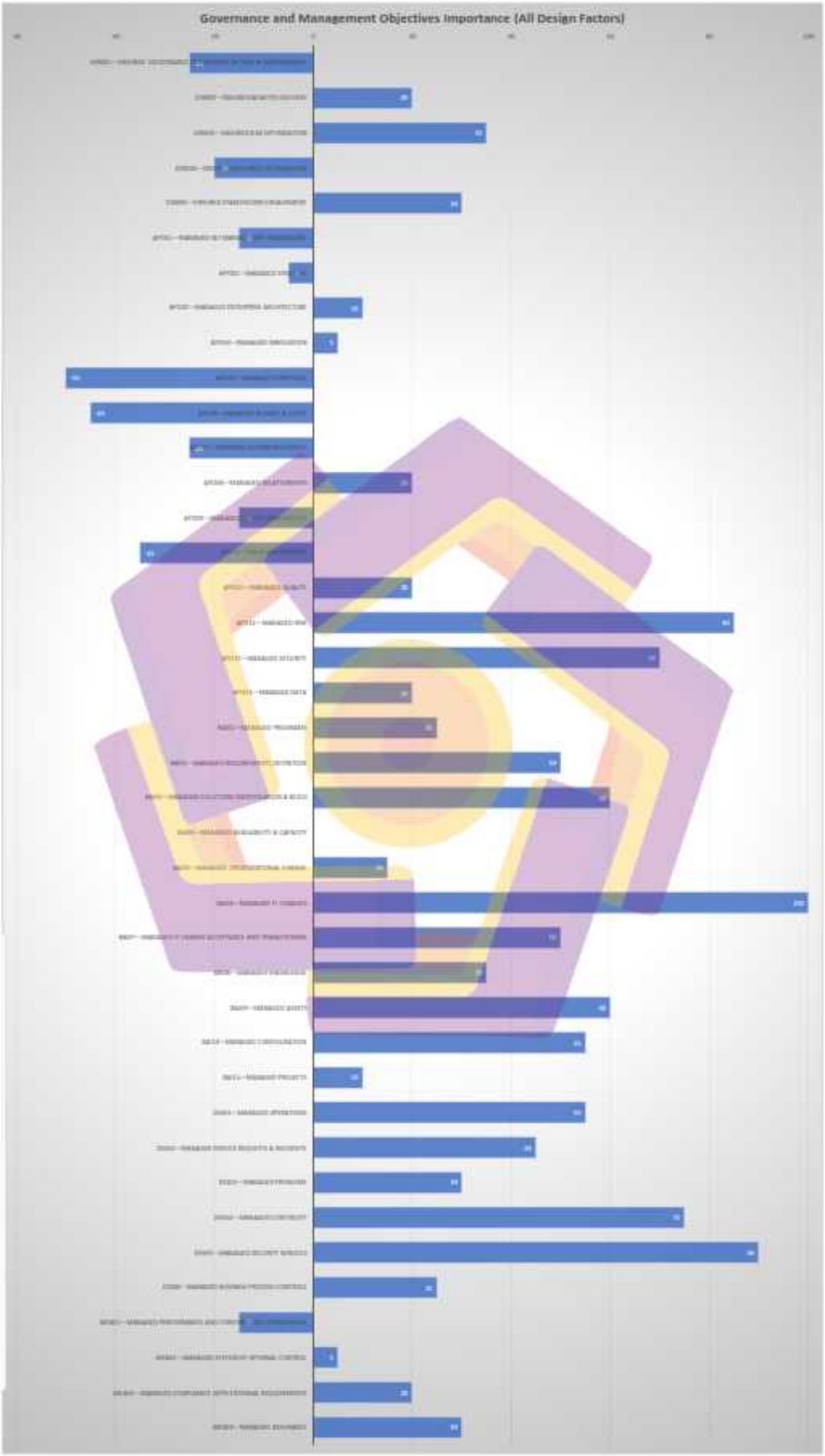
Value	Importance (100%)	Baseline
First mover	0%	33%
Follower	50%	33%
Slow adopter	50%	33%



Page intentionally left blank

Tabel mapping Design Factor 10 Technology Adoption Strategy

DF10	First Mover	Follower	Slow Adopter
EDM01	3,5	2,5	1,5
EDM02	4,0	2,5	1,5
EDM03	1,5	1,0	1,0
EDM04	2,5	2,0	1,5
EDM05	1,5	1,0	1,0
APO01	2,5	1,5	1,0
APO02	4,0	3,0	1,5
APO03	2,0	1,0	1,0
APO04	4,0	3,0	1,0
APO05	4,0	2,5	1,0
APO06	1,0	1,5	1,0
APO07	2,5	1,0	1,0
APO08	3,0	1,5	1,0
APO09	1,5	1,5	1,0
APO10	2,5	1,5	1,0
APO11	1,5	1,5	1,0
APO12	2,0	1,5	1,0
APO13	1,0	1,0	1,0
APO14	2,5	2,0	1,0
BAI01	4,0	3,0	1,5
BAI02	3,5	2,5	1,0
BAI03	4,0	2,5	1,0
BAI04	1,5	1,5	1,0
BAI05	3,0	2,0	1,0
BAI06	2,5	2,0	1,0
BAI07	3,5	2,5	1,0
BAI08	1,5	1,0	1,0
BAI09	1,0	1,0	1,0
BAI10	1,5	1,0	1,0
BAI11	3,5	2,5	1,0
DSS01	1,0	1,0	1,0
DSS02	1,0	1,0	1,0
DSS03	1,5	1,0	1,0
DSS04	1,5	1,0	1,0
DSS05	1,5	1,0	1,0
DSS06	1,0	1,0	1,0
MEA01	3,0	2,0	1,0
MEA02	1,0	1,0	1,0
MEA03	1,0	1,0	1,0
MEA04	1,0	1,0	1,0


Governance and Management Objectives Importance (All Design Factors)

Mapping Table: Enterprise Goals—Alignment Goals

Figure 5.1—Mapping Enterprise Goals and Alignment Goals

		EG01 Portfolio of competitive products and services	EG02 Managed business risk	EG03 Compliance with external laws and regulations	EG04 Quality of financial information	EG05 Customer-oriented service culture	EG06 Business service continuity and availability	EG07 Quality of management information	EG08 Optimization of internal business process functionality	EG09 Optimization of business process costs	EG10 Staff skills, motivation and productivity	EG11 Compliance with internal policies	EG12 Managed digital transformation programs	EG13 Product and business innovation
AG01	I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02	Managed I&T-related risk		P				S							
AG03	Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04	Quality of technology-related financial information				P			P		P				
AG05	Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06	Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07	Security of information, processing infrastructure and applications, and privacy		P				P							
AG08	Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10	Quality of I&T management information				P			P		S				
AG11	I&T compliance with internal policies		S	P								P		
AG12	Competent and motivated staff with mutual understanding of technology and business					S					P			
AG13	Knowledge, expertise and initiatives for business innovation	P		S									S	P

Mapping Table: Alignment Goals—Governance and Management Objectives

Figure—5.2 Mapping Governance and Management Objectives to Alignment Goals

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T compliance and support for business compliance with external laws and regulations	Managed I&T-related risk	Realized benefits from I&T-enabled investments and services portfolio	Quality of technology-related financial information	Delivery of I&T services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of I&T management information	I&T compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02	Ensured benefits delivery			P		S	S		S					S
EDM03	Ensured risk optimization	S	P					P				S		
EDM04	Ensured resource optimization			S		S	S		S	P			S	
EDM05	Ensured stakeholder engagement				S						P	S		
APO01	Managed I&T management framework	S	S	P		S		S	S	S	S	P		
APO02	Managed strategy			S		S	S		P				S	S
APO03	Managed enterprise architecture			S		S	P	S	P					
APO04	Managed innovation			S			P		S				S	P
APO05	Managed portfolio			P		P	S		S	S				
APO06	Managed budget and costs			S	P					P	S			
APO07	Managed human resources			S		S				S			P	P
APO08	Managed relationships			S		P	P		S	S			P	P
APO09	Managed service agreements					P			S					
APO10	Managed vendors					P	S			S				
APO11	Managed quality			S	S	S				P	P			
APO12	Managed risk		P					P						
APO13	Managed security	S	S					P						
APO14	Managed data	S	S		S			S			P			
BAI01	Managed programs			P			S		S	P				
BAI02	Managed requirements definition			S		P	P		S	P			S	
BAI03	Managed solutions identification and build			S		P	P		S	P				
BAI04	Managed availability and capacity					P		S		S				
BAI05	Managed organizational changes			P		S	S		P	P			S	
BAI06	Managed IT changes		S			S	P		S					
BAI07	Managed IT change acceptance and transitioning		S				P			S				
BAI08	Managed knowledge			S			S		S	S			P	P
BAI09	Managed assets				P						S			
BAI10	Managed configuration					S		P						
BAI11	Managed projects			P		S	P			P				
DSS01	Managed operations					P			S					
DSS02	Managed service requests and incidents		S			P		S						
DSS03	Managed problems		S			P		S						
DSS04	Managed continuity		S			P		P						
DSS05	Managed security services	S	P			S		P				S		
DSS06	Managed business process controls		S			S		S	P			S		
MEA01	Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02	Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03	Managed compliance with external requirements	P										S		
MEA04	Managed assurance	S	S		S	S		S			S	P		