CESS (Journal of Computing Engineering, System and Science) *e-ISSN: 2502-714x*
Vol. 9, No. 2, Juli 2024, pp.613-630 *p-ISSN: 2502-7131*

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess

Analisa Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 Pada Dinas Kominfo Provinsi Sulawesi Utara

Analysis of Information Technology Governance Using the 2019 COBIT Framework at the North Sulawesi Province Communications and Information Service

Joe Yuan Mambu[1*], Jofan Erlich Kaligis[2], Antares Mario Willar[3], Stenly Adam[4]

[1,2,3,4] Fakultas Ilmu Komputer, Universitas Klabat, Airmadidi
email: [1]joeyuan.mambu@unklab.ac.id, [3]s2200324@student.unklab.ac.id, [3]s2200405@student.unklab.ac.id, [4]stenly.adam@unklab.ac.id

A B S T R A K

Teknologi Informasi (TI) menjadi esensial dalam operasi bisnis modern, mempengaruhi daya saing, efektivitas, dan efisiensi organisasi. Keberhasilan tata kelola TI terletak pada kesesuaian dengan tujuan organisasi dan adaptasi terhadap perubahan teknologi. COBIT 2019, sebuah framework yang membantu manajemen bisnis dalam mengelola TI, menjadi kunci dalam memandu strategi pengembangan. Penelitian di Dinas Kominfo Sulawesi Utara menemukan tiga proses prioritas: APO12 - *Managed Risk*, DSS01 - *Managed Operations*, dan DSS05 - *Managed Security Services*. Hasil penelitian menunjukkan tingkat kapabilitas dan keefektifan masing-masing proses, dengan APO12 berada pada kapabilitas level 2 dan rating 66%, DSS01 pada level 4 dengan rating 83%, dan DSS05 pada level 2 dengan rating 84%. Evaluasi ini memberikan wawasan yang berharga untuk meningkatkan kinerja dan keamanan TI di institusi tersebut, serta memastikan kontribusi TI yang optimal terhadap tujuan organisasi. Dengan demikian, pemahaman yang mendalam tentang aspek TI yang spesifik dan perannya dalam konteks bisnis lokal menjadi kunci dalam mengambil langkah-langkah yang relevan dan efektif dalam pengelolaan TI.

Kata Kunci: *Teknologi Informasi; Tata Kelola; COBIT 2019; Desain Faktor; Level Kapabilitas*

A B S T R A C T

Information Technology (IT) has become essential in modern business operations, influencing competitiveness, effectiveness, and organizational efficiency. The success of IT governance lies in its alignment with organizational goals and its ability to adapt to technological changes. COBIT 2019, a framework that assists in managing IT, is crucial in guiding development strategies. Research conducted at the North Sulawesi Communication and Information Office

**Penulis Korespondensi:*
email: joeyuan.mambu@unklab.ac.id

identified three priority processes: APO12 - managed Risk, DSS01 - managed operations, and DSS05 - managed security services. The research findings revealed the level of capability and effectiveness of each process, with APO12 at capability level 2 with a rating of 66%, DSS01 at level 4 with a rating of 83%, and DSS05 at level 2 with a rating of 84%. This evaluation provides valuable insights to enhance the performance and security of IT within the institution, ensuring its optimal contribution to organizational goals. Thus, a deep understanding of specific IT aspects and its role in the local business context is key to taking relevant and effective steps in IT management.

Keywords: *Information Techonology; Governance; COBIT 2019; Design Factor; Capability Level*

1. PENDAHULUAN

Di era digital yang terus berkembang, pengaturan teknologi informasi (TI) yang efisien dan efektif sangat penting bagi organisasi. Organisasi semakin bergantung pada TI dan dapat secara efektif dan efisien mengintegrasikan sumber daya TI dengan proses organisasi dan manajerial lainnya. Tata kelola TI diadopsi secara luas oleh organisasi di Indonesia, baik organisasi pemerintahan maupun swasta [1]. Salah satu organisasi Pemerintah yang menggunakan TI adalah instansi Dinas Kominfo. Teknologi informasi (TI) telah menjadi bagian yang tak terpisahkan dalam dunia Pemerintahan saat ini. Sebagai lembaga yang menyediakan layanan masyarakat, Dinas Kominfo harus memiliki sistem TI yang baik dan terkelola dengan baik pula.

Tata Kelola IT adalah suatu kerangka kerja yang digunakan oleh organisasi untuk mengelola dan mengontrol sumber daya teknologi informasi mereka agar dapat menghasilkan nilai bisnis yang maksimal [2]. Tujuannya adalah untuk menjamin bahwa TI mendukung tujuan organisasi secara optimal, dengan mengontrol risiko yang terkait dengan penggunaan TI dan memastikan bahwa penggunaannya sesuai dengan hukum dan peraturan yang berlaku [3]. Untuk mencapai hal tersebut, perlu diterapkan suatu kerangka kerja atau *framework* yang dapat membantu dalam mengelola TI secara efektif dan efisien. Salah satu *framework* yang dapat digunakan adalah *Control Objectives for Information and related Technology* (COBIT) [4].

COBIT 2019 adalah kerangka kerja TI terbaru yang dikembangkan oleh *Information Systems Audit and Control Association* (ISACA) dan *Information Technology Governance Institute (ITGI)*. COBIT adalah sekumpulan dokumentasi dan panduan untuk mengarahkan tata kelola TI yang membantu auditor, manajemen dan pengguna untuk menjembatani pemisah antar resiko bisnis, kebutuhan dan permasalahan lainnya saat penerapan teknologi informasi [5]. COBIT 2019 memiliki fokus pada pengelolaan TI yang berbasis nilai, mengidentifikasi risiko, dan memperbaiki kinerja TI organisasi. COBIT merupakan kerangka kerja yang menyediakan panduan terstruktur dan menyeluruh untuk pengelolaan TI, mencakup strategi, pengendalian, pengelolaan sumber daya, evaluasi kinerja, dan pemahaman risiko [6]. COBIT membantu mengoptimalkan investasi berbasis TI serta memastikan penyampaian layanan dan menyediakan indikator yang jelas apabila terjadi kegagalan.

Dinas Kominfo Provinsi Sulut adalah salah satu lembaga Pemerintah yang telah menerapkan TI dalam operasinya. Sebagai institusi yang berfokus pada layanan Masyarakat. Dinas Kominfo juga menghadapi tantangan dalam mengoptimalkan pengelolaan TI mereka. Untuk memastikan pelayanan kesehatan berkualitas, Dinas Kominfo harus mengadopsi kerangka kerja yang sesuai dalam mengatur TI mereka. Oleh karena itu, penelitian ini

bertujuan untuk menerapkan COBIT 2019 sebagai kerangka kerja untuk meningkatkan tata kelola TI di Dinas Kominfo.

Dengan mengimplementasikan COBIT, Dinas Kominfo dapat meningkatkan pengelolaan TI, efisiensi operasional, keamanan informasi, dan mematuhi peraturan serta kebijakan yang ada. Tujuan penelitian ini adalah untuk menganalisis dan menjelaskan implementasi Tata Kelola Teknologi Informasi dengan menggunakan kerangka kerja COBIT di Dinas Kominfo Provinsi Sulawesi Utara [7].

Meskipun ada banyak penelitian yang telah mengkaji implementasi tata kelola TI menggunakan kerangka kerja COBIT di berbagai jenis organisasi, masih terdapat keterbatasan studi yang fokus pada penerapan di instansi pemerintah khususnya di tingkat provinsi di Indonesia. Penelitian terdahulu lebih banyak berfokus pada sektor swasta atau organisasi skala besar, sedangkan penelitian mengenai tata kelola TI di instansi pemerintah daerah seperti Dinas Kominfo Provinsi Sulawesi Utara masih sangat terbatas. Penelitian ini mengisi kekosongan tersebut dengan menyediakan analisis mendalam tentang penerapan COBIT 2019 di lingkungan pemerintahan lokal, serta memberikan rekomendasi spesifik yang dapat diaplikasikan untuk meningkatkan tata kelola TI di instansi tersebut. Kebaruan dari penelitian ini terletak pada pendekatan yang komprehensif dalam menganalisis 11 faktor desain COBIT 2019 dalam konteks instansi pemerintah daerah, yang belum banyak dibahas dalam literatur sebelumnya. Hasil penelitian ini diharapkan dapat memberikan kontribusi nyata bagi pengembangan praktik tata kelola TI di instansi pemerintah lainnya di Indonesia.

Dalam penelitian ini, akan dianalisis tingkat kematangan tata kelola TI di Dinas Kominfo dan rekomendasi perbaikan yang dapat diaplikasikan. Pada proses perancangan sistem tata kelola terdapat 11 faktor desain yang dipertimbangkan diantaranya ialah [8]:

1. *Design Factor 1: Enterprise Strategy*
   Pada Desain Faktor 1, penerapan prinsip-prinsip seperti *Growth/Acquisition*, *Innovation/Differentiation, Cost Leadership, dan Client Service/Stability* sangat penting dalam pengelolaan TI [9]. Penerapan prinsip-prinsip tersebut dapat membantu organisasi dalam meningkatkan pelayanan kesehatan, meningkatkan efisiensi dan efektivitas pengelolaan TI, dan memastikan stabilitas organisasi.
2. *Design Factor 2 – Enterprise Goals*
   Desain faktor 2 dalam COBIT 2019 terkait dengan pertanyaan-pertanyaan yang berkaitan dengan tujuan perusahaan atau *Enterprise Goals* (EG). Terdapat 13 pertanyaan dalam desain faktor 2 yang mengacu pada tujuan perusahaan, seperti portofolio produk dan layanan yang kompetitif, manajemen risiko bisnis dan tata kelola, kepatuhan terhadap regulasi dan aturan eksternal, kualitas informasi keuangan, budaya layanan pelanggan, kelangsungan dan ketersediaan layanan bisnis, kualitas manajemen informasi, optimasi proses bisnis internal, optimasi biaya proses bisnis, keterampilan, motivasi, dan produktivitas staf, kepatuhan terhadap kebijakan internal, program transformasi digital yang terkelola, dan inovasi produk dan bisnis [10].
3. *Design Factor 3 – IT Risk Profile*
   COBIT 2019 menyediakan 19 kriteria untuk Risk Profile, seperti keputusan investasi IT, manajemen siklus hidup program dan proyek, pengawasan biaya IT, keahlian dan perilaku IT, kepatuhan, dan manajemen data dan informasi [11].
4. *Design Factor 4 – IT Related Issues*
   Pada tahap Desain Faktor 4 dilakukan identifikasi dan analisis isu terkait TI yang ada. Identifikasi dilakukan dengan mempertimbangkan isu terkait TI yang sedang dihadapi atau

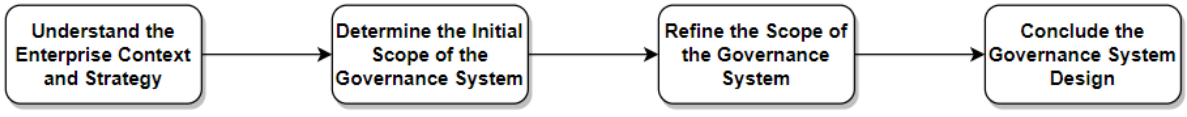
risiko yang telah terjadi. Isu yang terkait dengan bidang TI harus diidentifikasi dengan jelas dalam konteks kriteria yang tercantum dalam framework COBIT 2019, sehingga dapat digunakan untuk mengatasi masalah yang muncul di masa depan dengan lebih efektif. Penilaian isu terkait TI disesuaikan dengan tingkat kepentingannya, yaitu 1: *No Issue* , 2: *Issue*, 3: *Serious Issue* [12].

5. *Design Factor 5 – Threat Landscape*
   Ancaman Design Factor 5 ini terbagi menjadi dua yaitu normal, dimana perusahaan beroperasi di bawah tingkat ancaman yang dianggap normal dan tingkat ancaman tinggi.
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 [13].
7. *Design Factor 7 – Role of IT*
   Peran TI dalam perusahaan juga menjadi faktor yang penting. Dimana menilai apakah TI diposisikan sebagai *Support, Factory, Turnaround,* dan *Strategic.*
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,* dan *Insourced* [14].
9. *Design Factor 9 – IT Implementation Methods*
   Terdapat beberapa tipe metode implementasi TI seperti *Agile, DevOps, Traditional,* dan *Hybrid* [2].
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. Kemudian terdapat *follower* dimana perusahaan menunggu yang lain menerapkan teknologi tersebut baru dia ikuti, dan *Slow Adopter* dimana perusahaan sangat lambat dalam pengadopsian teknologi baru [5].

Hasil yang didapatkan dari setiap desain factor selanjutnya akan dianalisa untuk dapat menghasilkan informasi dan pengetahuan yang terkait dengan sistem tata Kelola Dinas Kominfo Provinsi Sulawesi Utara.

2. METODE PENELITIAN

Untuk metode penelitian yang digunakan dalam merancang sistem tata kelola TI yang mengacu pada serangkaian tahapan yang diadaptasikan sebagai alur kerja desain tata kelola pada COBIT 2019 [15]. Yang terdapat pada gambar dibawah ini:



Gambar 1. Alur Kerja Desain Sistem Tata Kelola pada COBIT 2019.

Pada Gambar 1 terdapat 4 proses dalam merancang sistem tata kelola TI. Proses pertama: peneliti melakukan wawancara dengan stakeholder dan observasi pada Dinas Kominfo untuk memahami langkah awal dalam merancang tata kelola TI. Ini melibatkan identifikasi strategi, tujuan, profil risiko, dan masalah terkait informasi dan teknologi

berdasarkan kriteria desain faktor COBIT 2019. Proses kedua: peneliti mewawancara dengan stakeholder untuk menentukan ruang lingkup awal sistem tata kelola dengan mempertimbangkan aspek dari *design factor* 1 hingga design factor 4. Proses ketiga: peneliti mengidentifikasi perbaikan ruang lingkup awal sistem tata kelola dengan mempertimbangkan aspek dari design factor 5 hingga design factor 11. Wawancara dengan stakeholder dilakukan untuk mendapatkan informasi yang diperlukan. Proses terakhir: Semua input dari tahap sebelumnya digabungkan untuk menghasilkan kesimpulan desain sistem tata kelola. Keluaran pada tahap ini adalah ringkasan nilai setiap proses dari skala -100 hingga 100. Nilai ini menentukan tingkat kemampuan yang dibutuhkan, dengan proses yang bernilai 50 atau lebih dianggap sangat penting dan memerlukan tingkat kemampuan lebih tinggi.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Wawancara *Design Factor*

Bagian ini membahas tentang hasil dari *Design Factor* yang telah kami dapatkan dari wawancara yang telah dilakukan pada kepala bagian IT di Dinas Kominfo Provinsi Sulawesi Utara. Untuk mendapatkan hasil dan prioritas dari tata kelola IT Dinas Kominfo Provinsi Sulawesi Utara, maka terdapat 10 faktor yang perlu untuk dinilai yaitu strategi perusahaan, tujuan perusahaan, resiko perusahaan, masalah terkait IT, ancaman lanskap, kepatuhan, peran IT, sumber model dari IT, metode implementasi IT, strategi adopsi teknologi dan ukuran perusahaan [18].

3.1.1. Design Factor 1 - *Enterprise Strategy*

Berdasarkan hasil wawancara yang kami lakukan pada penilaian *Design Factor* 1, bahwa perusahaan ini hanya lebih berfokus pada *Client Service* saja karena Dinas Kominfo Provinsi Sulawesi Utara ini selalu mengutamakan pelayanan pada masyarakat sehingga untuk *Growth, Innovation dan Cost Leadership*, dari perusahaan sudah tidak terlalu memfokuskan strategi pada tiga bagian tersebut karena sudah cukup baik.

3.1.2 Design Factor 2 - *Enterprise Goals*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor 2*, bahwa yang menjadi prioritas utama dari Dinas Kominfo Provinsi Sulawesi Utara terdapat pada EG03, EG06, EG07, EG10, EG11, EG12,. Untuk bagian EG03 atau kepatuhan hukum dan peraturan eksternal merupakan salah satu prioritas yang cukup penting dari perusahaan karena hukum dan peraturan sangat digunakan dalam lingkungan dari Dinas Kominfo Provinsi Sulawesi Utara ini. Untuk bagian berikut yaitu EG02 atau Risiko bisnis yang terkelola menjadi salah satu juga prioritas yang cukup penting dari instansi karena Dinas Kominfo bergerak dibagian pemerintah dimana resiko yang tinggi dan harus berjalan. Untuk bagian EG03 atau Kepatuhan terhadap hukum dan peraturan eksternal menjadi salah satu prioritas utama dari instansi karena instansi harus menaati Undang-Undang yang berjalan seperti SOP yang telah ditetapkan. Untuk bagian berikutnya yaitu EG04 atau Kualitas informasi keuangan menjadi salah satu prioritas yang cukup penting bagi instansi karena Dinas Kominfo ini dikelola oleh pemerintah jadi tinggal mengikuti peraturan pemerintah. Untuk bagian berikutnya yaitu EG05 atau Budaya layanan yang mengutamakan pelanggan juga menjadi salah satu prioritas yang cukup penting dari instansi karena selalu mengutamakan masyarakat agar merasa puas dengan pelayanan. Untuk bagian berikutnya yaitu EG06 atau Kelangsungan dan ketersediaan layanan bisnis menjadi salah satu prioritas utama instansi juga karena kebutuhan dan permintaan yang besar sehingga ketersediaan layanan yang baik membutuhkan waktu pelayanan yang lebih. Bagian

berikutnya yaitu EG07 atau Kualitas manajemen informasi menjadi salah satu juga prioritas utama instansi karena keterbukaan informasi dan penyampaian informasi yang baik mulai dari pejabat struktural, staff bahkan yang menerima pelayan yaitu masyarakat bisa mendapatkan informasi yang baik. Untuk bagian berikutnya yaitu EG08 atau Optimasi fungsionalitas proses bisnis internal menjadi salah satu prioritas yang cukup penting dari instansi karena proses bisnis menjadi bagian dari jalannya alur pelayanan. Untuk bagian EG09 atau Optimasi biaya proses bisnis juga menjadi salah satu prioritas yang cukup penting dari instansi karena agar instansi dapat sebisa mungkin mengurangi biaya pengeluaran. Untuk bagian selanjutnya yaitu EG10 atau keterampilan, motivasi, dan produktivitas staf menjadi salah satu prioritas yang utama dari instansi karena dengan melihat kenyamanan staf dapat meningkatkan produktivitas dan motivasi kerja. Untuk bagian berikutnya yaitu EG11 atau Kepatuhan terhadap kebijakan internal menjadi salah satu juga prioritas yang utama dari instansi karena seluruh pusat pelayan wajib mengikuti SOP yang sudah tersedia. Untuk bagian EG12 atau Program transformasi digital yang terkelola juga menjadi salah satu prioritas utama dari instansi karena Dinas Kominfo sendiri diharuskan untuk mengikuti perkembangan digital untuk mencari informasi yang lebih baik. Dan yang terakhir yaitu untuk bagian EG13 atau Inovasi produk dan bisnis menjadi salah satu prioritas yang cukup penting dari instansi dikarenakan inovasi yang dibuat yaitu program sosial kepada masyarakat [20].

3.1.3 Design Factor 3 - *Risk Profile*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor 3*, bahwa banyak yang menjadi dampak yang besar Instansi ini. Diantaranya ada IT - *Investment decision* making, portofolio definition and maintenance karena sistem yang digunakan di Instansi telah diatur dari pusat dan tidak dapat di ubah itu yang menjadi dampak cukup besar jika instansi berinvestasi dalam jumlah yang besar namun dalam tahap implementasi gagal. Selanjutnya ada program and project karena instansi dapat mengalami human error, dimana seperti korupsi. Untuk Perencanaan seharusnya sudah matang, namun waktu untuk mengimplementasikan sering terjadinya Korupsi. Selanjutnya ada *IT cost & oversight* karena instansi ini termasuk pekerjaan non-profit yang tujuannya untuk kemakmuran masyarakat yang dimana semua penganggaran itu berasal dari Masyarakat dan instansi akan berusaha sebaik mungkin untuk mengelolanya. Selanjutnya ada *IT expertise*, skills and behaviour karena peraturan yang seringnya melukakan perpindahan pekerja atau PNS maka instansi sangat rentan untuk memiliki hubungan atau pemahaman yang kurang baik. Selanjutnya ada *Enterprise/IT architecture* karena disaat gagal, perusahaan akan mengalami kerugian namun tidak terlalu fatal. Selanjutnya ada IT operational infrastructure incidents, ini menjadi dampak yang besar bagi Instansi karena jika terjadi maka akan diganti dan biaya yang dikeluarkan tidak sedikit. Selanjutnya ada Unauthorized action untuk saat ini instansi tidak semua menyimpan data secara digital ada yang manual walaupun resiko terjadinya cukup sering namun dampaknya tidak begitu fatal karena sudah menyediakan self defense terlebih dahulu. Selanjutnya ada *Software adoption/usage* dampaknya sangat mempengaruhi instansi namun instansi harus tetap berjalan walaupun sangat lambat. Selanjutnya ada *Hardware Incident* sangat berdampak dan sering terjadi di dalam instansi dikarenakan adanya penyalahgunaan saat staf menggunakan hardware. Selanjutnya ada *Software Failures* dampak dan resiko tidak begitu tinggi didalam instansi dikarenakan semua termasuk software telah diatur sesuai SOP yang telah ada dikarenakan sudah ada rencana yang telah dipikirkan sebelum dampak tersebut terjadi. Selanjutnya ada *Logical Attacks* seperti yang telah diketahui bahwa instansi sangat rentan terjadinya serangan hacker dikarenakan instansi adalah tempat pengelolaan

informasi yang sangat penting namun untuk dampak yang dirasakan tidak begitu fatal dikarenakan sudah adanya sistem backup yang disediakan dari pusat. Selanjutnya ada *Third Party/Supplier Incident* untuk sekarang resiko dan dampak tidak begitu fatal bagi pihak instansi dikarenakan instansi telah menyediakan solusi jika hal tersebut terjadi. Selanjutnya ada *Non-compliance* karena sudah ada SOP yang telah di berikan dari pusat maka hal tersebut tidak begitu fatal, bagi instansi termasuk resiko yang sangat kecil. Selanjutnya ada *Geopolitical Issue* seperti yang telah dibilang bahwa instansi memiliki SOP maka dari itu dampak maupun resiko tidak begitu fatal yang dirasakan oleh instansi. Selanjutnya ada *Industrial Action* karena dulu pernah adanya demo yang dimana membuat instansi untuk bekerja dirumah. Selanjutnya ada Acts of Nature dapat menjadi dampak besar bagi instansi karena bisa membuat fasilitas instansi rusak. Selanjutnya ada *Technology-based innovation* karena instansi adalah tempat pengelolaan informasi jadi instansi telah menyediakan solusi jika hal tersebut terjadi. Selanjutnya ada Environmental karena instansi tidak terlalu fokus ke hal tersebut. Untuk yang terakhir ada *Data and Information Management* karena sudah adanya sistem backup yang disediakan oleh pusat membuat dampak tersebut tidak begitu fatal, namun resiko nya cukup tinggi dikarenakan data yang disimpan instansi begitu penting.

3.1.4 Design Factor 4 - *Related Issue*

Dari hasil wawancara yang kami lakukan pada penilaian Design Factor 4, ditemukan beragam isu terkait Teknologi Informasi (TI) pada Dinas Kominfo Provinsi Sulawesi Utara. Beberapa isu yang teridentifikasi termasuk ketidakpuasan dalam kontribusi TI terhadap nilai bisnis, kegagalan inisiatif TI yang menyebabkan ketidakpuasan dari departemen bisnis, insiden penting terkait TI seperti kehilangan data atau pelanggaran keamanan, masalah dalam penyampaian layanan oleh outsourcing TI, kegagalan memenuhi persyaratan regulasi atau kontrak TI, laporan audit yang menunjukkan kinerja TI yang buruk, pengeluaran TI yang tersembunyi, tumpang tindih antara proyek-proyek TI, kurangnya sumber daya TI dan keahlian staf, kegagalan proyek TI dalam memenuhi kebutuhan bisnis, serta kurangnya keterlibatan manajemen senior dengan TI

Beberapa isu tersebut dianggap sebagai normal issue, yang menunjukkan bahwa isu-isu tersebut memang telah terjadi atau sedang terjadi, namun belum memberikan dampak yang signifikan pada perusahaan. Sementara itu, beberapa isu lainnya, seperti kegagalan memenuhi persyaratan regulasi atau kontrak TI, masalah regulatif audit yang menunjukkan kinerja TI yang buruk, dan masalah kualitas data serta integrasi data yang terjadi secara reguler, dianggap sebagai serious issue karena dapat berdampak secara signifikan pada operasional dan reputasi perusahaan.

Namun, ada beberapa area juga menunjukkan bahwa tidak ada isu yang signifikan yang terjadi pada perusahaan (*no issue*), seperti kompleksitas model operasional TI yang terlalu tinggi, kurangnya pemahaman /atau ketidakpatuhan terhadap regulasi keamanan dan privasi, dan ketidakmampuan untuk memanfaatkan teknologi baru atau berinovasi menggunakan TI. Dengan mengidentifikasi dan mengelola isu-isu TI dengan cermat, Dinas Kominfo Provinsi Sulawesi Utara dapat memastikan kelangsungan operasional yang optimal dan pencapaian tujuan strategisnya dalam lingkungan bisnis yang semakin kompleks dan berubah-ubah.

3.1.5 Design Factor 5 - *Threat Landscape*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor* 5, narasumber diajukan pertanyaan mengenai sebesar apa ancaman yang dapat terjadi dalam dunia pekerjaan khususnya, ancaman yang dapat terjadi dalam bidang geopolitik, demografi dan lain sebagainya. Dari hasil wawancara dan hasil analisis peneliti sehingga didapati bahwa Dinas

Kominfo Provinsi Sulawesi Utara adalah 80% pada tingkat normal, dimana perusahaan beroperasi dibawah tingkat ancaman yang normal, dan 20% di tingkat ancaman yang tinggi karena peraturan pemerintah yaitu SOP yang digunakan untuk produktifitas dan kinerja dari perusahaan.

3.1.6 Design Factor 6 - *Compliance Requirements*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor* 6, narasumber diajukan pertanyaan mengenai sepatuh apa perusahaan terhadap regulasi dari pemerintah setempat. Pertanyaan pada design factor 6 ini dapat membantu mengetahui seberapa patuh Dinas Kominfo Provinsi Sulawesi Utara terhadap regulasi pemerintahan. Hasil ini didapatkan dari hasil wawancara dan analisa peneliti bahwa perusahaan diharuskan selalu mengikuti regulasi yang dikeluarkan oleh pemerintahan yang telah di tetapkan untuk melayani masyarakat yang sudah sesuai dengan standar yang ditetapkan oleh pusat dan juga pemerintah.

3.1.7 Design Factor 7 - Role *of IT*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor* 7, bahwa perusahaan menggunakan IT sebagai *Support* dalam proses operasional perusahaan. Mengapa demikian, karena IT bukan hanya sebagai *Strategic* bagi perusahaan ini, namun IT berperan penting bagi Instansi karena merupakan pendukung bagi tiap-tiap proyek untuk melayani masyarakat. Dinas Kominfo Provinsi Sulawesi Utara mengangkat peran *IT* sebagai *Support* dengan nilai 5 yang menjadikan nya sebagai *primary value*.

3.1.8 Design Factor 8 - *Role of IT*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor* 8, diketahui bahwa *sourcing model* pada Dinas Kominfo Provinsi Sulawesi Utara adalah 70% pada tingkat *Insourced*. Hal ini didasari oleh perusahaan menggunakan staff IT sendiri dalam menyediakan infrastruktur-infrastruktur bagi perusahaan. Selanjutnya 25% pada tingkat *Cloud* sebagai *vendor* berbasis internet yang digunakan oleh perusahan. Untuk model *Outsourcing* bernilai 15% karena perusahaan menggunakan Tenaga Harian Lepas (THL).

3.1.9 Design Factor 9 - *Implementation Methods*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor* 9, diketahui bahwa Dinas Kominfo Provinsi Sulawesi Utara pada metode *devOps* dengan persentase 80%, untuk metode *agile* 0% dan 20% untuk metode *traditional*. Karena perusahaan melakukan pengembangan dan pendekatan dengan metode klasik agar lebih mudah diterima oleh masyarakat.

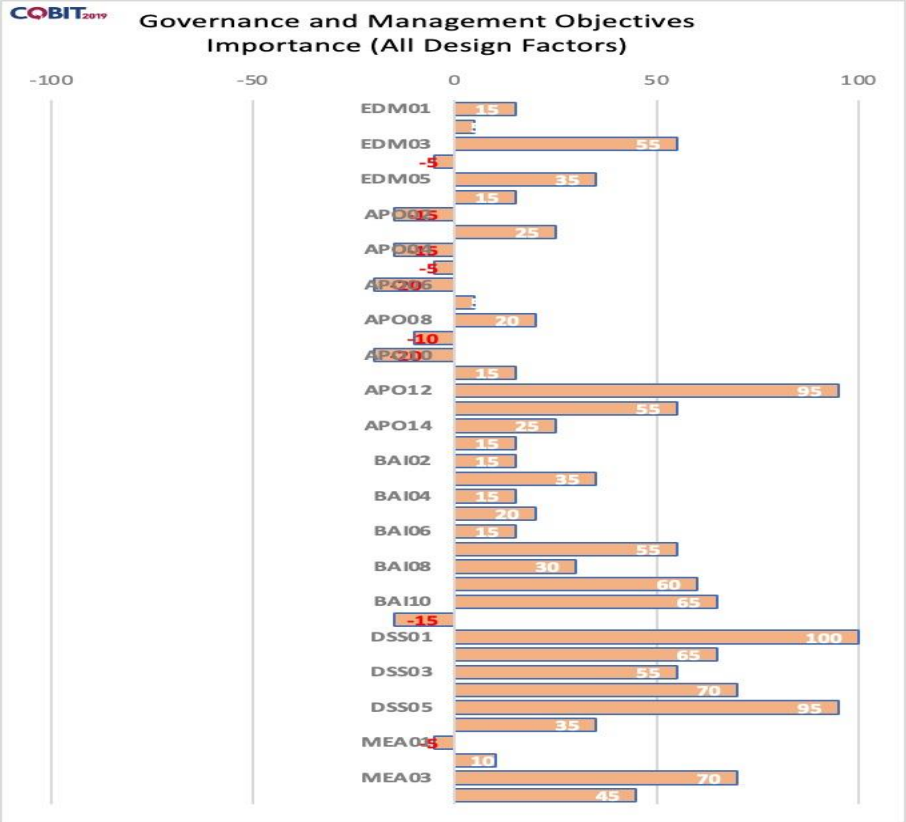
3.1.10 Design Factor 10 - *Technology Adoption Strategy*

Dari hasil wawancara yang kami lakukan pada penilaian *Design Factor* 10, diketahui bahwa berdasarkan hasil persentase dari *technology adoption strategy* pada Dinas Kominfo Provinsi Sulawesi Utara 10% sebagai first mover, 70% sebagai follower, dan 20% sebagai slow adopter.

Karena dari segi TI yang paling penting ada di jaringan dan aplikasi operasional yang digunakan oleh perusahaan, maka berdasarkan wawancara Dinas Kominfo Provinsi Sulawesi Utara mengadopsi strategi *Follower* untuk menunggu agar semua metode stabil agar memastikan tidak adanya kesalahan dalam melakukan pelayanan. Tetapi Instansi juga ikut serta dalam pengembangan jika ada aplikasi baru dari pusat maka perusahaan akan menjadi *First mover* maupun *slow adopter*.

3.2 Penentuan Objective Prioritas

Hasil dari pengisian ke-10 *design factor* didapati 3 *objectives* prioritas yang memiliki nilai lebih dari 80 yang didasari dan disesuaikan dengan kondisi perusahaan. Tiga *objectives* prioritas diantaranya APO12- *Managed Risk*, DSS01- *Managed Operations* dan DSS05- *Managed Security Services.* Berdasarkan hasil yang didapatkan maka akan dilanjutkan ke tahap inti.



Gambar 2. Hasil Objektif Prioritas.

3.3 Mapping RACI Chart

Bagian ini merupakan tahap penentuan responden untuk masing-masing *objectives* prioritas berdasarkan dengan buku COBIT 2019. Pada masing-masing *objectives* prioritas terdapat *accountable* yaitu sebagai pihak yang bertanggung jawab terhadap aktivitas dan *responsible* yaitu pihak yang merespon dan menyelesaikan aktivitas.

- Berdasarkan tabel responden untuk objective prioritas APO12.01 sampai dengan APO12.06 berada di posisi *Chief Risk Officer* sebagai *Accountable* atau pihak yang memiliki tanggung jawab penuh terhadap aktifitas dari *objectives* APO12.
- Berdasarkan responden untuk *objectives* prioritas DSS01.01 sampai DSS01.02 berada pada posisi *chief information officer* sebagai *accountable* dan DSS01.03 sampai DSS01.05 berada pada posisi *Chief Technology Officer* atau pihak yang memiliki tanggung jawab penuh terhadap aktivitas dari *objectives* DSS01.
- Berdasarkan responden untuk *objectives* prioritas DSS05.01 sampai DSS05.05, DSS05.07 berada pada posisi *chief information security officer* dan DSS05.06 berada pada *chief information officer* sebagai *accountable* atau pihak yang memiliki tanggung jawab penuh terhadap aktivitas dari *objectives* DSS05.

3.4 Hasil Wawancara Untuk *Objectives* Prioritas

Setelah hasil design factor dan penentuan responden telah didapatkan, maka dilanjutkan dengan wawancara yang dilakukan peneliti dengan responden yang sudah ditetapkan sesuai dengan RACI chart [20]. Berdasarkan hasil wawancara yang sudah dilakukan maka, dibuat perhitungan untuk mendapatkan kapabilitas level dari setiap objectives prioritas dan akan dikategorikan sesuai dengan NPFL. Apabila hasil dari kapabilitas level untuk objectives prioritas tidak mencapai F (*fully*) maka level kapabilitas tidak dapat dilanjutkan atau berhenti pada level tersebut. Setiap *objectives* prioritas dilakukan perhitungan mulai dari kapabilitas level 2 karena sesuai dengan yang sudah ditentukan dan ditulis dalam buku COBIT 2019 *governance and management objectives*.

3.4.1 APO12 – *Managed Risk*

Pada bagian ini aktivitas-aktivitas *objective* prioritas APO12 dapat dilihat pada table 4.13 yang menunjukan aktivitas level 2. Aktivitas-aktivitas ini nantinya akan digunakan untuk menentukan pencapaian kapabilitas level dari *objective* prioritas DSS01.

3.4.1.1 Aktivitas APO12 Level 2

Terdapat dua belas aktivitas pada *Objective* prioritas APO12 untuk level 2 dan berdasarkan wawancara terhadap responden, semua aktivitas yang ditanyakan peneliti telah dilakukan oleh Dinas Kominfo Provinsi Sulawesi Utara.

Tabel 1. Hasil Aktivitas APO12 level 2

Sub-Objectives	Aktivitas	Check Box
APO12.01 – Collect Data	Establish and maintain methods for the collection, classification, and analysis of IT risk-related data.	☑
APO12.02 – Analyze Risk	Record relevant and significant data related to IT risks in the company's internal and external operating environment.	☑
APO12.03 – Maintain a risk profile.	Inventory business processes and document their dependencies on IT service management processes and IT infrastructure resources. Identify support personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers, and external providers/outsourcers.	☑
APO12.03 – Maintain a risk profile.	Determine and approve IT services and IT infrastructure resources critical to maintaining business process operations. Analyze dependencies and identify weak points.	☑
APO12.03 – Maintain a risk profile.	Collect current risk scenarios by category, business line and functional area.	☒
APO12.05 – Define a risk management action portfolio	Manage inventory of existing control activities to reduce risk and enable risks to be taken in line with risk appetite and tolerance. Group control activities and link them to specific IT risk scenarios and IT risk scenario aggregations.	☒

Didapatkan hasil persentase sebesar 66.6% dari hasil tabel 1 setelah dilakukan perhitungan terhadap kapabilitas level 2 pada *objective* prioritas APO12 yang artinya berdasarkan NPLF, APO12 level 2 ini berada pada *rating Fully Achieved* sehingga dinyatakan mencapai kapabilitas level 2 dan tidak dapat dilanjutkan pada penilaian kapabilitas level 3.

3.4.2 DSS01 – *Managed Operations*

Pada bagian ini aktivitas-aktivitas *objective* prioritas DSS01 dapat yang menunjukan aktivitas level 2, aktivitas level 3, dan aktivitas level 4. Aktivitas-aktivitas ini nantinya akan digunakan untuk menentukan pencapaian kapabilitas level dari *objective* prioritas DSS01.

3.4.2.1 Aktivitas DSS01 Level 2

Terdapat dua belas aktivitas pada *Objective* prioritas DSS01 untuk level 2 dan berdasarkan wawancara terhadap responden, semua aktivitas yang ditanyakan peneliti telah dilakukan oleh Dinas Kominfo Provinsi Sulawesi Utara.

Tabel 2. Hasil Aktivitas DSS01 level 2

Sub-Objectives	Activity	Check Box
DSS01.01 - Perform operational procedures.	Develop and maintain operational procedures and related activities to support all delivered services	☑
DSS01.01 - Perform operational procedures.	Maintain a schedule of operational activities and perform the activities.	☑
DSS01.03 - Monitor I&T infrastructure	Log events. Identify the level of information to be recorded, based on a consideration of risk and performance.	☑
DSS01.04 - Manage the environment.	Identify natural and man-made disasters that might occur in the area where the IT facilities are located. Assess the potential effect on the IT facilities	☑
DSS01.04 - Manage the environment.	Identify how I&T equipment, including mobile and off-site equipment, is protected against environmental threats. Ensure that the policy limits or excludes eating, drinking and smoking in sensitive areas, and prohibits storage of stationery and other supplies that pose a fire hazard within computer rooms.	☑
DSS01.04 - Manage the environment.	Keep the IT sites and server rooms clean and in a safe condition at all times (i.e., no mess, no paper or cardboard boxes, no filled dustbins, no flammable chemicals or materials).	☑
DSS01. 05 - Manage facilities.	Examine the IT facilities' requirement for protection against power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning.	☑
DSS01. 05 - Manage facilities.	Regularly test the uninterruptible power supply's mechanisms. Ensure that power can be switched to the supply without any significant effect on business operations	☑
DSS01. 05 - Manage facilities.	Ensure that the facilities housing the I&T systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility.	☑
DSS01. 05 - Manage facilities.	Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and access to wiring cabinets is restricted to authorized personnel. Properly protect cabling against damage caused by fire, smoke, water, interception and interference.	☑
DSS01. 05 - Manage facilities.	Ensure that cabling and physical patching (data and phone) are structured and organized. Cabling and conduit structures should be documented (e.g., blueprint building plan and wiring diagrams).	☑
DSS01. 05 - Manage facilities.	On regular basis, educate personnel on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents.	☑

Didapatkan hasil persentase sebesar 100% berdasarkan tabel 2 setelah dilakukan perhitungan terhadap kapabilitas level 2 pada *objective* prioritas DSS01 yang artinya berdasarkan NPLF, DSS01 level 2 ini berada pada *rating Fully Achieved* sehingga dinyatakan mencapai kapabilitas level 2 dan dapat dilanjutkan pada penilaian kapabilitas level 3.

3.4.2.2 Aktivitas DSS01 Level 3

Terdapat empat belas aktivitas pada *Objective* prioritas DSS01 untuk level 3 dan berdasarkan wawancara terhadap responden, semua aktivitas yang ditanyakan peneliti telah dilakukan oleh Dinas Kominfo Provinsi Sulawesi Utara.

Tabel 3. Hasil Aktivitas DSS01 level 3

Sub-Objectives	Activity	Check Box
DSS01.01 - Perform operational procedures.	Verify that all data expected for processing are received and processed completely, accurately and in a timely manner. Deliver output in accordance with enterprise requirements. Support restart and reprocessing needs. Ensure that users are receiving the right outputs in a secure and timely manner.	☑
DSS01.02 - Manage outsourced I&T services	Ensure that the enterprise's requirements for security of information processes adhere to contracts and SLAs with third parties hosting or providing services.	☑
DSS01.02 - Manage outsourced I&T services	Ensure that the enterprise's operational business and IT processing requirements and priorities for service delivery adhere to contracts and SLAs with third parties hosting or providing services.	☑
DSS01.02 - Manage outsourced I&T services	Integrate critical internal IT management processes with those of outsourced service providers. This should cover, for example, performance and capacity planning, change management, configuration management, service request and incident management, problem management, security management, business continuity, and the monitoring of process performance and reporting.	☑
DSS01.03 - Monitor I&T infrastructure.	Identify and maintain a list of infrastructure assets that need to be monitored, based on service criticality and the relationship between configuration items and services that depend on them.	☑
DSS01.03 - Monitor I&T infrastructure.	Define and implement rules that identify and record threshold breaches and event conditions. Find a balance between generating spurious minor events and significant events so event logs are not overloaded with unnecessary information.	☒
DSS01.03 - Monitor I&T infrastructure.	Produce event logs and retain them for an appropriate period to assist in future investigations.	☑
DSS01.03 - Monitor I&T infrastructure.	Ensure that incident tickets are created in a timely manner when monitoring identified deviations from defined thresholds.	☑
DSS01. 04 - Manage the environment.	Situate and construct IT facilities to minimize and mitigate susceptibility to environmental threats (e.g., theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, explosives). Consider specific security zones and/or fireproof cells (e.g., locating production and development environments/servers away from each other).	☑
DSS01. 04 - Manage the environment.	Compare measures and contingency plans against insurance policy requirements and report results. Address points of noncompliance in a timely manner.	☒
DSS01. 04 - Manage the environment.	Respond to environmental alarms and other notifications. Document and test procedures, which should include prioritization of alarms and contact with local emergency response authorities. Train personnel in these procedures.	☑
DSS01. 05 - Manage facilities.	Ensure that IT sites and equipment are maintained according to the supplier's recommended service intervals and specifications. Ensure that maintenance is carried out only by authorized personnel.	☑

DSS01. 05 - Manage facilities.	Analyze the facilities housing's high-availability systems for redundancy and fail-over cabling requirements (external and internal).	☑
DSS01. 05 - Manage facilities.	Ensure that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications.	☑

Didapatkan hasil persentase sebesar 85.7% berdasarkan tabel 3 setelah dilakukan perhitungan terhadap kapabilitas level 3 pada *objective* prioritas DSS01 yang artinya berdasarkan NPLF, DSS01 level 3 ini berada pada *rating Fully Achieved* sehingga dinyatakan mencapai kapabilitas level 3 dan dapat dilanjutkan pada penilaian kapabilitas level 4.

3.4.2.3 Aktivitas DSS01 Level 4

Terdapat enam aktivitas pada *Objective* prioritas DSS01 untuk level 4 dan berdasarkan wawancara terhadap responden, semua aktivitas yang ditanyakan peneliti telah dilakukan oleh Dinas Kominfo Provinsi Sulawesi Utara.

Tabel 4. Hasil Aktivitas DSS01 level 4

Sub-Objectives	Activity	Check Box
DSS01.01 - Perform operational procedures.	Manage the performance and throughput of the scheduled activities.	☑
DSS01.02 - Manage outsourced I&T services	Plan for independent audit and assurance of the operational environments of outsourced providers to confirm that agreed requirements are being adequately addressed.	☒
DSS01.03 - Monitor I&T infrastructure.	Establish procedures for monitoring event logs. Conduct regular reviews.	☑
DSS01. 04 - Manage the environment.	Regularly monitor and maintain devices that proactively detect environmental threats (e.g., fire, water, smoke, humidity).	☑
DSS01. 05 - Manage facilities.	Record, monitor, manage and resolve facilities incidents in line with the I&T incident management process. Make available reports on facilities incidents for which disclosure is required by laws and regulations.	☑
DSS01. 05 - Manage facilities.	Analyze physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.	☑

Didapatkan hasil persentase sebesar 83.3% berdasarkan tabel 4 setelah dilakukan perhitungan terhadap kapabilitas level 4 pada *objective* prioritas DSS01 yang artinya berdasarkan NPLF, DSS01 level 4 ini berada pada *rating Fully Achieved* sehingga dinyatakan mencapai kapabilitas level 4 dan tidak dapat dilanjutkan pada penilaian kapabilitas level 5.

3.4.3 DSS05 – *Managed Security Services*

Pada bagian ini aktivitas-aktivitas objective prioritas DSS05 yang menunjukan aktivitas level 2. Aktivitas-aktivitas ini nantinya akan digunakan untuk menentukan pencapaian kapabilitas level dari objective prioritas DSS05.

3.4.3.1 Aktivitas DSS05 Level 2

Terdapat dua puluh enam aktivitas pada *Objective* prioritas DSS05 untuk level 2 dan berdasarkan wawancara terhadap responden, semua aktivitas yang ditanyakan peneliti telah dilakukan oleh Dinas Kominfo Sulawesi Utara.

Tabel 5. Hasil Aktivitas DSS05 level 2

Sub-Objectives	Aktivitas	Check Box
DSS05.01 Protect against malicious software	Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).	☑
DSS05.01 Protect against malicious software.	Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).	☑
DSS05.02 Manage network and connectivity security.	Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.	☑
DSS05.02 Manage network and connectivity security.	Implement network filtering mechanisms, such as firewalls and intrusion detection software. Enforce appropriate policies to control inbound and outbound traffic.	☑
DSS05.02 Manage network and connectivity security.	Apply approved security protocols to network connectivity.	☑
DSS05.02 Manage network and connectivity security.	Configure network equipment in a secure manner.	☑
DSS05.03 Manage endpoint security.	Configure operating systems in a secure manner.	☑
DSS05.03 Manage endpoint security.	Implement device lockdown mechanisms.	☑
DSS05.03 Manage endpoint security.	Manage remote access and control (e.g., mobile devices, teleworking).	☑
DSS05.03 Manage endpoint security.	Manage network configuration in a secure manner.	☑
DSS05.03 Manage endpoint security.	Implement network traffic filtering on endpoint devices.	☑
DSS05.03 Manage endpoint security.	Protect system integrity.	☑
DSS05.03 Manage endpoint security.	Provide physical protection of endpoint devices.	☑
DSS05.03 Manage endpoint security.	Dispose of endpoint devices securely.	☑
DSS05.03 Manage endpoint security.	Manage malicious access through email and web browsers. For example, block certain websites and deactivate click-through on links for smartphones.	☑
DSS05.04 Manage user identity and logical access.	Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.	☑
DSS05.05 Manage physical access to I&T assets.	Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.	☑
DSS05.05 Manage physical access to I&T assets.	Ensure all personnel display properly approved identification at all times.	☒
DSS05.05 - Manage physical access to I&T assets.	Require visitors to be escorted at all times while on-site.	☑
DSS05.05 - Manage physical access to I&T assets.	Restrict and monitor access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls and security devices on interior and exterior doors.	☑
DSS05.06 - Manage sensitive documents and output devices.	Establish procedures to govern the receipt, use, removal and disposal of sensitive documents and output devices into, within, and outside of the enterprise.	☒

DSS05.06 Manage sensitive documents and output devices.	Ensure cryptographic controls are in place to protect sensitive electronically stored information.	☑
DSS05.07 - Manage vulnerabilities and monitor the infrastructure for security-related events.	Continually use a portfolio of supported technologies, services and assets (e.g., vulnerability scanners, fuzzers and sniffers, protocol analyzers) to identify information security vulnerabilities.	☑
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events	Define and communicate risk scenarios, so they can be easily recognized, and the likelihood and impact understood.	☑
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events	Regularly review the event logs for potential incidents.	☒
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events	Ensure that security--related incident tickets are created in a timely manner when monitoring identifies potential incidents.	☒

Didapatkan hasil persentase sebesar 84.6% setelah dilakukan perhitungan terhadap kapabilitas level 2 pada *objective* prioritas DSS05 yang artinya berdasarkan NPLF, DSS05 level 2 ini berada pada *rating Fully Achieved* sehingga dinyatakan mencapai kapabilitas level 2 dan tidak dapat dilanjutkan pada penilaian kapabilitas level 3.

3.5 Kesenjangan Level Kapabilitas

Adapun hasil yang didapatkan yakni tidak didapati ada kesenjangan dari masing-masing objective prioritas berdasarkan hasil perhitungan kapabilitas level saat ini dengan kapabilitas level yang diharapkan sebagaimana yang didapatkan dari hasil analisa *design toolkit.* Dapat dilihat pada tabel 6.

Tabel 6. Kesenjangan Level Kapabilitas Proses

No.	Domain Proses	Level Kapabilitas diharapkan	Level Kapabilitas Saat Ini	Kesenjangan
1	APO12- Managed Risk	5	2	3
2	DSS01—Managed Operations	5	4	1
3	DSS05—Managed Security Services	4	2	2

3.5 Rekomendasi Aktivitas Objectives Prioritas

Rekomendasi diberikan berdasarkan framework COBIT 2019. Rekomendasi yang diberikan berupa aktivitas-aktivitas yang belum dijalankan pada Dinas Kominfo Provinsi Sulawesi utara. Pada hasil perhitungan kapabilitas level untuk Dinas Kominfo Provinsi Sulawesi utara, didapati objective prioritas APO12, DSS01, dan DSS05 belum mencapai kapabilitas level yang diharapkan. Maka rekomendasi yang diberikan akan sesuai dengan setiap objectives prioritas.

Berdasarkan hasil perhitungan kapabilitas level dari objective APO12 hasil yang didapatkan bahwa tidak memenuhi kapabilitas level 2, dan hasil ini belum mencapai level kapabilitas yang diharapkan yaitu level 5. Adapun rekomendasi yang diberikan terdapat pada tabel 7.

Tabel 7. Rekomendasi Aktivitas APO12

Sub-Objectives	*Capability Level*	Rekomendasi Agar Bisa Mencapai Level yang Diharapkan
APO12.03 – Maintain a risk profile	2	Perusahaan menggabungkan skenario risiko saat ini berdasarkan kategori, garis bisnis, dan are fungsional agar perusahaan dapat memahami risiko secara komprehensif dan dapat mengambil tindakan yang sesuai untuk meminimalkan dampak.
APO12.05 – Define a risk management action portfolio	2	Identifikasi risiko IT secara menyeluruh, evaluasi risiko yang mendalam, pengelolaan inventaris kontrol yang ada dengan efektif, menghubungkan kontrol dengan skenario risiko IT spesifik, menetapkan tingkat risk appetite dan tolerance yang sesuai, mengimplementasikan mekanisme pemantauan dan pelaporan risiko yang efektif, serta melakukan peningkatan kontinu terhadap kontrol yang ada. Dengan mengintegrasikan aktivitas-aktivitas ini secara holistik, perusahaan dapat mengurangi risiko secara signifikan dan memungkinkan pengambilan risiko yang sejalan dengan tujuan dan strategi bisnis.

Kemudian pada *objective* prioritas DSS01, berdasarkan hasil perhitungan kapabilitas level didapati bahwa DSS01 belum memenuhi kapabilitas level 5 namun berada di level 4 pada, *sub-objectives* DSS01.02 perusahaan belum melakukan aktivitas yang dapat menunjang atau meningkatkan proses perubahan dalam perusahaan. Adapun rekomendasi yang diberikan terdapat pada tabel 8.

Tabel 8. Rekomendasi Aktivitas DSS01

Sub-Objectives	*Capability Level*	Rekomendasi Agar Bisa Mencapai Level yang Diharapkan
DSS01.02 – Manage outsourced I&T services.	4	Melakukan integrasikan pada proses manajemen TI internal yang penting dengan proses dari penyedia layanan outsourcing. Ini harus mencakup, misalnya, kinerja dan perencanaan kapasitas, manajemen perubahan, manajemen konfigurasi, permintaan layanan dan manajemen insiden, manajemen masalah, manajemen keamanan, kelangsungan bisnis, dan pemantauan kinerja proses dan pelaporan.

Terakhir, pada *objective* prioritas DSS05 dari hasil perhitungan kapabilitas level didapatkan hasil tidak memenuhi kapabilitas level 3 dan hasil ini belum mencapai level kapabilitas yang diharapkan yaitu kapabilitas level 4. Adapun rekomendasi yang diberikan terdapat pada tabel 9.

Tabel 9. Rekomendasi Aktivitas DSS05

Sub-Objectives	*Capability Level*	Rekomendasi Agar Bisa Mencapai Level yang Diharapkan
DSS05.05 *Manage physical access to I&T assets.*	2	Memastikan semua staf/karyawan menampilkan identifikasi yang disetujui dengan benar setiap saat
DSS05.06 *Manage sensitive documents and output devices.*	2	Menetapkan prosedur untuk mengatur penerimaan, penggunaan, pemindahan, dan pembuangan dokumen sensitif dan perangkat keluaran ke dalam, di dalam, dan di luar perusahaan.
DSS05.07 *Manage vulnerabilities and monitor the infrastructure for security-related events*	2	Memastikan bahwa tiket insiden terkait keamanan dibuat tepat waktu saat pemantauan mengidentifikasi potensi insiden
DSS05.07 *Manage vulnerabilities and monitor the infrastructure for security-related events*	2	Mencatat event terkait keamanan dan simpan catatan untuk periode yang sesuai

4. KESIMPULAN

Setelah menyelesaikan sepuluh desain faktor menggunakan toolkit COBIT 2019, tiga tujuan prioritas diidentifikasi, yaitu APO12—Managed Risk, DSS01—Managed Operations, dan DSS05—Managed Security Services. Untuk domain APO12, terdapat kesenjangan besar sebesar 3 level, menunjukkan perlunya upaya yang signifikan untuk meningkatkan pengelolaan risiko agar sesuai dengan level kapabilitas yang diharapkan. Dinas Kominfo Sulut telah melaksanakan beberapa aktivitas yang tercantum dalam tujuan prioritas APO12 pada level 2. Namun, masih ada aktivitas yang belum direalisasikan, terutama pada sub tujuan APO12.03 dan APO12.05, yang memerlukan peningkatan dalam pengaturan profil risiko dan mendefinisikan portofolio tindakan manajemen risiko. Hasil perhitungan menunjukkan bahwa objektif prioritas APO12 untuk level 2 mencapai 66.6%, yang berarti telah sepenuhnya mencapai kapabilitas level 2 namun belum dapat dilanjutkan ke penilaian kapabilitas level 3. Dalam hal DSS01, kesenjangan yang lebih kecil, yakni 1 level, menunjukkan bahwa kapabilitas saat ini cukup mendekati target yang diinginkan, dengan hanya memerlukan peningkatan minor untuk mencapai level yang diharapkan; yaitu pada DSS01.02. Hasil perhitungan menunjukkan bahwa persentase kapabilitas untuk DSS01 pada level 4 adalah 83.3%, yang berarti DSS01 berada pada rating Fully Achieved. Dengan demikian, kapabilitas level 4 telah tercapai dan penilaian untuk level 5 tidak diperlukan. Sementara itu, pada DSS05, terdapat kesenjangan sebesar 2 level. Hasil perhitungan menunjukkan persentase kapabilitas DSS05 pada level 2 adalah 84.6%, yang berarti berada pada rating Fully Achieved. Dengan demikian, kapabilitas level 2 telah tercapai dan penilaian untuk level 3 tidak diperlukan. Namun masih terdapat aktifitas-aktifitas yang belum direalisasikan meliputi DSS05.05 hingga DSS05.07 menandakan perlunya upaya yang substansial untuk memperbaiki layanan keamanan agar sesuai dengan tingkat kapabilitas yang diinginkan.

REFERENSI

[1] I. G. M. S. Dharma, I. G. M. A. Sasmita, and I. M. S. Putra, “Evaluasi Dan Implementasi Tata Kelola TI Menggunakan COBIT 2019 (Studi Kasus Pada Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Tabanan,” JITTER- J. Ilm. Teknol. dan Komput, vol. 2, no. 2, 2021.

[2] L. H. A. G. I. Belo and Y. T. Wiranti, “Perancangan Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 Pada PT Telekomunikasi Indonesia Regional VI Kalimantan,” Jurnal Sist. Inf. Ilmu Komput. Prima, vol. 4, pp. 26-27, 2020.

[3] A. Wijaya, “An INFORMATION TECHNOLOGY GOVERNANCE AUDIT PLANNING CALIBRATION LABORATORY USING COBIT 2019,” J. Fasilkom, vol. 10, no. 3, pp. 241-247, 2020, doi: 10.37859/jf.v10i3.2272.

[4] S. F. Bayastura, S. Krisdina, and A. P. Widodo, “Analysis and Design of Information Technology Governance Using the Cobit 2019 Jiko,” vol. 4, no. 1. pp. 68-75, 2021. doi: 10.33387/jiko.

[5] A. A. Mariatama, “Perancangan Tata Kelola Teknologi Informasi dengan Menggunakan Framework COBIT 2019 pada PT JWT Global Logistics Indonesia,” Bachelor thesis, Inst. Teknol. Kalimantan, 2021.

[6] D. Mirza, L. Suryani, L. Latip, and V. Aditiya, “Literature Riview: Peran Teknologi Informasi dalam Meningkatkan Efisiensi dan Efektivitas Birokrasi,” Jurnal Administrasi Publik dan Bisnis, vol. 5, no. 1, Art. no. 1, Mar. 2023, doi: 10.36917/japabis.v5i1.84.

[7] M. F. A. Faraby, "Audit Tata Kelola Teknologi Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Agam Menggunakan Framework Cobit 2019," bachelorThesis, Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta, 2023. Accessed: Jul. 25, 2024. [Online]. Available: https://repository.uinjkt.ac.id/dspace/handle/123456789/71422

[8] P. Anastasia and L. Atrinawati, "PERANCANGAN TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019 PADA HOTEL XYZ," JSI: Jurnal Sistem Informasi (E-Journal), vol. 12, Oct. 2020, doi: 10.36706/jsi.v12i2.12329.

[9] M. Solehuddin, Z. Hulwani, and A. P. Widodo, "Perencanaan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 pada DPMPTSP"," jikstik, vol. 20, no. 2, pp. 155-164, Jun. 2021.

[10] A. C. Amorim, M. M. Silva, R. Pereira, and M. Gonçalves, "Using agile methodologies for adopting COBIT," *Information Systems*, vol. 101, no. 3, p. 211, 2021, doi: 10.1016/j.is.2020.101496.

[11] B. V. Tulus and A. R. Tanaamah, "Design of Information Technology Governance in Educational Institutions using COBIT 2019 Framework," Journal of Information Systems and Informatics, vol. 5, no. 1, pp. 31-43, Feb. 2023, doi: 10.51519/journalisi.v5i1.408.

[12] P. A. Adawiyah and L. H. Atrinawati, "PERANCANGAN TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019 PADA PT. XYZ," JTSI, vol. 1, no. 2, pp. 1–9, Dec. 2020, doi: 10.33365/jtsi.v1i2.301.

[13] M. Masduki and M. Masduki, "Introduction and Methodology," in Public Service Broadcasting and Post-Authoritarian Indonesia, Singapore: Springer, 2020, pp. 1-24, doi: 10.1007/978-981-15-7650-8_1.

[14] Mambu, J. Y., Fanesa, V., Pythagoras, M., & Lumingkewas, C. (2023). Identifikasi Level Kapabilitas IT Governance Menggunakan Framework Cobit 2019 Pada PT Icon+. Jurnal Informasi Dan Teknologi, 5(2), 19-29. https://doi.org/10.37034/jidt.v5i2.322

[15] P. A. Adawiyah and L. H. Atrinawati, "Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019," J. Teknol. dan Sist. Inf, vol. 1, no. 2, pp. 1-9, 2020, doi: 10.33365/jtsi.v1i2.301.

[16] D. Darmawan and A. F. Wijaya, "Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ," Journal of Computer and Information Systems Ampera, vol. 3, no. 1, Art. no. 1, Jan. 2022, doi: 10.51519/journalcisa.v3i1.139.

[17] G. I. Belo, L. H. Atrinawati, and Y. T. Wiranti, "Perancangan Tata Kelola Teknologi Informasi menggunakan COBIT 2019 pada PT Telekomunikasi Indonesia Regional VI Kalimantan," Jurnal Sistem Informasi dan Ilmu Komputer Prima (JUSIKOM PRIMA), vol. 4, no. 1, Art. no. 1, Sep. 2020, doi: 10.34012/jusikom.v4i1.1202.

[18] H. Shofiyah, Suprapto, and A. R. Perdanakusuma, "Evaluasi Kapabilitas Teknologi Informasi pada Kantor Kesehatan Pelabuhan (KKP) Kelas II Probolinggo Menggunakan Kerangka Kerja COBIT 2019"," IJSTECH, vol. 1, no. 3, pp. 148-162, Feb. 2024.