TESIS

AUDIT TATA KELOLA TEKNOLOGI INFORMASI LEMBAGA PEMERINTAH BIDANG PELAYANAN METROLOGI MENGGUNAKAN COBIT 2019

(Studi Kasus: Balai Standardisasi Metrologi Legal Regional II Kementerian Perdagangan)

Disusun oleh:

Nama : **Angga Wijaya Narwa Putra**
NIM : **19.52.1259**
Konsentrasi : **Business Intelligence**

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

TESIS

AUDIT TATA KELOLA TEKNOLOGI INFORMASI LEMBAGA PEMERINTAH BIDANG PELAYANAN METROLOGI MENGGUNAKAN COBIT 2019

(Studi Kasus: Balai Standardisasi Metrologi Legal Regional II Kementerian Perdagangan)

AUDIT OF INFORMATION TECHNOLOGY GOVERNANCE OF THE GOVERNMENT INSITUTE IN THE FIELD OF METROLOGY SERVICES USING COBIT 2019

(Case Study: Balai Standardisasi Metrologi Legal Regional II Ministry of Trade)

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Magister

Disusun oleh:

Nama	**: Angga Wijaya Narwa Putra**
NIM	**: 19.52.1259**
Konsentrasi	**: Business Intelligence**

PROGRAM STUDI S2 TEKNIK INFORMATIKA

PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2021

HALAMAN PENGESAHAN

AUDIT TATA KELOLA TEKNOLOGI INFORMASI LEMBAGA PEMERINTAH BIDANG PELAYANAN METROLOGI MENGGUNAKAN COBIT 2019
(Studi Kasus: Balai Standardisasi Metrologi Legal Regional II Kementerian Perdagangan)

AUDIT OF INFORMATION TECHNOLOGY GOVERNANCE OF THE GOVERNMENT INSITUTE IN THE FIELD OF METROLOGY SERVICES USING COBIT 2019
(Case Study: Balai Standardisasi Metrologi Legal Regional II Ministry of Trade)

Dipersiapkan dan Disusun oleh

Angga Wijaya Narwa Putra

19.52.1259

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Rabu, 9 Juni 2021

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

Yogyakarta, 9 Juni 2021
Rektor

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

HALAMAN PERSETUJUAN

AUDIT TATA KELOLA TEKNOLOGI INFORMASI LEMBAGA PEMERINTAH BIDANG PELAYANAN METROLOGI MENGGUNAKAN COBIT 2019
(Studi Kasus: Balai Standardisasi Metrologi Legal Regional II Kementerian Perdagangan)

AUDIT OF INFORMATION TECHNOLOGY GOVERNANCE OF THE GOVERNMENT INSITUTE IN THE FIELD OF METROLOGY SERVICES USING COBIT 2019
(Case Study: Balai Standardisasi Metrologi Legal Regional II Ministry of Trade)

Dipersiapkan dan Disusun oleh

Angga Wijaya Narwa Putra

19.52.1259

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Rabu, 9 Juni 2021

Pembimbing Utama	**Anggota Tim Penguji**
Dr. Andi Sunyoto, M.Kom	**Dr.Arief Setyanto, S.Si, M.T.**
NIK. 190302052	**NIK. 190302026**
	Alva Hendi Muhammad, S.T,M.Eng.Ph.D
Pembimbing Pendamping	**NIK. 190302493**
Drs. Asro Nasiri, M.Kom	**Dr.Andi Sunyoto, M.Kom**
NIK. 190302152	**NIK. 190302052**

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

Yogyakarta, 9 Juni 2021
Direktur Program Pascasarjana

Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Angga Wijaya Narwa Putra
NIM : 19.52.1259
Konsentrasi : Business Intelligence

Menyatakan bahwa Tesis dengan judul berikut:
Audit Tata Kelola Teknologi Informasi Lembaga Pemerintah Bidang Pelayanan Metrologi menggunakan COBIT 2019
(Studi Kasus: Balai Standardisasi Metrologi Legal Regional II Kementerian Perdagangan)
Dosen Pembimbing Utama : Dr. Andi Sunyoto, M.Kom
Dosen Pembimbing Pendamping : Drs. Asro Nasiri, M.Kom

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 Juni 2021
Yang Menyatakan,

Angga Wijaya Narwa Putra

HALAMAN MOTTO

Hiduplah yang berarti. Jadilah orang yang berguna bagi banyak orang

KATA PENGANTAR

Segala puji syukur kehadirat Alloh Subhanahu Wa Ta'ala yang telah melimpahkan anugerah dan karunia-Nya sehingga penulis dapat menyelesaikan Tesis yang berjudul "Audit Tata Kelola Teknologi Informasi Lembaga Pemerintah Bidang Pelayanan Metrologi menggunakan COBIT 2019 (Studi Kasus: Balai Standardisasi Metrologi Legal Regional II Kementerian Perdagangan)". Tesis ini disusun sebagai salah satu syarat menyelesaikan studi magister di Program Studi Magister Teknik Infromatika Universitas AMIKOM Yogyakarta. Dengan ini, penulis menyampaikan penghormatan dan terima kasih kepada pihak-pihak yang telah memberikan bantuan dan dukungan baik berupa moral maupun material secara langsung maupun tidak langsung antara lain kepada:

1. Ibu Dr. Kusrini, M.Kom selaku Ketua Program Studi Magister Teknik Informatika;
2. Bapak Dr. Andi Sunyoto, M.Kom selaku dosen pembimbing 1 Tesis yang telah meluangkan waktu, tenaga dan pikiran dalam memberikan bimbingan, pengarahan, dan ilmu pengetahuan;
3. Bapak Drs. Asro Nasiri, M.Kom selaku dosen pembimbing 2 Tesis yang telah meluangkan waktu, tenaga dan pikiran dalam memberikan bimbingan, pengarahan, dan ilmu pengetahuan;
4. Bapak Dr. Arief Setyanto, M.T. dan Bapak Alva Hendi Muhammad, Ph.D selaku dosen penguji yang telah memberikan saran;

5. Bapak M.Hendro Purnomo, ST, MSE selaku Kepala BSML Regional II yang telah mengizinkan penelitian di BSML Regional II;
6. Orang tua serta istri dan anak tercinta yang selalu memberikan dukungan bagi penulis;
7. Teman-teman MTI angkatan 2019 yang selalu memotivasi, mengingatkan, memberi masukan, dan selalu memberi suntikan semangat kepada penulis;
8. Semua pihak yang tidak dapat disebutkan satu persatu, yang telah banyak memberikan berbagai macam bantuan dalam penyusunan Tesis ini.

Akhir kata, penulis berharap Tesis ini dapat memberikan manfaat kepada pembaca mengenai proses audit teknologi informasi. Penulis menyadari bahwa tesis ini masih jauh dari kesempurnaan dan memiliki banyak kekurangan. Oleh karena itu, dengan kerendahan hati penulis mengharapkan masukan dan saran yang membangun untuk perbaikan ke depan.

Yogyakarta, 16 Juni 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Seiring perkembangan teknologi informasi, tata kelola teknologi informasi menjadi hal yang penting untuk diimplementasikan tak terkecuali pada Lembaga Pemerintahan. Pemerintah Pusat melalui Perpres nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (SPBE) telah mewajibkan implementasi tata kelola teknologi informasi pada seluruh Lembaga Pemerintahan. Pada lembaga pemerintah terutama bidang pelayanan, implementasi SPBE ini menjadi sangat penting karena membantu peningkatan mutu pelayanan terhadap masyarakat. Balai Standardisasi Metrologi Legal (BSML) Regional II merupakan Lembaga Pemerintah Pusat bidang pelayanan metrologi yang telah memiliki akreditasi ISO 17025 dan 90001 dapat menjadi tolok ukur bagi Lembaga Pemerintahan sejenis dalam implementasi SPBE. Dalam rangka percepatan implementasi SPBE maka diperlukan audit tata kelola teknologi informasi untuk mengetahui tingkat kapabilitas saat ini. Audit tata kelola teknologi informasi selain berfungsi untuk mengetahui ketidaksesuaian pengelolaan juga berfungsi untuk mengoptimalkan kinerja sehingga dapat tercapai visi dan misi perusahaan. COBIT 2019 sebagai framework edisi terbaru dari ISACA melakukan perbaikan dalam hal *goal cascading* menggunakan faktor desain. Penelitian ini menghasilkan kegiatan audit tata kelola teknologi informasi pada Lembaga Pemerintah pelayanan metrologi khususnya BSML Regional II berikut tingkat kapabilitasnya dan rekomendasi bagi rencana implementasi SPBE. Hasil auditnya adalah tingkat kapabilitas tata kelola teknologi informasi pada BSML Regional II pada tingkat 1 (inisial) atau dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif serta rekomendasi disusun untuk memperbaiki pengelolaan teknologi informasi pada objek penelitian.

Kata kunci: audit tata kelola, cobit 2019, Lembaga pemerintahan, faktor desain

ABSTRACT

Along with the development of information technology, information technology governance is an important thing to implement, including in Government Institutions. The Central Government through Perpres No. 95 Tahun 2018 concerning Electronic-Based Government Systems (SPBE) has required the implementation of information technology governance in all Government Institutions. In government agencies, especially in the service sector, the implementation of this SPBE is very important because it helps improve the quality of service to the community. The Center for Legal Metrology Standardization (BSML) Regional II is a Central Government Institution in the field of metrology services which has ISO 17025 and 90001 accreditation which can be a benchmark for similar Government Agencies in implementing SPBE. In order to accelerate the implementation of SPBE, an audit of information technology governance is needed to determine the current level of capability. Information technology governance audit, besides functioning to identify management mismatches, also functions to optimize performance so that the company's vision and mission can be achieved. COBIT 2019 as the latest edition of ISACA's framework makes improvements in terms of goal cascading using design factors. This research resulted in an audit of information technology governance at government institutions for metrology services, especially BSML Regional II, its level of capability and recommendations for SPBE implementation plans. The result of the audit is the level of information technology governance capability at BSML Regional II at level 1 (initial) or it can be categorized as an initial activity or activity that is intuitive in nature and recommendations are formulated to improve information technology management on the object of research.

Keywords: Governance Audit, COBIT 2019, Government Institution, design factor

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam rangka mengikuti perkembangan teknologi informasi, pemerintah Indonesia mencanangkan program implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE). Program tersebut berlandaskan Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasi Elektronik. Dalam peraturan tersebut, salah satu hal yang ditekankan adalah tata kelola teknologi informasi dalam rangka implementasi SPBE tertuang pada pasal 4 Perpres tersebut.

Pada lembaga pemerintah terutama bidang pelayanan, implementasi SPBE ini menjadi sangat penting karena membantu peningkatan mutu pelayanan terhadap masyarakat. Dilihat dari fungsi dan peranan teknologi informasi yang sangat penting, maka diperlukan suatu tata kelola teknologi informasi yang dapat mengevaluasi teknologi informasi secara keseluruhan di perusahaan. Evaluasi ini sangat diperlukan. Hal ini bertujuan untuk meningkatkan keuntungan yang optimal yang didapatkan dari proyek teknologi informasi dan dapat mengelola risiko yang berkaitan dengan teknologi informasi (Joshi et al., 2018). Tata kelola teknologi informasi adalah proses yang memandu dan mengelola investasi juga keputusan yang berhubungan dengan TI di dalam perusahaan tersebut supaya mencapai tujuan (Alreemy et al, 2016).

Lembaga pemerintah bidang pelayanan metrologi pun dituntut untuk mengimplementasikan SPBE. Balai Standardisasi Metrologi Legal (BSML) Regional II Direktorat Metrologi Kementerian Perdagangan Republik Indonesia merupakan kepanjangan tangan dari Direktorat Metrologi, Direktorat Jenderal Perlindungan Konsumen dan Tertib Niaga Kementerian Perdagangan yang mengawal Undang-Undang Nomer 2 Tahun 1981 tersebut. BSML Regional II merupakan satuan kerja tersendiri dan hal itu didukung oleh Peraturan Menteri Perdagangan Nomer 60/M-DAG/PER/8/2016 tentang Organisasi dan Tata Kerja unit Pelaksanan Teknis Bidang Kemetrologian dan Bidang Standardisasi Pengendalian Mutu di Lingkungan Kementerian Perdagangan. Sebagai lembaga dibawah pemerintah pusat yang telah terakreditasi ISO 17025 dan ISO 9001, BSML Regional II diharapkan dapat menjadi contoh sekaligus tolok ukur bagi lembaga pemerintah bidang pelayanan metrologi pada program implementasi SPBE.

Untuk menjamin segala kebijakan yang telah ditentukan tersebut diterapkan dan berjalan dengan baik perlu dilakukan sebuah evaluasi (audit) terhadap tata kelola TI yang ada agar seluruh mekanisme manajemen TI sesuai dengan perencanaan, serta tujuan dan proses bisnis perusahaan. Berkaitan dengan hal tersebut, terdapat beberapa penelitian terdahulu yang dijadikan acuan dan referensi pada penelitian ini. Pada penelitian sebelumnya yang pertama dengan judul Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 (Miranti, 2019) mengatakan bahwa tata kelola teknologi informasi adalah bagian dari suatu perusahaan yang melibatkan pemangku kepentingan perusahaan untuk memastikan kelanjutan strategi organisasi dan teknologi informasi. Penelitian yang

kedua adalah Audit Sistem Informasi pada Sistem Admisi UIN Sunan Kalijaga Yogyakarta menggunakan framework COBIT4.1 (Taslihudin, 2016) dihasilkan bahwa evaluasi ini dapat mendeteksi secara dini permasalah yang terjadi sebelum terlambat. Pada penelitian lain dengan judul Audit Sistem Informasi Akademik menggunakanan Cobit 5 di Universitas Jenderal Achmad Yani (Ekowansyah dkk, 2017) mengatakan bahwa proses TI yang baik akan menghasilkan kegiatan operasional yang baik pula. Penelitian selanjutnya dengan judul Evaluasi Tata Kelola Teknologi Informasi Menggunakan *Framework* COBIT 5 Domain DSS Studi Kasus : PT. PLN (Persero) Kantor Pusat (Baharuddin dkk, 2019) berkesimpulan penggunaan Cobit 5 untuk mengevaluasi tata kelola teknologi informasi di suatu perusahaan dapat memberikan rekomendasi bagi perusahaan sehingga dapat mencapai level yang diinginkan. Sedangkan penelitian dengan judul Audit Tata Kelola Teknologi Informasi pada PT.Pelabuhan Indonesia III (Persero) menggunakan kerangka kerja Cobit 5 (Heppy, 2017) yang bertujuan untuk memperoleh ukuran kapabilitas proses TI saat ini dan yang akan diharapkan serta penyusunan rekomendasi guna menyelarasan tata kelola TI dengan strategi bisnis perusahaan telah berhasil dengan menggunakan kerangka kerja COBIT 5. Dan sebagai bentuk penyempurnaan dari COBIT 5, dalam penelitian berjudul *Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4* (Nachrowi dkk, 2020) mengatakan bahwa penelitian terhadap COBIT 5 yang bertujuan untuk memperbaiki *goal cascading* telah dilakukan, dimana COBIT 2019 telah mengimplementasikan faktor desain dalam

proses goal cascading sehingga akan menyempurnakan desain sistem tata kelola suatu perusahaan berdasarkan penggunaan IT di perusahaan tersebut.

Dalam penelitian yang berjudul *An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model* (Zhang, 2013) mencoba melakukan penelitian yang lebih objektif (selama ini jurnal dikeluarkan oleh komunitas dan perusahaan pengguna COBIT) dan salah satu kesimpulannya adalah bagaimana COBIT mencakup framework lain sehingga diharapkan audit tata kelola menggunakan COBIT akan diperoleh hasil audit yang maksimal. Dibandingkan dengan *framework* lainnya, COBIT 2019 memiliki cakupan jangkauan masalah yang luas sehingga dapat mudah digunakan untuk segala bentuk perusahaan dan karena COBIT 2019 sudah mencakup materi yang ada pada kerangka kerja lain (ISACA,2019), yaitu:

1. ISO/EIC 38500 (masuk ke dalam area tata kelola domain EDM)
2. ITIL V3 2011 dan ISO/EIC 20000 (masuk ke dalam area manajemen domain APO, BAI dan DSS)
3. ISO/IEC 27000 series (masuk ke dalam area manajemen domain APO dan DSS khusus proses yang berhubungan dengan keamanan dan manajemen risiko, serta domain MEA khusus aktivitas mengawasi dan mengevaluasi)
4. ISO/IEC 31000 series (masuk ke dalam area tata kelola domain EDM dan area manajemen APO khusus proses yang berhubungan dengan manajemen risiko)
5. PRINCE2 (masuk ke dalam area manajemen domain APO khusus proses yang berhubungan dengan portofolio dan domain BAI khusus proses yang berhubungan dengan manajemen proyek dan program).

Selain itu COBIT juga telah digunakan secara luas oleh professional IT karena menyediakan panduan dan konsep internal yang konsisten untuk penilaian IT. Keunggulan lainnya COBIT 2019 ini merupakan penyempurnaan dari COBIT 5 dengan menambahkan beberapa item dan pendekatan yang disesuaikan dengan kondisi perkembangan teknologi informasi saat ini. COBIT 2019 dibangun berdasarkan 2 set prinsip, yaitu prinsip di dalam sistem tata kelola dan prinsip *framework* tata kelola. Prinsip *framework* tata kelola memiliki 6 prinsip dasar yaitu memenuhi kebutuhan pemangku kepentingan, mendukung perusahaan dari ujung ke ujung, menerapkan kerangka kerja yang terintegrasi, mengaktifkan pendekatan holistic, memisahkan tata kelola dari manajemen dan yang terkini adalah sistem tata kelola yang dinamis (ISACA, 2019).

1.2. Rumusan Masalah

Rumusan masalah ini dapat digunakan sebagai tolok ukur penelitian dapat dikatakan berhasil dan selesai atau belum. Untuk itu Rumusan Masalah sangat penting. Setelah melihat identifikasi permasalahan di atas maka dapat dibuat rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Berapakah tingkat kapabilitas tata kelola teknologi informasi Lembaga Pemerintah Bidang Pelayanan Metrologi yang telah terakreditasi ISO 17025 saat ini (as is) menggunakan COBIT 2019?;
2. Apa rekomendasi yang diusulkan berdasarkan hasil audit COBIT 2019 sebagai solusi permasalahan tata kelola teknologi informasi Lembaga Pemerintah Bidang Pelayanan Metrologi?

1.3. Batasan Masalah

Untuk lebih memfokuskan penelitian dan menyederhanakan permasalahan agar dapat diselesaikan dengan pendekatan metode ilmiah, peneliti menentukan ruang lingkup penelitian. Batasan yang digunakan dalam penelitian tugas akhir ini adalah sebagai berikut :

1. Kegiatan penelitian ini hanya dilakukan pada Lembaga pemerintah bidang pelayanan metrologi khususnya BSML Regional II;
2. Responden yang diambil adalah pegawai BSML Regional II yang sesuai dengan panduan cobit 2019;
3. *Framework* audit tata kelola yang digunakan adalah *framework* cobit 2019.

Adapun asumsi yang digunakan pada penelitian ini adalah :

1. Para responden mempunyai kemampuan yang tinggi dalam menentukan dan memberikan penilaian terhadap setiap variabel dalam penentuan kriteria;
2. Para *decision maker* mempunyai kemampuan yang tinggi dalam menentukan nilai/tingkat kepentingan dan ketergantungan kriteria yang ada sehingga tidak perlu diragukan lagi kekonsistensian jawaban dari *decision maker*.

1.4. Tujuan Penelitian

Tujuan Penelitian adalah sebagai berikut:

1. Membuat sebuah perencanaan audit tata kelola tekologi informasi yang ada di Lembaga pemerintah bidang pelayanan metrologi dalam hal ini BSML Regional II menggunakan COBIT 2019;
2. Memperoleh tingkat kapabilitas tata kelola TI saat ini dan yang di harapkan di Lembaga pemerintah bidang pelayanan metrologi menggunakan COBIT 2019;
3. Menyusun rekomendasi sebagai solusi permasalahan tata kelola teknologi informasi yang akan digunakan untuk percepatan implementasi SPBE.

1.5. Manfaat Penelitian

Hasil dari penelitian ini diharapkan akan memberikan manfaat terhadap pengembangan tata kelola teknologi informasi yang berada di BSML Regional II antara lain:

1. Dapat menyelaraskan antara kebutuhan dan tujuan Lembaga pemerintah bidang pelayanan metrologi dari sisi TI;
2. Pengetahuan baru tentang audit tata kelola teknologi informasi menggunakan COBIT 2019;
3. Sebagai kajian perencanaan pada program percepatan implementasi SPBE di lingkungan Lembaga pemerintah bidang pelayanan metrologi.

1.6. Hipotesis

Berdasarkan perumusan masalah yang telah diungkap, maka kesimpulan sementara (hipotesa) yang dapat ditarik adalah dengan menggunakan framework COBIT 2019, maka akan dihasilkan hasil audit pada BSML Regional II. Rincian hipotesa yang mungkin terjadi pada penelitian ini adalah tingkat kapabilitas tata kelola teknologi informasi pada BSML Regional II berdasarkan domain yang terpilih dan rekomendasi bagi percepatan implementasi SPBE pada Lembaga pemerintah bidang pelayanan metrologi pada umumnya.

BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Berdasarkan penjelasan yang telah diutarakan sebelumnya, penelitian ini merupakan penelitian yang membahas mengenai audit tata kelola TI pada Lembaga pemerintah bidang pelayanan metrologi khususnya BSML Regional II Kementerian Perdagangan. Output yang ingin dihasilkan dari penelitian ini berupa penjelasan mengenai tingkat kapabilitas pengelolaan TI saat ini dan yang diharapkan serta pemberian rekomendasi akan diberikan kepada stakeholder BSML Regional II dan sebagai tolok ukur bagi Lembaga pemerintah bidang pelayanan metrologi guna percepatan implementasi SPBE. Adapun penyelesaian penelitian ini tidak terlepas dari penelitian yang telah dilakukan sebelumnya yang relevan, yang berfungsi sebagai bahan kajian dalam penyelesaian permasalahan yang ada.

Penelitian pertama judulnya adalah Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 (Miranti, 2019). Tujuan utama penelitian ini adalah untuk mengetahui kondisi tata kelola teknologi informasi PT. Praweda Ciptakarsa Informastika. Penulis mengatakan bahwa tata kelola teknologi informasi adalah bagian dari suatu perusahaan yang melibatkan pemangku kepentingan perusahaan untuk memastikan kelanjutan strategi organisasi dan teknologi informasi. Dalam penelitian ini menggunakan framework COBIT5 dengan tahapan Assesment Process Activities. Hasilnya berupa nilai kapabiltias beberapa domain yang terpilih dan memberikan rekomendasi bagi perusahaan.

Penelitian yang kedua adalah Audit Sistem Informasi pada Sistem Admisi UIN Sunan Kalijaga Yogyakarta menggunakan framework COBIT4.1 (Taslihudin, 2016). Penelitian ini berfokus pada domain Monitor and Evaluate (ME) dengan framework COBIT 4.1. Salah yang dihasilkan bahwa evaluasi ini dapat mendeteksi secara dini permasalah yang terjadi sebelum terlambat.

Pada penelitian ketiga dengan judul Audit Sistem Informasi Akademik menggunakanan COBIT 5 di Universitas Jenderal Achmad Yani (Ekowansyah dkk, 2017) mengatakan bahwa proses TI yang baik akan menghasilkan kegiatan operasional yang baik pula.

Penelitian selanjutnya dengan judul Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Domain DSS Studi Kasus : PT. PLN (Persero) Kantor Pusat (Baharuddin dkk, 2019). Domain yang dipilih adalah Deliver, Service, Support (DSS). Peneliti berkesimpulan penggunaan COBIT 5 untuk mengevaluasi tata kelola teknologi informasi di suatu perusahaan dapat memberikan rekomendasi bagi perusahaan sehingga dapat mencapai level yang diinginkan.

Penelitian pada jurnal internasional dengan judul Adopted COBIT-5 Framework for System Design of Indonesia Navy IS/IT : An Evaluation (Putra, 2017) digunakan metode maturity level untuk menilai pada masing-masing domain dengan framework COBIT 5.Sedangkan penelitian dengan judul Audit Tata Kelola Teknologi Informasi pada PT.Pelabuhan Indonesia III (Persero) menggunakan kerangka kerja COBIT 5 (Heppy,2017). Penelitian ini menggunakan seluruh domain yang ada di framework COBIT5 yaitu sebanyak 37. Penelitian ini bertujuan

untuk memperoleh ukuran kapabilitas proses TI saat ini dan yang akan diharapkan serta penyusunan rekomendasi guna menyelarasan tata kelola TI dengan strategi bisnis perusahaan.

Dan sebagai bentuk penyempurnaan dari COBIT 5, dalam penelitian berjudul Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4 (Nachrowi dkk, 2020) mengatakan bahwa penelitian terhadap COBIT 5 yang bertujuan untuk memperbaiki *goal cascading* telah dilakukan, dimana COBIT 2019 telah mengimplementasikan faktor desain dalam proses *goal cascading* sehingga akan menyempurnakan desain sistem tata kelola suatu perusahaan berdasarkan penggunaan IT di perusahaan tersebut.

2.2. Keaslian Penelitian

Tabel 2.1. Matriks literatur review dan posisi penelitian

Audit Tata Kelola Teknologi Informasi Lembaga Pemerintah Bidang Pelayanan Metrologi menggunakan COBIT 2019

(Studi Kasus: BSML Regional II Kementerian Perdagangan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	Evaluasi Tata Kelola Teknologi Informasi Menggunakan *Framework* COBIT 5 (Studi Kasus: PT.Praweda Ciptakarsa Informatika)	Alfia Miranti, UIN Syarif Hidayatullah, 2019.	• Mengetahui capability level • Mengetahui gap kondisi saat ini • Memberikan rekomendasi	Ada 3 domain yang terpilih yaitu EDM 04, APO01, APO04 dengan masing-masing nilai kapabilitas dan juga diberikan rekomendasi kepada Perusahaan yang diaudit terhadap temuan yang dihasilkan	Penelitian lebih lanjut diharapkan untuk menggunakan domain atau fokus area yang berbeda sehingga didapatkan pemotretan kondisi tata kelola TI lebih jelas	Penggunaan framework COBIT 2019 memberikan pendekatan baru terutama penetapan domain yang akan dijadikan sebagai audit, selain itu pemilihan domain yang akan menjadi fokus area audit berbeda. Rekomendasi digunakan sebagai perencanaan implementasi SPBE secara umum.
2	Audit Sistem Informasi pada Sistem Admisi UIN Sunan Kalijaga Yogyakarta menggunakan *Framework* COBIT 4.1	A.B.Tashlihudin, UIN Sunan Kalijaga Yogyakarta, 2016.	• Membuat perencanaan audit dengan hasil wawancara • Melakukan audit dengan domain ME • Memberikan rekomendasi	Dihasilkan template wawancara audit berdasarkan framework COBIT 4.1, hasil audit dikemukakan berdasarkan domain ME, dan auditiy masih dibawah standar	Domain yang menjadi fokus area audit dipilih ME- *Monitor and Evaluate*(masih menggunakan framework COBIT 4.1) yang berbeda dengan COBIT 5 yang disempurnakan dengan COBIT 2019	Domain yang menjadi fokus area audit pada penelitian ini berbeda, menggunakan framework COBIT 2019 pada penelitian ini didapatkan 5 domain yang akan menjadi fokus area audit yaitu EDM 03, APO 12, DSS 02, DSS 04, DSS 05.

Tabel 2.1. Matriks literatur review dan posisi penelitian (lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
3	Audit Sistem Informasi Akademik Menggunakan COBIT 5 di Universitas Jenderal Achmad Yani,	Erdis Ekowansyah, Yulison H Chrisnanto, Puspita, Nurul Sabrina, Prosiding Seminar Nasional Komputer dan Informatika (SENASKI) 2017	mengukur dan mengetahui tingkat kematangan teknologi informasi akademik yang diterapkan Unjani berdasarkan data yang diperoleh dari sampel lingkungan kampus Unjani.	Berdasarkan penelitian yang telah dilakukan mengenai tingkat kematangan teknologi yang telah diterapkan Unjani, secara keseluruhan unjani berada pada level 3 atau Established	Penelitian ini fokus pada domain APO, EDM dan BAI. Responden yang dijadikan auditee adalah pengguna sistem informasi. Proses audit dilakukan dengan menyebarkan kuesioner tanpa tindak lanjut pengecekkan dokumen	Penggunaan COBIT 2019 sebagai penyempurnaan COBIT 5. Pemilihan responden berdasarkan RACI chart, dan proses audit yang akan dilakukan peneliti melibatkan pengecekkan dokumen. Selain itu objek yang akan diaudit berbeda.
4	Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Domain DSS (Deliver, Service, Support) (Studi Kasus : PT. PLN (Persero) Kantor Pusat)	A.F.Baharuddin,Suprapto, A.R.Perdanakusuma, Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Vol. 3, No. 9, September 2019	Untuk mengetahui capability level dan gap pada tata kelola teknologi informasi PT. PLN (Persero) Kantor Pusat pada domain DSS	Didapatkan hasil capability level dan gap pada domain DSS01, DSS02, DSS03, DSS04, DSS05, DSS06	Domain yang menjadi fokus area audit yaitu Domain DSS, Penulis berpendapat bahwa domain ini yang relevan dan diperlukan pada perusahaan yang di audit. Pemilihan domain perlu diperkuat dengan statemen atau penelusuran menggunakan framework yang digunakan dalam hal ini COBIT 5	Penggunaan framework COBIT 2019 memiliki penyempurnaan pada masing-masing komponen sistem tata kelola. Penentuan domain yang akan menjadi fokus area menggunakan framework COBIT 2019 dan pada penelitian ini didapatkan 5 domain yang akan menjadi fokus area audit yaitu EDM 03, APO 12, DSS 02, DSS 04, DSS 05

Tabel 2.1. Matriks literatur review dan posisi penelitian (lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
5	Adopted COBIT-5 Framework for System Design of Indonesia Navy IS/IT : An Evaluation	I Nengah Putra, Abdul Hakim, Sholeh H Pramono, Herman Tolle, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17, 2017	Untuk mengetahui level tata kelola TI pada TNI AL menggunakan COBIT 5	Penelitian ini menghasilkan nilai level pada domain APO, EDM, BAI, DSS. Framework COBIT 5 dapat digunakan untuk evaluasi tata kelola TI yang ada	Penelitian ini fokus pada bagaimana mengkomunikasikan framework COBIT5 untuk dapat digunakan sebagai panduan dalam tata kelola TI, sehingga diperlukan responden yang tepat	Pelaksanaan audit melibatkan pengguna dan pelaku TI pada perusahaan tersebut, pada COBIT 2019 ditentukan responden yang memang perlu dijadikan sebagai audity menggunakan RACI Chart. Pada penelitian ini didapatkan 6 responden yang akan menjadi audity.
6	Audit Tata Kelola Teknologi Informasi pada PT. Pelabuhan Indonesia III (Persero) dengan Kerangka Kerja Cobit 5	Heppy Oktianatasari, Institut Teknologi Sepuluh Nopember, Surabaya, 2017	Menyusun rekomendasi guna menyelaraskan pengelolaan proses TI dengan strategi bisnis perusahaan.	Penelitian ini tidak mengkhususkan domain yang akan menjadi fokus area audit tata kelola TI. Hasilnya berupa level pada masing-masing domain dan dilakukan pemberian rekomendasi	Penelitian selanjutnya diharapkan berkomunikasi dengan audity untuk lebih fokus dalam penentuan domain yang menjadi fokus area tata kelola TI sehingga didapatkan hasil audit yang tepat guna	Penelitian yang akan dilakukan menggunakan framework COBIT 2019, pada perencanaan audit diakukan identifikasi identitas dan kebijakan perusahaan sehingga didapatkan domain yaitu EDM 03, APO 12, DSS 02, DSS 04, DSS 05. Objek organisasi yang akan diaudit berbeda.

Tabel 2.1. Matriks literatur review dan posisi penelitian (lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
7	COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities	Steven De Haes, Wim Van Grembergen, Roger S. Debreceny, Journal of Information systems volume 27 No.1, Spring 2013	Untuk mengetahui peranan framework COBIT 5 dalam bidang tata kelola bisnis dan peluang penelitian di bidang tata kelola teknologi informasi	COBIT merupakan framework yang lengkap dan handal dalam penangan tata kelola teknologi informasi	Bagaimana membuat COBIT menjadi sebuah artefak atau standar yang akan menjadi kebertrimaan bagi seluruh pengguna atau stakeholder di dunia	Pemilihan audit menggunakan COBIT dengan versi terbaru yaitu COBIT 2019 diharapkan menjadi metode tempuh yang tepat guna
8	Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4	Erika Nachrowi, Yani Nurhadryani, Heru Sukoco, Resti Journal Vol. 4 No. 4 (2020) hal. 764 - 774	Merencanakan kegiatan evaluasi tata kelola dan manajemen TI menggunakan COBIT 2019 dan ITIL 4	Penyusunan rekomendasi atas hasil kegiatan audit kepada objek audit	Penyempurnaan COBIT 5 yaitu COBIT 2019 memberikan desain tata kelola yang lebih tepat dan disesuaikan dengan karakteristik objek audit	Penelitian ini mengaudit sebuah objek secara garis besar dan objek yang di audit berbeda. Pada penelitian yang akan dilakukan fokus pada lembaga pemerintah bidang pelayanan metrologi

2.3. Landasan Teori

2.3.1. Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi merupakan bagian dari pengelolaan suatu organisasi atau perusahaan secara keseluruhan yang terdiri dari kepemimpinan dan struktur organisasi serta proses yang ada guna untuk memastikan kelanjutan teknologi informasi organisasi dan pengembangan strategi serta tujuan organisasi. Definisi lain tata kelola teknologi informasi yaitu sesuatu yang mencakup sistem informasi, teknologi dan komunikasi, bisnis, hukum maupun isu-isu lain yang melibatkan hampir seluruh pemangku kepentingan (*stakeholder*), baik direktur, manajemen eksekutif, pemilik proses, suplier, pengguna TI bahkan pengaudit SI/TI (Miranti, 2019).

Berdasarkan definisi-definisi diatas, maka tata kelola teknologi informasi adalah bagian dari sutu perusahaan yang melibatkan pemangku kepentingan untuk memastikan kelanjutan strategi organisasi dam teknologi informasi.

Tujuan tata kelola teknologi informasi adalah mengontrol penggunaannya dalam memastikan bahwa kinerja TI memenuhi dan sesuai dengan tujuan sebagai berikut (Surendro, 2009):

1. Menyelaraskan teknologi informasi dengan strategi organisasi serta realisasi dari keuntungan-keuntungan yang telah dijanjikan dari penerapan TI;
2. Penggunaan teknologi informasi memungkinkan organisasi mengambil peluang-peluang yang ada, serta memaksimalkan pemanfaatan TI dalam memaksimalkan keuntungan dari penerapan TI tersebut;
3. Bertanggung jawab terhadap penggunaan sumber daya TI;

4. Manajemen risiko-risiko yang ada terkait teknologi informasi secara tepat.

2.3.2. Audit Tata Kelola Teknologi Informasi

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 (Heppy, 2017)

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.

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 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 Efektifitas sistem informasi perusahaan informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan pengguna;
4. Meningkatkan efisiensi sistem. Efsiensi menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai.

2.3.2.1. 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 risiko yang dapat muncul yang diakibatkan dari pengimpelementasian TI di perusahaan

menjadikan audit semakin penting untuk dilakukan. Terdapat beberapa alasan penting mengapa audit TI perlu dilakukan antara lain (Heppy, 2017):

1. Kerugian akibat kehilangan data

   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. Risiko yang ditimbulkan jika saja dokter salah melakukan penginputan data pasien ke dalam sistem TI yang tentu dapat membahayakan nyawa dari pasien tersebut;

3. Risiko kebocoran data

   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. Risiko 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

   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 risiko. Risiko 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. COBIT 2019

COBIT (*Contol Objective for Information and related Technology*) adalah suatu panduan standar praktik manajemen teknologi informasi. Standar COBIT dikeluarkan oleh IT Governance Institute yang merupakan bagian dari ISACA (ISACA, 2019). Versi terbaru dari COBIT adalah COBIT 2019. Maksud utama COBIT ialah menyediakan kebijakan yang jelas dan *good practice* untuk IT *governance*, membantu manajemen senior dalam memahami dan mengelola risiko-risiko yang berhubungan dengan IT. ISACA (*Information Systems Audit and Control Association*) sendiri adalah suatu organisasi profesi internasional di bidang tata kelola teknologi informasi yang didirikan di Amerika Serikat pada tahun 1967.

2.3.3.1. Pendahuluan

COBIT adalah kerangka kerja untuk tata kelola dan pengelolaan informasi dan teknologi perusahaan bersifat menyeluruh. Dengan kata lain, I&T perusahaan tidak terbatas pada departemen TI suatu organisasi, tetapi tentu saja seluruh organisasi. Kerangka COBIT membuat perbedaan yang jelas antara tata kelola dan manajemen. Kedua disiplin ilmu ini mencakup aktivitas yang berbeda, memerlukan struktur organisasi yang berbeda, dan melayani tujuan yang berbeda. Tata kelola memastikan bahwa: Kebutuhan, kondisi dan pilihan pemangku kepentingan dievaluasi untuk menentukan tujuan usaha yang disepakati dan seimbang . Arahan

ditetapkan melalui pembuatan prioritas dan pengambilan keputusan. Kinerja dan kepatuhan dipantau berdasarkan arah dan tujuan yang disepakati . Di kebanyakan perusahaan, tata kelola secara keseluruhan adalah tanggung jawab dewan direksi, di bawah kepemimpinan ketua. Tanggung jawab tata kelola khusus dapat didelegasikan ke struktur organisasi khusus pada tingkat yang sesuai, terutama di perusahaan yang lebih besar dan kompleks. Manajemen merencanakan, membangun, menjalankan dan memantau kegiatan, sejalan dengan arahan yang ditetapkan oleh badan tata kelola, untuk mencapai tujuan perusahaan. Di kebanyakan perusahaan, manajemen adalah tanggung jawab manajemen eksekutif, di bawah kepemimpinan *chief executive officer* (CEO). COBIT mendefinisikan komponen untuk membangun dan mempertahankan sistem tata kelola: proses, struktur organisasi, kebijakan dan prosedur, arus informasi, budaya dan perilaku, keterampilan, dan infrastruktur. Keuntungan tata kelola TI, yaitu disebutkan ada 3:

1. Realisasi Benefit

   Menciptakan peluang, nilai tambah bagi dunia bisnis melalui optimalisasi IT, termasuk mengeliminasi pengembangan IT yang tidak berguna;

2. Optimasi Risiko

   Integrasi proses bisnis dengan proses tata kelola IT dapat meminimalisir risiko yang akan terjadi pada bisnis. Manajemen dapat mengandalkan tata kelola IT yang sejalan dengan arah dan tujuan bisnis;

3. Optimasi Sumber Daya

   Hal ini menyakinkan bahwa tata kelola yang baik dan menjadi bagian dari rencana strategi perusahaan akan dapat menguntungkan proses bisnis. Dan

seperti diketahui bahwa teknologi IT saat ini menjadi hal yang penting dan keharusan bagi sebuah perusahaan.

Keunggulan COBIT 2019 dengan versi sebelumnya, antara lain:

1. Fleksibilitas dan keterbukaan

   Definisi dan penggunaan faktor desain memungkinkan COBIT disesuaikan untuk penyelarasan yang lebih baik dengan konteks khusus pengguna. Arsitektur terbuka COBIT memungkinkan penambahan area fokus baru atau memodifikasi yang sudah ada, tanpa implikasi langsung untuk struktur dan konten model inti COBIT;

2. Ketebaruan dan relevansi

   Model COBIT ini mendukung referensi dan penyelarasan konsep yang berasal dari sumber lain (misalnya, standar TI terbaru dan peraturan kepatuhan);

3. Preskriptif aplikasi

   Models seperti COBIT dapat deskriptif dan preskriptif. Model konseptual COBIT dibangun dan disajikan sedemikian rupa sehingga instansinya (yaitu, penerapan komponen tata kelola COBIT yang disesuaikan) dianggap sebagai resep untuk sistem tata kelola TI yang disesuaikan;

4. Manajemen Kinerja IT

   Struktur model manajemen kinerja COBIT diintegrasikan ke dalam model konseptual.

2.3.2.2. Metodologi dan Pedoman Desain

Target/ Responden dari COBIT 2019

Target audiens untuk COBIT adalah pemangku kepentingan untuk EGIT (*Enterpirse Governance* IT) dan, selanjutnya pemangku kepentingan untuk tata kelola perusahaan. Para pemangku kepentingan ini dan manfaat yang dapat mereka peroleh dari COBIT ditunjukkan pada tabel 2.2. dibawah ini. Jika di COBIT 5 dijelaskan lebih detail terkait jabatan apa saja yang sebaiknya menjadi audity dalam kegiatan audit tata kelola TI ini. Harapannya kegiatan audit tata kelola pada perusahaan akan dapat menghasilkan output dan rekomendasi yang tepat.

Tabel 2.2. Target responden audit menggunakan COBIT 2019

Stakeholder	*Benefit*
	Internal Stakeholder
Boards	*Provides insight on how to get value from the use of I&T and explains relevant board responsibilities*
Executive Management	*Provides guidance on how to organize and monitor performance of I&T across the enterprise*
Business Managers	*Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for new strategic opportunities*
IT Managers	*Provides guidance on how best to build and structure the IT departement, manage performance of IT run an efficient and effective IT operation, control IT cost, align IT strategy to business priorities, etc*
Assurance Providers	*Helps to manage dependency on external service providers, get assurance over IT, and ensure the exitence of an affective and efficient system of internal controls*
Risk Management	*Helps to ensure the identification and management of all IT-related risk*
	External Stakeholders
Regulators	*Helps to ensure the enterprise is compliant with applicable rules and regulations and has the right governance system in place to manage and sustain compliance*
Business Partners	*Helps to ensure that a business partner's opertaions are secure, reliable and compliant with applicable rules and regulations*
IT vendors	*Helps to ensure that and IT vendor's operations are secure, reliable and compliant with applicable rules and regulations*

Prinsip COBIT 2019

COBIT 2019 dikembangkan berdasarkan dua set prinsip:

1. Prinsip yang menjelaskan persyaratan inti dari sistem tata kelola untuk informasi dan teknologi perusahaan;
2. Prinsip kerangka tata kelola yang dapat digunakan untuk membangun sistem tata kelola untuk perusahaan.

Adapun 6 (enam) prinsip untuk sistem tata kelola yaitu:

1. Setiap perusahaan membutuhkan sistem tata kelola untuk memenuhi kebutuhan pemangku kepentingan dan untuk menghasilkan nilai dari penggunaan I&T. Nilai mencerminkan keseimbangan antara manfaat, risiko, dan sumber daya, dan perusahaan membutuhkan strategi dan sistem tata kelola yang dapat ditindaklanjuti untuk mewujudkan nilai ini;
2. Sistem tata kelola untuk I&T perusahaan dibangun dari sejumlah komponen yang dapat dari berbagai jenis dan yang bekerja bersama secara holistik;
3. Sistem tata kelola harus dinamis. Ini berarti bahwa setiap kali satu atau lebih faktor desain diubah, dampak dari perubahan ini pada sistem EGIT harus dipertimbangkan. Pandangan dinamis tentang EGIT akan mengarah pada sistem EGIT yang layak dan tahan di masa depan;
4. Sistem tata kelola harus dengan jelas membedakan antara tata kelola dan aktivitas dan struktur manajemen;
5. Sistem tata kelola harus disesuaikan dengan kebutuhan perusahaan, menggunakan seperangkat faktor desain sebagai parameter untuk menyesuaikan dan memprioritaskan komponen sistem tata kelola;

6. Sistem tata kelola harus mencakup perusahaan dari ujung ke ujung, dengan fokus tidak hanya pada fungsi TI tetapi juga pada semua teknologi dan pemrosesan informasi yang dilakukan perusahaan untuk mencapai tujuannya, terlepas dari di mana pemrosesan tersebut dilakukan di perusahaan.

Sedangkan 3 (tiga) prinsip kerangka tata kelola adalah:

1. Kerangka tata kelola harus didasarkan pada model konseptual, mengidentifikasi komponen utama dan hubungan antar komponen, untuk memaksimalkan konsistensi dan memungkinkan otomatisasi;
2. Kerangka tata kelola harus terbuka dan fleksibel. Ini harus memungkinkan penambahan konten baru dan kemampuan untuk mengatasi masalah baru dengan cara yang paling fleksibel, sambil menjaga integritas dan konsistensi;
3. Kerangka tata kelola harus selaras dengan standar, kerangka kerja, dan peraturan utama yang relevan.

Agar informasi dan teknologi dapat berkontribusi pada tujuan perusahaan, sejumlah tujuan tata kelola dan manajemen harus dicapai. Tujuan tata kelola dan manajemen di COBIT dikelompokkan menjadi lima domain. Domain memiliki nama dengan kata kerja yang mengungkapkan tujuan utama dan area aktivitas dari tujuan yang terkandung di dalamnya, secara lengkap digambarkan pada gambar 2.1. Adapun pengelompokkannya sebagai berikut:

1. Tujuan tata kelola dikelompokkan dalam domain *Evaluate, Direct and Monitor* (EDM). Dalam domain ini, badan pengatur mengevaluasi pilihan strategis, mengarahkan manajemen senior pada pilihan strategis yang dipilih dan memantau pencapaian strategi.

2. Tujuan manajemen dikelompokkan dalam empat domain:

   i. *Align, Plan, and Organize* (APO) membahas keseluruhan organisasi, strategi dan kegiatan pendukung untuk I&T;

   ii. *Build, Acquire and Implement* (BAI) menangani definisi, akuisisi, dan implementasi solusi I&T dan integrasi mereka dalam proses bisnis;

   iii. *Delivery, Services and Support* (DSS) membahas pengiriman operasional dan dukungan layanan I&T, termasuk keamanan;

   iv. *Monitor, Evaluate and Assess* (MEA) membahas pemantauan kinerja dan kesesuaian I&T dengan target kinerja internal, sasaran pengendalian internal, dan persyaratan eksternal

Gambar 2.1. Domain pada COBIT 2019

Untuk memenuhi tujuan tata kelola dan manajemen, setiap perusahaan perlu menetapkan, menyesuaikan, dan mempertahankan sistem tata kelola yang dibangun dari sejumlah komponen seperti terlihat pada gambar 2.2., yaitu:

1. Proses menggambarkan serangkaian praktik dan aktivitas yang terorganisir untuk mencapai tujuan tertentu dan menghasilkan satu set output yang mendukung pencapaian tujuan terkait TI secara keseluruhan;
2. Struktur organisasi adalah entitas pembuat keputusan utama dalam suatu perusahaan;
3. Prinsip, kebijakan dan kerangka kerja menerjemahkan perilaku yang diinginkan menjadi pedoman praktis untuk pengelolaan sehari-hari;
4. Informasi tersebar luas di seluruh organisasi dan mencakup semua informasi yang dihasilkan dan digunakan oleh perusahaan. COBIT berfokus pada informasi yang diperlukan untuk berfungsinya sistem tata kelola perusahaan secara efektif;
5. Budaya, etika dan perilaku individu dan perusahaan sering dianggap remeh sebagai faktor dalam keberhasilan kegiatan tata kelola dan manajemen;
6. Orang, keterampilan dan kompetensi dibutuhkan untuk keputusan yang baik, pelaksanaan tindakan korektif dan penyelesaian semua kegiatan dengan sukses;
7. Layanan, infrastruktur, dan aplikasi mencakup infrastruktur, teknologi, dan aplikasi yang menyediakan sistem tata kelola untuk pemrosesan I&T bagi perusahaan.

Gambar 2.2. Komponen COBIT 2019 dalam setiap sistem tata kelola

Area Fokus

Area fokus menjelaskan topik, domain, atau masalah tata kelola tertentu yang dapat ditangani oleh kumpulan tujuan 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.

Faktor Desain

Faktor desain adalah faktor yang dapat mempengaruhi desain sistem tata kelola perusahaan dan memposisikannya untuk sukses dalam penggunaan I&T. Pada COBIT 2019, faktor inilah yang akan mempengaruhi pemilihan domain dalam rangka audit maupun perancangan sistem tata kelola teknologi informasi seperti terlihat pada gambar 2.3.

Gambar 2.3. Faktor desain COBIT 2019

COBIT 2019 melakukan pembaharuan dalam proses penentuan domain yang akan menjadi area audit. Dengan desain faktor ini, setiap kasus akan menjadi lebih detail dan tepat karena disesuaikan dengan kondisi dan parameter perusahaan yang di audit. Adapun faktor desain pada COBIT 2019 dijelaskan sebagai berikut:

1. Strategi Bisnis, dapat memiliki strategi yang berbeda, yang dapat dinyatakan sebagai salah satu atau lebih dari tipe, dijelaskan pada tabel 2.3. sebagai berikut

Tabel 2.3. Jenis strategi bisnis dalam faktor desain

Strategy Archetype	*Explanation*
Growth/ Acquisition	*The enterprise has 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*

2. Sasaran perusahaan, yang mendukung strategi perusahaan. Strategi perusahaan diwujudkan dengan pencapaian (sekumpulan) tujuan perusahaan. Sasaran-sasaran ini didefinisikan dalam kerangka COBIT, yang disusun sepanjang dimensi *Balanced Scorecard* terlihat pada tabel 2.4.

Tabel 2.4. Sasaran perusahaan dalam faktor desain

Reference	*Balance Scorecard (BSC) Dimension*	*Enterprise Goal*
EG01	*Financial*	*Portofolio of competitive products and services*
EG02	*Financial*	*Managed business risk*
EG03	*Financial*	*Compliance with external law 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 functionally*
EG09	*Internal*	*Optimization of business process costs*
EG10	*Internal*	*Staff skills, motivation and productivity*
EG11	*Internal*	*Compliance with internal policies*
EG12	*Growth*	*Managed digital tranformation programs*
EG13	*Growth*	*Product and business innovation*

3. Profil risiko perusahaan dan isu-isu terkini terkait dengan I & T. Profil risiko mengidentifikasi jenis risiko terkait I & T yang saat ini dihadapi oleh perusahaan dan menunjukkan area risiko mana yang melebihi selera risiko, dijelaskan pada tabel 2.5 di bawah ini;

Tabel 2.5. *Risk category* dalam faktor desain

Reference	*Risk Category*
1	*IT investment decision making, portofolio 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	*Enviromental*
19	*Data dan information management*

4. Masalah terkait I & T. Metode terkait untuk penilaian risiko I&T bagi perusahaan adalah dengan mempertimbangkan masalah terkait I & T mana yang saat ini dihadapi, atau, dengan kata lain, risiko terkait I & T yang telah terwujud. Selengkapnya dijelaskan pada tabel 2.6;

Tabel 2.6. Masalah terkait I&T dalam faktor desain

Reference	*Description*
A	*Frustation between different IT entities across the organization because of a perception of low contribution to business value*
B	*Frustation between business departements (i.e.,the IT customer) and the IT departement 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 IT outsourcer (s)*
E	*Failure to meet IT-related regulatory or contractual requirements*
F	*Regular audit findings or other assessment reports about poor IT performance or reported*
G	*Substantial hidden and rogue IT spending, that is, IT spending by user departements outside the control of the normal IT investment decision mechanism 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 commited 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/ora technology specialist 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*
S	*Ignorance of and/or noncompliance with privacy regulations*
T	*Inability to exploit new technologies or innovate using I&T*

5. Tantangan. Tantangan dalam IT yang akan dihadapi oleh perusahan. Adapun jenis tantangan dijelaskan pada tabel 2.7;

Tabel 2.7. Tantangan dalam faktor desain

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

6. Kepatuhan peraturan. Yang dimaksud disini adalah tingkat kepatuhan perusahaan terhadap peraturan yang ada (terutama peraturan pemerintah) dijelaskan pada tabel 2.8;

Tabel 2.8. Kepatuhan peraturan dalam faktor desain

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*

7. Peran IT. Seberapa besar peran IT didalam perusahaan akan mempengaruhi faktor desain dijelaskan pada tabel 2.9;

Tabel 2.9. Peran IT dalam faktor desain

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 runnng and continuity of the business processes and services. However, IT is not seen as a driver for innovating business process 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*

8. *Source Model* IT. Sumber penyediaan IT mempengaruhi akan mempengaruhi desain faktor seperti terlihat pada tabel 2.10;

Tabel 2.10. *Source model* IT dalam faktor desain

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 mix model is applied, combining the other three models in varying degrees*

9. Metode Implementasi IT. Dalam pengembangan dan implementasi IT dalam sistem perusahaan ada beberapa metode seperti terlihat pada tabel 2.11, hal ini juga berpengaruh pada faktor desain;

Tabel 2.11. Model implementasi IT dalam faktor desain

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

10. Strategi dalam mengadopsi teknologi. Kebijakan perusahan dalam penanganan terhadap pembaruan teknologi dijelaskan pada tabel 2.12;

Tabel 2.12. Strategi adopsi teknologi dalam faktor desain

Technology Adoption Strategy	*Explanation*
First mover	*The enterprises generally adopts new technologies as early as possible and tries to gain first-mover advantage*
Follower	*The enterprises 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*

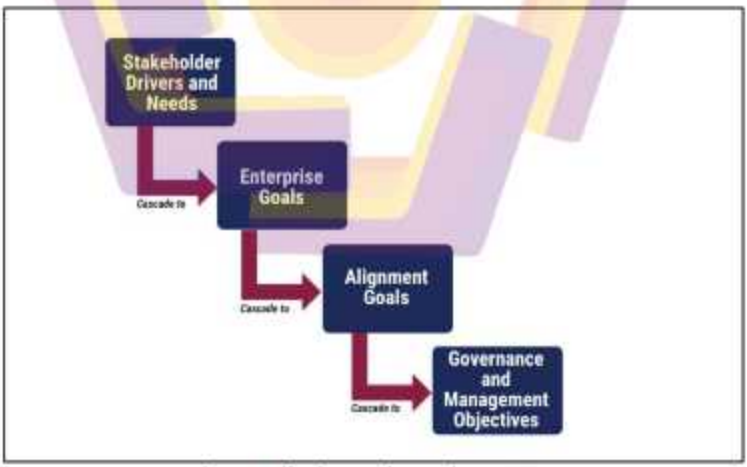
11. Size bisnis/perusahaan. Dan yang terakhir adalah size dari perusahaan, dilihat dari jumlah pekerja/ pegawai tetap yang dipekerjakan dijelaskan pada tabel 2.13;

Tabel 2.13. Size perusahaan dalam faktor desain

Enterprise Size	*Explanation*
Large enterprise (default)	*Enterprise with more than 250 full-time employees*
Small enterprise	*Enterprise with 50 to 250 full-time employees*

Goal Cascade/ pendetailan target

Saat membuat desain tata kelola maka hal yang harus dilakukan adalah mendetailkan target pada masing-masing level. Kebutuhan *stakeholder* diturunkan menjadi target perusahaan, lalu diturunkan menjadi *Alignment goals*, terakhir menjadi *governance and managemen objectives* seperti terlihat pada gambar 2.4. di bawah ini.



Gambar 2.4. *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 perusahaan. Berikut penjelasannya pada tabel 2.14.

Tabel 2.14. *Enterprise goals* dalam COBIT 2019

References	*BSC Dimension*	*Enterprise Goal*	*Example Metrics*
EG01	Keuangan	Portofolio kompetitif produk dan layanan	1. Persentase produk dan layanan yang memenuhi atau melampaui produk dan layanan target pendapatan dan / atau pangsa pasar 2. Persentase produk dan layanan yang memenuhi atau melampaui target kepuasan pelanggan 3. Persentase produk dan layanan yang memberikan daya saing keunungan 4. Waktu untuk memasarkan produk dan layanan
EG02	Keuangan	Risiko bisnis yang dikelola	1. Persen dari tujuan dan layanan bisnis penting dicakup oleh penilaian risiko 2. Rasio insiden signifikan yang tidak teridentifikasi dalam penilaian risiko vs. insiden total 3. Frekuensi pembaruan profil risiko yang sesuai
EG03	Keuangan	Kepatuhan terhadap hukum dan aturan	1. Biaya ketidakpatuhan peraturan, termasuk penyelesaian dan fines 2. Jumlah penyebab masalah ketidakpatuhan peraturan komentar publik atau publisitas negatif 3. Jumlah masalah ketidakpatuhan yang dicatat oleh regulator atau otoritas pengawas 4. Jumlah masalah ketidakpatuhan peraturan yang berkaitan dengan perjanjian kontrak dengan mitra
EG04	Keuangan	Kualitas Keuangan Informasi	1. Survei kepuasan pemangku kepentingan utama terkait dengan transparansi, pemahaman dan akurasi perusahaan informasi keuangan 2. Biaya ketidakpatuhan peraturan terkait keuangan peraturan

Tabel 2.14. lanjutan

References	*BSC Dimension*	*Enterprise Goal*	*Example Metrics*
EG05	Pelanggan	Budaya layanan yang berorientasi pada pelanggan	1. Jumlah gangguan layanan pelanggan 2. Persentase pemangku kepentingan bisnis memuaskan pelanggan itu pemberian layanan memenuhi tingkat yang disepakati 3. Jumlah keluhan pelanggan 4. Tren hasil survei kepuasan pelanggan
EG06	Pelanggan	Kontinuitas layanan bisnis dan ketersediaan	1. Jumlah layanan pelanggan atau proses bisnis gangguan yang menyebabkan insiden signifikan 2. Biaya insiden bisnis 3. Jumlah jam pemrosesan bisnis yang hilang karena gangguan layanan yang tidak direncanakan 4. Persen keluhan sebagai fungsi dari komitmen layanan target kesediaan
EG07	Pelanggan	Kualitas manajemen informasi	1. Tingkat kepuasan dewan direksi dan manajemen eksekutif terhadap informasi pengambilan keputusan 2. Jumlah insiden yang disebabkan oleh bisnis yang salah keputusan berdasarkan informasi yang tidak akurat 3. Waktu untuk memberikan informasi pendukung agar efektif keputusan bisnis 4. Ketepatan waktu informasi manajemen
EG08	Internal	Optimasi proses bisnis internal	1. Tingkat kepuasan dewan direksi dan manajemen eksekutif proses bisnis terhadap kemampuan proses bisnis 2. Tingkat kepuasan pelanggan terhadap pemberian layanan kemampuan 3. Tingkat kepuasan terhadap pemasok atas kemampuannya
EG09	Internal	Biaya proses optimasi bisnis	1. Rasio biaya vs. tingkat layanan yang dicapai 2. Tingkat kepuasan dewan direksi dan manajemen eksekutif terhadap biaya proses bisnis

Tabel 2.14. lanjutan

References	*BSC Dimension*	*Enterprise Goal*	*Example Metrics*
EG10	Internal	Kemampuan staf, motivasi dan produktivitas	1. Produktivitas staf dibandingkan dengan tolok ukur 2. Tingkat kepuasan pemangku kepentingan dengan keahlian staf dan keterampilan 3. Persentase staf yang keterampilannya relatif kurang memadai kompetensi yang dibutuhkan untuk peran mereka 4. Persen staf yang puas
EG11	Internal	Kepatuhan terhadap kebijakan internal	1. Jumlah insiden yang terkait dengan ketidakpatuhan terhadap kebijakan kebijakan 2. Persentase pemangku kepentingan yang memahami kebijakan 3. Persentase kebijakan yang didukung oleh standar yang efektif dan praktek kerja
EG12	Pertumbuhan	Program transformasi digital yang terkelola	1. Jumlah program tepat waktu dan sesuai anggaran program transformasi 2. Persentase pemangku kepentingan yang puas terhadap pelaksanaan program 3. Persen program transformasi bisnis yang dihentikan 4. Persentase program transformasi bisnis dengan regular pembaruan terlaporkan
EG13	Pertumbuhan	Produk dan inovasi bisnis	1. Tingkat kesadaran dan pemahaman tentang bisnis inovasi peluang inovasi 2. Kepuasan pemangku kepentingan dengan tingkat produk dan keahlian dan ide inovasi 3. Jumlah inisiatif produk dan layanan yang disetujui dan dihasilkan dari ide inovatif

Alignment Goals

Penyelarasan tujuan perusahaan agar dapat diperoleh tata kelola TI yang baik. Target penyelarasan ini diturunkan dari target perusahaan. Berikut penjelasan pendetailan target perusahaan menjadi *alignment goals* pada tabel 2.15

Tabel 2.15. *Alignment goals*

References	*BSC Dimension*	*Enterprise Goal*	*Example Metrics*
AG01	Keuangan	Kepatuhan dan dukungan IT dalam kepatuhan bisnis terhadap hukum dan aturan	1. Biaya ketidakpatuhan TI, termasuk penyelesaian dan denda, untuk kepatuhan bisnis dengan dan dampak hilangnya reputasi hukum dan peraturan eksternal 2. Jumlah masalah ketidakpatuhan terkait TI yang dilaporkan atau komentar publik atau rasa malu 3. Jumlah masalah ketidakpatuhan yang terkait dengan kontrak perjanjian
AG02	Keuangan	Risiko terkait I&T yang dikelola	1. Frekuensi pembaruan profil risiko yang sesuai 2. Persen penilaian risiko perusahaan termasuk risiko I & T 3. Jumlah insiden terkait I & T signifikan yang tidak terkait diidentif
AG03	Keuangan	Manfaat yang disadari dari I&T, investasi yang memungkinkan dan layanan portofolio	1. Persen dari investasi yang mendukung I & T yang diklaim memungkinkan investasi dan keuntungan dalam kasus bisnis terpenuhi atau terlampaui portofolio layanan 2. Persen dari layanan I&T yang mengharapkan keuntungan (seperti dinyatakan dalam perjanjian tingkat layanan)
AG04	Keuangan	Kualitas terkait teknologi informasi keuangan	1. Kepuasan pemangku kepentingan utama tentang tingkat informasi keuangan transparansi, pemahaman dan akurasi informasi keuangan TI 2. Persen layanan I&T biaya operasional dan manfaat yang diharapkan
AG05	Pelanggan	Pemenuhan I&T sejalan dengan kebutuhan bisnis	1. Persentase pemangku kepentingan bisnis puas dengan layanan TI dengan pengiriman memenuhi tingkat layanan yang disepakati 2. Jumlah gangguan bisnis akibat layanan TI insidentil
AG06	Pelanggan	Kemampuan untuk pemenuhan kebutuhan bisnis melalui solusi operasional	1. Tingkat kepuasan eksekutif bisnis dengan TI, persyaratan operasional responsivitas terhadap persyaratan baru 2. Waktu rata - rata ke pasar untuk layanan baru terkait I & T dan aplikasi 3. Waktu rata-rata untuk mengubah tujuan I&T strategis menjadi inisiatif yang disepakati dan disetujui

Tabel 2.15. lanjutan

References	*BSC Dimension*	*Enterprise Goal*	*Example Metrics*
AG07	Internal	Keamanan informasi, infrastruktur, pengolahan dan aplikasi, serta privasi	1. Jumlah insiden kerahasiaan yang menyebabkan kerugian finansial, infrastruktur dan gangguan bisnis atau rasa malu publik, dan privasi 2. Jumlah insiden ketersediaan yang menyebabkan kerugian finansial, gangguan bisnis atau rasa malu 3. Jumlah insiden integritas yang menyebabkan kerugian finansial, gangguan bisnis atau rasa malu
AG08	Internal	Mengaktifkan dan mendukung proses bisnis melalui integrasi teknologi dan aplikasi	1. Waktu untuk menjalankan layanan atau proses bisnis 2. Jumlah program bisnis yang mendukung I & T yang tertunda atau menimbulkan biaya tambahan karena masalah integrasi teknologi 3. Jumlah perubahan proses bisnis yang perlu ditunda atau dikerjakan ulang karena masalah integrasi teknologi 4. Jumlah aplikasi atau infrastruktur penting beroperasi secara silo dan tidak terintegrasi
AG09	Internal	Penyampaian program yang tepat waktu, sesuai anggaran dan kebutuhan meeting dan berkualitas standar	1. Jumlah program / proyek tepat waktu dan sesuai anggaran dan rapat 2. Jumlah program yang membutuhkan pengerjaan ulang yang signifikan karena persyaratan dan cacat kualitas 3. Persentase pemangku kepentingan yang puas terhadap kualitas program /proyek
AG10	Internal	Kualitas manajemen I&T dan informasi	1. Tingkat kepuasan pengguna dengan kualitas dan ketepatan waktu dan ketersediaan informasi manajemen terkait I&T, pengambilan memperhitungkan sumber daya yang tersedia 2. Rasio dan luasnya keputusan bisnis yang keliru informasi terkait I & T yang salah atau tidak tersedia adalah kuncinya faktor 3. Persentase informasi yang memenuhi kriteria
AG11	Internal	Kepatuhan I&T terhadap kebijakan internal	1. Jumlah insiden yang terkait dengan ketidakpatuhan dengan kebijakan IT 2. Jumlah pengecualian untuk kebijakan internal 3. Frekuensi tinjauan dan pembaruan

Tabel 2.15. lanjutan

References	*BSC Dimension*	*Enterprise Goal*	*Example Metrics*
AG12	Pembelajaran dan pertumbuhan	Kompeten dan staf yang termotivasi dengan ukuran pemahaman terhadap teknologi dan bisnis	1. Persentase pebisnis yang paham I & T (yaitu, mereka yang memiliki pengetahuan dan pemahaman yang diperlukan tentang I&T untuk memandu, pemahaman tentang teknologi mengarahkan, berinovasi, dan melihat peluang I&T untuk mereka dan bisnis domain keahlian) 2. Persentase orang IT yang paham bisnis (yaitu, mereka yang memiliki ekstensi dibutuhkan pengetahuan dan pemahaman yang relevan domain bisnis untuk memandu, mengarahkan, berinovasi, dan melihat peluang I&T untuk domain bisnis) 3. Jumlah atau persentase pelaku bisnis yang memiliki manajemen teknologi yang mapan
AG13	Pembelajaran dan pertumbuhan	Pengetahuan, keahlian dan inisiatif untuk inovasi bisnis	1. Tingkat kesadaran dan pemahaman eksekutif bisnis untuk kemungkinan berinovasi I&T 2. Jumlah inisiatif yang disetujui sebagai hasil dari inovasi ide I&T Jumlah juara inovasi yang diakui

Governance and Management Objectives

Model inti COBIT ke dalam 40 tujuan tata kelola dan manajemen. Pernyataan tujuan adalah penjabaran lebih lanjut (tingkat detail berikutnya) dari setiap tujuan tata kelola dan manajemen. Dapat dijelaskan pada tabel 2.16 di bawah ini.

Tabel 2.16. *Governance and management objectives* pada COBIT 2019

Reference	Nama	Tujuan
EDM01	*Ensured governance framework setting and maintenancee*	Memberikan pendekatan yang konsisten, terintegrasi dan selaras dengan pendekatan tata kelola perusahaan. Keputusan terkait I & T haruslah dibuat sejalan dengan strategi dan tujuan perusahaan dan nilai yang diinginkan terwujud. Untuk itu, pastikan I&T terkait proses diawasi secara efektif dan transparan; pemenuhan dengan persyaratan hukum, kontrak, dan peraturan yang dikonfirmasi;

Tabel 2.16. lanjutan

Reference	Nama	Tujuan
EDM02	*Ensured benefits delivery*	Dapatkan nilai optimal dari inisiatif, layanan yang mendukung I & T , dan aktiva; penyampaian solusi dan layanan yang hemat biaya ; dan gambaran biaya yang andal dan akurat serta kemungkinan manfaatnya kebutuhan bisnis didukung secara efektif dan efisien.
EDM03	*Ensured risk optimization*	Pastikan bahwa risiko perusahaan terkait I & T tidak melebihi selera risiko perusahaan dan toleransi risiko, dampak dari risiko I&T untuk nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan kepatuhan diminimalkan.
EDM04	*Ensured resource optimization*	Pastikan bahwa kebutuhan sumber daya perusahaan terpenuhi di secara optimal, biaya I&T dioptimalkan, dan ada peningkatan kemungkinan realisasi manfaat dan kesiapan untuk perubahan di masa depan.
EDM05	*Ensured stakeholder engagement*	Pastikan bahwa pemangku kepentingan mendukung strategi I&T dan peta jalan, komunikasi dengan pemangku kepentingan efektif dan tepat waktu dan dasar pelaporan ditetapkan untuk meningkatkan kinerja. Identifikasi area untuk perbaikan, dan konfirmasikan bahwa I & T terkait tujuan dan strategi sejalan dengan strategi perusahaan
APO01	*Managed I&T management framework*	Menerapkan pendekatan manajemen yang konsisten untuk perusahaan persyaratan tata kelola yang harus dipenuhi, mencakup tata kelola komponen seperti proses manajemen; organisasi struktur; peran dan tanggung jawab; aktivitas yang andal dan berulang; item informasi; kebijakan dan prosedur; keterampilan dan kompetensi; budaya dan perilaku; dan layanan, infrastruktur dan aplikasi.
APO02	*Managed strategy*	Mendukung strategi transformasi digital organisasi dan berikan nilai yang diinginkan melalui peta jalan inkremental perubahan. Gunakan pendekatan I&T holistik, memastikan bahwa setiap inisiatif secara jelas terkait dengan strategi menyeluruh. Aktifkan perubahan semua aspek organisasi yang berbeda, dari saluran dan proses untuk data, budaya, keterampilan, model operasi dan insentif
APO03	*Managed enterprise architecture*	Mewakili berbagai blok bangunan yang membentuk perusahaan dan keterkaitannya, serta prinsip-prinsip yang memandu mereka desain dan evolusi dari waktu ke waktu, untuk memungkinkan standar, res dan penyampaian tujuan operasional dan strategis yang efisien

Tabel 2.16. lanjutan

Reference	Nama	Tujuan
APO04	*Managed innovation*	Raih keunggulan kompetitif, inovasi bisnis, ditingkatkan pengalaman pelanggan, dan peningkatan efektivitas operasional dan e siensi dengan memanfaatkan perkembangan I&T dan teknologi yang muncul
APO05	*Managed portfolio*	Mengoptimalkan kinerja keseluruhan portofolio program di menanggapi kinerja program, produk dan layanan individu dan mengubah prioritas dan permintaan perusahaan.
APO06	*Managed budget and costs*	Membina kemitraan antara TI dan pemangku kepentingan perusahaan untuk memungkinkan penggunaan yang efektif dan efisien dari sumber daya terkait I & T da memberikan transparansi dan akuntabilitas biaya dan bisnis nilai solusi dan layanan. Memungkinkan perusahaan untuk membuatnya keputusan yang diinformasikan mengenai penggunaan solusi I&T dan jasa.
APO07	*Managed human resources*	Mengoptimalkan kemampuan sumber daya manusia untuk memenuhi kebutuhan peru tujuan.
APO08	*Managed relationships*	Memungkinkan terciptanya pengetahuan, keterampilan, dan perilaku yang benar hasil yang lebih baik, kepercayaan yang meningkat, rasa saling percaya dan penggunaan sumber daya yang efektif yang merangsang hubungan yang produktif dengan pemangku kepentingan bisnis.
APO09	*Managed service agreements*	Pastikan produk, layanan, dan tingkat layanan I&T memenuhi saat ini dan kebutuhan perusahaan di masa depan.
APO10	*Managed vendors*	Mengoptimalkan kemampuan I&T yang tersedia untuk mendukung strategi I&T dan peta jalan, meminimalkan risiko yang terkait dengan kinerja buruk atau ® vendor yang tidak patuh, dan memastikan harga yang kompetitif
APO11	*Managed quality*	Pastikan pengiriman solusi dan layanan teknologi yang konsisten kepada memenuhi persyaratan kualitas perusahaan dan memuaskan kebutuhan pemangku kepentingan.
APO12	*Managed risk*	Integrasikan manajemen risiko perusahaan terkait I & T dengan manajemen risiko perusahaan secara keseluruhan (ERM) dan menyeimbangkan biaya dan keuntungan mengelola risiko perusahaan yang berhubungan dengan I & T.
APO13	*Managed security*	Menjaga dampak dan terjadinya insiden keamanan informasi dalam tingkat selera risiko perusahaan.

Tabel 2.16. lanjutan

Reference	Nama	Tujuan
APO14	*Managed data*	Pastikan pemanfaatan yang efektif dari aset data penting untuk dicapai tujuan dan sasaran perusahaan
BAI01	*Managed programs*	Sadarilah nilai bisnis yang diinginkan dan kurangi risiko yang tidak terduga penundaan, biaya dan erosi nilai. Untuk melakukannya, tingkatkan komunikasi dan keterlibatan bisnis dan pengguna akhir, memastikan nilai dan kualitas hasil dan tindak lanjut program proyek dalam program, dan memaksimalkan program kontribusi terhadap portofolio investasi.
BAI02	*Managed requirements definition*	Ciptakan solusi optimal yang memenuhi kebutuhan perusahaan sementara meminimalkan risiko
BAI03	*Managed solutions identification and build*	Pastikan pengiriman produk dan layanan digital yang gesit dan terukur. Menetapkan solusi tepat waktu dan hemat biaya (teknologi, bisnis proses dan arus kerja) yang mampu mendukung perusahaan tujuan strategis dan operasional.
BAI04	*Managed availability and capacity*	Menjaga ketersediaan layanan, pengelolaan sumber daya yang efisien dan optimalisasi kinerja sistem melalui prediksi kinerja masa depan dan persyaratan kapasitas.
BAI05	*Managed organizational change*	Mempersiapkan dan berkomitmen pemangku kepentingan untuk perubahan dan pengurangan risiko kegagalan.
BAI06	*Managed IT changes*	Memungkinkan pengiriman perubahan bisnis yang cepat dan andal. Mengurangi risiko yang berdampak negatif pada stabilitas atau integritas lingkungan yang berubah.
BAI07	*Managed IT change acceptance and transitioning*	Menerapkan solusi dengan aman dan sesuai dengan kesepakatan harapan dan hasil
BAI08	*Managed knowledge*	Memberikan pengetahuan dan informasi manajemen yang diperlukan mendukung semua staf dalam tata kelola dan manajemen perusahaan I&T dan memungkinkan pengambilan keputusan yang terinformasi
BAI09	*Managed assets*	Perhitungkan semua aset I&T dan optimalkan nilai yang diberikan oleh mereka menggunakan.
BAI10	*Managed configuration*	Menyediakan informasi yang memadai tentang aset layanan untuk memungki layanan untuk dikelola secara efektif. Menilai dampak perubahan dan menangani insiden layanan.

Tabel 2.16. lanjutan

Reference	Nama	Tujuan
BAI11	*Managed projects*	Sadarilah hasil proyek yang telah ditentukan dan kurangi risikonya penundaan tak terduga, biaya dan erosi nilai dengan meningkatkan komunikasi dan keterlibatan bisnis dan pengguna akhir. Pastikan nilai dan kualitas hasil proyek dan maksimalkan kontribusi mereka pada program dan investasi yang telah ditetapkan portofolio
DSS01	*Managed operations*	Memberikan hasil produk dan layanan operasional I&T sesuai rencana.
DSS02	*Managed service requests and incidents*	Capai peningkatan produktivitas dan minimalkan gangguan melalui resolusi cepat dari pertanyaan dan insiden pengguna. Nilai dampaknya perubahan dan menangani insiden layanan. Selesaikan permintaan pengguna dan memulihkan layanan sebagai tanggapan atas insiden.
DSS03	*Managed problems*	Tingkatkan ketersediaan, tingkatkan tingkat layanan, kurangi biaya, perbaiki kenyamanan dan kepuasan pelanggan dengan mengurangi jumlah masalah operasional, dan mengidentifikasi akar penyebab sebagai bagian dar resolusi.
DSS04	*Managed continuity*	Beradaptasi dengan cepat, lanjutkan operasi bisnis, dan pertahankan ketersediaan sumber daya dan informasi pada tingkat yang dapat diterima perusahaan jika terjadi gangguan yang signifikan (misalnya, ancaman, peluang, tuntutan).
DSS05	*Managed security services*	Minimalkan dampak bisnis dari keamanan informasi operasional kerentanan dan insiden
DSS06	*Managed business process controls*	Menjaga integritas informasi dan keamanan informasi aset yang ditangani dalam proses bisnis di perusahaan atau nya operasi outsourcing.
MEA01	*Managed performance and conformance monitoring*	Memberikan transparansi kinerja dan kesesuaian dan dorongan pencapaian tujuan.
MEA02	*Managed system of internal control*	Mendapatkan transparansi bagi pemangku kepentingan utama tentang kecuk sistem pengendalian internal dan dengan demikian memberikan kepercayaan keyakinan dalam pencapaian tujuan perusahaan dan sebuah pemahaman yang memadai tentang risiko residual
MEA03	*Managed compliance with external requirements*	Pastikan perusahaan memenuhi semua eksternal yang berlaku Persyaratan
MEA04	*Managed assurance*	Memungkinkan organisasi untuk merancang dan mengembangkan efisiensi inisiatif jaminan yang efektif, memberikan panduan tentang perencanaan, pelingkupan, melaksanakan dan menindaklanjuti tinjauan jaminan, menggunakan peta jalan berdasarkan pendekatan jaminan yang diterima dengan baik

Manajemen Kinerja di COBIT

Manajemen kinerja adalah bagian penting dari sistem tata kelola dan manajemen. Manajemen kinerja mewakili istilah umum untuk semua aktivitas dan metode. Ini mengungkapkan seberapa baik tata kelola dan sistem manajemen dan semua komponen perusahaan bekerja, dan bagaimana mereka dapat ditingkatkan untuk mencapai tingkat yang diperlukan. Ini mencakup konsep dan metode seperti tingkat kemampuan dan tingkat kematangan. COBIT menggunakan istilah COBIT *Performance Management* (CPM) untuk menggambarkan kegiatan ini, dan konsep tersebut merupakan bagian integral dari kerangka kerja COBIT. Prinsip Manajemen Kinerja COBIT 2019 didasarkan pada prinsip-prinsip berikut:

1. CPM harus mudah dipahami dan digunakan;
2. CPM harus konsisten dengan, dan mendukung, model konseptual COBIT. Ini harus memungkinkan pengelolaan kinerja semua jenis komponen sistem tata kelola; harus dimungkinkan untuk mengelola kinerja proses serta kinerja jenis komponen lainnya (misalnya, struktur organisasi atau informasi), jika pengguna ingin melakukannya;
3. CPM harus memberikan hasil yang andal, berulang dan relevan;
4. CPM harus fleksibel, sehingga dapat mendukung kebutuhan organisasi yang berbeda dengan prioritas dan kebutuhan yang berbeda;
5. CPM harus mendukung berbagai jenis penilaian, dari penilaian mandiri hingga penilaian atau audit formal

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 IT proses 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 proses 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 26 fungsi-fungsi lainnya terhadap suatu aktifitas tertentu. RACI chart mendefinisikan apa dan kepada siapa harus didelegasikan yang terdiri dari (Heppy, 2017):

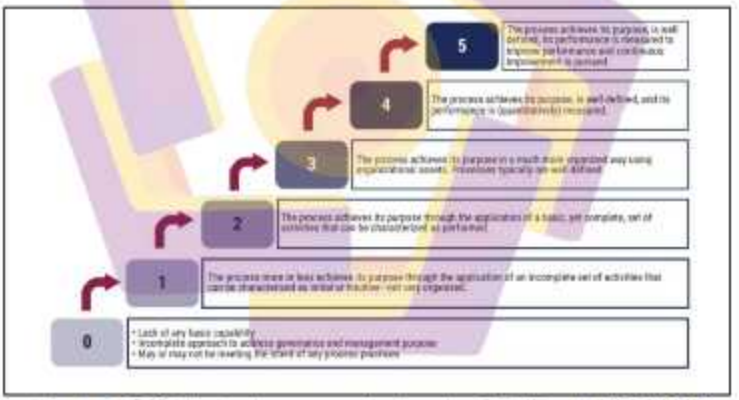
a. R = *Responsible*, artinya pihak yang harus memastikan aktivitas tersebut berhasil dilaksanakan.
b. A= *Accountable*, artinya pihak yang mempunyai kewenangan untuk menyetujui atau menerima pelaksanaan sebuah aktivitas.
c. C = *Consulted*, artinya pihak yang mana pendapatnya dibutuhkan dalam aktivitas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

2.3.2.3. Mengelola Kinerja Proses

Tingkat Kemampuan

COBIT 2019 mendukung skema kapabilitas proses berbasis CMMI . Proses dalam setiap tujuan tata kelola dan manajemen dapat beroperasi pada berbagai tingkat kemampuan, mulai dari 0 hingga 5. Tingkat kemampuan adalah ukuran seberapa baik suatu proses diimplementasikan dan dilakukan seperti dijelakan pada gambar 2.5 di bawah ini.



Gambar 2.5. Tingkatan kemampuan berdasarkan CMMI pada COBIT 2019

Kegiatan Proses Penilaian

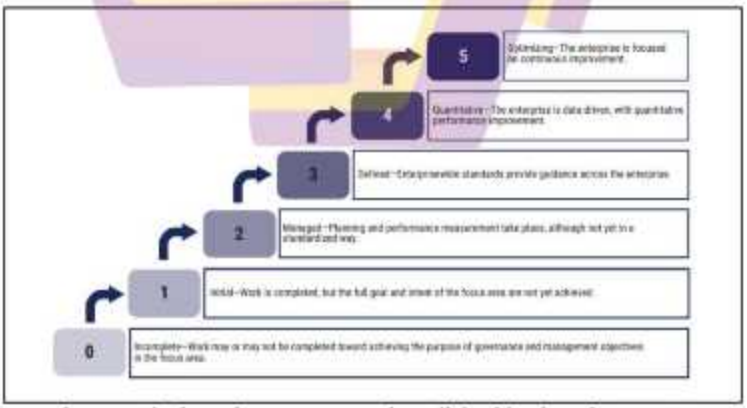
Suatu tingkat kemampuan dapat dicapai dengan derajat yang berbeda-beda, yang dapat diekspresikan dengan serangkaian peringkat. Kisaran peringkat yang tersedia bergantung pada konteks di mana penilaian kinerja dibuat: Beberapa metode formal yang mengarah ke sertifikasi independen menggunakan rangkaian

peringkat lulus / gagal biner. Metode yang kurang formal (sering digunakan dalam konteks peningkatan kinerja) bekerja lebih baik dengan rentang peringkat yang lebih besar, seperti rangkaian berikut:

1. *Fully*; Tingkat kemampuan dicapai lebih dari 85 persen. (Ini tetap merupakan panggilan penilaian, tetapi dapat dibuktikan dengan pemeriksaan atau penilaian komponen enabler, seperti aktivitas proses, tujuan proses atau praktik yang baik struktur organisasi.)
2. *Largely*; Tingkat kemampuan dicapai antara 50 persen dan 85 persen.
3. *Partially;* Tingkat kapabilitas dicapai antara 15 persen dan 50 persen.
4. *Not;* Tingkat kemampuan dicapai kurang dari 15 persen.

Tingkat Kematangan Fokus Area

Pada tingkat kematangan suatu kegiatan dapat didefinisikan sudah dalah tahap incomplete, initial, managed, defined, quantitative dan paling optimal adalah optimizing seperti terlihat pada gambar 2.6 di bawah ini.



Gambar 2.6. Tingkatan kematangan untuk penilaian kinerja pada COBIT 2019

2.3.2.4. Tahapan dan langkah dalam proses desain audit tata kelola teknologi informasi menggunakan framework COBIT 2019

Tahapan dan langkah yang berbeda dalam proses desain, seperti yang diilustrasikan dalam gambar 2.7. akan menghasilkan rekomendasi untuk memprioritaskan tujuan tata kelola dan manajemen atau komponen sistem tata kelola terkait, untuk tingkat kapabilitas target, atau untuk mengadopsi varian tertentu dari komponen sistem tata kelola. Beberapa langkah atau sub-langkah ini dapat menghasilkan beberapa alternatif panduan, yang tidak dapat dihindari saat mempertimbangkan sejumlah besar faktor desain, sifat umum keseluruhan dari panduan faktor desain dan tabel pemetaan yang digunakan.

Gambar 2.7. Langkah dalam proses pembuatan desain sistem tata kelola TI pada COBIT 2019

Audit tata kelola teknologi informasi berfungsi untuk mengetahui kondisi perusahaan terkini. Audit yang paling tepat dan relevan harus sejalan dengan strategi bisnis perusahaan yang dipilih. (ISACA, 2019). Sebelum dilakukan audit maka ditentukan terlebih dahulu domain yang menjadi area audit. Penetuan domain

menggunakan COBIT 2019 melalui pendekatan penilaian faktor desain. Berikut tabel-tabel yang akan digunakan dalam pemilihan domain berdasarkan pembobotan pada masing-masing faktor desain.

1. Tabel *Mapping Enterprise Strategy* (tabel 2.17)

Tabel 2.17. Tabel *mapping- enterprise strategy* pada COBIT 2019

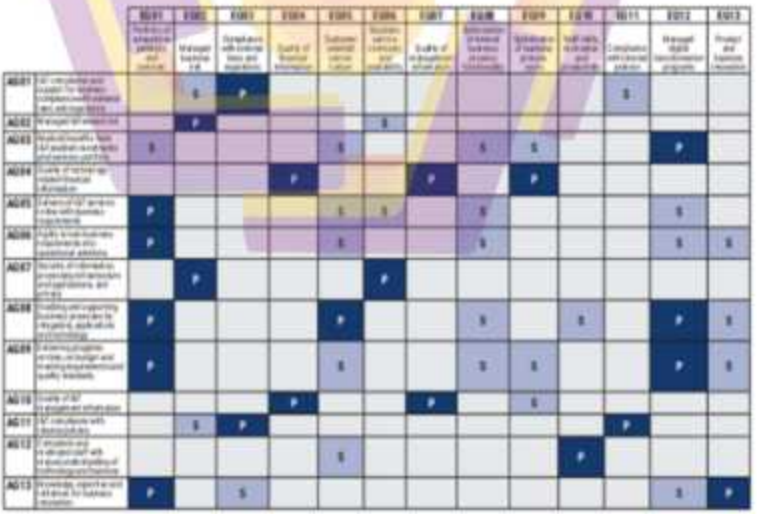
Kode	Growth/ Acquisition	Inovation/ Differentiation	Cost Leadership	Client Service/ Stability
EDM01	1.0	1.0	1.5	1.5
EDM02	1.5	1.0	2.0	3.5
EDM03	1.0	1.0	1.0	2.0
EDM04	1.5	1.0	4.0	1.0
EDM05	1.5	1.5	1.0	2.0
APO01	1.0	1.0	1.0	1.0
APO02	3.5	3.5	1.5	1.0
APO03	4.0	2.0	1.0	1.0
APO04	1.0	4.0	1.0	1.0
APO05	3.5	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

Tabel 2.17 (lanjutan)

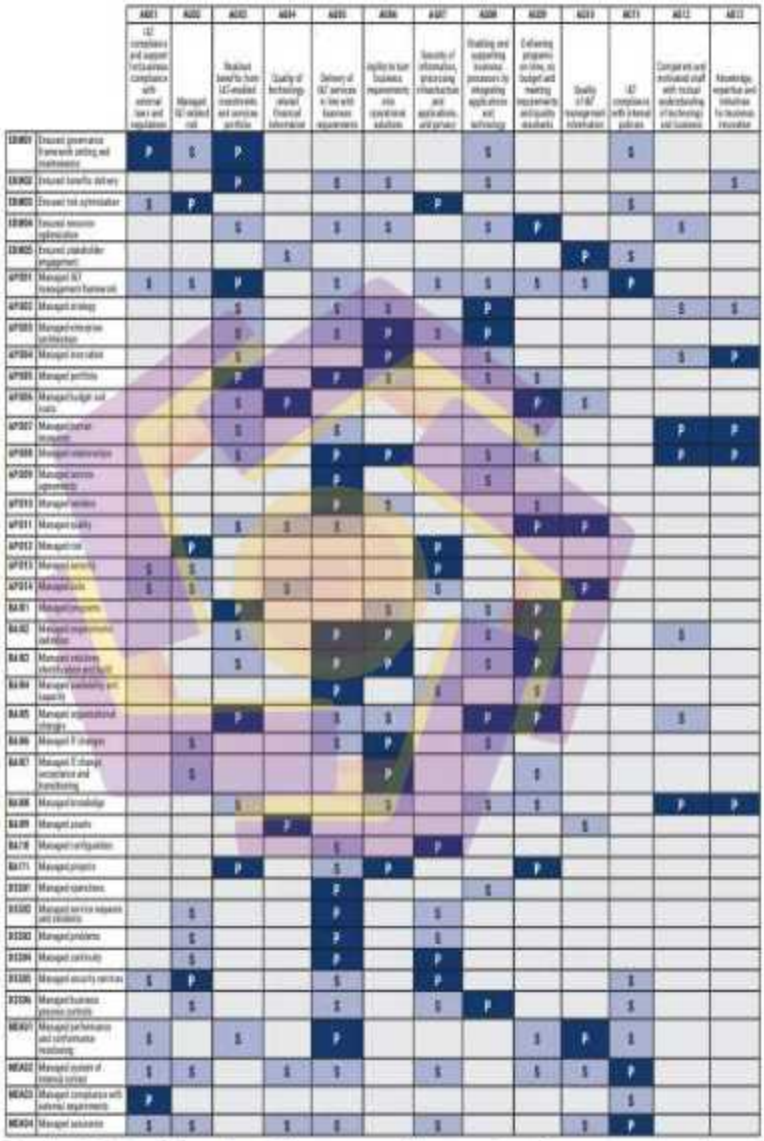
Kode	Growth/ Acquisition	Inovation/ Differentiation	Cost Leadership	Client Service/ Stability
DSS04	1.0	1.0	1.0	4.0
DSS05	1.0	1.0	1.0	2.5
DSS06	1.0	1.0	1.0	1.5
MEA01	1.0	1.0	1.0	1.0
MEA02	1.0	1.0	1.0	1.0
MEA03	1.0	1.0	1.0	1.0
MEA04	1.0	1.0	1.0	1.0

2. Tabel *Mapping Enterprise Goals*

Dalam memasukan faktor desain *enterprise goals* tidak dapat berdiri sendiri, dari *enterprise goals* diturunkan menjadi *alignment goals*. Setelah itu dari *alignment goals* akan ada pembobotan berupa kategori *primary* dan *secondary* untuk menentukkan domain yang lebih prioritas. Berikut gambar 2.8 dan 2.9 dapat menjelaskan penyelarasan dari *enterprise goal* menjadi domain.



Gambar 2.8. Penyelarasan dari *enterprise goals* menjadi *aligment goals* pada COBIT 2019



Gambar 2.9. Pemilihan domain dengan pembobotan pada *alignment goals* pada COBIT 2019

3. Tabel Mapping berdasarkan Risiko IT (tabel 2.18)

Tabel 2.18. Tabel Mapping- Risiko IT pada COBIT 2019

Kode	risk01	risk02	risk03	risk04	risk05	risk06	risk07	risk08	risk09	risk10
EDM01	3.0	2.0	3.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0
EDM02	3.0	2.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0
EDM03	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
EDM04	3.0	0.0	4.0	3.0	2.0	0.0	0.0	0.0	0.0	0.0
EDM05	3.0	1.0	3.0	0.0	0.0	0.0	2.0	0.0	0.0	1.0
APO01	2.0	3.0	2.0	0.0	2.0	2.0	4.0	2.0	0.0	2.0
APO02	2.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0	1.0	0.0
APO03	2.0	0.0	0.0	0.0	4.0	0.0	0.0	2.0	0.0	2.0
APO04	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	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
APO06	2.0	3.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
APO07	0.0	0.0	0.0	4.0	0.0	2.0	3.0	3.0	0.0	0.0
APO08	0.0	0.0	0.0	2.0	2.0	0.0	0.0	4.0	0.0	0.0
APO09	0.0	0.0	2.0	0.0	0.0	0.0	2.0	3.0	0.0	1.0
APO10	0.0	0.0	3.0	0.0	0.0	0.0	2.0	2.0	3.0	2.0
APO11	0.0	2.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	4.0
APO12	0.0	3.0	0.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0
APO13	0.0	0.0	0.0	0.0	0.0	0.0	4.0	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
BAI01	0.0	4.0	0.0	0.0	2.0	0.0	0.0	3.0	0.0	0.0
BAI02	2.0	2.0	0.0	0.0	2.0	0.0	0.0	3.0	0.0	2.0
BAI03	0.0	3.0	0.0	0.0	2.0	0.0	0.0	2.0	0.0	3.0
BAI04	0.0	1.0	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
BAI06	0.0	0.0	0.0	0.0	0.0	3.0	4.0	0.0	0.0	2.0
BAI07	0.0	0.0	0.0	0.0	0.0	2.0	3.0	2.0	0.0	4.0
BAI08	0.0	0.0	0.0	2.0	0.0	3.0	0.0	3.0	0.0	3.0
BAI09	0.0	0.0	0.0	0.0	0.0	1.0	3.0	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
BAI11	0.0	4.0	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
DSS02	0.0	0.0	0.0	0.0	0.0	3.0	2.0	3.0	2.0	2.0
DSS03	0.0	0.0	0.0	0.0	0.0	3.0	1.0	4.0	0.0	3.0
DSS04	0.0	0.0	0.0	0.0	0.0	3.0	3.0	0.0	3.0	0.0
DSS05	0.0	0.0	0.0	0.0	0.0	3.0	4.0	0.0	2.0	0.0
DSS06	0.0	0.0	0.0	0.0	0.0	3.0	4.0	2.0	0.0	0.0
MEA01	1.0	2.0	2.0	0.0	0.0	2.0	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
MEA03	0.0	1.0	0.0	0.0	0.0	1.0	2.0	0.0	0.0	0.0
MEA04	1.0	2.0	0.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0

Tabel 2.18. lanjutan

Kode	risk11	risk12	risk13	risk14	risk15	risk16	risk17	risk18	risk19
EDM01	0.0	0.0	3.0	2.0	0.0	0.0	2.0	2.0	2.0
EDM02	0.0	0.0	1.0	0.0	0.0	0.0	3.0	1.0	3.0
EDM03	2.0	0.0	3.0	3.0	0.0	0.0	0.0	2.0	3.0
EDM04	0.0	2.0	1.0	0.0	2.0	0.0	0.0	2.0	3.0
EDM05	0.0	1.0	3.0	3.0	0.0	0.0	0.0	2.0	2.0
APO01	3.0	3.0	3.0	0.0	0.0	0.0	3.0	2.0	3.0
APO02	1.0	2.0	0.0	0.0	0.0	0.0	2.0	2.0	1.0
APO03	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	0.0	0.0	4.0	0.0	0.0
APO05	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0
APO06	0.0	2.0	0.0	2.0	0.0	0.0	2.0	2.0	0.0
APO07	2.0	0.0	0.0	2.0	4.0	0.0	2.0	2.0	0.0
APO08	2.0	2.0	0.0	0.0	0.0	0.0	3.0	0.0	2.0
APO09	2.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
APO10	2.0	4.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0
APO11	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0
APO12	3.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0
APO13	4.0	0.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0
APO14	2.0	0.0	3.0	0.0	2.0	4.0	2.0	0.0	4.0
BAI01	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI02	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI03	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI04	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI05	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI06	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	3.0
BAI07	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	0.0	2.0	0.0	0.0	0.0	2.0
BAI09	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI10	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI11	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
DSS01	2.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0
DSS02	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
DSS03	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
DSS04	4.0	0.0	2.0	0.0	3.0	4.0	0.0	0.0	2.0
DSS05	4.0	0.0	3.0	0.0	3.0	2.0	0.0	0.0	3.0
DSS06	2.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	3.0
MEA01	3.0	2.0	2.0	2.0	0.0	2.0	0.0	0.0	2.0
MEA02	3.0	2.0	2.0	3.0	0.0	2.0	0.0	0.0	2.0
MEA03	3.0	2.0	4.0	2.0	0.0	0.0	0.0	0.0	2.0
MEA04	3.0	2.0	2.0	4.0	0.0	2.0	2.0	0.0	2.0

4. Tabel Mapping masalah terkait I&T (tabel 2.19)

Tabel 2.19. Tabel Mapping- masalah terkait IT pada COBIT 2019

Kode	A	B	C	D	E	F	G	H	I	J
EDM01	3.0	3.0	1.0	1.0	2.0	2.0	2.0	1.0	1.0	1.0
EDM02	2.5	3.0	1.0	1.0	1.5	2.5	2.0	1.5	0.5	2.5
EDM03	1.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
EDM04	1.0	1.0	1.0	1.0	1.0	2.0	3.0	3.5	3.5	1.0
EDM05	1.0	1.0	1.0	1.0	1.5	2.0	1.0	1.0	0.0	1.0
APO01	2.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
APO02	1.5	1.5	1.5	1.5	1.0	1.5	1.0	1.0	0.0	1.0
APO03	1.0	1.5	1.0	2.0	0.5	1.5	2.0	1.5	1.0	3.5
APO04	1.0	1.0	1.0	1.0	0.5	0.5	0.5	0.5	0.0	0.0
APO05	3.0	3.0	3.0	1.5	2.0	2.0	1.5	3.5	0.5	2.0
APO06	3.5	2.0	1.0	1.5	1.5	2.0	4.0	3.0	1.0	2.0
APO07	1.5	1.0	1.0	1.0	1.0	1.5	2.0	2.0	4.0	1.0
APO08	2.5	2.0	1.0	2.5	1.5	1.0	2.5	2.0	1.5	1.0
APO09	2.0	1.5	2.0	4.0	1.0	2.5	1.5	2.0	0.5	1.0
APO10	1.0	1.0	2.0	4.0	1.5	1.5	1.5	0.0	1.5	1.0
APO11	1.0	1.0	3.0	1.5	1.0	3.0	0.0	0.0	0.0	2.0
APO12	1.0	0.5	2.5	1.5	2.0	2.0	1.0	1.0	0.5	1.0
APO13	0.0	0.0	3.5	1.0	2.0	1.0	0.0	1.0	0.0	0.5
APO14	1.0	1.5	3.0	1.0	2.5	1.5	1.0	1.5	0.0	1.5
BAI01	0.0	1.0	1.5	0.0	0.0	0.0	0.0	3.0	1.0	3.5
BAI02	0.0	3.0	0.0	0.0	0.5	2.0	0.0	2.0	0.0	3.5
BAI03	1.0	2.0	2.0	0.0	0.0	2.0	0.0	1.0	0.0	3.0
BAI04	0.5	0.0	2.0	3.0	0.0	2.0	0.0	0.0	0.0	0.0
BAI05	1.0	3.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	3.0
BAI06	0.0	0.0	1.0	3.0	0.5	1.5	0.0	1.0	0.0	1.5
BAI07	0.0	1.0	2.5	2.0	0.5	1.5	0.0	0.5	0.0	2.0
BAI08	0.0	0.0	0.0	1.5	0.5	0.5	0.0	1.0	2.0	0.5
BAI09	0.5	0.5	1.0	0.0	0.0	0.0	2.0	2.0	0.0	0.0
BAI10	0.0	0.0	2.5	2.0	0.5	0.0	0.0	0.5	0.0	0.0
BAI11	1.0	2.0	2.5	0.0	0.0	0.0	2.0	3.0	1.0	4.0
DSS01	0.0	0.0	2.5	2.0	1.0	2.0	0.0	0.5	0.0	0.0
DSS02	1.0	1.0	4.0	3.0	1.0	2.5	0.0	0.0	0.0	0.0
DSS03	1.0	1.0	3.0	3.0	0.0	3.0	0.0	0.0	0.0	0.0
DSS04	0.0	0.0	3.0	1.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS05	0.0	0.0	4.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS06	0.0	1.0	0.5	0.0	3.0	0.5	0.0	0.0	0.0	1.0
MEA01	1.0	1.5	2.0	2.0	2.5	3.0	1.0	2.0	1.5	1.0
MEA02	0.0	0.0	2.0	2.0	2.5	2.0	2.0	0.0	0.5	2.0
MEA03	0.0	0.0	2.0	2.0	4.0	0.5	0.0	0.0	0.0	0.0
MEA04	1.0	1.0	3.0	1.5	3.0	4.0	2.0	1.0	1.0	0.5

Tabel 2.19. lanjutan

Kode	K	L	M	N	O	P	Q	R	S	T
EDM01	3.0	3.5	1.0	1.0	1.0	1.0	2.0	3.0	1.5	1.0
EDM02	1.5	1.0	3.0	2.0	1.0	1.0	2.0	2.0	1.0	2.5
EDM03	1.0	0.0	1.0	1.5	1.0	2.0	1.0	1.0	2.5	1.0
EDM04	1.5	0.0	4.0	2.0	1.0	1.5	2.0	2.5	0.0	1.0
EDM05	3.0	1.5	1.5	0.5	0.0	0.5	1.0	1.0	1.0	0.0
APO01	1.5	4.0	1.0	2.0	1.0	1.0	1.5	2.0	0.5	1.0
APO02	2.5	0.5	0.5	1.5	1.5	0.5	2.0	2.0	0.0	2.5
APO03	0.5	0.5	1.0	4.0	1.0	3.5	2.0	3.0	0.0	2.0
APO04	0.5	1.0	0.5	2.0	1.0	0.0	0.5	0.5	0.0	4.0
APO05	2.0	1.5	2.0	1.0	0.5	0.0	2.5	2.5	0.0	2.0
APO06	1.0	1.5	4.0	0.0	0.0	0.0	1.0	2.0	0.0	0.0
APO07	0.0	0.0	1.0	0.0	3.0	0.0	0.5	0.5	1.5	1.0
APO08	1.0	1.0	0.5	1.0	4.0	1.0	3.0	3.5	0.0	0.5
APO09	0.0	0.0	1.0	0.0	0.0	0.0	1.0	1.5	0.0	0.0
APO10	0.0	0.0	1.0	0.0	0.0	0.0	0.5	2.0	1.0	0.0
APO11	0.0	0.0	0.0	0.5	0.5	3.0	2.0	2.0	0.0	1.0
APO12	1.0	1.0	1.0	1.0	1.0	2.0	1.0	1.5	2.5	1.0
APO13	0.0	0.0	0.0	0.0	0.0	1.5	2.0	1.0	2.0	1.0
APO14	0.0	0.0	0.5	2.5	0.5	4.0	2.5	2.0	3.0	0.5
BAI01	0.0	0.0	1.5	0.5	1.0	0.0	1.5	2.0	0.0	1.0
BAI02	0.0	1.0	1.0	2.0	2.0	1.5	2.5	3.0	0.5	1.0
BAI03	0.0	0.5	1.0	1.0	1.0	0.5	2.0	2.0	1.0	0.5
BAI04	0.0	0.0	0.5	0.0	0.0	1.0	1.0	1.0	0.0	0.5
BAI05	1.0	0.0	0.0	0.5	2.0	0.0	0.5	1.5	0.0	1.0
BAI06	0.0	1.0	0.5	1.0	0.5	2.0	2.0	2.0	1.0	1.0
BAI07	0.0	1.0	0.0	1.0	0.5	2.0	2.0	2.0	0.0	1.0
BAI08	0.0	0.5	0.0	1.0	3.0	2.0	1.0	1.5	0.0	0.5
BAI09	0.0	0.0	2.0	1.0	0.0	0.0	1.0	1.5	0.0	0.0
BAI10	0.0	0.0	1.0	1.5	0.0	1.5	1.0	2.0	0.0	0.0
BAI11	0.0	0.0	1.5	2.0	0.5	0.0	1.0	1.5	0.0	0.5
DSS01	0.0	0.0	1.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS02	0.0	0.0	1.0	0.0	0.0	1.0	1.0	1.0	0.0	0.0
DSS03	0.0	0.0	0.0	1.0	1.5	1.0	1.0	1.0	0.5	0.0
DSS04	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS05	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	2.0	0.0
DSS06	0.0	0.0	0.0	0.0	1.5	2.5	1.5	1.0	2.0	0.0
MEA01	1.0	1.0	2.0	1.0	1.0	1.0	1.5	1.0	2.5	1.0
MEA02	1.0	1.0	1.5	1.0	0.0	2.0	1.0	1.0	2.5	0.0
MEA03	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	4.0	0.0
MEA04	1.0	1.0	1.5	0.0	1.0	1.0	1.0	1.0	2.5	1.0

5. Tabel mapping *Threat Landscape* (tabel 2.20)

Tabel 2.20. Tabel Mapping- *Threat Landscape* pada COBIT 2019

Kode	*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

6. Tabel mapping *Compliance* (tabel 2.21)

Tabel 2.21. Tabel Mapping - *Compliance* pada COBIT 2019

Kode	*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

7. Tabel mapping Peran IT (2.22)

Tabel 2.22. Tabel Mapping- Peran IT pada COBIT 2019

Kode	*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

8. Tabel mapping *Source Model* IT (tabel 2.23)

Tabel 2.23. Tabel Mapping- *source model* IT pada COBIT 2019

Kode	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	3.0	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

9. Tabel mapping Implementasi IT (tabel 2.24)

Tabel 2.24. Tabel Mapping- Implementasi IT pada COBIT 2019

Kode	*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

10. Tabel mapping Strategi Adopsi Teknologi (tabel 2.25)

Tabel 2.25. Tabel Mapping- Strategi Adopsi Teknologi pada COBIT 2019

Kode	*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	1.0	1.0	1.0
BAI11	1.5	2.5	1.0
DSS01	3.5	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	1.5	1.0	1.0
DSS06	1.5	1.0	1.0
MEA01	1.0	2.0	1.0
MEA02	3.0	1.0	1.0
MEA03	1.0	1.0	1.0
MEA04	1.0	1.0	1.0

2.3.4. Balai Standardisasi Metrologi Legal (BSML) Regional II

Penyelenggaraan metrologi legal sebagaimana diamanatkan dalam Undang-Undang Nomer 2 Tahun 1981 tentang Metrologi Legal bertujuan untuk melindungi kepentingan umum/konsumen dalam hal jaminan kebenaran hasil pengukuran, ketertiban dan kepastian hukum dalam pemakaian satuan ukuran, standar satuan, metode pengukuran dan alat-alat ukur, takar, timbang dan perlengkapannya (UTTP). Prinsip dasar dari penyelenggaraan metrologi legal ini meliputi:

1. UTTP yang digunakan menentukan kuanta dalam transaksi perdagangan bertanda tera sah;
2. Tera/tera ulang UTTP dilakukan oleh pegawai berhak;
3. Pengujian UTTP berpedoman pada syarat teknis UTTP yang ditetapkan;
4. Standar uji/kerja dan standar ukuran tertelusur;
5. Lembaga pelaksana melalui UPT/UPTD untuk pelayanan tera/tera ulang dan unit kerja untuk pengawasan dan pembinaan;

Balai Standardisasi Metrologi Legal (BSML) Regional II merupakan kepanjangan tangan dari Direktorat Metrologi, Direktorat Jenderal Perlindungan Konsumen dan Tertib Niaga Kementerian Perdagangan yang mengawal Undang-Undang Nomer 2 Tahun 1981 tersebut. BSML Regional II merupakan satuan kerja tersendiri dan hal itu didukung oleh Peraturan Menteri Perdagangan Nomer 60/M-DAG/PER/8/2016 tentang Organisasi dan Tata Kerja unit Pelaksanan Teknis Bidang Kemetrologian dan Bidang Standardisasi Pengendalian Mutu di Lingkungan Kementerian Perdagangan. Pada pasal 16, dijelaskan bahwa BSML adalah Unit Pelaksana Teknis di Bidang standardisasi penyelenggaraan

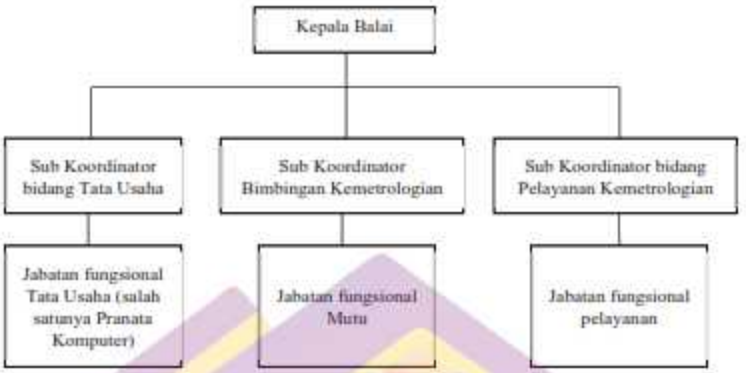
kemetrologian yang berada di bawah dan bertanggung jawab kepada Direktur Metrologi, Direktorat Jenderal Perlndungan Konsumen dan Tertib Niaga.

Pada pasal 17 disebutkan bahwa BSML memiliki tugas verifikasi standar ukuran, uji banding laboratorium metrologi legal, fasilitasi tera dan tera ulang UTTP, penerapan sistem mutu, bimbingan teknis, penyuluhan, pemantauan dan pengawasan kemetrologian.

Pada pasal 18 dijelaskan untuk menjalankan tugas maka BSML menyelenggarakan fungsi yaitu:

1. Penyusunan rencana dan program Balai;
2. Pelaksanaan verifikasi standar satuan ukuran metrologi legal;
3. Pelaksanaan uji banding laboratorium metrologi legal;
4. Fasilitasi tera dan/atau tera ulang UTTP;
5. Penerapan sistem mutu;
6. Fasilitasi pegawai berhak, pengamat tera, pengawas kemetrologian;
7. Pelaksanaan bimbingan teknis di bidang kemetrologian;
8. Pelaksanaan penyuluhan, pemantauan, dan pengawasan kemetrologian; dan
9. Pelaksanaan urusan tata usaha dan rumah tangga Balai.

Struktur Organisasi BSML Regional II



Gambar 2.10. Struktur organisasi BSML Regional II

BSML dikepalai oleh seorang Kepala Balai dan terdiri atas Sub Koordinator bidang Tata Usaha, Sub Koordinator Bimbingan Kemetrologian, Sub Koordinator bidang Pelayanan Kemetrologian, dan kelompok jabatan fungsional. Dalam pasal 20 Permendag yang sama, dijelaskan bahwa Sub Koordinator bidang Tata Usaha mempunyai tugas melakukan penyusunan program, urusan kepegawaian, administrasi keuangan, pelengkapan, pengelolaan Barang Milik Negara, tata persuratan, kearsipan dan rumah tangga Balai. Sub Koordinator bidang Pelayanan Kemetrologian mempunyai tugas melakukan fasilitasi tera/tera ulang UTTP, verifikasi standar ukuran metrologi legal, uji banding laboratorium metrologi legal, dan penerapan sistem mutu. Sedangkan Sub Koordinator Bimbingan Kemetrologian mempunyai tugas melakukan penyuluhan, pemantauan, dan pengawasan kemetrologian, fasilitasi pegawai berhak, pengamat tera, pengawas kemetrologian dan pelaksanaan bimbingan teknis kemetrologian seperti terlihat pada gambar 2.10 di atas.

Dalam rangka mengikuti perkembangan teknologi informasi, pemerintah Indonesia mencanangkan program implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE). Program tersebut berlandaskan Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasi Elektronik. Dalam peraturan tersebut, salah satu hal yang ditekankan adalah tata kelola teknologi informasi dalam rangka implementasi SPBE tertuang pada pasal 4 Perpres tersebut.

Pada Peraturan Menteri Perdagangan Nomor 46/M-DAG/PER/7/2017 tentang Penyelenggaraan Teknologi Informasi dan Komunikasi di Lingkungan Kementerian Perdagangan, pasal 2 menyebutkan bahwa tata kelola *e-government* di lingkungan Kementerian Perdagangan dilaksanakan pada tingkat Kementerian dan Unit Kerja. Di detailkan lagi pada pasal 4 yaitu tata kelola *e-government* pada tingkat unit kerja dilaksanakan oleh setiap unit kerja di lingkungan Kementerian Perdagangan. Dari aturan diatas, BSML Regional II bertanggung jawab atas tata kelola teknologi informasi di unitnya.

BSML Regional II telah mengimplementasikan ISO 9001 tentang ISO 17025 tentang Persyaratan umum kompetensi Laboratorium Pengujian dan Laboratorium Kalibrasi. Dapat dilihat dalam panduan mutu PM-BSML, pada klausul 7.11 tentang pengendalian data dan manajemen informasi dapat dijelaskan sebagai berikut.

Klausul:7.11. Pengendalian Data dan Manajemen Informasi

Klausul:7.11.1. Sistem pengelolaan data dan informasi dikelola secara mandiri dengan ketentuan sebagai berikut:

a. segala dokumen dan rekaman yang terkait penerapan sistem mutu di kelola oleh Tim Mutu
b. segala rekaman yang muncul atas pelayanan verifikasi dikelola oleh Tim Pelayanan Verifikasi
c. dokumen dan rekaman dalam bentuk softcopy disimpan di Server yang dioperasikan pada lingkungan terkondisi dengan hak akses terbatas dan di backup secara berkala
d. dipelihara dengan cara yang menjamin integritas data dan informasi
e. mencakup kegagalan sistem perekaman dan tindakan segera dan tindakan korektif yang sesuai

Klausul: 7.11.2. Instruksi kerja, cerapan, manual peralatan dan referensi yang termutakhir tersedia bagi personil di laboratorium dan Server.

Klausul: 7.11.3. Perhitungan dan transfer data diperiksa secara tepat dan sistematis.

BAB III

METODE PENELITIAN

3.1. Jenis, Sifat, dan Pendekatan Penelitian

Jenis penelitian dalam tesis yang berjudul "Audit Tata Kelola Teknologi Informasi Lembaga Pemerintah Bidang Pelayanan Metrologi menggunakan COBIT 2019 (Studi Kasus: BSML Regional II Kementerian Perdagangan)" adalah studi kasus.

Lalu sifat penelitian ini adalah penelitian deskriptif. Penelitian deskriptif adalah jenis penelitian yang bertujuan menyajikan gambaran lengkap untuk eksplorasi suatu fenomena dengan mendeskripsikan sejumlah variable yang berkenaan dengan unit yang diteliti.

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

3.2. Metode Pengumpulan Data

Pengumpulan data merupakan salah satu faktor penting yang mendukung keberhasilan dalam sebuah penelitian. Proses pengumpulan data berkaitan dengan bagaimana cara mengumpulkan data, siapa sumbernya dan alat apa yang digunakan. Pengumpulan data pada sebuah penelitian membutuhkan beberapa metode yang harus dilakukan dalam rangka untuk mendapatkan hasil penelitian yang maksimal. Secara umum data penelitian terbagi menjadi dua jenis yaitu data

primer dan data sekunder. Data primer merupakan jenis data penelitian yang diperoleh langsung dari sumber yang menjadi objek penelitian. Sedangkan data sekunder merupakan jenis data penelitian yang diperoleh dari berbagai macam sumber, baik melalui dokumen ataupun sejenisnya, namun tetap relevan terhadap objek penelitian. Adapun pengumpulan data primer yang dilakukan pada penelitian ini menggunakan metode wawancara dan kuisioner. Dan data yang dikumpulkan adalah data tingkat kapabilitas proses TI saat ini dan yang diharapkan. Kuesioner pada penelitian ini dilakukan pengumpulan dan pengolahan menggunakan beberapa metode agar mendapatkan hasil yang maksimal. Adapun metode-metode yang digunakan pada penelitian ini antara lain RACI *Chart*. RACI *Chart* merupakan sebuah metode dengan memanfaatkan tabel RACI pada COBIT 2019 untuk melakukan pengolahan data hasil kuisioner. Penggunaan metode ini bertujuan untuk melakukan pemilihan data praktek TI berdasarkan peran (*role*) yang ada pada kuisioner. Pemilihan data praktek TI dilakukan dikarenakan satu praktek TI pada kuisioner dapat diisi oleh 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 proses pemilihan 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 diteliti, sehingga data yang diolah akan lebih valid. Sama halnya seperti pada proses sebelumnya, data dari responden dengan tingkat tanggung jawab *Accountable* 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 selanjutnya adalah melakukan pengolahan dan analisa terhadap data yang ada. Data yang digunakan pada proses ini adalah data hasil wawancara dan survey kuisioner yang telah diberikan dan diisi oleh pihak-pihak yang telah ditentukan.

a. Analisis Kondisi Tingkat Kapabilitas

Analisis Kondisi Tingkat Kapabilitas merupakan proses yang dilakukan untuk mengetahui kondisi tingkat kapabilitas teknologi informasi (TI) 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. Analisis kondisi tingkat kapabilitas saat ini (*as-is*) merupakan sebuah proses untuk mengidentifikasi atau mendapatkan potret kondisi teraktual tingkat kapabilitas TI pada perusahaan. Proses identifikasi pada penelitian ini dilakukan dengan melihat hasil kuisioner yang telah diisi sebelumnya oleh pihak yang telah ditentukan pada perusahaan. Kuisioner yang dibagikan terdiri dari 6 level atau tingkat kapabilitas seperti yang dijelaskan pada bagian CMMI penelitian ini. Tingkat kapabilitas dari

sebuah proses ditentukan atas dasar pencapaian proses atribut tertentu menurut ISO/IEC 15504-2:2003. 3.5.1.2.

b. Analisis Kesenjangan (*Gap*)

Analisis kesenjangan (*gap*) dilakukan dengan tujuan untuk memberikan kemudahan dalam perbaikan tata kelola yang ada. Analisis kesenjangan (*gap*) digunakan untuk melakukan perbandingan antara tingkat kapabilitas pengelolaan teknologi informasi (TI) saat ini (*as-is*) dengan tingkat kapabilitas pengelolaan TI maksimal. Jika hasil analisis kesenjangan (*gap*) menyatakan terdapat kesamaan antara keduanya, maka proses pengelolaan TI perusahaan dinyatakan sudah berjalan dengan baik atau sesuai yang diharapkan. Sebaliknya, jika hasil analisis menyatakan adanya kesenjangan antara tingkat kapabilitas pengelolaan TI saat ini (*as-is*) dengan yang diharapkan maka perlu dilakukannya peningkatan terhadap pengelolaan TI saat ini agar dapat mencapai tingkat kapablitas yang telah ditentukan. Peningkatan tingkat kapabilitas pengelolaan TI saat ini (*as-is*) dapat dilakukan dengan perbaikan terhadap tata kelola TI perusahaan secara meyeluruh atau hanya pada bagian tertentu. Perbaikan tata kelola TI dilakukan berdasarkan informasi mengenai proses-proses mana saja yang memiliki kesenjangan dan membutuhkan perbaikan tata kelola TI dan manajemen pada perusahaan.

c. 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 di lapangan. Agar hasil audit ini tepat dan dapat dipertanggungjawabkan maka diperlukan proses validasi data.

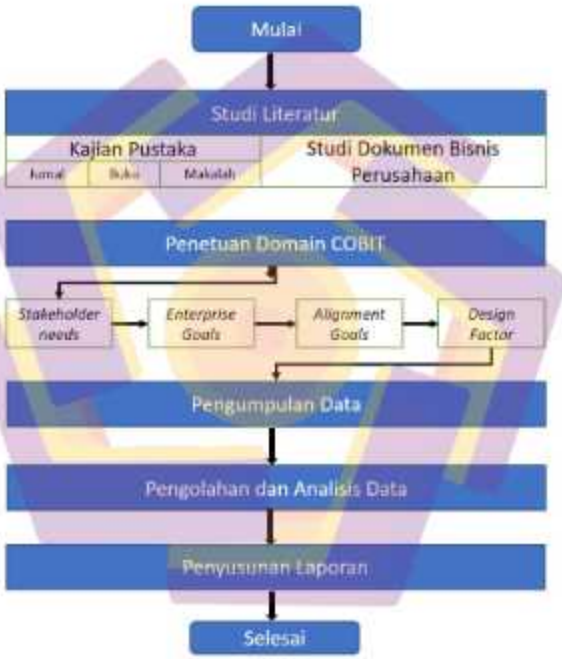
Proses validasi data audit dapat ditempuh menggunakan metode evaluasi dan cek data yang digunakan sebagai input audit oleh komite yang ditunjuk. Seperti yang dilakukan oleh LPMP Jawa Tengah pada laporan evaluasi dan validasi audit mutu sekolah di Jawa Tengah yang diunggah pada halaman web www.lpmp.net yang diakses penulis pada tanggal 8 November 2020. Untuk itu pada penelitian ini akan dilakukan validasi data input audit oleh tim mutu BSML Regional II dan dibuktikan dengan persetujuan hasil audit.

d. Rekomendasi Perbaikan

Dalam proses audit teknologi informasi, rekomendasi perbaikan diperlukan agar kekurangan ataupun kelemahan sumber daya TI perusahaan 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 praktik di setiap domain dan proses TI yang teridentifikasi pada masing-masing level dari tingkat kapabilitas pada COBIT 2019. Pada COBIT 2019 terdapat beberapa pendefinisian dari aktivitas serta praktik yang dapat dijadikan acuan oleh perusahaan 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 Lembaga pemerintah bidang pelayanan metrologi.

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 permasalahan hingga pengambilan kesimpulan. Penelitian mengenai audit tata

kelola teknologi informasi (TI) ini akan dilakukan dalam beberapa tahap seperti terlihat pada gambar 3.1. di atas, yaitu:

a. Studi Literatur

Merupakan sebuah proses pencarian referensi yang relevan terhadap contoh kasus yang ada atau permasalahan yang ditemukan pada penelitian. Referensi yang digunakan dapat berasal dari buku, jurnal, artikel laporan penelitian, dan situs-situs yang ada pada internet. Keluaran atau output yang dihasilkan dari proses ini adalah terkoleksi atau terkumpulnya referensi yang relevan terhadap perumusan masalah dari penelitian. Adapun tujuan dari studi kepustakaan ini adalah untuk memperkuat permasalahan yang ada serta sebagai pendukung dasar teori dalam melakukan studi dan juga menjadi dasar untuk melakukan proses audit tata kelola teknologi informasi. Studi literatur dibagi menjadi 2:

1. Kajian Pustaka. Kajian pustaka merupakan sebuah proses dari penyusunan sebuah laporan penelitian yang diarahkan kepada pencarian dan pengumpulan informasi dan data melalui dokumen-dokumen yang ada. Dokumen tersebut dapat berbentuk dokumen tertulis, foto, gambar, ataupun dokumen elektronik yang dapat mendukung dalam proses penulisan tesis ini.
2. Studi Dokumen Bisnis Perusahaan. Studi dokumen perusahaan merupakan sebuah proses pencarian atau pengumpulan informasi dan data-data mengenai perusahaan yang akan dijadikan objek penelitian. Proses ini dapat dilakukan dengan melakukan wawancara langsung kepada pihak terkait pada perusahaan ataupun dengan mencari referensi dokumen melalui annual

report (laporan tahunan) dan melalui dokumen perusahaan. Tujuan dilaksanakannya studi dokumen perusahaan pada penelitian ini adalah untuk mengetahui dan memahami sejauh mana pengelolaan TI yang sudah berjalan dan penerapan manajemen tata kelola untuk aplikasi operasional perusahaan. Adapun Informasi dan data yang dibutuhkan meliputi visi dan misi, profil departemen yang ada, *standard operational procedure* (SOP) dan struktur organisasi perusahaan. Pelaksanaan studi dokumen ini diharapkan dapat menjadi landasan teori dalam proses penyusunan perumusan masalah pada penelitian ini.

b. Penentuan domain menggunakan COBIT 2019

Pemilihan domain pada COBIT merupakan sebuah proses yang dilakukan untuk mengidentifikasi keadaan dan pencapaian bisnis yang ingin diraih oleh perusahaan yang dipetakan ke dalam beberapa domain berdasarkan panduan COBIT 2019. Proses pemilihan domain pada penelitian ini dilakukan dengan melakukan analisa dokumen dan juga wawancara dengan pihak terkait pada perusahaan. Adapun dokumen yang diteliti dan digunakan sebagai informasi penunjang proses identifikasi adalah visi dan misi perusahaan, tata kelola teknologi informasi (TI) yang digunakan, dan informasi lainnya yang memiliki relevansi terhadap proses audit TI yang dilakukan.

Tahapannya yaitu:

a. Identifikasi *Stakeholder Needs* dan *Enterprise Goal*. Tahap pertama dalam proses pemilihan domain COBIT adalah melakukan identifikasi terhadap

kebutuhan dari pemangku kepentingan dan tujuan bisnis perusahaan, yang pada COBIT 2019 dinyatakan sebagai *Stakeholder Needs* dan *Enterprise Goal*. *Stakeholder Needs* merupakan kebutuhan dari setiap pemangku kepentingan pada perusahaan. Setiap perusahaan memiliki banyak pemangku kepentingan dan pada umumnya perusahaan selalu berusaha untuk menciptakan nilai bagi para pemangku kepentingan mereka. Penciptaan nilai tersebut tentu akan membuat beberapa pertentangan dan perbedaan diantara mereka. Keberadaaan tata kelola adalah tentang bagaimana melakukan negosiasi dan memutuskan antara nilai kebutuhan para pemangku kepentingan yang berbeda dengan melibatkan mereka ketika membuat keputusan terkait manfaat, risiko dan penilaian sumber daya yang ada yang akan dilakukan dengan metode wawancara. Hasil identifikasi kebutuhan stakeholder tersebut dapat digunakan untuk menjadi dasar untuk melakukan identifikasi terhadap Enterprise Goal atau tujuan bisnis yang dimiliki oleh perusahaan. Selanjutnya dilakukan identifikasi Enterpise Goals.

b. Identifikasi *Alignment Goals*, Setelah kebutuhan stakeholder dan tujuan bisnis teridentifikasi, proses selanjutnya adalah melakukan identifikasi terhadap *Alignment Goals* dari perusahaan dengan cara menggunakan tabel COBIT 2019.

c. Identifikasi Domain dan Proses TI. Merupakan tahap terakhir dalam proses pemilihan domain pada COBIT. Caranya 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

c. Pengumpulan data, merupakan tahapan untuk mendapatkan gambaran mengenai kondisi proses TI saat ini yang ada pada perusahaan. Pengumpulan data ini dilakukan melalui proses wawancara dan penyebaran kuisioner kepada *stakeholder* terkait sesuai dengan COBIT 2019

d. Pengolahan dan analisis data, merupakan tahapan untuk mengetahui kondisi tingkat kapabilitas perusahaan. Tahapan ini terdiri dari:

   a. Analisis Tingkat Kapabalitas

   b. Analisis Kesenjangan (Gap)

   c. Penyusunan dan Pemberian Rekomendasi

e. Penyusunan Laporan Penelitian, merupakan tahap terakhir dari penelitian ini. Laporan ini diharapkan dapat menjelaskan kegiatan penelitian secara keseluruhan.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1. Penentuan Domain COBIT

4.1.1. Penentuan Responden

RACI chart dapat membantu auditor 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 perusahaan.

Hasil penentuan responden berdasarkan RACI chart COBIT 2019 dan diimplementasikan pada Organisasi BSML Regional II ditampilkan pada tabel 4.1. sebagai berikut.

Tabel 4.1. Hasil RACI chart secara keseluruhan

No.	RACI Chart pada COBIT 2020	Struktur Organisasi BSML Regional II
1.	Chief Executive Officer adalah orang yang berkedudukan tinggi yang bertanggung jawab atas seluruh manajemen organisasi	Kepala BSML Regional II memiliki tanggung jawab atas seluruh manajemen BSML
2.	Business Process Owner adalah orang yang bertanggung jawab atas perfomansi proses bisnis	Sub Koordinator Bidang Pelayanan Kemetrologian BSML Regional II bertanggung jawab atas proses bisnis BSML Regional II
		Senior Pranata Komputer memiliki tupoksi untuk menjalankan segala aktivitas untuk memastikan performansi bisnis terutam bidang IT
3.	Service Manager adalah struktural yang bertanggung jawab atas pelayanan untuk mendukung kebutuhan bisnis	Sub Koordinator Bagian Tata Usaha BSML Regional II berperan untuk memberikan segala support dan memastikan pelayanan terjamin
4.	Information Security Manager adalah struktural yang bertanggung jawab atas keamanan cyber.	Sub Koordinator Bimbingan Kemetrologian bertanggung jawab atas seluruh tata kelola dan implementasi mutu di BSML

Tabel 4.1. lanjutan

No.	RACI Chart pada COBIT 2020	Struktur Organisasi BSML Regional II
5.	Privacy Officer adalah staf yang bertanggung jawab mengelola kebijakan organisasi, tata kelola, kebutuhan legal	Senior Perencana Ahli BSML Regional II bertugas untuk merancang kebijakan organisasi, serta keterkaitan dengan pemenuhan aturan dan hukum
6.	Head Human Resources adalah struktural yang bertanggung jawab atas sumber daya manusia	Sub Koordinator Bagian Tata Usaha adalah struktural di BSML Regional II yang mengurusi sumber daya manusia

Setelah dilakukan identifkasi responden menggunakan RACI *chart* COBIT 2019, didapatkan 6 responden dalam audit tata kelola teknologi informasi pada BSML Regional II yaitu:

a. Kepala BSML Regional II;
b. Sub Koordinator Bagian Tata Usaha BSML Regional II;
c. Sub Koordinator Bagian Pelayanan Kemetrologian BSML Regional II;
d. Sub Koordinator Bagian Bimbingan Kemetrologian BSML Regional II;
e. Senior Pranata Komputer;
f. Senior Perencana Ahli.

4.1.2. Penentuan *Enterprise Goals* melalui *Stakeholder Needs*

Dalam menentukan domain yang akan menjadi prioritas audit maka dilakukan proses identifikasi *stakeholder needs* pada BSML Regional II. Proses ini dilakukan melalui wawancara dengan Kepala Balai dan didukung dengan aturan Permendag No.60 Tahun 2016 yang menjelaskan tugas pokok dan fungsi Organisasi BSML Regional II. Hasilnya ditampilkan pada tabel 4.2. sebagai berikut.

Tabel 4.2. Kebutuhan *Stakeholder*

Kebutuhan *Stakeholder*	
Kebutuhan	Keterangan
Optimasi Risiko	BSML Regional II sebagai kepanjangan tangan Direktorat Metrologi wajib menjalankan tupoksinya. Dalam menjalankan bisnisnya, optimasi risiko akan memperkecil kerugian dan hambatan.
Optimasi Sumber Daya	Dengan sumber daya yang dimiliki, diharapkan BSML Regional II dapat menjalankan tupoksi dengan optimal guna memastikan layanan metrologi terselenggara dengan baik.

Dilihat dari kebutuhan stakeholder pada tabel 4.2. diatas ada 2 pokok kebutuhan yang teridentifikasi. Selanjutnya dari pokok kebutuhan *stakeholder* didetailkan menjadi *enterprise goals*. Adapun *enterprise goals* BSML Regional II yang teridentifkasi ditampilkan pada tabel 4.3. sebagai berikut.

Tabel 4.3. Hasil pemilihan *Enterprise Goals*

Referensi	*BSC Dimension*	*Enterprise Goals*
EG02	Keuangan	Risiko bisnis yang dikelola
EG06	Pelanggan	Kontinuitas dan ketersediaan layanan bisnis

Sebagai lembaga kalibrasi pemerintah yang membawahi 154 Kabupaten/Kota mulai Pulau Jawa, Bali, NTB dan NTT, BSML Regional II wajib menjaga kontinuitas dan ketersediaan layanan bisnisnya serta meminimalisir atau mengelola risiko bisnis.

4.1.3. Penentuan *Alignment Goals*

Setelah melakukan identifikasi enterprise goals, dengan menggunakan tabel mapping yang telah disediakan COBIT 2019 dilakukan identifikasi 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 ditampilkan pada tabel 4.4 karena dimaksudkan agar nantinya rekomendasi yang berujung pada rencana strategis menjadi lebih fokus.

Tabel 4.4. Hasil identifikasi *alignment goals*

References	*BSC Dimension*	*Alignment Goals*
AG02	Keuangan	Risiko terkait IT yang dikelola
AG07	Internal	Keamanan informasi, infrastruktur, pengolahan dan aplikasi, serta privasi

4.1.4. Penentuan Objek Manajemen dan Tata kelola IT

Keunggulan dari COBIT 2019 dibandingkan dengan COBIT 5 atau versi sebelumnya adalah pada tahap dan metodologi penentuan objek manajemen dan tata kelola IT yang sering disebut sebagai domain atau fokus area. Tabel 4.5. berikut menunjukkan hasil identifikasi faktor desain yang sesuai dengan model bisnis BSML Regional II.

Tabel 4.5. Hasil identifikasi faktor desain

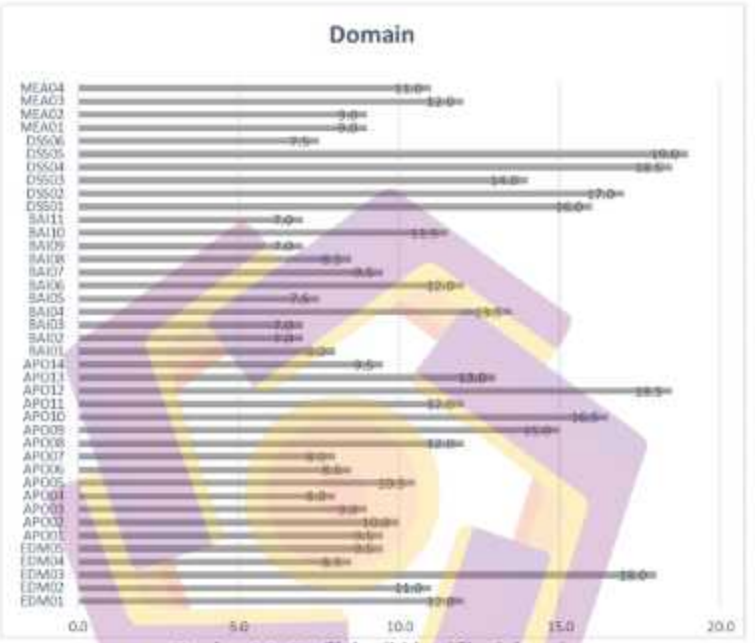
Faktor Desain	Hasil Identifikasi	Keterangan
Strategi Bisnis	*Client Service/ Stability*	Model Bisnis BSML Regional II memiliki fokus kepada kestabilan bisnis dan pelayanan yang berorientasi pada pelanggan
Enterprise Goals	EG02	Risiko bisnis yang dikelola
	EG06	Kontinuitas dan ketersediaan layanan bisnis
Profil risiko perusahaan	*Hardware Incidents*	Dalam menjalankan bisnis, kejadian kerusakan hardware menjadi isu yang penting

Lanjutan Tabel 4.5.

Faktor Desain	Hasil Identifikasi	Keterangan
Permasalahan IT	*Service delivery problems by IT outsourcer (s)*	Permasalahn provider jaringan menjadi salah masalah utama yang terjadi di BSML Regional II
Tantangan	*Normal*	BSML Regional II menjalankan bisnisnya dengan relatif stabil
Kepatuhan terhadap peraturan	*High compliance requiremnets*	Sebagai lembaga pemerintah tentunya kepatuhan terhadap hukum menjadi wajib hukumnya. Segala aktifitas selalu berdasarkan peraturan.
Peran IT	*Factory*	Ketika terjadi permasalahan pada IT akan memberi dampak langsung pada proses bisnis namun bukan menjadi core bisnis dari BSML Regional II
Source Model IT	*Insourced*	BSML Regional II menyediakan dan mengupayakan IT secara mandiri dengan PDSI sebagai pusatnya
Model Implementasi IT	*Traditional*	Pengembangan IT (termasuk *software*) secara tradisional dan *software* dikembangkan tanpa mempengaruhi bisnis
Strategi mengadopsi teknologi	*Slow Adopter*	Dalam mengadopsi teknologi menunggu teknologi tersebut menjadi *mainstream* dan cenderung lambat
Size Bisnis	*Small Enterprise*	Jumlah pegawai tetap BSML Regional II antara 50 hingga 250 pekerja

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.

Dari 11 faktor desain diatas lalu dilakukan proses identifikasi domain. Adapun hasil identifikasi domain ditampilkan gambar 4.1. sebagai berikut.



Gambar 4.1. Grafik hasil identifikasi domain

Setelah dilakukan pembobotan maka terpilih 5 (lima) domain peringkat teratas. Hal itu menunjukkan bahwa 5 (lima) domain tersebut memiliki peranan penting dalam tata kelola teknologi informasi di perusahaan (ISACA,2019). Untuk itu dalam penelitian ini dipilihlah 5 domain tersebut untuk dilakukan audit. Kelima domain tersebut adalah sebagai berikut:

1. EDM 03 *Ensured Risk Optimization*

   Tujuan dari domain EDM 03 adalah untuk memastikan bahwa risiko perusahaan terkait I & T tidak melebihi batas risiko yang dijinkan oleh

perusahaan dan meminimalkan kegagalan operasional IT. BSML Regional II yang melayani 154 Kabupaten/Kota yang tersebar di Pulau Jawa, Bali, kepulauan NTB, dan NTT maka perlu memastikan layanannya berjalan dengan baik dan lancar yang salah satu pendukungnya adalah IT.

2. APO 12 *Managed Risk*

   Tujuan dari APO 12 adalah mengintegrasikan manajemen IT dengan manajemen perusahaan secara keseluruhan terutama terkait risiko IT dan memaksimalkan pengelolaan risiko IT. Dengan menginterasikan manajemen IT terutama terkait risiko, BSML Regional II dapat memaksimalkan pengelolaan risiko IT terutama dalam rangka percepatan implementasi Sistem Pemerintah Berbasis Elektronik.

3. DSS 02 *Managed Service Request and Incidents*

   Tujuan dari DSS 02 adalah untuk mencapai meningkatkan produktivitas dan meminimalkan insiden. BSML Regional II dengan renstranya dalam rangka peningkatan layanan metrologi di era industri 4.0 perlu melakukan pemenuhan domain ini.

4. DSS 04 *Managed Continuity*

   Tujuan dari DSS 04 adalah bagaimana mempertahankan layanan yang bekelanjutan dan mempertahankan kesigapan jika terjadi gangguan yang signifikan. Hal itu sejalan dengan peran BSML Regional II yang salah satu tugasnya adalah memberikan layanan verifikasi dalam rangka menjaga ketertelusuran standar nasional, maka sangat penting untuk menjaga layanan berkelanjutan.

5. DSS 05 *Managed Security Services*

Tujuan dari DSS 05 adalah meminimalkan dampak bisnis dari keamanan informasi operasional terkait insiden dan kerentanan. Sebagai lembaga pemerintah yang berhubungan dengan banyak stakeholder maka BSML Regional II perlu menjaga proses bisnisnya dari kerentanan dan insiden. Terlebih data yang dikelola oleh BSML Regional II merupakan data milik UPT seluruh Kabupaten/Kota yang ada di wilayah Pulau Jawa, Bali, dan Kepulauan Nusa Tenggara.

4.2. Perencanaan Asesmen

Pada tahap perencanaan asesmen, akan dijelaskan daftar responden untuk pelaksanaan audit sesuai dengan COBIT 2019. Dalam menentukan hasil responden, acuan yang digunahakan adalah struktur organisasi yang ada pada BSML Regional II yang akan disesuaikan dengan RACI chart yang dianjurkan oleh COBIT 2019.

Dalam RACI chart, hanya yang memiliki peran responsible yang akan dijadikan responden evaluasi. Hal ini karena peran responsible merupakan orang yang bertanggung jawab dalam mendapatkan tugas dan melakukan tugas tersebut dan juga memastikan aktifitas atau kegiatan operasional berjalan sukses. Berikut daftar responden pada domain 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* pada audit BSML Regional II.

4.2.1. Hasil Responden pada Objek EDM 03 *Ensured Risk Optimization*

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang akan ikut serta dalam pelaksanaan audit domain EDM 03 *Ensured Risk Optimization* adalah dapat ditunjukkan pada gambar 4.2 di bawah ini.

Gambar 4.2. RACI chart EDM 03 *Ensured Risk Optimization*

Jabatan-jabatan yang bertanda R memiliki arti responsible yaitu merupakan responden yang bertanggung jawab pada aktivitas domain ini. Diharapkan responden yang memang melakukan aktivitas sesuai dengan area audit sehingga hasil audit tepat dan dapat dipertanggungjawabkan. Pada Organisasi BSML Regional II untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar di atas akan dijabarkan konversinya pada tabel 4.6. di bawah ini.

Tabel 4.6. Hasil identifikasi responden EDM 03

No.	RACI Chart EDM 03 pada COBIT 2020	Struktur Organisasi BSML Regional II
1.	Executive Commitee	-
2.	Chief Executive Officer adalah orang yang berkedudukan tinggi yang bertanggung jawab atas seluruh manajemen organisasi	Kepala BSML Regional II memiliki tanggung jawab atas seluruh manajemen BSML
3.	Chief Risk Officer	-
4.	Chief Information Officer	-
5.	I&T Governance Board	-

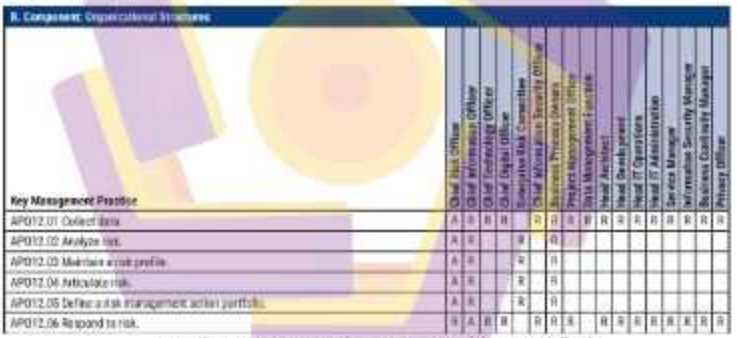
Tabel 4.6. Hasil identifikasi responden EDM 03 (lanjutan)

No.	RACI Chart EDM 03 pada COBIT 2020	Struktur Organisasi BSML Regional II
6.	Enterprise Risk Komitee	-
7.	Chief Information Security Officer	-

Berdasarkan RACI *chart* yang sudah disesuaikan pada jabatan fungsional pada BSML Regional II didapatkan 1 (satu) responden dari 7 (tujuh) peran yang direkomendasikan COBIT 2019.

4.2.2. Hasil Responden pada Objek APO 12 *Managed Risk*

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang akan ikut serta dalam pelaksanaan audit domain APO 12 *Managed Risk* adalah dapat ditunjukkan pada gambar 4.3. di bawah ini.



Gambar 4.3. RACI chart APO 12 *Managed Risk*

Seperti pada domain EDM 03, 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 dipertanggungjawabkan. Pada Organisasi BSML Regional II untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar di atas akan dijabarkan konversinya pada tabel 4.7. di bawah ini.

Tabel 4.7. Hasil identifikasi responden APO 12

No.	RACI Chart APO 12 pada COBIT 2020	Struktur Organisasi BSML Regional II
1.	Chief Information Officer	-
2.	Chief Technology Officer	-
3.	Chief Digital Officer	-
4.	Enterprise Risk Komitee	-
5.	Chief Information Security Officer	-
6.	Business Process Owner adalah orang yang bertanggung jawab atas perfomansi proses bisnis	Sub Koordinator Bidang Pelayanan Kemetrologian BSML Regional II bertanggung jawab atas proses bisnis BSML Regional II
		Senior Pranata Komputer memiliki tupoksi untuk menjalankan segala aktivitas untuk memastikan performansi bisnis terutam bidang IT
7.	Project Management Office dan Data Management Function	-
8.	Head Arcithect and Development	-
9.	Head IT Operation And Administration	-
10.	Service Manager adalah struktural yang bertanggung jawab atas pelayanan untuk mendukung kebutuhan bisnis	Sub Koordinator Bagian Tata Usaha BSML Regional II berperan untuk memberikan segala support dan memastikan pelayanan terjamin
11.	Information Security Manager adalah struktural yang bertanggung jawab atas keamanan cyber.	Sub Koordinator Bimbingan Kemetrologian bertanggung jawab atas seluruh tata kelola dan implementasi mutu di BSML
12.	Business Continuity Manager	-
13.	Privacy Officer adalah staf yang bertanggung jawab mengelola kebijakan organisasi, tata kelola, kebutuhan legal	Senior Perencana Ahli BSML Regional II bertugas untuk merancang kebijakan organisasi, serta keterkaitan dengan pemenuhan aturan dan hukum

Berdasarkan RACI *chart* yang sudah disesuaikan pada jabatan fungsional pada BSML Regional II didapatkan 5 (lima) responden dari 13 (tiga belas) peran yang direkomendasikan COBIT 2019.

4.2.3. Hasil Responden pada Objek DSS 02 *Managed Service Request and Incidents*

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang akan ikut serta dalam pelaksanaan audit domain DSS 02 *Managed Service Request and Incidents* adalah dapat ditunjukkan pada gambar 4.4. di bawah ini.

B. Component: Organizational Structures						
Key Management Practice	Chief Technology Officer	Business Process Owners	Head Development	Head IT Operations	Service Manager	Information Security Manager
DSS02.01 Define classification schemes for incidents and service requests.	A		R	R	R	
DSS02.02 Record, classify and prioritize requests and incidents.	A			R	R	
DSS02.03 Verify, approve and fulfill service requests.	A	R	R	R	R	
DSS02.04 Investigate, diagnose and allocate incidents.	A	R		R	R	
DSS02.05 Resolve and recover from incidents.	A		R	R	R	R
DSS02.06 Close service requests and incidents.	A			R	R	R
DSS02.07 Track status and produce reports.	A			R	R	

Gambar 4.4. RACI chart DSS 02 *Managed Service Request and Incidents*

Seperti pada domain EDM 03, 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 dipertanggungjawabkan. Pada Organisasi BSML Regional II untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar di atas akan dijabarkan konversinya pada tabel 4.8. di bawah ini.

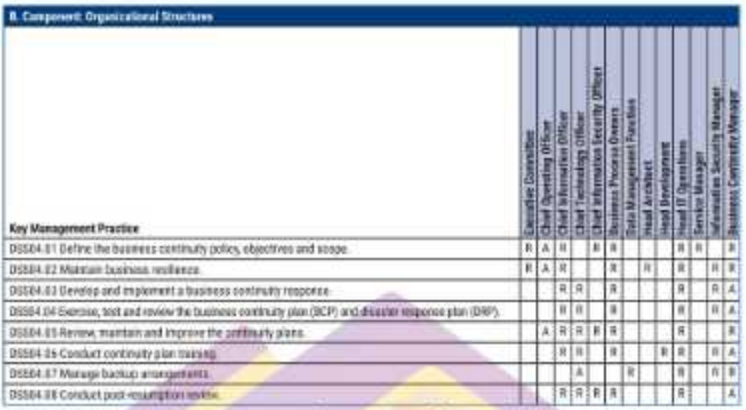
Tabel 4.8. Hasil identifikasi responden DSS 02

No.	RACI Chart DSS 02 pada COBIT 2020	Struktur Organisasi BSML Regional II
1.	Business Process Owner adalah orang yang bertanggung jawab atas perfomansi proses bisnis	Sub Koordinator Bidang Pelayanan Kemetrologian BSML Regional II bertanggung jawab atas proses bisnis BSML Regional II
		Senior Pranata Komputer memiliki tupoksi untuk menjalankan segala aktivitas untuk memastikan performansi bisnis terutam bidang IT
2.	Head Development	-
3.	Head IT Operation	-
4.	Service Manager adalah struktural yang bertanggung jawab atas pelayanan untuk mendukung kebutuhan bisnis	Sub Koordinator Bagian Tata Usaha BSML Regional II berperan untuk memberikan segala support dan memastikan pelayanan terjamin
5.	Information Security Manager adalah struktural yang bertanggung jawab atas keamanan cyber.	Sub Koordinator Bimbingan Kemetrologian bertanggung jawab atas seluruh tata kelola dan implementasi mutu di BSML

Berdasarkan RACI *chart* yang sudah disesuaikan pada jabatan fungsional pada BSML Regional II didapatkan 4 (empat) responden dari 5 (lima) peran yang direkomendasikan COBIT 2019.

4.2.4. Hasil Responden pada Objek DSS 04 *Managed Continuity*

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang akan ikut serta dalam pelaksanaan audit domain DSS 04 *Managed Continuity* adalah dapat ditunjukkan pada gambar 4.5. di bawah ini.



B. Component: Organizational Structures																
Key Management Practice	Executive Committee	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Chief Information Security Officer	Business Process Owners	Data Management Function	Head Architect	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager
DSS04.01 Define the business continuity policy, objectives and scope.	R	A	R		R	R				R	R		R
DSS04.02 Maintain business resilience.	R	A	R			R		R		R		R	R
DSS04.03 Develop and implement a business continuity response.			R	R		R				R		R	A
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).			R	R		R				R		R	A
DSS04.05 Review, maintain and improve the continuity plans.		A	R	R	R	R				R			R
DSS04.06 Conduct continuity plan training.			R	R		R			R	R		R	A
DSS04.07 Manage backup arrangements.				A			R			R		R	R
DSS04.08 Conduct post-resumption review.			R	R	R	R				R			A

Gambar 4.5. RACI chart DSS 04 *Managed Continuity*

Seperti pada domain EDM 03, 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 dipertanggungjawabkan. Pada Organisasi BSML Regional II untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar di atas akan dijabarkan konversinya pada tabel 4.9. di bawah ini.

Tabel 4.9. Hasil identifikasi responden DSS 04

No.	RACI Chart DSS 04 pada COBIT 2020	Struktur Organisasi BSML Regional II
1.	Executive Commitee	-
2.	Chief Information Officer	-
3.	Chief Technology Officer	-
4.	Chief Information Security Officer	-

Tabel 4.9 (lanjutan)

No.	RACI Chart DSS 04 pada COBIT 2020	Struktur Organisasi BSML Regional II
5.	Business Process Owner adalah orang yang bertanggung jawab atas perfomansi proses bisnis	Sub Koordinator Bidang Pelayanan Kemetrologian BSML Regional II bertanggung jawab atas proses bisnis BSML Regional II
		Senior Pranata Komputer memiliki tupoksi untuk menjalankan segala aktivitas untuk memastikan performansi bisnis terutam bidang IT
6.	Data Management Function	-
7.	Head Arcithect and Development	-
8.	Head IT Operation	Sub Koordinator Bagian Tata Usaha BSML Regional II sebagai atas Senior Pranata Komputer
9.	Service Manager adalah struktural yang bertanggung jawab atas pelayanan untuk mendukung kebutuhan bisnis	Sub Koordinator Bagian Tata Usaha BSML Regional II berperan untuk memberikan segala support dan memastikan pelayanan terjamin
10.	Information Security Manager adalah struktural yang bertanggung jawab atas keamanan cyber.	Sub Koordinator Bimbingan Kemetrologian bertanggung jawab atas seluruh tata kelola dan implementasi mutu di BSML
11.	Business Continuity Manager	-

Berdasarkan RACI *chart* yang sudah disesuaikan pada jabatan fungsional pada BSML Regional II didapatkan 4 (empat) responden dari 11 (sebelas) peran yang direkomendasikan COBIT 2019, karena ada beberapa jabatan BSML Regional II yang memiliki fungsi atau peran lebih dari satu.

4.2.5. Hasil Responden pada Objek DSS 05 *Managed Security Services*

Sesuai dengan hasil pemetaan RACI chart yang ada pada COBIT 2019, responden yang akan ikut serta dalam pelaksanaan audit domain DSS 05 *Managed Security Services* adalah dapat ditunjukkan pada gambar 4.6. di bawah ini.

B. Component: Organizational Structures								
Key Management Practice	Chief Executive 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 IT 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 4.6. RACI chart DSS 05 *Managed Security Services*

Seperti pada domain EDM 03, 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 dipertanggungjawabkan. Pada Organisasi BSML Regional II untuk jabatan-jabatan sesuai dengan yang telah disebutkan pada gambar di atas akan dijabarkan konversinya pada tabel 4.10. di bawah ini.

Tabel 4.10. Hasil identifikasi responden DSS 05

No.	RACI Chart DSS 05 pada COBIT 2020	Struktur Organisasi BSML Regional II
1.	Business Process Owner adalah orang yang bertanggung jawab atas perfomansi proses bisnis	Sub Koordinator Bidang Pelayanan Kemetrologian BSML Regional II bertanggung jawab atas proses bisnis BSML Regional II
		Senior Pranata Komputer memiliki tupoksi untuk menjalankan segala aktivitas untuk memastikan performansi bisnis terutam bidang IT
2.	Head Human Resources	-
3.	Head Development	-
4.	Head IT Operation	Sub Koordinator Bagian Tata Usaha BSML Regional II sebagai atas Senior Pranata Komputer
5.	Information Security Manager adalah struktural yang bertanggung jawab atas keamanan cyber.	Sub Koordinator Bimbingan Kemetrologian bertanggung jawab atas seluruh tata kelola dan implementasi mutu di BSML
6.	Privacy Officer adalah staf yang bertanggung jawab mengelola kebijakan organisasi, tata kelola, kebutuhan legal	Senior Perencana Ahli BSML Regional II bertugas untuk merancang kebijakan organisasi, serta keterkaitan dengan pemenuhan aturan dan hukum

Berdasarkan RACI *chart* yang sudah disesuaikan pada jabatan fungsional pada BSML Regional II didapatkan 5 (lima) responden dari 6 (enam) peran yang direkomendasikan COBIT 2019.

4.3. Briefing dan Pengumpulan Data

Pada tahap breafing akan dijelaskan mengenai proses audit yang akan dilakukan di BSML Regional II. Para responden yang telah disebutkan pada sub bab sebelumnya diberikan penjelasan mengenai tahapan audit menggunakan framework COBIT 2019. Penjelasan ini terdiri dari penjelasan cara pengisian kuesioner dan maksud dari setiap pernyataan yang ada pada kuesioner. Domain yang akan menjadi fokus area audit 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*.

Tujuan dari briefing ini adalah agar responden paham dan mengetahui pelaksanaan audit tata kelola teknologi informasi pada BSML Regional II, responden tidak salah dalam memberikan keterangan kepada auditor sehingga kegiatan audit ini sesuai dengan kondisi yang sebenarnya.

Adapun jadwal briefing dan pengumpulan data dapat dilihat pada tabel 4.11. di bawah ini.

Tabel 4.11. Jadwal Kegiatan Audit Tata Kelola Teknologi Informasi pada BSML Regional II

No.	Kegiatan	Waktu Pelaksanaan
	Persiapan:	
1	Melakukan Koordinasi dengan pihak terkait untuk membahas rencana audit yang akan dilakukan	1 Desember 2020
2	Menyiapkan dokumentasi yang berkaitan dengan audit (Lembar kerja, wawancara, dll)	1 Desember 2020
	Pendahuluan:	
3	Melakukan sosialisasi dengan pihak terkait untuk kegiatan audit yang akan dilakukan	2 Desember 2020

Tabel 4.11(lanjutan)

No.	Kegiatan	Waktu Pelaksanaan
4	Mengumpulkan dokumentasi berkaitan dengan audit yang akan dilakukan seperti • Rencana Strategis (Renstra) • Panduan Mutu • Struktur Organisasi dan Tata Kerja (SOTK) • Standar Operasional Prosedur (SOP) • dll	3-4 Desember 2020
5	Melakukan review terhadap dokumentasi yang berkaitan	7 Desember 2020
	Pelaksanaan :	
6	Melakukan Wawancara (interview) dengan pimpinan Laboratorium Kalibrasi BSML Regional II	8 Desember 2020
7	Melakukan observasi langsung ke Kementerian Pekerjaan Umum dan Perumahan Rakyat	9 Desember 2020
8	Mengunpulkan data melalui survey yang dibuat untuk diisi oleh pimpinan dan staff dapat dibantu melalui wawancara	10 Desember 2020
9	Melakukan penilaian tingkat kapabilitas tata kelola teknologi informasi pada BSML Regional II	11 Desember 2020
10	Melakukan klarifikasi hasil Audit	14 Desember 2020
	Pelaporan:	
11	Membuat laporan hasil audit dan rekomendasi untuk perbaikan ketidaksesuaian	15 - 30 Desember 2020

4.4. Hasil Audit dan Analisa Data

Pada audit periode ini, dengan memperhatikan kewajiban, kebutuhan dan kemampuan, BSML melalui tim mutu menetapkan target tingkat kapabilitas pada level 2 (dua) sebagaimana tertuang dalam surat pernyataan Ketua Tim Mutu (surat terlampir). Dan hal itu sesuai dengan rekomendasi dari ISACA dalam panduan COBIT yaitu penetapan target harus achieveable dan step by step.

Setelah dilakukan audit tata kelola teknologi informasi pada objek penelitian baik menggunakan metode wawancara maupun kuesioner, maka dilakukan identifikasi hasil audit dan dikelola sehingga dapat dilakukan analisa. Dengan menggunakan CMMI (*Capability Maturity Model Integration*) tingkat kapabilitas dapat didefinisikan 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 terstandardisasi, tidak tergantung pada orang
4. Defined – nilai 3, memiliki arti bahwa setiap kegiatan/aktivitas sudah tercantum dalam intruksi kerja atau SOP, proses menjadi lebih stabil dan berulang, diharapkan hasilnya konsisten;
5. Quantitative – nilai 4, memiliki arti bahwa setiap kegiatan sudah memiliki tujuan yang terukur untuk kualitas dan prduktivitasnya, salah satu cirinya adalah sudah ada *activity based costing*;
6. Optimized – nilai 5, memiliki arti bahwa proses pengembangan sistem terstandardisasi secara kontinu dimonitor dan ditingkatkan berdasarkan analisa atau evaluasi. Cirinya adalah adanya mekanisme pencegahan kegagalan, mekanisme evaluasi dan peningkatan kualitas proses.

Penilaian ini yang akan menjadi tolok ukur dalam melakukan analisa tingkat kapabilitas tata kelola teknologi informasi pada BSML Regional II Kementerian Perdagangan.

Berikut hasil audit pada masing-masing domain yang terpilih.

4.4.1. Hasil Rekapitulasi Audit pada Domain EDM 03 *Ensure Risk Optimization*

a. EDM 03.01 *Evaluate risk management*

Tabel 4.12. Hasil Rekapitulasi kuesioner EDM 03.01

No	Deskripsi	Skor Input as is
1	Memahami organisasi dan konteksnya yang terkait dengan risiko I&T.	1
2	Mentukan kebijakan risiko organisasi, yaitu tingkat risiko terkait I & T yang ditetapkan oleh perusahaan untuk mencapai tujuan perusahaan.	1
3	Mentukan tingkat toleransi risiko terhadap kebijakan risiko, yaitu penyimpangan yang masih ditoleransi	0
4	Menentukan sejauh mana penyelarasan strategi risiko I&T dengan strategi risiko perusahaan dan memastikan kebijakan risiko berada di bawah kapasitas risiko organisasi	1
5	Secara proaktif mengevaluasi faktor risiko I&T sebelum keputusan strategis perusahaan dan memastikan bahwa pertimbangan risiko merupakan bagian dari proses keputusan strategis perusahaan.	1
6	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan mengenai kerugian terkait I & T dan toleransinya	1
7	Mempertahankan personel yang diperlukan untuk mengelola Manajemen Risiko I&T	0
	rata-rata	0.71

Berdasarkan hasil tabel 4.12 di atas, audit EDM 03.01 dilakukan pada 1 responden yaitu Kepala Balai SML Regional II dan menilai kondisi saat ini berada pada tingkat kapabilitas 0.71 atau tingkat 1. Fakta yang ditemukan adalah:

1. BSML Regional II telah mencoba memahami risiko IT melalui dokumen laporan ketidaksesuaian Tahun 2020;
2. Namun BSML Regional II belum menentukkan profil risiko IT;
3. Kepala BSML Regional II belum menunjuk secara spesifik personel yang mengelola manajemen risiko IT.

b. EDM 03.02 *Direct risk management*

Tabel 4.13. Hasil Rekapitulasi kuesioner EDM 03.02

No	Deskripsi	Skor Input as is
1	Memastikan integrasi strategi risiko I&T ke dalam penerapan manajemen risiko dan kegiatan operasional.	1
2	Mengarahkan pengembangan komunikasi risiko (mencakup semua tingkatan perusahaan).	1
3	Penerapan langsung dari mekanisme yang sesuai untuk merespon dengan cepat terhadap perubahan risiko dan segera melaporkannya tingkat manajemen yang sesuai, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana dan bagaimana).	1
4	Arahkan bahwa risiko, peluang, masalah, dapat diidentifikasi dan dilaporkan oleh siapa pun kepada pihak yang sesuai kapanpun. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan	1
5	Identifikasi tujuan utama dari tata kelola risiko dan proses manajemen yang akan dipantau, dan identifikasi metode pengolahan data	1
	rata-rata	1

Berdasarkan hasil tabel 4.13 di atas, audit EDM 03.02 dilakukan pada 1 responden yaitu Kepala Balai SML Regional II dan menilai kondisi saat ini berada pada tingkat kapabilitas 1. Fakta yang ditemukan adalah:

1. BSML Regional II telah melakukan perencanaan penerapan strategi risiko IT dengan membuat klausul 7.11. pada dokumen Panduam Mutu PM-BSML II (Rev.01);
2. Belum ditemukan bukti penerapan strategi risiko pada IT kegiatan operasional;
3. BSML Regional II telah mencoba mengidentifikasi risiko melalui dokumen identifikasi risiko dan peluang BSML II.

c. EDM 03.03 *Monitor risk management*

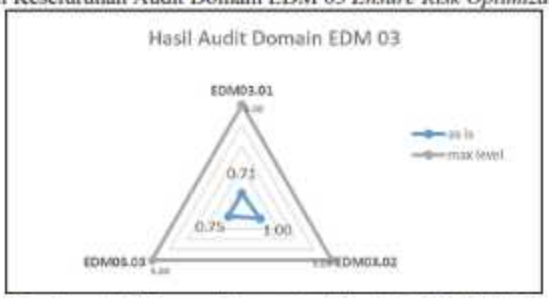
Tabel 4.14. Hasil Rekapitulasi kuesioner EDM 03.03

No	Deskripsi	Skor Input
		as is
1	Laporkan masalah manajemen risiko kepada dewan atau komite eksekutif.	1
2	Pantau sejauh mana profil risiko dikelola dalam kebijakan risiko dan ambang batas toleransi perusahaan	1
3	Pantau tujuan utama tata kelola risiko dan proses manajemen terhadap target, analisis penyebab penyimpangan, dan memulai tindakan perbaikan untuk mengatasi penyebab yang mendasarinya.	0
4	Memungkinkan peninjauan pemangku kepentingan atas kemajuan perusahaan menuju tujuan yang diidentifikasi	1
	rata-rata	0.75

Berdasarkan hasil tabel 4.14 di atas, audit EDM 03.03 dilakukan pada 1 responden yaitu Kepala Balai SML Regional II dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,75 atau tingkat 1. Fakta yang ditemukan adalah:

1. Kepala BSML Reginal II melaporkan segala kegiatan melalui dokumen pelaporan bulanan kepada Direktur Metrologi;
2. BSML Regional II melalui dokumen identifikasi risiko dan peluang, telah merencanakan pemantauan risiko namun belum diterapkan.

d. Hasil Keseluruhan Audit Domain EDM 03 *Ensure Risk Optimization*



Gambar 4.7. Diagram Representasi Hasil Audit EDM 03

Berdasarkan diagram representasi pada gambar 4.7. di atas diperoleh kesimpulan bahwa tingkat kapabilitas pada domain EDM 03 *Ensure Risk Optimization* 0,82 atau pada level 1 artinya proses EDM 03 sudah dilakukan namun belum terencana dan belum terdokumentasikan dengan baik. Adapun target yang ingin dicapai yaitu tingkat kapabilitas level 2, sehingga terdapat gap. Rekomendasi pada domain EDM 03 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

4.4.2. Hasil Rekapitulasi Audit pada Domain APO 12 *Managed Risk*

a. APO 12.01 *Collect Data*

Tabel 4.15. Hasil Rekapitulasi kuesioner APO 12.01

No	Deskripsi	Skor Input				
		as is				
		1	2	3	4	5
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko I&T.	0	1	0	1	1
2	Catat data terkait risiko I&T yang relevan dan signifikan di lingkungan internal dan eksternal perusahaan	1	1	1	0	0
3	Mengadopsi atau mendefinisikan risiko untuk definisi yang konsisten dari skenario risiko dan dampak	1	0	1	1	1
4	Catat data tentang peristiwa risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak.	1	0	1	1	1
5	Survei dan analisis data risiko I&T terkait kerugian dari data dan tren yang tersedia secara eksternal	0	1	1	1	0
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi umum faktor di berbagai peristiwa.	0	0	0	0	1
7	Tentukan kondisi spesifik yang dapat mempengaruhi risiko.	1	1	1	1	1

Tabel 4.15 (lanjutan)

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
8	Lakukan analisis faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.	0	1	1	1	1
		0.50	0.63	0.75	0.75	0.75
rata-rata		0.68				

Berdasarkan hasil tabel 4.15 di atas, audit APO 12.01 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,68 atau tingkat 1. Fakta yang ditemukan adalah:

1. BSML Regional II telah merancang kegiatan pencatatan data sesuai klausul 7.11. PM-BSML II;
2. Pencatatan data dan insiden dilakukan oleh pranata komputer sebagai bagian dari laporan kerja harian pegawai belum sebagai produk organisasi;

b. APO 12.02 *Analyze Risk*

Tabel 4.16. Hasil Rekapitulasi kuesioner APO 12.02

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
1	Menentukan cakupan yang tepat dari upaya analisis risiko, dengan mempertimbangkan semua faktor risiko.	1	1	1	0	0
2	Membangun dan memperbarui skenario risiko I&T secara teratur; identifikasi kerugian terkait I & T	0	0	0	1	1

Tabel 4.16 (lanjutan)

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	1	1	1	1	1
4	Bandingkan risiko saat ini (ekspostur kerugian terkait I & T) dengan toleransi risiko yang dapat diterima.	0	1	1	1	1
5	Mengusulkan respons risiko untuk risiko yang melebihi tingkat toleransi.	1	1	1	1	1
6	Identifikasi persyaratan dan target untuk respons mitigasi risiko yang optimal.	1	0	0	0	0
7	Validasi hasil analisis risiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	1	1	0	0	1
8	Menganalisis manfaat dari opsi respons risiko yang dipilih. Konfirmasikan respons risiko yang optimal.	1	0	1	0	1
		0.75	0.63	0.63	0.50	0.75
	rata-rata	0.65				

Berdasarkan hasil tabel 4.16 di atas, audit APO 12.02 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,65 atau tingkat 1. Fakta yang ditemukan adalah:

1. Pada dokumen identifikasi risiko dan peluang, BSML Regional II sudah mencoba memetakan risiko namun belum dilakukan analisa;
2. Belum adanya informasi respon pada setiap identifikasi risiko sehingga belum dapat dibuktikan perencanaan respon terhadap risiko yang ada;

c. APO 12.03 *Maintain A Risk Profile*

Tabel 4.17. Hasil Rekapitulasi kuesioner APO 12.03

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
1	Menginventarisir proses bisnis dan proses manajemen layanan IT. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.	1	1	1	0	0
2	Menentukan dan menyetujui layanan IT dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.	1	1	1	1	1
3	Mengumpulkan skenario risiko saat ini menurut kategori, lini bisnis, dan area fungsional.	1	0	1	1	1
4	Secara teratur menangkap semua informasi profil risiko dan menggabungkannya ke dalam profil risiko gabungan.	1	1	0	1	1
5	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	1	0	1	1	1
6	Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini secara cepat.	1	1	1	1	0
7	Menangkap informasi tentang peristiwa risiko IT yang telah terwujud untuk dimasukkan dalam profil risiko IT perusahaan.	0	0	0	1	1
		0.86	0.57	0.71	0.86	0.71
rata-rata		0.74				

Berdasarkan hasil tabel 4.17 di atas, audit APO 12.03 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,74 atau tingkat 1. Fakta yang ditemukan adalah:

1. Penentuan layanan IT dan manajemennya merupakan bagian dari kegiatan layanan perkantoran dalam kertas kerja BSML Regional II dan

itu menjadi tupoksi Sub Koordinator Tata Usaha, namun belum ditemukan dokumen proses yang tertuang;

2. Belum ditemukan proses adopsi atau analisis dari contoh manajemen IT hasil *benchmarking* atau interkomparasi.

d. APO 12.04 *Articulate Risk*

Tabel 4.18. Hasil Rekapitulasi kuesioner APO 12.04

No	Deskripsi	Skor Input				
		as is				
		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 perusahaan.	1	1	1	1	1
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait IT.	1	1	1	1	1
3	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, dan gap.	1	1	1	1	1
4	Secara berkala, identifikasi peluang terkait IT yang akan memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan.	1	1	1	0	1
5	Meninjau hasil penilaian pihak ketiga yang obyektif dan audit internal. Sertakan mereka di profil risiko.	1	1	1	1	1
		1	1	1	0.8	1
rata-rata		0.96				

Berdasarkan hasil tabel 4.18 di atas, audit APO 12.04 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,96 atau tingkat 1. Fakta yang ditemukan adalah:

1. Proses identifikasi risiko dan peluang dalam proses bisnis telah dilakukan dan terdokumentasi, pelaporan kepada *stakeholder* disampaikan dalam kegiatan audit internal;
2. Belum ditemukan format pelaporan profil dan manajemen risiko IT pada BSML Regional II.

e. APO 12.05 *Define a risk management action portfolio*

Tabel 4.19 Hasil Rekapitulasi kuesioner APO 12.05

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
1	Klasifikasikan aktivitas pengendalian dan petakan pada skenario risiko IT.	0	1	1	0	1
2	Tentukan apakah setiap entitas organisasi memantau risiko dan memiliki peran.	1	1	1	1	1
3	Buat proposal proyek yang dirancang untuk mengurangi risiko dan / atau proyek yang memiliki peluang dengan mempertimbangkan risiko IT	1	1	0	1	0
		0.67	1	0.67	0.67	0.67
rata-rata		0.73				

Berdasarkan hasil tabel 4.19 di atas, audit APO 12.05 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,73 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 4.20. Hasil Rekapitulasi kuesioner APO 12.06

No	Deskripsi	Skor Input as is				
		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.	0	0	1	1	1
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	0
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	0	0	1
		0.6	0.6	0.8	0.8	0.8
rata-rata		0.72				

Berdasarkan hasil tabel 4.20 di atas, audit APO 12.06 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,72 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*

Gambar 4.8. Diagram Representasi Hasil Audit APO 12

Berdasarkan diagram representasi pada gambar 4.8. di atas diperoleh kesimpulan bahwa tingkat kapabilitas pada domain APO 12 *Managed Risk* sebesar 0,75 atau pada level 1 artinya proses APO 12 sudah dilakukan namun belum terencana dan belum terdokumentasikan dengan baik. Adapun target yang ingin dicapai yaitu tingkat kapabilitas level 2, sehingga terdapat gap. Rekomendasi pada domain APO 12 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

4.4.3. Hasil Rekapitulasi Audit pada Domain DSS 02 *Managed Service Request and Incidents*

a. DSS 02.01 *Define classification schemes for incidents and service requests*

Tabel 4.21. Hasil Rekapitulasi kuesioner DSS 02.01

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Gunakan informasi untuk memastikan pendekatan yang konsisten untuk menangani dan menginformasikan pengguna tentang masalah.	0	1	0	1
2	Tentukan skema solusi bagi sebuah insiden untuk memungkinkan penyelesaian yang efisien dan efektif.	0	1	1	0
3	Tentukan model permintaan layanan sesuai dengan jenis permintaan layanan untuk mengaktifkan layanan mandiri dan efisien.	1	0	0	1
4	Tetapkan aturan dan prosedur tingkatan insiden terutama di bidang keamanan IT.	1	1	1	1
5	Definisikan sumber pengetahuan tentang insiden dan permintaan dan jelaskan bagaimana menggunakannya.	1	0	1	1
		0.60	0.60	0.60	0.80
rata-rata		0.65			

Berdasarkan hasil tabel 4.21 di atas, audit DSS 02.01 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,65 atau tingkat 1. Hal ini dapat diartikan bahwa kegiatan identifikasi 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. BSML Regional II telah mengatur terkait insiden keamanan IT dibuktikan dengan adanya kebijakan pemusnahan dokumen dan rekaman dan kebijakan penyimpanan dokumen dan rekaman, namun belum ada bukti pelaksanaan berupa berita acara;
2. Penggunaan sumber pengetahuan belum dilakukan oleh BSML Regional II.

b. DSS 02.02 *Record, classify and prioritize requests and incidents*

Tabel 4.22. Hasil Rekapitulasi kuesioner DSS 02.02

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Catat semua permintaan, insiden layanan, informasi yang relevan, sehingga dapat ditangani secara efektif.	1	1	1	1
2	Untuk mengaktifkan analisis tren, klasifikasikan permintaan layanan dan insiden berdasarkan jenis dan kategori.	1	1	1	1
3	Memprioritaskan permintaan layanan dan insiden berdasarkan definisi layanan SLA tentang dampak dan urgensi bisnis.	1	1	1	1
		1.0	1.0	1.0	1.0
rata-rata		1.00			

Berdasarkan hasil tabel 4.22 di atas, audit DSS 02.02 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 1,0. Hal ini dapat diartikan bahwa kegiatan pencatatan dan klasifikasi insiden 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. BSML Regional II telah mempunyai dokumen SLA pada proses bisnisnya, namun IT sebagai pendukung layanan belum dilibatkan;
2. Kepala BSML Regional II dalam meeting audit internal telah menginstruksikan untuk melakukan pencatatan segala insiden, namun belum dilakukan.

c. DSS 02.03 *Verify, approve and fulfill service requests*

Tabel 4.23 Hasil Rekapitulasi kuesioner DSS 02.03

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Verifikasi semua permintaan layanan menggunakan prosedur yang ada.	1	1	1	1
2	Setiap perubahan standar yang disepakati dilakukan pengesahan melaui penandatangan dokumen.	1	1	1	1
3	Memenuhi permintaan dengan melakukan prosedur permintaan yang dipilih. Jika memungkinkan, gunakan menu otomatis bantuan mandiri untuk item yang sering diminta.	1	0	1	1
		1	0.67	1	1
rata-rata		0.92			

Berdasarkan hasil tabel 4.23 di atas, audit DSS 02.03 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,92 atau tingkat 1. Hal ini dapat diartikan bahwa kegiatan verifikasi permohonan layanan 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. Kegiatan permintaan layanan melalui TNDK Tata Naskah Dinas Elektronik sudah dilakukan namun belum ada prosedur batas waktu dan kewajiban pemenuhan;

d. DSS 02.04 *Investigate, diagnose and allocate incidents*

Tabel 4.24 Hasil Rekapitulasi kuesioner DSS 02.04

No	Deskripsi	Skor Input			
		as is			
		1	2	3	4
1	Identifikasi dan analisa gejala yang relevan untuk menetapkan kemungkinan penyebab insiden. Gunakan referensi pengetahuan.	1	1	1	1
2	Jika ada potensi permasalahan maka harus dicatat sebagai input masalah baru.	1	1	1	1
3	Mendistribusikan pengelolaan insiden kepada personel yang memiliki keahlian dan tupoksi tertentu.	0	0	1	1
		0.67	0.67	1	1
rata-rata		0,83			

Berdasarkan hasil tabel 4.24 di atas, audit DSS 02.04 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,83 atau tingkat 1. Hal ini dapat diartikan bahwa kegiatan investigasi inisiden 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. Proses identifikasi risiko dan peluang telah dilakukan namun sebatas pemenuhan kegiatan surveillance, belum ada bukti jadwal dan evaluasi untuk melihat kemungkinan adanya pembaharuan;
2. Skema pendistribusian pekerjaan sudah dilakukan sesuai dengan jabatan fungsional tertentu namun keahlian belum dilakukan evaluasi.

e. DSS 02.05 *Resolve and recover from incidents*

Tabel 4.25 Hasil Rekapitulasi kuesioner DSS 02.05

No	Deskripsi	Skor Input			
		as is			
		1	2	3	4
1	Pilih dan terapkan resolusi insiden yang paling tepat	1	1	0	0
2	Catat apakah solusi yang digunakan tepat	0	0	1	1
3	Lakukan tindakan pemulihan setelah terjadi insiden.	1	1	1	1
4	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat digunakan sebagai sumber pengetahuan di masa mendatang	0	1	1	1
		0.5	0.75	0.75	0.75
rata-rata		0.69			

Berdasarkan hasil tabel 4.25 di atas, audit DSS 02.05 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,69 atau tingkat 1. Hal ini dapat diartikan bahwa kegiatan pemulihan jika terjadi insiden 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. Penetapan solusi berdasarkan identifikasi risiko dan peluang sudah dilakukan BSML Regional II namun belum dilakukan evaluasi apakah hal itu yang paling tepat;
2. Tindakan pemulihan dilakukan dan dicatat dalam laporan kerja harian staf pranata komputer namun tindaklanjut setelahnya belum ada.

f. DSS 02.06 *Close service requests and incidents*

Tabel 4.26. Hasil Rekapitulasi kuesioner DSS 02.06

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Verifikasi dengan konsumen atau pengguna, mengenai kepuasan pelayanan	1	1	1	1
2	Tutup permintaan layanan dan insiden	1	1	1	1
		1	1	1	1
rata-rata		1.00			

Berdasarkan hasil tabel 4.26 di atas, audit DSS 02.06 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 1,0. Hal ini dapat diartikan bahwa kegiatan penutupan layanan dalam rangka insiden sudah pernah dilakukan melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif. Fakta yang ditemukan adalah:

1. Adanya kotak saran di gedung pelayanan BSML Regional II, namun belum ada prosedur penanganan terhadap hasilnya;
2. Penutupan layanan karena insiden pernah dilakukan dan tercatat dalam lembar kerja harian. Penggunaan fakta dan peristiwa sebagai input kebijakan belum dilakukan.

g. DSS 02.07 *Track status and produce reports*

Tabel 4.27. Hasil Rekapitulasi kuesioner DSS 02.07

No	Deskripsi	Skor Input			
		as is			
		1	2	3	4
1	Melakukan pemantauan terhadap eskalasi insiden dan status terhadap temuan insiden yang baru	0	0	0	0
2	Identifikasi informasi pemangku kepentingan dan kebutuhan mereka akan data atau laporan.	1	1	1	1
3	Menghasilkan dan mendistribusikan laporan tepat waktu dan atau dapat dilakukan melalui online.	1	1	1	1
4	Menganalisis insiden dan permintaan layanan menurut kategori dan jenis.	1	1	1	1
5	Gunakan informasi sebagai masukan untuk perencanaan perbaikan berkelanjutan.	0	0	0	0
		0.60	0.60	0.60	0.60
rata-rata		0.60			

Berdasarkan hasil tabel 4.27 di atas, audit DSS 02.07 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,60 atau tingkat 1. Hal ini dapat diartikan bahwa kegiatan pelaporan dan tindaklanjut insiden sudah pernah dilakukan melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif. Fakta yang ditemukan adalah:

1. Penanganan insiden telah dilakukan oleh pranata komputer dan dilaporkan dalam laporan kerja harian namun tidak dilakukan evaluasi sehingga potensi insiden tidak dapat diketahui;
2. Penggunaan sumber pengetahuan belum dilakukan oleh BSML Regional II.

h. Hasil Keseluruhan Audit Domain DSS 02 *Managed Service Request and Incidents*

Gambar 4.9. Diagram Representasi Hasil Audit DSS 02

Berdasarkan diagram representasi pada gambar 4.9. di atas diperoleh kesimpulan bahwa tingkat kapabilitas pada domain DSS 02 *Managed Service Request and Incidents* sebesar 0,81 atau pada level 1. Adapun target yang ingin dicapai yaitu tingkat kapabilitas level 2, sehingga terdapat gap. Rekomendasi pada domain DSS 02 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

4.4.4. Hasil Rekapitulasi Audit pada Domain DSS 04 *Managed Continuity*

a. DSS 04.01 *Define the business continuity policy, objectives and scope*

Tabel 4.28 Rekapitulasi kuesioner DSS 04.01

No	Deskripsi	Skor Input			
		as is			
		1	2	3	4
1	Mengidentifikasi proses bisnis internal dan outsourcing yang diperlukan untuk memenuhi kewajiban hukum.	1	1	1	1

Tabel 4.28. Lanjutan

No	Deskripsi	Skor Input as is			
		1	2	3	4
2	Mengidentifikasi *stakeholder* yang bertanggung jawab untuk mendefinisikan dan menyetujui kebijakan dan ruang lingkup keberlanjutan bisnis.	1	1	1	1
3	Tentukan dan dokumentasikan tujuan dan ruang lingkup kebijakan untuk ketahanan bisnis.	1	1	1	1
4	Mengidentifikasi proses bisnis pendukung yang penting dan layanan IT terkait.	1	1	0	0
		1.0	1.0	0.75	0.75
rata-rata		0.88			

Berdasarkan hasil tabel 4.28 di atas, audit DSS 04.01 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,88 atau tingkat 1. Hal ini dapat diartikan bahwa definisi kebijakan proses bisnis dan ruang lingkup sudah ada melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif. Fakta yang ditemukan adalah:

1. Kepala BSML Regional II sebagai pemangku utama telah mengeluarkan maklumat pelayanan dapat diartikan sebagai identifikasi stakeholder dan ruang lingkup;
2. Belum ada ditemukan bukti aktifitas identifikasi pelayanan pendukung.

b. DSS 04.02 *Maintain business resilience*

Tabel 4.29 Rekapitulasi kuesioner DSS 04.02

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Identifikasi potensi yang mungkin menimbulkan peristiwa yang dapat mengganggu secara signifikan.	0	1	1	1

Tabel 4.29. Lanjutan

No	Deskripsi	Skor Input as is			
		1	2	3	4
2	Melakukan analisis dampak bisnis untuk mengevaluasi dampak dari waktu ke waktu dari gangguan terhadap proses bisnis.	1	1	0	0
3	Tetapkan waktu minimum yang diperlukan untuk memulihkan proses bisnis, berdasarkan penetapan toleransi	0	1	1	0
4	Identifikasi stakeholder yang berpengaruh terhadap keberlangsungan proses bisnis.	1	0	1	0
5	Identifikasi tindakan yang akan mengurangi kemungkinan dan dampak melalui peningkatan pencegahan dan peningkatan ketahanan.	1	0	1	1
6	Menganalisis persyaratan kontinuitas untuk mengidentifikasi kemungkinan bisnis strategis.	0	0	0	1
7	Identifikasi kebutuhan sumber daya dan biaya untuk setiap opsi teknis strategis dan buat rekomendasi strategis.	0	1	0	1
8	Dapatkan persetujuan pimpinan untuk opsi strategis yang dipilih.	0	0	0	0
		0.38	0.50	0.50	0.50
rata-rata		0.47			

Berdasarkan hasil tabel 4.29 di atas, audit DSS 04.02 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,47 atau tingkat 1. Fakta yang ditemukan adalah:

1. Identifikasi peluang dalam kegiatan identifikasi peluang dan risiko sudah dilakukan, namun belum dibuktikan bahwa dari peluang akan diperoleh potensi;
2. BSML Regional II telah menetapkan perencanaan masa datang dituangkan dalam renstra 5 tahunan namun perlu penyempurnaan terhadap korelasinya keberlangsungan bisnis.

c. DSS 04.03 *Develop and implement a business continuity response*

Tabel 4.30 Rekapitulasi kuesioner DSS 04.03

No	Deskripsi	Skor Input			
		as is			
		1	2	3	4
1	Tentukan tindakan respons insiden dan komunikasi yang akan diambil jika terjadi gangguan.	1	1	1	1
2	Pastikan mitra outsourcing memiliki rencana kesinambungan yang efektif.	0	0	0	0
3	Tentukan kondisi dan prosedur pemulihan yang akan memungkinkan dimulainya kembali pelayanan.	1	1	1	1
4	Mengembangkan dan memelihara BCP dan DRP yang berisi prosedur yang harus diikuti untuk memungkinkan kelanjutan proses bisnis.	0	0	0	0
5	Tentukan dan dokumentasikan sumber daya yang diperlukan untuk mendukung kelangsungan dan prosedur pemulihan, dengan mempertimbangkan orang, fasilitas dan infrastruktur IT.	1	1	1	0
6	Tentukan dan dokumentasikan persyaratan cadangan informasi yang diperlukan untuk mendukung rencana.	1	0	1	1
7	Tentukan keterampilan yang dibutuhkan untuk personel yang terlibat dalam melaksanakan rencana dan prosedur.	0	0	0	1
8	Distribusikan rencana dan dokumentasi pendukung secara aman kepada pihak yang berwewenang. Pastikan rencananya dan dokumentasi dapat diakses dalam semua skenario bencana.	1	0	0	0
		0.63	0.38	0.5	0.5
rata-rata		0.50			

Berdasarkan hasil tabel 4.30 di atas, audit DSS 04.03 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,50 atau tingkat 1. Fakta yang ditemukan adalah:

1. Dalam pemilihan *outsourcing* penyedia layanan, BSML Regional II belum memperhatikan stabilitas dan komitmen penyedia;

2. BSML Regional II sudah menyusun renstra sebagai bagian dari BCP namun belum ditemukan dokumen sebagai DRP.

d. DSS 04.04 *Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)*

Tabel 4.31 Rekapitulasi kuesioner DSS 04.04

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Tentukan tujuan untuk memverifikasi kelengkapan BCP dan DRP dalam memenuhi risiko bisnis.	0	0	1	1
2	Tentukan dan sepakati peran dan tanggung jawab dan penguturan penyimpanan data yang menyebabkan gangguan minimum pada proses bisnis.	0	1	0	1
3	Tetapkan peran dan tanggung jawab untuk pengelolaan rencana keberlangsungan bisnis	1	1	1	0
4	Jadwalkan latihan dan aktivitas pengujian sebagaimana ditentukan dalam rencana kontinuitas.	0	0	0	0
5	Lakukan pembekalan dan analisis pasca latihan untuk mempertimbangkan pencapaiannya.	0	0	0	0
6	Berdasarkan hasil review, susun rekomendasi untuk perbaikan rencana kontinuitas saat ini.	1	0	0	0
		0.33	0.33	0.33	0.33
rata-rata		0.33			

Berdasarkan hasil tabel 4.31 di atas, audit DSS 04.04 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,33 atau tingkat 1 namun sangat rendah. Hal ini dapat diartikan bahwa review BCP dan DRP belum pernah dilakukan. Fakta yang ditemukan adalah:

1. Belum ada kegiatan verifikasi dan evaluasi BCP;
2. Belum ada perencanaan atau kegiatan penyusunan DRP, lebih lanjut belum ada pembekalan atau pelatihan terkait hal tersebut.

e. DSS 04.05 *Review, maintain and improve the continuity plans*

Tabel 4.32 Rekapitulasi kuesioner DSS 04.05

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Secara teratur, tinjau rencana kesinambungan dan kapabilitas terhadap asumsi yang dibuat dan tujuan strategis.	0	1	1	1
2	Secara teratur, tinjau rencana kesinambungan untuk mempertimbangkan dampak perubahan baru terhadap organisasi perusahaan.	1	0	0	0
3	Pertimbangkan apakah penilaian dampak bisnis yang direvisi mungkin diperlukan.	1	1	0	1
4	Merekomendasikan perubahan dalam kebijakan, rencana, prosedur, infrastruktur, serta peran dan tanggung jawab melalui proses manajemen perubahan TI.	1	1	1	1
		0.75	0.75	0.5	0.75
rata-rata		0.69			

Berdasarkan hasil tabel 4.32 di atas, audit DSS 04.05 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,69 atau tingkat 1. Fakta yang ditemukan adalah:

1. Kegiatan rekomendasi perubahan kebijakan hanya sebatas informasi yang didokumentasikan melalui nota dinas belum ada bukti tindak lanjut terutama pada tata kelola IT;
2. Aktifitas evaluasi dan review renstra dilakukan melalui laporan bulanan, namun tidak ada analisa dampak bagi BSML Regional II.

f. DSS 04.06 *Conduct continuity plan training*

Tabel 4.33 Rekapitulasi kuesioner DSS 04.06

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Merencanakan pelatihan BCP dan DRP	0	0	0	0

Tabel 4.33. Lanjutan

No	Deskripsi	Skor Input as is			
		1	2	3	4
2	Pastikan bahwa rencana pelatihan mempertimbangkan frekuensi pelatihan dan mekanisme penyampaian pelatihan	0	0	0	0
3	Mengembangkan kompetensi berdasarkan pelatihan praktik, termasuk keikutsertaan dalam latihan dan tes.	1	1	1	1
4	Berdasarkan hasil latihan dan tes, pantau keterampilan dan kompetensi	0	0	1	0
		0.25	0.25	0.5	0.25
rata-rata		0.31			

Berdasarkan hasil tabel 4.33 di atas, audit DSS 04.06 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,31 atau tingkat 1 namun rendah. Fakta yang ditemukan adalah:

1. Belum ada kegiatan merencanakan pelatihan BCP dan DRP pada BSML Regional II;
2. Karena belum dilakukan pelatihan maka belum ditemukan kegiatan evaluasi pasca pelatihan terhadap personel yang mengikuti.

g. DSS 04.07 *Manage backup arrangements*

Tabel 4.34 Rekapitulasi kuesioner DSS 04.07

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Mencadangkan sistem, aplikasi, data, dan dokumentasi sesuai jadwal yang ditentukan. Pertimbangkan juga pencadangan online otomatis dan tentukan sumber data, serta keamanan dan hak akses.	1	1	1	1
2	Tetapkan persyaratan untuk penyimpanan data cadangan di tempat dan di luar situs yang memenuhi persyaratan bisnis.	1	1	1	1
3	Mengelola data arsip dan cadangan secara berkala.	1	1	1	1

Tabel 4.34. Lanjutan

No	Deskripsi	Skor Input as is			
		1	2	3	4
4	Memastikan bahwa sistem, aplikasi, data, dan dokumentasi yang dikelola atau diproses oleh pihak ketiga dicadangkan secara memadai atau diamankan.	0	0	0	0
		0.75	0.75	0.75	0.75
rata-rata		0.75			

Berdasarkan hasil tabel 4.34 di atas, audit DSS 04.07 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,75 atau tingkat 1. Fakta yang ditemukan adalah:

1. Kegiatan backup data sudah ditetapkan menggunakan server dengan program freenas yang dapat diakses dari manapun, BSML Regional II juga mengklaim bahwa usaha keamanan penyimpanan data sudah dilakukan;
2. Untuk itu dilakukan uji coba untuk mengakses freenas;

   Pada gambar 4.10 terlihat pengujian akses FreeNas menggunakan username "angga" namun diujicobakan beberapa password acak, dan hasilnya tidak dapat masuk, maka pengujian login dapat dikatakan sesuai/optimal.

Gambar 4.10 Pengujian Menu Login dan Folder Data pada FreeNas

Pada gambar 4.10 di atas memperlihatkan folder yang dapat di akses oleh akun "angga".

Gambar 4.11. Tampilan pengelolaan folder pada FreeNAS

Pada gambar 4.11 terlihat pengaturan akun untuk menentukkan folder mana saja yang dapat diakses. Pada akun "angga" termasuk dalam anggota "pegawai" dan "teknik" sehingga folder yang dapat di akses

adalah folder shared (folder untuk semua pegawai) dan folder teknik yang dikhususkan untuk pegawai teknik.

3. Belum ada kegiatan backup data yang dikelola oleh pihak ketiga.

h. DSS 04.08 *Conduct post-resumption review*

Tabel 4.35 Rekapitulasi kuesioner DSS 04.08

No	Deskripsi	Skor Input as is			
		1	2	3	4
1	Mendokumentasikan kepatuhan terhadap BCP dan DRP.	0	0	0	0
2	Menentukan efektivitas renstra dalam korelasi keberlangsungan proses bisnis.	0	1	1	1
3	Mengidentifikasi kelemahan rencana dan membuat rekomendasi untuk perbaikan, libatkan puncak pimpinan.	1	1	1	1
		0.33	0.67	0.67	0.67
rata-rata		0.58			

Berdasarkan hasil tabel 4.35 di atas, audit DSS 04.08 dilakukan pada 4 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,58 atau tingkat 1. Fakta yang ditemukan adalah:

1. Belum adanya kegiatan menyusun dokumen DRP sehingga belum dapat diagendakan evaluasi;
2. Identifikasi renstra dilakukan melalui evaluasi triwulan dan dilaporkan kepada Direktur Metrologi.

i. Hasil Keseluruhan Audit Domain DSS 04 *Managed Continuity*

Gambar 4.12. Diagram Representasi Hasil Audit DSS 04

Berdasarkan diagram representasi pada gambar 4.12. di atas diperoleh kesimpulan bahwa tingkat kapabilitas pada domain DSS 04 *Managed Continuity* sebesar 0,57 atau pada level 1 artinya proses DSS 04 belum dilakukan sepenuhnya, masih yang belum ada perencanaan. Adapun target yang ingin dicapai yaitu tingkat kapabilitas level 2, sehingga terdapat gap. Rekomendasi pada domain DSS 04 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

4.4.5. Hasil Rekapitulasi Audit pada Domain DSS 05 *Managed Security Services*

a. DSS 05.01 *Protect against malicious software*

Tabel 4.36 Rekapitulasi kuesioner DSS 05.01

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
1	Instal dan aktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas pemrosesan.	1	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	1	1	1
3	Komunikasikan kesadaran akan ancaman malware. Lakukan pelatihan berkala tentang malware dalam email dan penggunaan Internet.	0	0	0	0	0
4	Mendistribusikan anti virus secara terpusat.	1	1	1	0	1
5	Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau keamanan produk dan layanan vendor).	0	1	0	1	0
		0.60	0.80	0.60	0.60	0.60
rata-rata		0.64				

Berdasarkan hasil tabel 4.36 di atas, audit DSS 05.01 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,64 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 BSML Regional II;
2. Evaluasi terhadap potensi ancaman *security* belum dilakukan.

b. DSS 05.02 *Manage network and connectivity security*

Tabel 4.37 Rekapitulasi kuesioner DSS 05.02

No	Deskripsi	Skor Input				
		as is				
		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	1	1	1	1	1
2	Menerapkan mekanisme penyaringan jaringan, seperti firewall	1	0	1	0	1
3	Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.	1	0	1	1	1
4	Konfigurasi peralatan jaringan dengan cara yang aman.	1	1	1	1	1
5	Berdasarkan penilaian risiko dan kebutuhan bisnis, menetapkan dan memelihara kebijakan keamanan konektivitas.	1	1	1	1	1
6	Menetapkan mekanisme terpercaya untuk transformasi informasi yang aman.	0	1	1	0	1
7	Melakukan pengujian keamanan sistem secara berkala untuk menentukan kecukupan perlindungan sistem	0	0	0	0	0
		0.71	0.57	0.85	0.57	0.85
rata-rata		0.71				

Berdasarkan hasil tabel 4.37 di atas, audit DSS 05.02 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,71 atau tingkat 1. Fakta yang ditemukan adalah:

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

c. DSS 05.03 *Manage endpoint security*

Tabel 4.38 Rekapitulasi kuesioner DSS 05.03

No	Deskripsi	Skor Input				
		as is				
		1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman	1	1	1	1	1
2	Menerapkan mekanisme penguncian perangkat.	1	1	1	1	1
3	Kelola akses dan kontrol jarak jauh (mis., Perangkat seluler, teleworking).	1	1	1	1	1
4	Kelola konfigurasi jaringan dengan cara yang aman.	1	1	1	1	1
5	Menerapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.	1	1	1	1	0
6	Lindungi integritas sistem	0	1	0	1	0
7	Memberikan perlindungan fisik perangkat titik akhir.	0	1	0	1	0
8	Kelola akses jahat melalui email dan browser web. Misalnya, blokir situs web tertentu.	1	1	1	0	1
		0.75	1	0.75	0.87	0.63
rata-rata		0.80				

Berdasarkan hasil tabel 4.38 di atas, audit DSS 05.03 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,64 atau tingkat 1. Fakta yang ditemukan adalah:

1. Seluruh perangkat komputer terutama pada bagian layanan dan laboratorium menggunakan *password*, dan penetapan user sudah dilakukan pada masing-masing laboratorium.
2. Situs web tertentu telah diblokir pada saat menggunakan jaringan kantor namun belum dilakukan evaluasi dan pengujian secara berkala. BSML Regional II telah mengklaim bahwa aktivitas blok telah dilakukan.

d. DSS 05.04 *Manage user identity and logical access*

Tabel 4.39 Rekapitulasi kuesioner DSS 05.04

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan.	1	1	1	1	1
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.	0	1	1	1	1
3	Pastikan pemantauan pada akun yang memiliki hak istimewa.	1	0	1	0	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.	1	1	1	1	1
5	Lakukan analisis pasca latihan untuk evaluasi.	0	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.	1	0	1	0	1
7	Menjaga jejak akses ke informasi tergantung pada tingkat kerahasiaan.	0	0	0	0	0
8	Lakukan tinjauan manajemen secara rutin pada semua akun dan hak istimewa terkait.	0	1	0	1	0
		0.5	0.5	0.63	0.5	0.63
rata-rata		0.55				

Berdasarkan hasil tabel 4.39 di atas, audit DSS 05.04 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,55 atau tingkat 1. Fakta yang ditemukan adalah:

1. Belum adanya kegiatan pelatihan sehingga evaluasi pelatihan belum dilakukan;

2. Pembagian hak akses freenas berdasarkan kelompok seksi dan jabatan fungsional tertentu sudah ada, namun belum ada pembagian tingkatan user dikarenakan belum ada hirarki data/dokumen.

e. DSS 05.05 *Manage physical access to I&T assets*

Tabel 4.40 Rekapitulasi kuesioner DSS 05.05

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
1	Daftarkan semua pengunjung, termasuk kontraktor dan vendor.	0	0	1	0	1
2	Pastikan semua personel menampilkan identifikasi yang disetujui dengan benar setiap saat.	1	1	1	1	1
3	Mengharuskan pengunjung untuk didampingi setiap saat saat berada di lokasi.	1	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	1
5	Kelola permintaan untuk mengizinkan akses resmi yang sesuai ke fasilitas komputasi.	1	1	1	1	1
6	Pastikan profil akses setiap terkini. Akses dasar ke situs IT (ruang server, gedung, area atau zona) pada fungsi pekerjaan dan tanggung jawab.	1	1	1	1	0
7	Lakukan pelatihan kesadaran keamanan informasi fisik secara teratur. Panduan Terkait (Standar, Kerangka Kerja, Persyaratan Kepatuhan)	0	0	0	0	0
		0.71	0.71	0.86	0.71	0.71
rata-rata		0.74				

Berdasarkan hasil tabel 4.40 di atas, audit DSS 05.05 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,74 atau tingkat 1. Fakta yang ditemukan adalah:

1. Setiap pengunjung telah dipersyaratkan mengisi form kunjungan menggunakan google form di pos satpam sebelum memasuki gedung BSML Regional II;
2. Pengunjung akan ditemani oleh pegawai BSML Regional II, namun belum ada penerapan daerah terlarang pada ruang server dan control room tiap laboratorium.
3. Belum ditemukan agenda pelatihan tentang kesadaran keamanan informasi fisik, termasuk server.

f. DSS 05.06 *Manage sensitive documents and output devices*

Tabel 4.41 Rekapitulasi kuesioner DSS 05.06

No	Deskripsi	Skor Input				
		as is				
		1	2	3	4	5
1	Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan dan pembuangan dokumen sensitif perusahaan	1	1	1	1	1
2	Tetapkan hak akses istimewa kepada jabatan tertentu berdasarkan keputusan manajemen	1	1	1	1	1
3	Buat inventarisasi dokumen sensitif perusahaan.	0	0	1	0	1
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.	0	0	0	0	1
		0.5	0.5	0.75	0.5	1
rata-rata		0.65				

Berdasarkan hasil tabel 4.41 di atas, audit DSS 05.06 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,6 atau tingkat 1. Fakta yang ditemukan adalah:

1. Setiap dokumen yang bersifat *confidential* dikelola oleh personel tertentu namun masih belum ada pembatasan akses bagi pegawai lain;
2. Belum ditemukan bukti kegiatan penanganan khusus terhadap dokumen penting BSML Regional II.

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

Tabel 4.42 Rekapitulasi kuesioner DSS 05.07

No	Deskripsi	Skor Input as is				
		1	2	3	4	5
1	Terus gunakan tools untuk mengidentifikasi kerentanan keamanan informasi.	0	0	1	1	1
2	Tentukan dan komunikasikan skenario risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.	1	1	1	1	1
3	Tinjau data peristiwa secara teratur untuk mengetahui potensi insiden.	0	0	0	0	1
4	Pastikan kejadian terkait keamanan dikelola tepat waktu untuk identifikasi potensi risiko	1	1	0	0	0
5	Catat kejadian terkait keamanan dan simpan catatan untuk periode yang sesuai	1	0	1	1	1
		0.6	0.4	0.6	0.6	0.8
rata-rata		0.60				

Berdasarkan hasil tabel 4.42 di atas, audit DSS 05.07 dilakukan pada 5 responden dan menilai kondisi saat ini berada pada tingkat kapabilitas 0,60 atau tingkat 1. Fakta yang ditemukan adalah:

1. Belum ditemukan kejadian keamanan, namun aktivitas tersebut telah menjadi tupoksi dari pranata komputer pada BSML Regional II 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*

Gambar 4.13. Diagram Representasi Hasil Audit DSS 05

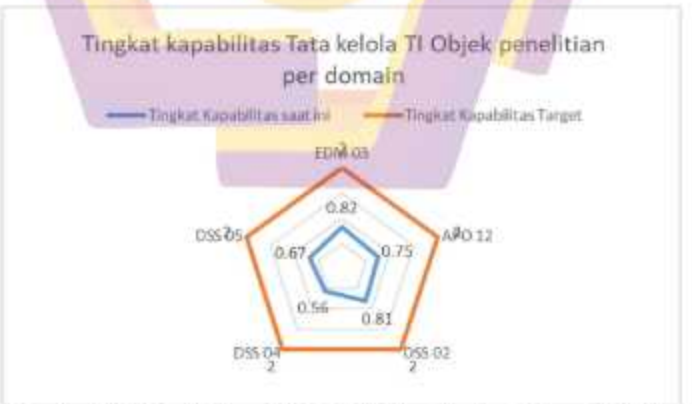
Berdasarkan diagram representasi pada gambar 4.13. di atas diperoleh kesimpulan bahwa tingkat kapabilitas pada domain DSS 05 *Managed Security Services* sebesar 0,67 atau pada level 1 artinya proses DSS 05 sudah dilakukan namun belum terencana dan belum terdokumentasikan dengan baik. Adapun target yang ingin dicapai yaitu tingkat kapabilitas level 2, sehingga terdapat gap. Rekomendasi pada domain DSS 05 diharapkan dapat meningkatkan tingkat kapabilitas pada level yang diinginkan.

i. Rekapitulasi Hasil Audit

Adapun rekapitulasi hasil audit tata kelola teknologi informasi BSML Regional II menggunakan framework COBIT 2019 dapat ditunjukkan pada tabel 4.43. Dan secara rata-rata menunjukkan angka 0.716 atau pada tingkat kapabilitas level 1. Sedangkan gap atau kesenjangan pada tiap domain dapat ditunjukkan pada gambar 4.14.

Tabel 4.43. Rekapitulasi hasil audit

No	Domain	Tingkat Kapabilitas saat ini	Tingkat Kapabilitas Target
1	EDM 03	0.82	2
2	APO 12	0.75	2
3	DSS 02	0.81	2
4	DSS 04	0.56	2
5	DSS 05	0.67	2
rata-rata		0.722	2



Gambar 4.14. Tingkat kapabilitas tata kelola teknologi informasi BSML Regional II

4.5. Rekomendasi

Berdasarkan hasil audit yang telah dilakukan, maka disusun rekomendasi. Rekomendasi ini dapat dijelaskan pada tabel 4.49 di bawah ini

Tabel 4.49. Rekomendasi Hasil Audit

No	Proses	Temuan	Rekomendasi
1	EDM 03.01	1. BSML Regional II telah mencoba memahami risiko IT melalui dokumen laporan ketidaksesuaian Tahun 2020; 2. Namun BSML Regional II belum menentukkan profil risiko IT; 3. Kepala BSML Regional II belum menunjuk secara spesifik personel yang mengelola manajemen risiko IT.	1. BSML Regional II diharapkan menetapkan profil risiko IT dituangkan dalam dokumen Panduan Mutu PM-BSML.II pada klausul 6 tentang sumber daya 2. Pada dokumen profil risiko IT yang telah dibuat, BSML Regional II diharapkan melakukan perencanaan jadwal kegiatan evaluasi profil risiko yang telah ditetapkan dan jadwal tersebut dimasukkan dalam notifikasi TNDE.
2	EDM 03.02	1. BSML Regional II telah melakukan perencanaan penerapan strategi risiko IT dengan membuat klausul 7.11. pada dokumen Panduam Mutu PM-BSML II (Rev.01); 2. Belum ditemukan bukti penerapan strategi risiko pada IT kegiatan operasional; 3. BSML Regional II telah mencoba mengidentifikasi risiko melalui dokumen identifikasi risiko dan peluang BSML II.	1. BSML Regional II direkomendasikan melakukan analisis sebelum menyusun perencanaan penerapan strategi risiko IT dan identifikasi risiko dituangkan dalam penambahan pada PM-BSML II klausul 7.11 2. Penerapan strategi risiko pada setiap kegiatan operasional BSML Regional II dibuktikan dengan dokumen dan evaluasi, tentukan personel yang terlibat tuangkan dalam PM-BSML II klausul 6.2
3	EDM 03.03	1. Kepala BSML Reginal II melaporkan segala kegiatan melalui dokumen pelaporan bulanan kepada Direktur Metrologi; 2. BSML Regional II melalui dokumen identifikasi risiko dan peluang, telah merencanakan pemantauan risiko namun belum diterapkan.	1. Dalam rangka penertiban format laporan dan kemudahan evaluasi dan pengolahan data, BSML Regional II dapat membangun sistem informasi layanan & risiko IT berbasis web yang memuat identfikasi peluang dan risiko, strategi risiko, pelaporan risiko serta evaluasinya, dikelola oleh personel tertentu.
4	APO 12.01	1. BSML Regional II telah merancang kegiatan pencatatan data sesuai klausul 7.11. PM-BSML II; 2. Pencatatan data dan insiden dilakukan oleh pranata komputer sebagai bagian	1. Menentukkan metode dalam rangka mengumpulkan data sehingga diharapkan hasil yang akan diraih sama dituangkan dalam PM-BSML II klausul 7.11;

Tabel 4.49. Rekomendasi Hasil Audit (lanjutan)

No	Proses	Temuan	Rekomendasi
		dari laporan kerja harian pegawai belum sebagai produk organisasi;	2. Menetapkan format laporan catatan data insiden, dan agar format laporan tersebut pasti seragam, maka pelaporan dilakukan melalui sistem informasi berbasis web dan data tersebut mudah diolah.
5	APO 12.02	1. Pada dokumen identifikasi risiko dan peluang, BSML Regional II sudah mencoba memetakan risiko namun belum dilakukan analisa; 2. Belum adanya informasi respon pada setiap identifikasi risiko sehingga belum dapat dibuktikan perencanaan respon terhadap risiko yang ada;	1. BSML Regional II diharapkan melakukan analisa pada kegiatan identifikasi risiko IT dengan dibuktikan adanya penggunaan data dukung pada saat identifikasi setiap risiko IT; 2. Pengolahan data dari sistem informasi insiden yang dibangun salah satunya adalah mengumpulkan respon pada setiap potensi risiko diambil dari data pelaporan insden yang diolah dan melakukan perencanaan respon berdasarkan evaluasi.
6	APO 12.03	1. Penentuan layanan IT dan manajemennya merupakan bagian dari kegiatan layanan perkantoran dalam kertas kerja BSML Regional II dan itu menjadi tupoksi Sub Koordinator Tata Usaha, namun belum ditemukan dokumen proses yang tertuang; 2. Belum ditemukan proses adopsi atau analisis dari contoh manajemen IT hasil benchmarking atau interkomparasi.	1. Setiap kegiatan pelayanan IT 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. BSML Regional II direkomendasikan melakukan interkomparasi dengan organisasi/ perusahaan dengan proses bisnis serupa, kemudian adopsi manajemen yang IT dapat diaplikasikan pada kantor BSML Regional II
7	APO 12.04	1.Proses identifikasi risiko dan peluang dalam proses bisnis telah dilakukan dan terdokumentasi, pelaporan kepada *stakeholder* disampaikan dalam kegiatan audit internal; 2.Belum ditemukan format pelaporan profil dan manajemen risiko IT pada BSML Regional II.	1. BSML Regional II perlu melakukan penjadwalan pelaporan insiden kepada *stakeholder* dan menetapkan format yang dituangkan pada sistem informasi yang dibangun, dan tertuang dalam PM-BSML II klausul 7.8 tentang pelaporan

Tabel 4.49. Rekomendasi Hasil Audit (lanjutan)

No	Proses	Temuan	Rekomendasi
8	APO 12.05	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.	1. Memperbaiki mekanisme disposisi pekerjaan terutama dalam hal risiko IT menggunakan TNDE Tata Naskah Dinas Elektronik dan mewajibkan seluruh pegawai menginstall aplikasi SIPEG pada gawainya.
9	APO 12.06	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.	1. Melakukan pencatatan data insiden menggunakan sistem informasi kemudian diolah, lakukan analisa korelasi antara insiden dengan respon; 2. Setelah itu, BSML Regional II dapat melakukan evaluasi hasil analisa tersebut.
10	DSS 02.01	1. BSML Regional II telah mempunyai dokumen terkait insiden keamanan IT dibuktikan dengan adanya kebijakan pemusnahan dokumen dan rekaman dan kebijakan penyimpanan dokumen dan rekaman, namun belum ada bukti pelaksanaan berupa berita acara; 2. Penggunaan sumber pengetahuan belum dilakukan oleh BSML Regional II.	1. BSML Regional II direkomendasikan untuk membuat berita acara pada setiap pelaksanaan pemusnahan dokumen, dan membuat jadwal perencanaan pemusnahan, dokumentasikan; 2. Dalam penumpulan data pelayanan dan insiden IT, BSML Regional II dapat menggunakan data dari log harian yang diinput oleh Pranata Komputer dengan pemanfaat sistem informasi yang dibangun
11	DSS 02.02	1. BSML Regional II telah mempunyai dokumen SLA pada proses bisnisnya, namun IT sebagai pendukung layanan belum dilibatkan; 2. Kepala BSML Regional II dalam meeting audit internal telah menginstruksikan untuk melakukan pencatatan segala insiden, namun belum dilakukan.	1. Dalam dokumen SLA pelayanan BSML Regional II, perlu ditambahkan poin gangguan layanan yang diakibatkan oleh insiden IT; 2. BSML Regional II diharapkan melakukan penetapan PIC manajemen insiden berikut pelaporannya, ditunagkan dalam SK Kepala BSML.
12	DSS 02.03	1. Mekanisme permintaan layanan melalui TNDE Tata Naskah Dinas Elektronik sudah diterapkan namun belum ada prosedur batas waktu dan kewajiban pemenuhan;	1. Menetapkan batas waktu pengerjaan pelayanan pada TNDE dengan menambahkan kolom waktu pada format, serta ditambahkan sistem notifikasi.

Tabel 4.49. Rekomendasi Hasil Audit (lanjutan)

No	Proses	Temuan	Rekomendasi
13	DSS 02.04	1.Proses identifikasi risiko dan peluang telah dilakukan namun sebatas pemenuhan kegiatan surveillance, belum ada bukti jadwal dan evaluasi untuk melihat kemungkinan adanya pembaharuan; 2.Skema pendistribusian pekerjaan sudah dilakukan sesuai dengan jabatan fungsional tertentu namun keahlian belum dilakukan evaluasi.	1. Melakukan perencanaan identifikasi risiko dengan menjadwalkan kegiatan tersebut; 2. Melakukan evaluasi hasil identifikasi risiko IT dan didokumentasikan; 3. BSML Regional II diharapkan melakukan uji kompetensi berkala pada setiap pegawai dengan jabatan fungsional tertentu dapat menggunakan CBT (Computer Based Test) dan lakukan evaluasi.
14	DSS 02.05	1.Penetapan solusi berdasarkan identifikasi risiko dan peluang sudah dilakukan BSML Regional II namun belum dilakukan evaluasi apakah hal itu yang paling tepat; 2.Tindakan pemulihan dilakukan dan dicatat dalam laporan kerja harian staf pranata komputer namun tindaklanjut setelahnya belum ada.	1. BSML Regional II dapat melakukan pengolahan data insiden yang merupakan produk sistem informasi insiden IT untuk evaluasi efisiensi solusi terhadap masing-masing risiko IT; 2. Dalam kegiatan pemulihan insiden, BSML Regional II dapat merencakan tindak lanjut yang akan dilakukan, dan lakukan analisis korelasi sehingga dapat diperoleh petunjuk sederhana.
15	DSS 02.06	1. BSML Regional II sudah menerapkan kaji ulang permintaan pelayanan, namun belum ada prosedur penanganan terhadap hasilnya; 2. Penutupan layanan karena insiden pernah dilakukan dan tercatat dalam lembar kerja harian. Penggunaan fakta dan peristiwa sebagai input kebijakan belum dilakukan.	1. BSML Regional II diharapkan menetapkan mekanisme tindak lanjut terhadap kaji ulang permintaan dan dituangkan dalam pelaporan; 2. Melakukan analisis menggunakan data insiden untuk menentukan kebijakan risiko IT.
16	DSS 02.07	1. Penanganan insiden telah dilakukan oleh pranata komputer dan dilaporkan dalam laporan kerja harian namun tidak dilakukan evaluasi sehingga potensi insiden tidak dapat diketahui; 2. Penggunaan sumber pengetahuan belum dilakukan oleh BSML Regional II.	1. Dengan memanfaatkan sistem informasi insiden IT, BSML Regional II dapat melakukan identifikasi potensi insiden menggunakan hasil olah data laporan insiden harian; 2. Menjadwalkan kegiatan evaluasi insiden untuk dijadikan sebagai data primer kebijakan dengan memanfaatkan TNDE dan aktifkan notifkasi.

Tabel 4.49. Rekomendasi Hasil Audit (lanjutan)

No	Proses	Temuan	Rekomendasi
17	DSS 04.01	1. Kepala BSML Regional II sebagai pemangku utama telah mengeluarkan maklumat pelayanan dapat diartikan sebagai identifikasi stakeholder dan ruang lingkup; 2. Belum ada ditemukan bukti aktifitas identifikasi pelayanan pendukung.	1. BSML Regional II perlu menetapkan peran dan fungsi masing-masing *stakeholder* pada proses bisnis; 2. Melakukan perencanaan identifikasi pelayanan pendukung, lalu terapkan dan diaplikasikan, kemudian evaluasi.
18	DSS 04.02	1. Identifikasi peluang dalam kegiatan identifikasi peluang dan risiko sudah dilakukan, namun belum dibuktikan bahwa dari peluang akan diperoleh potensi; 2. BSML Regional II telah menetapkan perencanaan masa datang dituangkan dalam renstra 5 tahunan namun perlu penyempurnaan terhadap korelasinya keberlangsungan bisnis.	1. Melakukan analisa peluang untuk memperoleh potensi. Dalam form identifikasi peluang dan risiko ditambahkan kolom potensi; 2. BSML Regional II harus melakukan penjabaran renstra 5 tahunan menjadi per tahun disertai analisa keberlangsungan bisnis, dan evaluasi apakah renstra tahunan tersebut dapat menunjang keberlangsungan bisnis.
19	DSS 04.03	1. Dalam pemilihan outsourcing penyedia layanan, BSML Regional II belum memperhatikan stabilitas dan komitmen penyedia; 2. BSML Regional II sudah menyusun renstra sebagai bagian dari BCP namun belum ditemukan dokumen sebagai DRP.	1. Membuat sistem pendaftaran vendor via online menggunakan kriteria tertentu sehingga dapat diperoleh yang diinginkan dan untuk menghindari konflik kepentingan; 2. BSML Regional II perlu membuat DRP dan melakukan implementasi sewaktu ada insiden dituangkan dalam dokumen PM-BSML II klausul 6.3
20	DSS 04.04	1. Belum ada kegiatan verifikasi dan evaluasi BCP; 2. Belum ada perencanaan atau kegiatan penyusunan DRP, lebih lanjut belum ada pembekalan atau pelatihan terkait hal tersebut	1. BSML Regional II direkomendaiskan melakukan penjadwalan evaluasi BCP dan menetapkan hasil evaluasi sebagai input kaji ulang dokumen; 2. Sebagai tindak lanjut penyusunan DRP, melakukan pelatihan dan ujian menggunakan CBT secara terjadwal
21	DSS 04.05	1. Kegiatan rekomendasi perubahan kebijakan hanya sebatas informasi yang didokumentasikan melalui nota dinas belum ada bukti tindak lanjut terutama pada tata kelola IT; 2. Aktifitas evaluasi dan review renstra dilakukan melalui laporan bulanan, namun tidak ada analisa dampak bagi BSML Regional II.	1. Memasukkan kegiatan analisa dampak pada evaluasi renstra, kegiatan tersebut terjadwal setiap bulan, informasi kegiatan dapat disampaikan melalui TNDE; 2. Menambahkan notifikasi pada setiap disposisi yang mewajibkan tindaklanjut bagi penerima disposisi.

Tabel 4.49. Rekomendasi Hasil Audit (lanjutan)

No	Proses	Temuan	Rekomendasi
22	DSS 04.06	1. Belum ada kegiatan merencanakan pelatihan BCP dan DRP pada BSML Regional II; 2. Karena belum dilakukan pelatihan maka belum ditemukan kegiatan evaluasi pasca pelatihan terhadap personel yang mengikuti.	1. BSML Regional II perlu melakukan penjadwalan kegiatan pelatihan BCP dan DRP, dan lakukan pelatihan secara daring, lalu evaluasi kompetensi peserta bisa menggunaan CBT
23	DSS 04.07	1. Kegiatan backup data sudah ditetapkan menggunakan server dengan program freenas yang dapat diakses dari manapun, BSML Regional II juga mengklaim bahwa usaha keamanan penyimpanan data sudah dilakukan; 2. Belum ada kegiatan backup data yang dikelola oleh pihak ketiga.	1. BSML Regional II harus menetapkan PIC backup data, dan melakukan pengelolaan terhadap data, jika perlu lakukan data cleansing, dan penghapusan redudansi data sebelum dilakukan backup. PIC tersebut adalah Pejabat fungsional Pranata Komputer; 2. Walaupun belum ada kegiatan backup yang diserahkan pada pihak ketiga namun perlu dibuat mekanisme proses backup data oleh pihak ketiga.
24	DSS 04.08	1. Belum adanya kegiatan menyusun dokumen DRP sehingga belum dapat diagendakan evaluasi; 2. Identifikasi renstra dilakukan melalui evaluasi triwulan dan dilaporkan kepada Direktur Metrologi.	1. Setelah proses implementasi DRP, dilakukan review dan dokumentasi terhadap pelaksanaan DRP; 2. Menetapkan mekanisme identifikasi renstra, menetapkan PIC yaitu Pejabat Perencana, dan lakukan evaluasi dituangkan dalam PM-BSML II klausul 7.8
25	DSS 05.01	1. Belum ditemukan kegiatan atau perencanaan pelatihan khusus mengenai bahaya *malware*, penggunaan email dan internet yang baik pada BSML Regional II; 2. Evaluasi terhadap potensi ancaman *security* belum dilakukan.	1. BSML Regional II perlu melakukan mitigasi risiko terkait serangan *malware* dan dilakukan simulasi serta mengadakan pelatihan bagi seluruh karyawan terutama pengguna layanan IT di kantor; 2. Merencanakan kegiatan identifikasi potensi ancaman security dan lakukan evaluasi; 3. Melakukan pengolahan data laporan harian terkait insiden menggunakan sistem informasi insiden IT.
26	DSS 05.02	1. Belum ada bukti pelaksanaan pengujian keamanan sistem pada BSML Regional II; 2. Penggunaan akun tertentu untuk mengakses jaringan dan server sudah diterapkan namun belum ditemukan manajemen akun.	1. BSML Regional II 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.

Tabel 4.49. Rekomendasi Hasil Audit (lanjutan)

No	Proses	Temuan	Rekomendasi
27	DSS 05.03	1. Seluruh perangkat komputer terutama pada bagian layanan dan laboratorium menggunakan *password*, dan penetapan user sudah dilakukan pada masing-masing laboratorium. 2. Situs web tertentu telah diblokir pada saat menggunakan jaringan kantor namun belum dilakukan evaluasi dan pengujian secara berkala. BSML Regional II telah mengklaim bahwa aktivitas blok telah dilakukan	1. Melakukan evaluasi penggunaan perangkat komputer, melakukan back up data pada masing-masing laboratorium. 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.
28	DSS 05.04	1. Belum adanya kegiatan pelatihan sehingga evaluasi pelatihan belum dilakukan; 2. Pembagian hak akses freenas berdasarkan kelompok seksi dan jabatan fungsional tertentu sudah ada, namun belum ada pembagian tingkatan user dikarenakan belum ada hirarki data/dokumen.	1. BSML Regional II perlu melakukan perencanaan pelatihan penggunaan komputer dan manajemen akun, kemudian lakukan dan evaluasi; 2. Menjadwalkan meeting dengan pimpinan untuk membahas hirarki user menggunakan TNDE dan dijabarkan dengan jelas *stakeholder* yang terlibat.
29	DSS 05.05	1. Setiap pengunjung telah dipersyaratkan mengisi form kunjungan menggunakan google form di pos satpam sebelum memasuki gedung BSML Regional II; 2. Pengunjung akan ditemani oleh pegawai BSML Regional II, namun belum ada penerapan daerah terlarang pada ruang server dan control room tiap laboratorium. 3. Belum ditemukan agenda pelatihan tentang kesadaran keamanan informasi fisik, termasuk server.	1. Membuat mekanisme penerimaan tamu, menggunakan google form sebagai DSS, 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; 3. Merencanakan pelatihan, lakukan dan evaluasi.
30	DSS 05.06	1. Setiap dokumen yang bersifat *confidential* dikelola oleh personel tertentu namun masih belum ada pembatasan akses bagi pegawai lain; 2. Belum ditemukan bukti kegiatan penanganan khusus terhadap dokumen penting BSML Regional II.	1. BSML Regional II dapat lebih mengoptimalkan fasilitas freeNAS dengan melakukan manajemen pada freenas untuk pengelolaan akses folder data; 2. Membuat jadwal meeting untuk agenda penanganan khusus terhadap dokumen penting BSML Regiona II menggunakan TNDE.
31	DSS 05.07	1. Belum ditemukan kejadian keamanan, namun aktivitas tersebut telah menjadi tupoksi dari pranata komputer pada BSML Regional II yang harus dicatat dalam laporan kerja harian;	1. Mempertegas tugas pada jabatan Pranata Komputer berikut kewenangan dan kewajibannya melalui SK Kabalai dan dapat diusulkan menjadi SK Direktur Jenderal;

Tabel 4.49. Rekomendasi Hasil Audit (lanjutan)

No	Proses	Temuan	Rekomendasi
31	DSS 05.07	2. Belum ada mekanisme peninjauan ulang terhadap kejadian atau aktivitas terkait keamanan.	2. Dengan menetapkan PIC, maka pencatatan data insiden terkait keamanan dapat diolah dan digunakan dalam membuat kebijakan.

Berdasarkan audit tata kelola teknologi informasi pada 5 domain yang terpilih menggunakan COBIT 2019 dan rekomendasi pada setiap subdomain tersebut di atas maka dapat disusun rekomendasi umum sebagai berikut:

1. Bidang Peraturan Atau Kebijakan

   Berdasarkan temuan pada domain EDM 03 dan APO 12 maka diperlukan petunjuk yang jelas dalam tata kelola teknologi informasi maka perlu adanya penurunan Peraturan Presiden pada masing-masing lembaga pemerintahan (Kementerian, Pemerintah Provinsi dan Pemerintah Kabupaten/Kota) hingga pada level juklak (petunjuk pelaksanaan) dan juknis (petunjuk teknis);

2. Organisasi

   Berdasarkan temuan pada domain EDM 03 dan DSS 02 maka pada tiap Satker (satuan kerja) pada Lembaga pemerintahan bidang pelayanan metrologi agar memasukkan tugas dan fungsi tata kelola teknologi informasi pada salah satu seksi;

3. Sumber Daya Manusia Atau SDM

   Sedangkan berdasarkan pada DSS 04 dan DSS 05 maka perlu pengembangan jabatan fungsional tertentu pranata komputer yang menjadi PIC dalam implementasi SPBE dan tata kelola teknologi informasi pada Lembaga pemerintahan bidang pelayanan metrologi.

   Pada penelitian yang berjudul Evaluasi Pengelolaan Sumber Daya Teknologi Informasi (IT Resource Management) dengan menggunakan Framework COBIT 5 (studi kasus : PT.Infomedia Nusantara) yang ditulis oleh Alvian Restu Naspati dkk, menjelaskan bahwa tingkat kapabilitas tata kelola IT pada

PT.Infomedia Nusantara pada level 3. Salah satu pendukung dari kapabilitas tata kelola IT pada perusahaan tersebut adalah sumber daya manusia (SDM) yang mengelola IT atau jika dalam pemerintahan disebut sebagai pranata komputer. Pengelolaan SDM yang baik dengan didukung evaluasi kompetensi SDM serta pengembangan keahlian berpengaruh terhadap tingkat kapabilitas tata kelola teknologi informasi. Sehingga dengan pengembangan pranata komputer pada lembaga pemerintahan bidang pelayanan metrologi dapat berperan untuk meningkatkan kapabilitas tata kelola IT.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil audit yang telah dilakukan pada BSML Regional II, maka dapat ditarik kesimpulan sebagai berikut:

1. Berdasarkan hasil audit tata kelola TI menggunakan COBIT 2019, tingkat kapabilitas tata kelola TI BSML Regional II 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. BSML Regional II sebagai lembaga pemerintahan yang telah terakreditasi ISO 17025 dan ISO 9001 masih berada pada level 1 sehingga tata kelola TI bagi Lembaga pemerintahan bidang pelayanan metrologi lainnya harus menjadi prioritas demi percepatan implementasi SPBE.
2. Rekomendasi yang dapat dilakukan guna percepatan implementasi SPBE pada Lembaga Pemerintah bidang pelayanan metrologi berdasarkan hasil audit COBIT 2019 adalah pada sisi peraturan/kebijakan yaitu penurunan petunjuk pelaksaanan, sisi organisasi yaitu menambahkan tupoksi tata kelola IT pada organisasi dan sisi SDM yaitu pengembangan SDM pranata komputer

5.2. Saran

Saran yang dapat diberikan untuk penelitian selanjutnya berdasarkan hasil kegiatan audit yang dilakukan pada BSML Regional II Kementerian Perdagangan adalah sebagai berikut:

1. Perlunya dilakukan kegiatan audit pada organisasi dengan proses bisnis yang sama.
2. Perlunya melakukan kegiatan audit menggunakan framework lainnya pada objek penelitian yang sama.
3. Perlunya memperluas responden audit namun tetap mempertimbangkan RACI Chart.

DAFTAR PUSTAKA

PUSTAKA BUKU

BSML Regional II, 2019, Panduan Mutu BSML Regional II ISO/IEC 17025:2017 & ISO 9001:2015, Yogyakarta

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

ISACA, 2019, COBIT 2019 *Framework: Governance and Management Objectives*, ISACA, USA

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

ISACA, 2019, COBIT 2019 *Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*, ISACA, USA

ISO/IEC, 2017, ISO/IEC 17025 Third Edition: *General requirements for the competence of testing and calibration laboratories*, Switzerland, 2017

Kementerian Perdagangan RI, 2016, Peraturan Menteri Perdagangan Republik Indonesia Nomor 60/M-DAG/PER/8/2016 tentang Organisasi dan Tata Kerja Unit Pelaksana Teknis Bidang Kemetrologian dan Bidang Standardisasi dan Pengendali Mutu Barang di Lingkungan Kementerian Perdagangan, Jakarta

Kementerian Perdagangan RI, 2017, Peraturan Menteri Perdagangan Republik Indonesia Nomor 46/M-DAG/PER/7/2017 tentang Penyelenggaraan Teknologi Informasi dan Komunikasi di Lingkungan Kementerian Perdagangan, Jakarta

Presiden RI, 2018, Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Jakarta

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

Weber, Ron., 1999, Information Systems Control and Audit. Prentice-Hall, Inc. NewJersey, Amerika Serikat

PUSTAKA MAJALAH, JURNAL ILMIAH ATAU PROSIDING

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

Baharuddin, A.F., Suprapto, Perdanakusuma,A.R., 2019, Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Domain DSS (Deliver, Service, Support) (Studi Kasus : PT. PLN (Persero) Kantor Pusat), Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Vol. 3, No. 9, September 2019

De Haes, S., Van Grembergen, W., Debreceny, R.S., 2013, *COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities*, Journal of Information systems volume 27 No.1, Spring 2013

Ekowansyah, E., Chrisnanto, Y.H., Puspita, Sabrina, N., 2017, Audit Sistem Informasi Akademik Menggunakan COBIT 5 di Universitas Jenderal Achmad Yani, Prosiding Seminar Nasional Komputer dan Informatika (SENASKI) 2017

ISACA, 2019, *Developing the IT Audit Plan Using COBIT 2019*, ISACA Journal Vol.3 2019

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.

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

Naspati, A.R., Suprapto, Herlambang, A.D., 2018, Evaluasi Pengelolaan Sumber Daya Teknologi Informasi (IT Resource Management) dengan menggunakan Framework COBIT 5 (studi kasus: PT.Infomedia Nusantara), Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Vol. 2 No. 11 (2018) 5384-5393

Putra, I.N., Hakim,A., Pramonon, S.H., Tolle, H, 2017, *Adopted COBIT-5 Framework for System Design of Indonesia Navy IS/IT : An Evaluation* International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17, 2017

Zhang, S., Fever, Hans Le, 2013, *An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model*, Journal of Economics, Business and Management, Vol. 1, No. 4, November 2013

PUSTAKA LAPORAN PENELITIAN

Miranti, A., 2019, Evaluasi Tata Kelola Teknologi Informasi Menggunakan *Framework* COBIT 5 (Studi Kasus: PT.Praweda Ciptakarsa Informatika), UIN Syarif Hidayatullah, Jakarta

Oktianatasari, H., 2017, Audit Tata Kelola Teknologi Informasi pada PT. Pelabuhan Indonesia III (Persero) dengan Kerangka Kerja Cobit 5, Institut Teknologi Sepuluh Nopember, Surabaya

Tashlihudin, A.B., 2016, Audit Sistem Informasi pada Sistem Admisi UIN Sunan Kalijaga Yogyakarta menggunakan *Framework* COBIT 4.1, UIN Sunan Kalijaga, Yogyakarta

LAMPIRAN

SURAT PERNYATAAN

Sehubungan dengan akan dilakukan kegiatan Audit Tata Kelola Teknologi Informasi pada BSML Regional II menggunakan framework COBIT 2019 dengan memperhatikan hal sebagai berikut:

1. Peraturan Menteri Perdagangan Nomor 46/M-DAG/PER/7/2017 tentang Penyelenggaraan Teknologi Informasi dan Komunikasi di Lingkungan Kementerian Perdagangan;
2. Persiapan reakreditasi Laboratorium Kalibrasi BSML Regional II;
3. Jumlah personel tim mutu 6 orang;
4. Beban kerja perkantoran dengan target yang meningkat 6 kali lipat dari tahun sebelumnya;

maka kami memutuskan untuk menetapkan target tingkat kapabilitas pada Audit Tata Kelola Teknologi Informasi pada BSML Regional II pada periode ini adalah level 2 (dua).

Demikian agar dapat menjadi perhatian bagi semua.

Yogyakarta, 3 Desember 2020
Ketua Tim Mutu

Arif Nurjaya, S.T., M.Eng

SURAT PERNYATAAN

Sehubungan dengan telah dilaksanakan kegiatan Audit Tata Kelola Teknologi Informasi pada BSML Regional II menggunakan framework COBIT 2019 dan telah dilakukan validasi hasil audit, maka dengan ini kami menyatakan bahwa kegiatan Audit Kelola Teknologi Informasi pada BSML Regional II yang dilaksanakan tanggal 3-13 Desember 2020 sudah menggunakan data yang valid. Seluruh temuan dan rekomendasi akan menjadi bahan yang akan dibahas dalam pertemuan tim mutu selanjutnya.

Demikian agar dapat menjadi perhatian bagi semua.

Yogyakarta, 14 Desember 2020

Ketua Tim Mutu

Arif Nurjaya, S.T., M.Eng

DAFTAR HADIR

BRIEFING AUDIT TATA KELOLA TEKNOLOGI INFORMASI 1,12,20

No.	Nama	Jabatan	Tanda Tangan
1	M Hendro Purnomo	Kepala Balai	
2	Eko Wachyudono	Sub Koordinator Tata Usaha	
3	Megawati	Senior Perencana Ahli	
4	Farida Nur Rizki	Bimbingan Kemetrologian	
5	Angga WNP	Auditor	
6	Anton Kurniadi	Senior Pranata Komputer	
7	AGUNG DWI Y.	PRANATA LABORATORIUM (Pelayanan Kemetrologian)	
8			
9			
10			
11			
13			
14			
15			
16			

KUESIONER SURVEY

Penilaian Capability Level EDM 03 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 **EDM 03 *Ensured Risk Optimization.*** 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat drukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Hendro Purnomo, ST. MSE
Email	
Seksi	Kepala Balai
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Evaluate, Direct, Monitor
Objek Tata kelola	: EDM 03 – Ensure Risk Optimization

Deskripsi:

Pastikan bahwa toleransi risiko perusahaan dipahami, diartikulasikan, dan dikomunikasikan, dan risiko terhadap nilai perusahaan yang terkait dengan penggunaan I&T diidentifikasi dan dikelola.

Tujuan:

Memastikan bahwa risiko perusahaan terkait I & T tidak melebihi kebijakan risiko dan toleransi risiko perusahaan, dampak risiko I&T terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan diminimalkan.

EDM03.01 Evaluate risk management

Secara terus menerus memeriksa dan mengevaluasi pengaruh risiko pada arus dan penggunaan I&T di masa mendatang di perusahaan. Pertimbangkan apakah risiko perusahaan kebijakan yang sesuai dan memastikan bahwa risiko terkait dengan nilai perusahaan penggunaan I&T diidentifikasi dan dikelola.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Memahami organisasi dan konteksnya yang terkait dengan risiko I&T.		✓							✓			
2	Mentukan kebijakan risiko organisasi, yaitu tingkat risiko terkait I & T yang ditetapkan oleh perusahaan untuk mencapai tujuan perusahaan.		✓							✓			
3	Mentukan tingkat toleransi risiko terhadap kebijakan risiko, yaitu penyimpangan yang masih ditoleransi	✓								✓			
4	Menentukan sejauh mana penyelarasan strategi risiko I&T dengan strategi risiko perusahaan dan memastikan kebijakan risiko berada di bawah kapasitas risiko organisasi		✓							✓			
5	Secara proaktif mengevaluasi faktor risiko I&T sebelum keputusan strategis perusahaan dan memastikan bahwa pertimbangan risiko merupakan bagian dari proses keputusan strategis perusahaan.		✓							✓			
6	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan mengenai kerugian terkait I & T dan toleransinya		✓							✓			
7	Mempertahankan personel yang diperlukan untuk mengelola Manajemen Risiko I&T	✓								✓			

EDM03.02 Direct risk management.

Mengarahkan pembentukan praktik manajemen risiko untuk menyediakan jaminan yang wajar bahwa praktik manajemen risiko I&T sesuai dan risiko I&T aktual tidak melebihi kebijakan risiko *stakeholder*.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Memastikan integrasi strategi risiko I&T ke dalam penerapan manajemen risiko dan kegiatan operasional.		✓							✓			
2	Mengarahkan pengembangan komunikasi risiko (mencakup semua tingkatan perusahaan).		✓							✓			
3	Penerapan langsung dari mekanisme yang sesuai untuk merespon dengan cepat terhadap perubahan risiko dan segera melaporkannya tingkat manajemen yang sesuai, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana dan bagaimana).		✓							✓			
4	Arahkan bahwa risiko, peluang, masalah, dapat diidentifikasi dan dilaporkan oleh siapa pun kepada pihak yang sesuai kapanpun. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan		✓							✓			
5	Identifikasi tujuan utama dari tata kelola risiko dan proses manajemen yang akan dipantau, dan identifikasi metode pengolahan data		✓							✓			

EDM03.03 Monitor risk management.

Pantau tujuan utama dan metrik proses manajemen risiko. Tentukan bagaimana penyimpangan atau masalah akan diidentifikasi, dilacak dan dilaporkan untuk remediasi.

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 masalah manajemen risiko kepada dewan atau komite eksekutif.		✓							✓			

2	Pantau sejauh mana profil risiko dikelola dalam kebijakan risiko dan ambang batas toleransi perusahaan		✓						✓			
3	Pantau tujuan utama tata kelola risiko dan proses manajemen terhadap target, analisis penyebab penyimpangan, dan memulai tindakan perbaikan untuk mengatasi penyebab yang mendasarinya.	✓							✓			
4	Memungkinkan peninjauan pemangku kepentingan atas kemajuan perusahaan menuju tujuan yang diidentifikasi		✓						✓			

KUESIONER SURVEY

Penilaian Capability Level APO 12 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan ditakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Megawati, SE, MPPM
Email	
Seksi	Senior Perencana Ahli
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Align, Plan, Organize
Objek Tata kelola	: APO 12 – Managed Risk
Deskripsi:	
Identifikasi, nilai, dan kurangi risiko terkait I & T secara berkelanjutan dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.	
Tujuan:	
Mengintegrasikan manajemen risiko perusahaan terkait I & T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola risiko perusahaan terkait I & T.	

APO 12.01 Collect Data

Identifikasi dan kumpulkan data yang relevan untuk mengaktifkan risiko terkait I & T yang efektif 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 risiko I&T.	✓								✓			
2	Catat data terkait risiko I&T yang relevan dan signifikan di lingkungan internal dan eksternal perusahaan.		✓							✓			
3	Mengadopsi atau mendefinisikan risiko untuk definisi yang konsisten dari skenario risiko dan dampak.		✓							✓			
4	Catat data tentang peristiwa risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak.		✓							✓			
5	Survei dan analisis data risiko I&T terkait kerugian dari data dan tren yang tersedia secara eksternal	✓								✓			
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi umum faktor di berbagai peristiwa.	✓								✓			
7	Tentukan kondisi spesifik yang dapat mempengaruhi risiko.		✓							✓			
8	Lakukan analisis faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.	✓								✓			

APO 12.02 Analyze Risk

Kembangkan pandangan yang dibuktikan tentang risiko I&T aktual, untuk mendukung keputusan risiko.

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 risiko, dengan mempertimbangkan semua faktor risiko.		✓							✓			
2	Membangun dan memperbarui skenario risiko I&T secara teratur; identifikasi kerugian terkait I & T	✓								✓			
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓							✓			
4	Bandingkan risiko saat ini (eksposur kerugian terkait I & T) dengan toleransi risiko yang dapat diterima.	✓								✓			
5	Mengusulkan respons risiko untuk risiko yang melebihi tingkat toleransi.		✓							✓			
6	Identifikasi persyaratan dan target untuk respons mitigasi risiko yang optimal.		✓							✓			
7	Validasi hasil analisis risiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.		✓							✓			
8	Menganalisis manfaat dari opsi respons risiko yang dipilih. Konfirmasikan respons risiko yang optimal.		✓							✓			

APO 12.03. Maintain A Risk Profile

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

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 bisnis dan proses manajemen layanan IT. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		✓							✓			
2	Menentukan dan menyetujui layanan IT dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.		✓							✓			
3	Mengumpulkan skenario risiko saat ini menurut kategori, lini bisnis, dan area fungsional.		✓							✓			
4	Secara teratur menangkap semua informasi profil risiko dan menggabungkannya ke dalam profil risiko gabungan.		✓							✓			
5	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.		✓							✓			
6	Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini secara cepat.		✓							✓			
7	Menangkap informasi tentang peristiwa risiko IT yang telah terwujud untuk dimasukkan dalam profil risiko IT perusahaan.	✓								✓			

APO 12.04. Articulate Risk

Komunikasikan informasi tentang status saat ini dari eksposur terkait I & T dan peluang 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 perusahaan.		✓							✓			
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait IT.		✓							✓			

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 IT 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 portfolio.

Kelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima 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 IT.	✓								✓			
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 IT		✓							✓			

APO 12.06. Respon to Risk

Menanggapi secara tepat waktu kejadian risiko 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Eko Wahyuliono, ST.MT
Email	
Seksi	Sub Koordinator Tata Usaha
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Align, Plan, Organize
Objek Tata kelola	: APO 12 – Managed Risk

Deskripsi:

Identifikasi, nilai, dan kurangi risiko terkait I & T secara berkelanjutan dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.

Tujuan:

Mengintegrasikan manajemen risiko perusahaan terkait I & T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola risiko perusahaan terkait I & T.

APO 12.01 Collect Data

Identifikasi dan kumpulkan data yang relevan untuk mengaktifkan risiko terkait I & T yang efektif 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 risiko I&T		✓							✓			
2	Catat data terkait risiko I&T yang relevan dan signifikan di lingkungan internal dan eksternal perusahaan		✓							✓			
3	Mengadopsi atau mendefinisikan risiko untuk definisi yang konsisten dari skenario risiko dan dampak	✓								✓			
4	Catat data tentang peristiwa risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak.	✓								✓			
5	Survei dan analisis data risiko I&T terkait kerugian dari data dan tren yang tersedia secara eksternal		✓							✓			
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi umum faktor di berbagai peristiwa.	✓								✓			
7	Tentukan kondisi spesifik yang dapat mempengaruhi risiko.		✓							✓			
8	Lakukan analisis faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.		✓							✓			

APO 12.02 Analyze Risk

Kembangkan pandangan yang dibuktikan tentang risiko I&T aktual, untuk mendukung keputusan risiko.

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 risiko, dengan mempertimbangkan semua faktor risiko.		✓							✓			
2	Membangun dan memperbarui skenario risiko I&T secara teratur; identifikasi kerugian terkait I & T	✓								✓			
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓							✓			
4	Bandingkan risiko saat ini (eksposur kerugian terkait I & T) dengan toleransi risiko yang dapat diterima.		✓							✓			
5	Mengusulkan respons risiko untuk risiko yang melebihi tingkat toleransi.		✓							✓			
6	Identifikasi persyaratan dan target untuk respons mitigasi risiko yang optimal.	✓								✓			
7	Validasi hasil analisis risiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.		✓							✓			
8	Menganalisis manfaat dari opsi respons risiko yang dipilih. Konfirmasikan respons risiko yang optimal.	✓								✓			

APO 12.03. Maintain A Risk Profile

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

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 bisnis dan proses manajemen layanan IT. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		✓							✓			
2	Menentukan dan menyetujui layanan IT dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.		✓							✓			
3	Mengumpulkan skenario risiko saat ini menurut kategori, lini bisnis, dan area fungsional.	✓								✓			
4	Secara teratur menangkap semua informasi profil risiko dan menggabungkannya ke dalam profil risiko gabungan.		✓							✓			
5	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	✓								✓			
6	Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini secara cepat.		✓							✓			
7	Menangkap informasi tentang peristiwa risiko IT yang telah terwujud untuk dimasukkan dalam profil risiko IT perusahaan..	✓								✓			

APO 12.04. Articulate Risk

Komunikasikan informasi tentang status saat ini dari eksposur terkait I & T dan peluang 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 perusahaan.		✓							✓			
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait IT.		✓							✓			

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 IT 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 portfolio.

Kelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima 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 IT.		✓							✓			
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 IT		✓							✓			

APO 12.06. Respon to Risk

Menanggapi secara tepat waktu kejadian risiko 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Name Responden	Farida Nur Rifqi, S.Si., M.Sc.
Email	farida.nur@yahoo.com.sg
Seksi	Bimbingan Kemasyarakatan
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Align, Plan, Organize
Objek Tata kelola	: APO 12 – Managed Risk

Deskripsi:

Identifikasi, nilai, dan kurangi risiko terkait I & T secara berkelanjutan dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.

Tujuan:

Mengintegrasikan manajemen risiko perusahaan terkait I & T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola risiko perusahaan terkait I & T.

APO 12.01 Collect Data

Identifikasi dan kumpulkan data yang relevan untuk mengaktifkan risiko terkait I & T yang efektif 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 risiko I&T.	✓								✓			
2	Catat data terkait risiko I&T yang relevan dan signifikan di lingkungan internal dan eksternal perusahaan		✓							✓			
3	Mengadopsi atau mendefinisikan risiko untuk definisi yang konsisten dari skenario risiko dan dampak		✓							✓			
4	Catat data tentang peristiwa risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak.		✓							✓			
5	Survei dan analisis data risiko I&T terkait kerugian dari data dan tren yang tersedia secara eksternal		✓							✓			
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi umum faktor di berbagai peristiwa.	✓								✓			
7	Tentukan kondisi spesifik yang dapat mempengaruhi risiko.		✓							✓			
8	Lakukan analisis faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.		✓							✓			

APO 12.02 Analyze Risk

Kembangkan pandangan yang dibuktikan tentang risiko I&T aktual, untuk mendukung keputusan risiko.

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 risiko, dengan mempertimbangkan semua faktor risiko.		✓							✓			
2	Membangun dan memperbarui skenario risiko I&T secara teratur; identifikasi kerugian terkait I & T	✓								✓			
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓							✓			
4	Bandingkan risiko saat ini (eksposur kerugian terkait I & T) dengan toleransi risiko yang dapat diterima.		✓							✓			
5	Mengusulkan respons risiko untuk risiko yang melebihi tingkat toleransi.		✓							✓			
6	Identifikasi persyaratan dan target untuk respons mitigasi risiko yang optimal.	✓								✓			
7	Validasi hasil analisis risiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	✓								✓			
8	Menganalisis manfaat dari opsi respons risiko yang dipilih. Konfirmasikan respons risiko yang optimal.		✓							✓			

APO 12.03. Maintain A Risk Profile

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

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 bisnis dan proses manajemen layanan IT. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		✓							✓			
2	Menentukan dan menyetujui layanan IT dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.		✓							✓			
3	Mengumpulkan skenario risiko saat ini menurut kategori, lini bisnis, dan area fungsional.		✓							✓			
4	Secara teratur menangkap semua informasi profil risiko dan menggabungkannya ke dalam profil risiko gabungan.	✓								✓			
5	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.		✓							✓			
6	Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini secara cepat.		✓							✓			
7	Menangkap informasi tentang peristiwa risiko IT yang telah terwujud untuk dimasukkan dalam profil risiko IT perusahaan..	✓								✓			

APO 12.04. Articulate Risk

Komunikasikan informasi tentang status saat ini dari eksposur terkait I & T dan peluang 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 perusahaan.		✓							✓			
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait IT.		✓							✓			

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 IT 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 portfolio.

Kelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima 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 IT.		✓							✓			
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 IT	✓								✓			

APO 12.06. Respon to Risk

Menanggapi secara tepat waktu kejadian risiko 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	ACUNG DWI YULIANTA, S.T., M.Eng.
Email	agungdy@gmail.com
Seksi	PENGAWASAN KEMETROLOGIAN
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Align, Plan, Organize
Objek Tata kelola	: APO 12 – Managed Risk

Deskripsi:

Identifikasi, nilai, dan kurangi risiko terkait I & T secara berkelanjutan dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.

Tujuan:

Mengintegrasikan manajemen risiko perusahaan terkait I & T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola risiko perusahaan terkait I & T.

APO 12.01 Collect Data

Identifikasi dan kumpulkan data yang relevan untuk mengaktifkan risiko terkait I & T yang efektif 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 risiko I&T.		✓							✓			
2	Catat data terkait risiko I&T yang relevan dan signifikan di lingkungan internal dan eksternal perusahaan	✓								✓			
3	Mengadopsi atau mendefinisikan risiko untuk definisi yang konsisten dari skenario risiko dan dampak		✓							✓			
4	Catat data tentang peristiwa risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak.		✓							✓			
5	Survei dan analisis data risiko I&T terkait kerugian dari data dan tren yang tersedia secara eksternal		✓							✓			
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi umum faktor di berbagai peristiwa.	✓								✓			
7	Tentukan kondisi spesifik yang dapat mempengaruhi risiko.		✓							✓			
8	Lakukan analisis faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.		✓							✓			

APO 12.02 Analyze Risk

Kembangkan pandangan yang dibuktikan tentang risiko I&T aktual, untuk mendukung keputusan risiko.

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 risiko, dengan mempertimbangkan semua faktor risiko.	✓								✓			
2	Membangun dan memperbarui skenario risiko I&T secara teratur, identifikasi kerugian terkait I & T		✓							✓			
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓							✓			
4	Bandingkan risiko saat ini (eksposur kerugian terkait I & T) dengan toleransi risiko yang dapat diterima.		✓							✓			
5	Mengusulkan respons risiko untuk risiko yang melebihi tingkat toleransi.		✓							✓			
6	Identifikasi persyaratan dan target untuk respons mitigasi risiko yang optimal.	✓								✓			
7	Validasi hasil analisis risiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.	✓								✓			
8	Menganalisis manfaat dari opsi respons risiko yang dipilih. Konfirmasikan respons risiko yang optimal.	✓								✓			

APO 12.03. Maintain A Risk Profile

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

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 bisnis dan proses manajemen layanan IT. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.	✓								✓			
2	Menentukan dan menyetujui layanan IT dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.		✓							✓			
3	Mengumpulkan skenario risiko saat ini menurut kategori, lini bisnis, dan area fungsional.		✓							✓			
4	Secara teratur menangkap semua informasi profil risiko dan menggabungkannya ke dalam profil risiko gabungan.		✓							✓			
5	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.		✓							✓			
6	Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini secara cepat.		✓							✓			
7	Menangkap informasi tentang peristiwa risiko IT yang telah terwujud untuk dimasukkan dalam profil risiko IT perusahaan.		✓							✓			

APO 12.04. Articulate Risk

Komunikasikan informasi tentang status saat ini dari eksposur terkait I & T dan peluang 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 perusahaan.		✓							✓			
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait IT.		✓							✓			

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 IT 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 portfolio.

Kelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima 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 IT.	✓								✓			
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 IT		✓							✓			

APO 12.06. Respon to Risk

Menanggapi secara tepat waktu kejadian risiko 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 terbentinya 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Anton Kurniadi, S.Kom
Email	
Seksi	Senior Pranata Komputer
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Align, Plan, Organize
Objek Tata kelola	: APO 12 – Managed Risk

Deskripsi:

Identifikasi, nilai, dan kurangi risiko terkait I & T secara berkelanjutan dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.

Tujuan:

Mengintegrasikan manajemen risiko perusahaan terkait I & T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat mengelola risiko perusahaan terkait I & T.

APO 12.01 Collect Data

Identifikasi dan kumpulkan data yang relevan untuk mengaktifkan risiko terkait I & T yang efektif 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 risiko I&T.		✓							✓			
2	Catat data terkait risiko I&T yang relevan dan signifikan di lingkungan internal dan eksternal perusahaan	✓								✓			
3	Mengadopsi atau mendefinisikan risiko untuk definisi yang konsisten dari skenario risiko dan dampak		✓							✓			
4	Catat data tentang peristiwa risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai kategori dampak		✓							✓			
5	Survei dan analisis data risiko I&T terkait kerugian dari data dan tren yang tersedia secara eksternal	✓								✓			
6	Melakukan pengelolaan data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi umum faktor di berbagai peristiwa.		✓							✓			
7	Tentukan kondisi spesifik yang dapat mempengaruhi risiko.		✓							✓			
8	Lakukan analisis faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.		✓							✓			

APO 12.02 Analyze Risk

Kembangkan pandangan yang dibuktikan tentang risiko I&T aktual, untuk mendukung keputusan risiko.

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 risiko, dengan mempertimbangkan semua faktor risiko.	✓								✓			
2	Membangun dan memperbarui skenario risiko I&T secara teratur; identifikasi kerugian terkait I & T		✓							✓			
3	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		✓							✓			
4	Bandingkan risiko saat ini (eksposur kerugian terkait I & T) dengan toleransi risiko yang dapat diterima.		✓							✓			
5	Mengusulkan respons risiko untuk risiko yang melebihi tingkat toleransi.		✓							✓			
6	Identifikasi persyaratan dan target untuk respons mitigasi risiko yang optimal.	✓								✓			
7	Validasi hasil analisis risiko dan analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis sejalan dengan persyaratan perusahaan.		✓							✓			
8	Menganalisis manfaat dari opsi respons risiko yang dipilih. Konfirmasikan respons risiko yang optimal.		✓							✓			

APO 12.03. Maintain A Risk Profile

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

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 bisnis dan proses manajemen layanan IT. Identifikasi personel, pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.	✓								✓			
2	Menentukan dan menyetujui layanan IT dan sumber daya infrastruktur IT mana yang penting untuk menopang operasi proses bisnis.		✓							✓			
3	Mengumpulkan skenario risiko saat ini menurut kategori, lini bisnis, dan area fungsional.		✓							✓			
4	Secara teratur menangkap semua informasi profil risiko dan menggabungkannya ke dalam profil risiko gabungan.		✓							✓			
5	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.		✓							✓			
6	Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini secara cepat.	✓								✓			
7	Menangkap informasi tentang peristiwa risiko IT yang telah terwujud untuk dimasukkan dalam profil risiko IT perusahaan..		✓							✓			

APO 12.04. Articulate Risk

Komunikasikan informasi tentang status saat ini dari eksposur terkait I & T dan peluang 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 perusahaan.		✓							✓			
2	Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan skenario paling mungkin, eksposur kerugian terkait IT.		✓							✓			

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 IT 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 portfolio

Kelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima 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 IT.		✓							✓			
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 IT	✓								✓			

APO 12.06. Respon to Risk

Menanggapi secara tepat waktu kejadian risiko 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 DSS 02 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 ***DSS02 - Managed Service Requests and Incidents.*** 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Eko Wahyudiono, ST, MT
Email	
Seksi	Sub Koordinator Tata Usaha
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Tata kelola	: DSS02 Managed Service Requests and Incidents

Deskripsi:

Memberikan tanggapan yang tepat waktu dan efektif untuk permintaan pengguna dan penyelesaian semua jenis insiden. Kembalikan layanan normal; rekam dan penuhi pengguna permintaan; dan merekam, menyelidiki, mendiagnosis, meningkatkan, dan menyelesaikan insiden.

Tujuan:

Capai peningkatan produktivitas dan minimalkan gangguan melalui resolusi cepat atas kueri dan insiden pengguna. Menilai dampak perubahan dan menangani insiden layanan. Selesaikan permintaan pengguna dan pulihkan layanan sebagai tanggapan atas insiden.

DSS02.01 Define classification schemes for incidents and service requests

Tentukan skema klasifikasi dan model untuk insiden dan permintaan layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Gunakan informasi untuk memastikan pendekatan yang konsisten untuk menangani dan menginformasikan pengguna tentang masalah.	✓								✓			
2	Tentukan skema solusi bagi sebuah insiden untuk memungkinkan penyelesaian yang efisien dan efektif.	✓								✓			
3	Tentukan model permintaan layanan sesuai dengan jenis permintaan layanan untuk mengaktifkan layanan mandiri dan efisien.		✓							✓			
4	Tetapkan aturan dan prosedur tingkatan insiden terutama di bidang keamanan IT.		✓							✓			
5	Definisikan sumber pengetahuan tentang insiden dan permintaan dan jelaskan bagaimana menggunakannya.		✓							✓			

DSS02.02 Record, classify and prioritize requests and incidents

Identifikasi, catat, dan klasifikasikan permintaan dan insiden layanan serta tetapkan prioritas sesuai dengan kekritisan bisnis dan perjanjian layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Catat semua permintaan, insiden layanan,		✓							✓			

	informasi yang relevan, sehingga dapat ditangani secara efektif.												
2	Untuk mengaktifkan analisis tren, klasifikasikan permintaan layanan dan insiden berdasarkan jenis dan kategori.		✓						✓				
3	Memprioritaskan permintaan layanan dan insiden berdasarkan definisi layanan SLA tentang dampak dan urgensi bisnis.		✓						✓				

DSS02.03 Verify, approve and fulfill service requests

Pilih prosedur permintaan yang sesuai dan verifikasi bahwa layanan permintaan memenuhi kriteria permintaan yang ditentukan. Dapatkan persetujuan, jika diperlukan, dan memenuhi permintaan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi semua permintaan layanan menggunakan prosedur yang ada.		✓							✓			
2	Setiap perubahan standar yang disepakati dilakukan pengesahan melalui penandatangan dokumen.		✓							✓			
3	Memenuhi permintaan dengan melakukan prosedur permintaan yang dipilih. Jika memungkinkan, gunakan menu otomatis bantuan mandiri untuk item yang sering diminta.		✓							✓			

DSS02.04 Investigate, diagnose and allocate incidents

Identifikasi dan catat gejala insiden, tentukan kemungkinan penyebabnya, dan alokasikan untuk resolusi.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Identifikasi dan analisa gejala yang relevan untuk menetapkan kemungkinan penyebab insiden. Gunakan referensi pengetahuan.		✓							✓			
2	Jika ada potensi permasalahan maka harus dicatat sebagai input masalah baru.		✓							✓			

3	Mendistribusikan pengelolaan insiden kepada personel yang memiliki keahlian dan tupoksi tertentu.	✓								✓			

DSS02.05 Resolve and recover from incidents

Dokumentasikan, terapkan, dan uji solusi atau solusi yang diidentifikasi. Lakukan tindakan pemulihan untuk memulihkan layanan terkait I & T.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Pilih dan terapkan resolusi insiden yang paling tepat		✓							✓			
2	Catat apakah solusi yang digunakan tepat	✓								✓			
3	Lakukan tindakan pemulihan setelah terjadi insiden.		✓							✓			
4	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat digunakan sebagai sumber pengetahuan di masa mendatang	✓								✓			

DSS02.06 Close service requests and incidents

Verifikasi penyelesaian insiden yang memuaskan dan / atau pemenuhan permintaan, dan tutup

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi dengan konsumen atau pengguna, mengenai kepuasan pelayanan		✓							✓			
2	Tutup permintaan layanan dan insiden		✓							✓			

DSS02.07 Track status and produce reports.

Lacak, analisis, dan laporkan insiden dan pemenuhan permintaan secara teratur. Periksa tren untuk memberikan informasi untuk peningkatan berkelanjutan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Melakukan pemantauan terhadap eskalasi insiden dan status terhadap temuan insiden yang baru	✓								✓			
2	Identifikasi informasi pemangku kepentingan dan kebutuhan mereka akan data atau laporan.		✓							✓			
3	Menghasilkan dan mendistribusikan laporan tepat waktu dan atau dapat dilakukan melalui online.		✓							✓			
4	Menganalisis insiden dan permintaan layanan menurut kategori dan jenis.		✓							✓			
5	Gunakan informasi sebagai masukan untuk perencanaan perbaikan berkelanjutan.	✓								✓			

KUESIONER SURVEY

Penilaian Capability Level DSS 02 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 ***DSS02 - Managed Service Requests and Incidents.*** 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Farida Nur Rifai, S.Si., M.Sc.
Email	farida9021@yahoo.com.sg
Seksi	Bimbingan Kemoteologian
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Tata kelola	: DSS02 Managed Service Requests and Incidents

Deskripsi:

Memberikan tanggapan yang tepat waktu dan efektif untuk permintaan pengguna dan penyelesaian semua jenis insiden. Kembalikan layanan normal; rekam dan penuhi pengguna permintaan; dan merekam, menyelidiki, mendiagnosis, meningkatkan, dan menyelesaikan insiden.

Tujuan:

Capai peningkatan produktivitas dan minimalkan gangguan melalui resolusi cepat atas kueri dan insiden pengguna. Menilai dampak perubahan dan menangani insiden layanan. Selesaikan permintaan pengguna dan pulihkan layanan sebagai tanggapan atas insiden.

DSS02.01 Define classification schemes for incidents and service requests.

Tentukan skema klasifikasi dan model untuk insiden dan permintaan layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Gunakan informasi untuk memastikan pendekatan yang konsisten untuk menangani dan menginformasikan pengguna tentang masalah.		✓							✓			
2	Tentukan skema solusi bagi sebuah insiden untuk memungkinkan penyelesaian yang efisien dan efektif.		✓							✓			
3	Tentukan model permintaan layanan sesuai dengan jenis permintaan layanan untuk mengaktifkan layanan mandiri dan efisien.	✓								✓			
4	Tetapkan aturan dan prosedur tingkatan insiden terutama di bidang keamanan IT.		✓							✓			
5	Definisikan sumber pengetahuan tentang insiden dan permintaan dan jelaskan bagaimana menggunakannya.	✓								✓			

DSS02.02 Record, classify and prioritize requests and incidents

Identifikasi, catat, dan klasifikasikan permintaan dan insiden layanan serta tetapkan prioritas sesuai dengan kekritisan bisnis dan perjanjian layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Catat semua permintaan, insiden layanan,		✓							✓			

	informasi yang relevan, sehingga dapat ditangani secara efektif.												
2	Untuk mengaktifkan analisis tren, klasifikasikan permintaan layanan dan insiden berdasarkan jenis dan kategori.		✓							✓			
3	Memprioritaskan permintaan layanan dan insiden berdasarkan definisi layanan SLA tentang dampak dan urgensi bisnis.		✓							✓			

DSS02.03 Verify, approve and fulfill service requests

Pilih prosedur permintaan yang sesuai dan verifikasi bahwa layanan permintaan memenuhi kriteria permintaan yang ditentukan. Dapatkan persetujuan, jika diperlukan, dan memenuhi permintaan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi semua permintaan layanan menggunakan prosedur yang ada.		✓							✓			
2	Setiap perubahan standar yang disepakati dilakukan pengesahan melalui penandatangan dokumen.		✓							✓			
3	Memenuhi permintaan dengan melakukan prosedur permintaan yang dipilih. Jika memungkinkan, gunakan menu otomatis bantuan mandiri untuk item yang sering diminta.	✓								✓			

DSS02.04 Investigate, diagnose and allocate incidents

Identifikasi dan catat gejala insiden, tentukan kemungkinan penyebabnya, dan alokasikan untuk resolusi.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Identifikasi dan analisa gejala yang relevan untuk menetapkan kemungkinan penyebab insiden. Gunakan referensi pengetahuan.		✓							✓			
2	Jika ada potensi permasalahan maka harus dicatat sebagai input masalah baru.		✓							✓			

3	Mendistribusikan pengelolaan insiden kepada personel yang memiliki keahlian dan tupoksi tertentu.	✓								✓				

DSS02.05 Resolve and recover from incidents

Dokumentasikan, terapkan, dan uji solusi atau solusi yang diidentifikasi. Lakukan tindakan pemulihan untuk memulihkan layanan terkait I & T.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Pilih dan terapkan resolusi insiden yang paling tepat		✓							✓			
2	Catat apakah solusi yang digunakan tepat	✓								✓			
3	Lakukan tindakan pemulihan setelah terjadi insiden.		✓							✓			
4	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat digunakan sebagai sumber pengetahuan di masa mendatang		✓							✓			

DSS02.06 Close service requests and incidents

Verifikasi penyelesaian insiden yang memuaskan dan / atau pemenuhan permintaan, dan tutup

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi dengan konsumen atau pengguna, mengenai kepuasan pelayanan		✓							✓			
2	Tutup permintaan layanan dan insiden		✓							✓			

DSS02.07 Track status and produce reports.

Lacak, analisis, dan laporkan insiden dan pemenuhan permintaan secara teratur. Periksa tren untuk memberikan informasi untuk peningkatan berkelanjutan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Melakukan pemantauan terhadap eskalasi insiden dan status terhadap temuan insiden yang baru	✓								✓			
2	Identifikasi informasi pemangku kepentingan dan kebutuhan mereka akan data atau laporan.		✓							✓			
3	Menghasilkan dan mendistribusikan laporan tepat waktu dan atau dapat dilakukan melalui online.		✓							✓			
4	Menganalisis insiden dan permintaan layanan menurut kategori dan jenis		✓							✓			
5	Gunakan informasi sebagai masukan untuk perencanaan perbaikan berkelanjutan.	✓								✓			

KUESIONER SURVEY

Penilaian Capability Level DSS 02 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 ***DSS02 - Managed Service Requests and Incidents.*** 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	AGUNG DWI YULIANTA, S.T., M.Eng
Email	agungdy@gmail.com
Seksi	PELAYANAN METROLOGIAN
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Tata kelola	: DSS02 Managed Service Requests and Incidents

Deskripsi:

Memberikan tanggapan yang tepat waktu dan efektif untuk permintaan pengguna dan penyelesaian semua jenis insiden. Kembalikan layanan normal; rekam dan penuhi pengguna permintaan; dan merekam, menyelidiki, mendiagnosis, meningkatkan, dan menyelesaikan insiden.

Tujuan:

Capai peningkatan produktivitas dan minimalkan gangguan melalui resolusi cepat atas kueri dan insiden pengguna. Menilai dampak perubahan dan menangani insiden layanan. Selesaikan permintaan pengguna dan pulihkan layanan sebagai tanggapan atas insiden.

DSS02.01. Define classification schemes for incidents and service requests.

Tentukan skema klasifikasi dan model untuk insiden dan permintaan layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Gunakan informasi untuk memastikan pendekatan yang konsisten untuk menangani dan menginformasikan pengguna tentang masalah.	✓								✓			
2	Tentukan skema solusi bagi sebuah insiden untuk memungkinkan penyelesaian yang efisien dan efektif.		✓							✓			
3	Tentukan model permintaan layanan sesuai dengan jenis permintaan layanan untuk mengaktifkan layanan mandiri dan efisien.	✓								✓			
4	Tetapkan aturan dan prosedur tingkatan insiden terutama di bidang keamanan IT.		✓							✓			
5	Definisikan sumber pengetahuan tentang insiden dan permintaan dan jelaskan bagaimana menggunakannya.		✓							✓			

DSS02.02 Record, classify and prioritize requests and incidents

Identifikasi, catat, dan klasifikasikan permintaan dan insiden layanan serta tetapkan prioritas sesuai dengan kekritisan bisnis dan perjanjian layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Catat semua permintaan, insiden layanan,		✓							✓			

	informasi yang relevan, sehingga dapat ditangani secara efektif.												
2	Untuk mengaktifkan analisis tren, klasifikasikan permintaan layanan dan insiden berdasarkan jenis dan kategori.		✓						✓				
3	Memprioritaskan permintaan layanan dan insiden berdasarkan definisi layanan SLA tentang dampak dan urgensi bisnis.		✓						✓				

DSS02.03 Verify, approve and fulfill service requests

Pilih prosedur permintaan yang sesuai dan verifikasi bahwa layanan permintaan memenuhi kriteria permintaan yang ditentukan. Dapatkan persetujuan, jika diperlukan, dan memenuhi permintaan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi semua permintaan layanan menggunakan prosedur yang ada.		✓							✓			
2	Setiap perubahan standar yang disepakati dilakukan pengesahan melaui penandatangan dokumen.		✓							✓			
3	Memenuhi permintaan dengan melakukan prosedur permintaan yang dipilih. Jika memungkinkan, gunakan menu otomatis bantuan mandiri untuk item yang sering diminta.		✓							✓			

DSS02.04 Investigate, diagnose and allocate incidents.

Identifikasi dan catat gejala insiden, tentukan kemungkinan penyebabnya, dan alokasikan untuk resolusi.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Identifikasi dan analisa gejala yang relevan untuk menetapkan kemungkinan penyebab insiden. Gunakan referensi pengetahuan.		✓							✓			
2	Jika ada potensi permasalahan maka harus dicatat sebagai input masalah baru.		✓							✓			

3	Mendistribusikan pengelolaan insiden kepada personel yang memiliki keahlian dan tupoksi tertentu.		✓							✓			

DSS02.05 Resolve and recover from incidents

Dokumentasikan, terapkan, dan uji solusi atau solusi yang diidentifikasi. Lakukan tindakan pemulihan untuk memulihkan layanan terkait I & T.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Pilih dan terapkan resolusi insiden yang paling tepat	✓								✓			
2	Catat apakah solusi yang digunakan tepat		✓							✓			
3	Lakukan tindakan pemulihan setelah terjadi insiden.		✓							✓			
4	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat digunakan sebagai sumber pengetahuan di masa mendatang		✓							✓			

DSS02.06 Close service requests and incidents

Verifikasi penyelesaian insiden yang memuaskan dan / atau pemenuhan permintaan, dan tutup

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi dengan konsumen atau pengguna, mengenai kepuasan pelayanan		✓							✓			
2	Tutup permintaan layanan dan insiden		✓							✓			

DSS02.07 Track status and produce reports

Lacak, analisis, dan laporkan insiden dan pemenuhan permintaan secara teratur. Periksa tren untuk memberikan informasi untuk peningkatan berkelanjutan.

NO	Aktivitas Tata Kelola	As – Is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Melakukan pemantauan terhadap eskalasi insiden dan status terhadap tematan insiden yang baru	✓								✓			
2	Identifikasi informasi pemangku kepentingan dan kebutuhan mereka akan data atau laporan.		✓							✓			
3	Menghasilkan dan mendistribusikan laporan tepat waktu dan atau dapat dilakukan melalui online.		✓							✓			
4	Menganalisis insiden dan permintaan layanan menurut kategori dan jenis.		✓							✓			
5	Gunakan informasi sebagai masukan untuk perencanaan perbaikan berkelanjutan.	✓								✓			

KUESIONER SURVEY

Penilaian Capability Level DSS 02 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra mahasswa 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 ***DSS02 - Managed Service Requests and Incidents***. 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Antoni Kurniadi, S.Kom
Email	
Seksi	Senior Pranata Komputer
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Tata kelola	: DSS02 Managed Service Requests and Incidents

Deskripsi:

Memberikan tanggapan yang tepat waktu dan efektif untuk permintaan pengguna dan penyelesaian semua jenis insiden. Kembalikan layanan normal; rekam dan penuhi pengguna permintaan; dan merekam, menyelidiki, mendiagnosis, meningkatkan, dan menyelesaikan insiden.

Tujuan:

Capai peningkatan produktivitas dan minimalkan gangguan melalui resolusi cepat atas kueri dan insiden pengguna. Menilai dampak perubahan dan menangani insiden layanan. Selesaikan permintaan pengguna dan pulihkan layanan sebagai tanggapan atas insiden.

DSS02.01. Define classification schemes for incidents and service requests.

Tentukan skema klasifikasi dan model untuk insiden dan permintaan layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Gunakan informasi untuk memastikan pendekatan yang konsisten untuk menangani dan menginformasikan pengguna tentang masalah.		✓							✓			
2	Tentukan skema solusi bagi sebuah insiden untuk memungkinkan penyelesaian yang efisien dan efektif.	✓								✓			
3	Tentukan model permintaan layanan sesuai dengan jenis permintaan layanan untuk mengaktifkan layanan mandiri dan efisien.		✓							✓			
4	Tetapkan aturan dan prosedur tingkatan insiden terutama di bidang keamanan IT.		✓							✓			
5	Definisikan sumber pengetahuan tentang insiden dan permintaan dan jelaskan bagaimana menggunakannya.		✓							✓			

DSS02.02 Record, classify and prioritize requests and incidents

Identifikasi, catat, dan klasifikasikan permintaan dan insiden layanan serta tetapkan prioritas sesuai dengan kekritisan bisnis dan perjanjian layanan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Catat semua permintaan, insiden layanan,		✓							✓			

	informasi yang relevan, sehingga dapat ditangani secara efektif.												
2	Untuk mengaktifkan analisis tren, klasifikasikan permintaan layanan dan insiden berdasarkan jenis dan kategori.		✓						✓				
3	Memprioritaskan permintaan layanan dan insiden berdasarkan definisi layanan SLA tentang dampak dan urgensi bisnis.		✓						✓				

DSS02.03 Verify, approve and fulfill service requests

Pilih prosedur permintaan yang sesuai dan verifikasi bahwa layanan permintaan memenuhi kriteria permintaan yang ditentukan. Dapatkan persetujuan, jika diperlukan, dan memenuhi permintaan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi semua permintaan layanan menggunakan prosedur yang ada.		✓							✓			
2	Setiap perubahan standar yang disepakati dilakukan pengesahan melalui penandatangan dokumen.		✓							✓			
3	Memenuhi permintaan dengan melakukan prosedur permintaan yang dipilih. Jika memungkinkan, gunakan menu otomatis bantuan mandiri untuk item yang sering diminta.		✓							✓			

DSS02.04 Investigate, diagnose and allocate incidents

Identifikasi dan catat gejala insiden, tentukan kemungkinan penyebabnya, dan alokasikan untuk resolusi.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Identifikasi dan analisa gejala yang relevan untuk menetapkan kemungkinan penyebab insiden. Gunakan referensi pengetahuan.		✓							✓			
2	Jika ada potensi permasalahan maka harus dicatat sebagai input masalah baru.		✓							✓			

3	Mendistribusikan pengelolaan insiden kepada personel yang memiliki keahlian dan tupoksi tertentu.		✓							✓				

DSS02.05 Resolve and recover from incidents

Dokumentasikan, terapkan, dan uji solusi atau solusi yang diidentifikasi. Lakukan tindakan pemulihan untuk memulihkan layanan terkait I & T.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Pilih dan terapkan resolusi insiden yang paling tepat	✓								✓			
2	Catat apakah solusi yang digunakan tepat		✓							✓			
3	Lakukan tindakan pemulihan setelah terjadi insiden.		✓							✓			
4	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat digunakan sebagai sumber pengetahuan di masa mendatang		✓							✓			

DSS02.06 Close service requests and incidents

Verifikasi penyelesaian insiden yang memuaskan dan / atau pemenuhan permintaan, dan tutup

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Verifikasi dengan konsumen atau pengguna, mengenai kepuasan pelayanan		✓							✓			
2	Tutup permintaan layanan dan insiden		✓							✓			

DSS02.07 Track status and produce reports.

Lacak, analisis, dan laporkan insiden dan pemenuhan permintaan secara teratur. Periksa tren untuk memberikan informasi untuk peningkatan berkelanjutan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Melakukan pemantauan terhadap eskalasi insiden dan status terhadap temuan insiden yang baru	✓								✓			
2	Identifikasi informasi pemangku kepentingan dan kebutuhan mereka akan data atau laporan.		✓							✓			
3	Menghasilkan dan mendistribusikan laporan tepat waktu dan atau dapat dilakukan melalui online.		✓							✓			
4	Menganalisis insiden dan permintaan layanan menurut kategori dan jenis		✓							✓			
5	Gunakan informasi sebagai masukan untuk perencanaan perbaikan berkelanjutan.	✓								✓			

KUESIONER SURVEY

Penilaian Capability Level DSS 04 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 ***DSS04 - Managed Continuity.*** 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Eko Wachyudiono, ST, MT
Email	
Seksi	Sub Koordinator Tata Usaha
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Manajemen	: DSS04 Managed Continuity

Deskripsi:

Tetapkan dan pertahankan rencana untuk memungkinkan bisnis dan organisasi TI merespons insiden dan dengan cepat beradaptasi dengan gangguan. Ini akan memungkinkan operasi berkelanjutan dari proses bisnis penting dan layanan I&T yang diperlukan serta menjaga ketersediaan sumber daya, aset, dan informasi di tingkat yang dapat diterima perusahaan

Tujuan:

Beradaptasi dengan cepat, lanjutkan operasi bisnis dan pertahankan ketersediaan sumber daya dan informasi pada tingkat yang dapat diterima oleh perusahaan dalam acara tersebut gangguan yang signifikan (misalnya, ancaman, peluang, permintaan).

DSS04.01 Define the business continuity policy, objectives and scope

Tentukan kebijakan dan cakupan kelangsungan bisnis, selaras dengan perusahaan dan tujuan pemangku kepentingan, untuk meningkatkan ketahanan bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengidentifikasi proses bisnis internal dan outsourcing yang diperlukan untuk memenuhi kewajiban hukum.		✓							✓			
2	Mengidentifikasi stakeholder yang bertanggung jawab untuk mendefinisikan dan menyetujui kebijakan dan ruang lingkup keberlanjutan bisnis.		✓							✓			
3	Tentukan dan dokumentasikan tujuan dan ruang lingkup kebijakan untuk ketahanan bisnis.		✓							✓			
4	Mengidentifikasi proses bisnis pendukung yang penting dan layanan IT terkait.		✓							✓			

DSS04.02 Maintain business resilience

Evaluasi pilihan ketahanan bisnis dan pilih yang hemat biaya dan strategi yang layak yang akan memastikan kelangsungan perusahaan, pemulihan bencana dan penanganan insiden saat menghadapi bencana atau kejadian besar lainnya atau gangguan

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5

1	Identifikasi potensi yang mungkin menimbulkan peristiwa yang dapat mengganggu secara signifikan.	✓								✓				
2	Melakukan analisis dampak bisnis untuk mengevaluasi dampak dari waktu ke waktu dari gangguan terhadap proses bisnis.		✓							✓				
3	Tetapkan waktu minimum yang diperlukan untuk memulihkan proses bisnis, berdasarkan penetapan toleransi	✓								✓				
4	Identifikasi stakeholder yang berpengaruh terhadap keberlangsungan proses bisnis.		✓							✓				
5	Identifikasi tindakan yang akan mengurangi kemungkinan dan dampak melalui peningkatan pencegahan dan peningkatan ketahanan.		✓							✓				
6	Menganalisis persyaratan kontinuitas untuk mengidentifikasi kemungkinan bisnis strategis.	✓								✓				
7	Identifikasi kebutuhan sumber daya dan biaya untuk setiap opsi teknis strategis dan buat rekomendasi strategis.	✓								✓				
8	Dapatkan persetujuan pimpinan untuk opsi strategis yang dipilih.	✓								✓				

DSS04.03 Develop and implement a business continuity response
Mengembangkan rencana kesinambungan bisnis (BCP) dan rencana pemulihan bencana (DRP) berdasarkan strategi. Dokumentasikan semua prosedur yang diperlukan untuk perusahaan untuk melanjutkan aktivitas kritis jika terjadi insiden

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tentukan tindakan respons insiden dan komunikasi yang akan diambil jika terjadi gangguan.		✓							✓			
2	Pastikan mitra outsourcing memiliki rencana kesinambungan yang efektif.	✓								✓			
3	Tentukan kondisi dan prosedur pemulihan yang akan memungkinkan dimulainya kembali pelayanan.		✓							✓			

4	Mengembangkan dan memelihara BCP dan DRP yang berisi prosedur yang harus diikuti untuk memungkinkan kelanjutan proses bisnis.	✓								✓				
5	Tentukan dan dokumentasikan sumber daya yang diperlukan untuk mendukung kelangsungan dan prosedur pemulihan, dengan mempertimbangkan orang, fasilitas dan infrastruktur IT.		✓							✓				
6	Tentukan dan dokumentasikan persyaratan cadangan informasi yang diperlukan untuk mendukung rencana.		✓							✓				
7	Tentukan keterampilan yang dibutuhkan untuk personel yang terlibat dalam melaksanakan rencana dan prosedur.	✓								✓				
8	Distribusikan rencana dan dokumentasi pendukung secara aman kepada pihak yang berwewenang. Pastikan rencananya dan dokumentasi dapat diakses dalam semua skenario bencana.		✓							✓				

DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).

Uji kontinuitas secara teratur untuk menjalankan rencana hasil yang telah ditentukan sebelumnya, menjunjung tinggi ketahanan bisnis dan memungkinkan 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	Tentukan tujuan untuk memverifikasi kelengkapan BCP dan DRP dalam memenuhi risiko bisnis.	✓							✓	✓			
2	Tentukan dan sepakati peran dan tanggung jawab dan pengaturan penyimpanan data yang menyebabkan gangguan minimum pada proses bisnis.	✓							✓	✓			
3	Tetapkan peran dan tanggung jawab untuk pengelolaan rencana keberlangsungan bisnis		✓							✓			
4	Jadwalkan latihan dan aktivitas pengujian sebagaimana ditentukan dalam rencana kontinuitas.	✓								✓			

5	Lakukan pembekalan dan analisis pasca latihan untuk mempertimbangkan pencapaiannya.	✓								✓			
6	Berdasarkan hasil review, susun rekomendasi untuk perbaikan rencana kontinuitas saat ini.		✓							✓			

DSS04.05 Review, maintain and improve the continuity plans

Melakukan tinjauan manajemen atas kemampuan kontinuitas secara berkala interval untuk memastikan kesesuaian, kecukupan, dan efektivitasnya yang berkelanjutan. Kelola perubahan rencana sesuai dengan kontrol perubahan proses untuk memastikan bahwa rencana esinambungan selalu diperbarui dan mencerminkan kebutuhan bisnis yang sebenarnya.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Secara teratur, tinjau rencana kesinambungan dan kapabilitas terhadap asumsi yang dibuat dan tujuan strategis.	✓								✓			
2	Secara teratur, tinjau rencana kesinambungan untuk mempertimbangkan dampak perubahan baru terhadap organisasi perusahaan.		✓							✓			
3	Pertimbangkan apakah penilaian dampak bisnis yang direvisi mungkin diperlukan.		✓							✓			
4	Merekomendasikan perubahan dalam kebijakan, rencana, prosedur, infrastruktur, serta peran dan tanggung jawab melalui proses manajemen perubahan TI.		✓							✓			

DSS04.06 Conduct continuity plan training.

Memberikan pelatihan rutin kepada semua pihak internal dan eksternal terkait sesi mengenai prosedur dan peran serta tanggung jawab mereka dalam kasus gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Merencanakan pelatihan BCP dan DRP	✓								✓			
2	Pastikan bahwa rencana pelatihan mempertimbangkan frekuensi pelatihan dan mekanisme penyampaian pelatihan	✓								✓			
3	Mengembangkan kompetensi berdasarkan	✓	✓							✓			

	pelatihan praktik, termasuk keikutsertaan dalam latihan dan tes.												
4	Berdasarkan hasil latihan dan tes, pantau keterampilan dan kompetensi	✓							✓				

DSS04.07 Manage backup arrangements.
Menjaga ketersediaan informasi penting bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mencadangkan sistem, aplikasi, data, dan dokumentasi sesuai jadwal yang ditentukan. Pertimbangkan juga pencadangan online otomatis dan tentukan sumber data, serta keamanan dan hak akses.		✓							✓			
2	Tetapkan persyaratan untuk penyimpanan data cadangan di tempat dan di luar situs yang memenuhi persyaratan bisnis.		✓							✓			
3	Mengelola data arsip dan cadangan secara berkala.		✓							✓			
4	Memastikan bahwa sistem, aplikasi, data, dan dokumentasi yang dikelola atau diproses oleh pihak ketiga dicadangkan secara memadai atau diamankan.	✓								✓			

DSS04.08 Conduct post-resumption review.
Menilai kecukupan rencana kesinambungan bisnis (BCP) dan rencana respon bencana (DRP) setelah bisnis berhasil dilanjutkan proses dan layanan setelah gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mendokumentasikan kepatuhan terhadap BCP dan DRP.	✓								✓			
2	Menentukan efektivitas renstra dalam korelasi keberlangsungan proses bisnis.	✓								✓			
3	Mengidentifikasi kelemahan rencana dan membuat rekomendasi untuk perbaikan, libatkan puncak pimpinan.		✓							✓			

KUESIONER SURVEY

Penilaian Capability Level DSS 04 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narva Putra 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 ***DSS04 - Managed Continuity***. 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Farida Nur Rifai, S.Si, M.Si.
Email	farida.gozi@yahoo.com
Seksi	Bimbingan Kemasyarakatan
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Manajemen	: DSS04 Managed Continuity

Deskripsi:

Tetapkan dan pertahankan rencana untuk memungkinkan bisnis dan organisasi TI merespons insiden dan dengan cepat beradaptasi dengan gangguan. Ini akan memungkinkan operasi berkelanjutan dari proses bisnis penting dan layanan I&T yang diperlukan serta menjaga ketersediaan sumber daya, aset, dan informasi di tingkat yang dapat diterima perusahaan

Tujuan:

Beradaptasi dengan cepat, lanjutkan operasi bisnis dan pertahankan ketersediaan sumber daya dan informasi pada tingkat yang dapat diterima oleh perusahaan dalam acara tersebut gangguan yang signifikan (misalnya, ancaman, peluang, permintaan).

DSS04.01 Define the business continuity policy, objectives and scope

Tentukan kebijakan dan cakupan kelangsungan bisnis, selaras dengan perusahaan dan tujuan pemangku kepentingan, untuk meningkatkan ketahanan bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengidentifikasi proses bisnis internal dan outsourcing yang diperlukan untuk memenuhi kewajiban hukum.		✓							✓			
2	Mengidentifikasi stakeholder yang bertanggung jawab untuk mendefinisikan dan menyetujui kebijakan dan ruang lingkup keberlanjutan bisnis.		✓							✓			
3	Tentukan dan dokumentasikan tujuan dan ruang lingkup kebijakan untuk ketahanan bisnis.		✓							✓			
4	Mengidentifikasi proses bisnis pendukung yang penting dan layanan IT terkait.		✓							✓			

DSS04.02 Maintain business resilience

Evaluasi pilihan ketahanan bisnis dan pilih yang hemat biaya dan strategi yang layak yang akan memastikan kelangsungan perusahaan, pemulihan bencana dan penanganan insiden saat menghadapi bencana atau kejadian besar lainnya atau gangguan

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5

1	Identifikasi potensi yang mungkin menimbulkan peristiwa yang dapat mengganggu secara signifikan.		✓							✓					
2	Melakukan analisis dampak bisnis untuk mengevaluasi dampak dari waktu ke waktu dari gangguan terhadap proses bisnis.		✓							✓					
3	Tetapkan waktu minimum yang diperlukan untuk memulihkan proses bisnis, berdasarkan penetapan toleransi		✓							✓					
4	Identifikasi stakeholder yang berpengaruh terhadap keberlangsungan proses bisnis.	✓								✓					
5	Identifikasi tindakan yang akan mengurangi kemungkinan dan dampak melalui peningkatan pencegahan dan peningkatan ketahanan.	✓								✓					
6	Menganalisis persyaratan kontinuitas untuk mengidentifikasi kemungkinan bisnis strategis.	✓								✓					
7	Identifikasi kebutuhan sumber daya dan biaya untuk setiap opsi teknis strategis dan buat rekomendasi strategis.		✓							✓					
8	Dapatkan persetujuan pimpinan untuk opsi strategis yang dipilih.	✓								✓					

DSS04.03 Develop and implement a business continuity response
Mengembangkan rencana kesinambungan bisnis (BCP) dan rencana pemulihan bencana (DRP) berdasarkan strategi. Dokumentasikan semua prosedur yang diperlukan untuk perusahaan untuk melanjutkan aktivitas kritis jika terjadi insiden

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tentukan tindakan respons insiden dan komunikasi yang akan diambil jika terjadi gangguan.		✓							✓			
2	Pastikan mitra outsourcing memiliki rencana kesinambungan yang efektif.	✓								✓			
3	Tentukan kondisi dan prosedur pemulihan yang akan memungkinkan dimulainya kembali pelayanan.		✓							✓			

4	Mengembangkan dan memelihara BCP dan DRP yang berisi prosedur yang harus diikuti untuk memungkinkan kelanjutan proses bisnis.	✓								✓				
5	Tentukan dan dokumentasikan sumber daya yang diperlukan untuk mendukung kelangsungan dan prosedur pemulihan, dengan mempertimbangkan orang, fasilitas dan infrastruktur IT.		✓							✓				
6	Tentukan dan dokumentasikan persyaratan cadangan informasi yang diperlukan untuk mendukung rencana.	✓								✓				
7	Tentukan keterampilan yang dibutuhkan untuk personel yang terlibat dalam melaksanakan rencana dan prosedur.	✓								✓				
8	Distribusikan rencana dan dokumentasi pendukung secara aman kepada pihak yang berwewenang. Pastikan rencananya dan dokumentasi dapat diakses dalam semua skenario bencana.	✓								✓				

DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)

Uji kontinuitas secara teratur untuk menjalankan rencana hasil yang telah ditentukan sebelumnya, menjunjung tinggi ketahanan bisnis dan memungkinkan 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	Tentukan tujuan untuk memverifikasi kelengkapan BCP dan DRP dalam memenuhi risiko bisnis.	✓								✓			
2	Tentukan dan sepakati peran dan tanggung jawab dan pengaturan penyimpanan data yang menyebabkan gangguan minimum pada proses bisnis.		✓							✓			
3	Tetapkan peran dan tanggung jawab untuk pengelolaan rencana keberlangsungan bisnis		✓							✓			
4	Jadwalkan latihan dan aktivitas pengujian sebagaimana ditentukan dalam rencana kontinuitas.	✓								✓			

5	Lakukan pembekalan dan analisis pasca latihan untuk mempertimbangkan pencapaiannya.	✓								✓			
6	Berdasarkan hasil review, susun rekomendasi untuk perbaikan rencana kontinuitas saat ini.	✓								✓			

DSS04.05 Review, maintain and improve the continuity plans

Melakukan tinjauan manajemen atas kemampuan kontinuitas secara berkala interval untuk memastikan kesesuaian, kecukupan, dan efektivitasnya yang berkelanjutan. Kelola perubahan rencana sesuai dengan kontrol perubahan proses untuk memastikan bahwa rencana esinambungan selalu diperbarui dan mencerminkan kebutuhan bisnis yang sebenarnya.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Secara teratur, tinjau rencana kesinambungan dan kapabilitas terhadap asumsi yang dibuat dan tujuan strategis.		✓							✓			
2	Secara teratur, tinjau rencana kesinambungan untuk mempertimbangkan dampak perubahan baru terhadap organisasi perusahaan.	✓								✓			
3	Pertimbangkan apakah penilaian dampak bisnis yang direvisi mungkin diperlukan.		✓							✓			
4	Merekomendasikan perubahan dalam *kebijakan, rencana, prosedur, infrastruktur*, serta peran dan tanggung jawab melalui proses manajemen perubahan TI.		✓							✓			

DSS04.06 Conduct continuity plan training.

Memberikan pelatihan rutin kepada semua pihak internal dan eksternal terkait sesi mengenai prosedur dan peran serta tanggung jawab mereka dalam kasus gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Merencanakan pelatihan BCP dan DRP	✓	.							✓			
2	Pastikan bahwa rencana pelatihan mempertimbangkan frekuensi pelatihan dan mekanisme penyampaian pelatihan	✓								✓			
3	Mengembangkan kompetensi berdasarkan		✓							✓			

	pelatihan praktik, termasuk keikutsertaan dalam latihan dan tes.												
4	Berdasarkan hasil latihan dan tes, pantau keterampilan dan kompetensi	✓								✓			

DSS04.07 Manage backup arrangements.

Menjaga ketersediaan informasi penting bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mencadangkan sistem, aplikasi, data, dan dokumentasi sesuai jadwal yang ditentukan. Pertimbangkan juga pencadangan online otomatis dan tentukan sumber data, serta keamanan dan hak akses.		✓							✓			
2	Tetapkan persyaratan untuk penyimpanan data cadangan di tempat dan di luar situs yang memenuhi persyaratan bisnis.		✓							✓			
3	Mengelola data arsip dan cadangan secara berkala.		✓							✓			
4	Memastikan bahwa sistem, aplikasi, data, dan dokumentasi yang dikelola atau diproses oleh pihak ketiga dicadangkan secara memadai atau diamankan.	✓								✓			

DSS04.08 Conduct post-resumption review.

Menilai kecukupan rencana kesinambungan bisnis (BCP) dan rencana respon bencana (DRP) setelah bisnis berhasil dilanjutkan proses dan layanan setelah gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mendokumentasikan kepatuhan terhadap BCP dan DRP.	✓								✓			
2	Menentukan efektivitas renstra dalam korelasi keberlangsungan proses bisnis.		✓							✓			
3	Mengidentifikasi kelemahan rencana dan membuat rekomendasi untuk perbaikan, libatkan puncak pimpinan.		✓							✓			

(3)

KUESIONER SURVEY

Penilaian Capability Level DSS 04 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 ***DSS04 - Managed Continuity.*** 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	AGUNG Dwi YULIANTA, S.T., M.Eng.
Email	agungdy@gmail.com
Seksi	PELAYANAN KEMETROLOGIAN
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Manajemen	: DSS04 Managed Continuity

Deskripsi:

Tetapkan dan pertahankan rencana untuk memungkinkan bisnis dan organisasi TI merespons insiden dan dengan cepat beradaptasi dengan gangguan. Ini akan memungkinkan operasi berkelanjutan dari proses bisnis penting dan layanan I&T yang diperlukan serta menjaga ketersediaan sumber daya, aset, dan informasi di tingkat yang dapat diterima perusahaan

Tujuan:

Beradaptasi dengan cepat, lanjutkan operasi bisnis dan pertahankan ketersediaan sumber daya dan informasi pada tingkat yang dapat diterima oleh perusahaan dalam acara tersebut gangguan yang signifikan (misalnya, ancaman, peluang, permintaan).

DSS04.01 Define the business continuity policy, objectives and scope

Tentukan kebijakan dan cakupan kelangsungan bisnis, selaras dengan perusahaan dan tujuan pemangku kepentingan, untuk meningkatkan ketahanan bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengidentifikasi proses bisnis internal dan outsourcing yang diperlukan untuk memenuhi kewajiban hukum		✓							✓			
2	Mengidentifikasi stakeholder yang bertanggung jawab untuk mendefinisikan dan menyetujui kebijakan dan ruang lingkup keberlanjutan bisnis.		✓							✓			
3	Tentukan dan dokumentasikan tujuan dan ruang lingkup kebijakan untuk ketahanan bisnis.		✓							✓			
4	Mengidentifikasi proses bisnis pendukung yang penting dan layanan IT terkait.	✓								✓			

DSS04.02 Maintain business resilience

Evaluasi pilihan ketahanan bisnis dan pilih yang hemat biaya dan strategi yang layak yang akan memastikan kelangsungan perusahaan, pemulihan bencana dan penanganan insiden saat menghadapi bencana atau kejadian besar lainnya atau gangguan

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5

1	Identifikasi potensi yang mungkin menimbulkan peristiwa yang dapat mengganggu secara signifikan.		✓							✓				
2	Melakukan analisis dampak bisnis untuk mengevaluasi dampak dari waktu ke waktu dari gangguan terhadap proses bisnis.	✓								✓				
3	Tetapkan waktu minimum yang diperlukan untuk memulihkan proses bisnis, berdasarkan penetapan toleransi		✓							✓				
4	Identifikasi stakeholder yang berpengaruh terhadap keberlangsungan proses bisnis.		✓							✓				
5	Identifikasi tindakan yang akan mengurangi kemungkinan dan dampak melalui peningkatan pencegahan dan peningkatan ketahanan.		✓							✓				
6	Menganalisis persyaratan kontinuitas untuk mengidentifikasi kemungkinan bisnis strategis.	✓								✓				
7	Identifikasi kebutuhan sumber daya dan biaya untuk setiap opsi teknis strategis dan buat rekomendasi strategis.	✓								✓				
8	Dapatkan persetujuan pimpinan untuk opsi strategis yang dipilih.	✓								✓				

DSS04.03 Develop and implement a business continuity response

Mengembangkan rencana kesinambungan bisnis (BCP) dan rencana pemulihan bencana (DRP) berdasarkan strategi. Dokumentasikan semua prosedur yang diperlukan untuk perusahaan untuk melanjutkan aktivitas kritis jika terjadi insiden

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tentukan tindakan respons insiden dan komunikasi yang akan diambil jika terjadi gangguan.		✓							✓			
2	Pastikan mitra outsourcing memiliki rencana kesinambungan yang efektif.	✓								✓			
3	Tentukan kondisi dan prosedur pemulihan yang akan memungkinkan dimulainya kembali pelayanan.		✓							✓			

4	Mengembangkan dan memelihara BCP dan DRP yang berisi prosedur yang harus diikuti untuk memungkinkan kelanjutan proses bisnis.	✓								✓				
5	Tentukan dan dokumentasikan sumber daya yang diperlukan untuk mendukung kelangsungan dan prosedur pemulihan, dengan mempertimbangkan orang, fasilitas dan infrastruktur IT.		✓							✓				
6	Tentukan dan dokumentasikan persyaratan cadangan informasi yang diperlukan untuk mendukung rencana.		✓							✓				
7	Tentukan keterampilan yang dibutuhkan untuk personel yang terlibat dalam melaksanakan rencana dan prosedur.	✓								✓				
8	Distribusikan rencana dan dokumentasi pendukung secara aman kepada pihak yang berwewenang. Pastikan rencananya dan dokumentasi dapat diakses dalam semua skenario bencana.	✓								✓				

DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)

Uji kontinuitas secara teratur untuk menjalankan rencana hasil yang telah ditentukan sebelumnya, menjunjung tinggi ketahanan bisnis dan memungkinkan 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	Tentukan tujuan untuk memverifikasi kelengkapan BCP dan DRP dalam memenuhi risiko bisnis.		✓							✓			
2	Tentukan dan sepakati peran dan tanggung jawab dan pengaturan penyimpanan data yang menyebabkan gangguan minimum pada proses bisnis.	✓								✓			
3	Tetapkan peran dan tanggung jawab untuk pengelolaan rencana keberlangsungan bisnis		✓							✓			
4	Jadwalkan latihan dan aktivitas pengujian sebagaimana ditentukan dalam rencana kontinuitas.	✓								✓			

5	Lakukan pembekalan dan analisis pasca latihan untuk mempertimbangkan pencapaiannya.	✓								✓				
6	Berdasarkan hasil review, susun rekomendasi untuk perbaikan rencana kontinuitas saat ini.	✓								✓				

DSS04.05 Review, maintain and improve the continuity plans

Melakukan tinjauan manajemen atas kemampuan kontinuitas secara berkala interval untuk memastikan kesesuaian, kecukupan, dan efektivitasnya yang berkelanjutan. Kelola perubahan rencana sesuai dengan kontrol perubahan proses untuk memastikan bahwa rencana esinambungan selalu diperbarui dan mencerminkan kebutuhan bisnis yang sebenarnya.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Secara teratur, tinjau rencana kesinambungan dan kapabilitas terhadap asumsi yang dibuat dan tujuan strategis.		✓							✓			
2	Secara teratur, tinjau rencana kesinambungan untuk mempertimbangkan dampak perubahan baru terhadap organisasi perusahaan.	✓								✓			
3	Pertimbangkan apakah penilaian dampak bisnis yang direvisi mungkin diperlukan.	✓								✓			
4	Merekomendasikan perubahan dalam kebijakan, rencana, prosedur, infrastruktur, serta peran dan tanggung jawab melalui proses manajemen perubahan TI.		✓							✓			

DSS04.06 Conduct continuity plan training.

Memberikan pelatihan rutin kepada semua pihak internal dan eksternal terkait sesi mengenai prosedur dan peran serta tanggung jawab mereka dalam kasus gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Merencanakan pelatihan BCP dan DRP	✓								✓			
2	Pastikan bahwa rencana pelatihan mempertimbangkan frekuensi pelatihan dan mekanisme penyampaian pelatihan	✓								✓			
3	Mengembangkan kompetensi berdasarkan		✓							✓			

	pelatihan praktik, termasuk keikutsertaan dalam latihan dan tes.												
4	Berdasarkan hasil latihan dan tes, pantau keterampilan dan kompetensi		✓						✓				

DSS04.07 Manage backup arrangements.

Menjaga ketersediaan informasi penting bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mencadangkan sistem, aplikasi, data, dan dokumentasi sesuai jadwal yang ditentukan. Pertimbangkan juga pencadangan online otomatis dan tentukan sumber data, serta keamanan dan hak akses.		✓							✓			
2	Tetapkan persyaratan untuk penyimpanan data cadangan di tempat dan di luar situs yang memenuhi persyaratan bisnis.		✓							✓			
3	Mengelola data arsip dan cadangan secara berkala.		✓							✓			
4	Memastikan bahwa sistem, aplikasi, data, dan dokumentasi yang dikelola atau diproses oleh pihak ketiga dicadangkan secara memadai atau diamankan.	✓								✓			

DSS04.08 Conduct post-resumption review.

Menilai kecukupan rencana kesinambungan bisnis (BCP) dan rencana respon bencana (DRP) setelah bisnis berhasil dilanjutkan proses dan layanan setelah gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mendokumentasikan kepatuhan terhadap BCP dan DRP.	✓								✓			
2	Menentukan efektivitas renstra dalam korelasi keberlangsungan proses bisnis.		✓							✓			
3	Mengidentifikasi kelemahan rencana dan membuat rekomendasi untuk perbaikan, libatkan puncak pimpinan.		✓							✓			

KUESIONER SURVEY

Penilaian Capability Level DSS 04 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 ***DSS04 - Managed Continuity.*** 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Anton Kurniadi, S.Kom
Email	
Seksi	Senior Pranata Komputer
Organisasi / Perusahaan	BSML Regional II
Paraf	

Domain	: Delivery, Service, and Support
Objek Manajemen	: DSS04 Managed Continuity

Deskripsi:

Tetapkan dan pertahankan rencana untuk memungkinkan bisnis dan organisasi TI merespons insiden dan dengan cepat beradaptasi dengan gangguan. Ini akan memungkinkan operasi berkelanjutan dari proses bisnis penting dan layanan I&T yang diperlukan serta menjaga ketersediaan sumber daya, aset, dan informasi di tingkat yang dapat diterima perusahaan

Tujuan:

Beradaptasi dengan cepat, lanjutkan operasi bisnis dan pertahankan ketersediaan sumber daya dan informasi pada tingkat yang dapat diterima oleh perusahaan dalam acara tersebut gangguan yang signifikan (misalnya, ancaman, peluang, permintaan).

DSS04.01 Define the business continuity policy, objectives and scope

Tentukan kebijakan dan cakupan kelangsungan bisnis, selaras dengan perusahaan dan tujuan pemangku kepentingan, untuk meningkatkan ketahanan bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mengidentifikasi proses bisnis internal dan outsourcing yang diperlukan untuk memenuhi kewajiban hukum.		✓							✓			
2	Mengidentifikasi stakeholder yang bertanggung jawab untuk mendefinisikan dan menyetujui kebijakan dan ruang lingkup keberlanjutan bisnis.		✓							✓			
3	Tentukan dan dokumentasikan tujuan dan ruang lingkup kebijakan untuk ketahanan bisnis.		✓							✓			
4	Mengidentifikasi proses bisnis pendukung yang penting dan layanan IT terkait.	✓								✓			

DSS04.02 Maintain business resilience

Evaluasi pilihan ketahanan bisnis dan pilih yang hemat biaya dan strategi yang layak yang akan memastikan kelangsungan perusahaan, pemulihan bencana dan penanganan insiden saat menghadapi bencana atau kejadian besar lainnya atau gangguan

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5

1	Identifikasi potensi yang mungkin menimbulkan peristiwa yang dapat mengganggu secara signifikan.		✓							✓				
2	Melakukan analisis dampak bisnis untuk mengevaluasi dampak dari waktu ke waktu dari gangguan terhadap proses bisnis.	✓								✓				
3	Tetapkan waktu minimum yang diperlukan untuk memulihkan proses bisnis, berdasarkan penetapan toleransi	✓								✓				
4	Identifikasi stakeholder yang berpengaruh terhadap keberlangsungan proses bisnis.	✓								✓				
5	Identifikasi tindakan yang akan mengurangi kemungkinan dan dampak melalui peningkatan pencegahan dan peningkatan ketahanan.		✓							✓				
6	Menganalisis persyaratan kontinuitas untuk mengidentifikasi kemungkinan bisnis strategis.		✓							✓				
7	Identifikasi kebutuhan sumber daya dan biaya untuk setiap opsi teknis strategis dan buat rekomendasi strategis.		✓							✓				
8	Dapatkan persetujuan pimpinan untuk opsi strategis yang dipilih.	✓								✓				

DSS04.03 Develop and implement a business continuity response

Mengembangkan rencana kesinambungan bisnis (BCP) dan rencana pemulihan bencana (DRP) berdasarkan strategi. Dokumentasikan semua prosedur yang diperlukan untuk perusahaan untuk melanjutkan aktivitas kritis jika terjadi insiden

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Tentukan tindakan respons insiden dan komunikasi yang akan diambil jika terjadi gangguan.		✓							✓			
2	Pastikan mitra outsourcing memiliki rencana kesinambungan yang efektif.	✓								✓			
3	Tentukan kondisi dan prosedur pemulihan yang akan memungkinkan dimulainya kembali pelayanan.		✓							✓			

4	Mengembangkan dan memelihara BCP dan DRP yang berisi prosedur yang harus diikuti untuk memungkinkan kelanjutan proses bisnis.	✓								✓				
5	Tentukan dan dokumentasikan sumber daya yang diperlukan untuk mendukung kelangsungan dan prosedur pemulihan, dengan mempertimbangkan orang, fasilitas dan infrastruktur IT.	✓								✓				
6	Tentukan dan dokumentasikan persyaratan cadangan informasi yang diperlukan untuk mendukung rencana.		✓							✓				
7	Tentukan keterampilan yang dibutuhkan untuk personel yang terlibat dalam melaksanakan rencana dan prosedur.		✓							✓				
8	Distribusikan rencana dan dokumentasi pendukung secara aman kepada pihak yang berwewenang. Pastikan rencananya dan dokumentasi dapat diakses dalam semua skenario bencana.	✓								✓				

DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).
Uji kontinuitas secara teratur untuk menjalankan rencana hasil yang telah ditentukan sebelumnya, menjunjung tinggi ketahanan bisnis dan memungkinkan 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	Tentukan tujuan untuk memverifikasi kelengkapan BCP dan DRP dalam memenuhi risiko bisnis.		✓							✓			
2	Tentukan dan sepakati peran dan tanggung jawab dan pengaturan penyimpanan data yang menyebabkan gangguan minimum pada proses bisnis.		✓							✓			
3	Tetapkan peran dan tanggung jawab untuk pengelolaan rencana keberlangsungan bisnis	✓								✓			
4	*Jadwalkan latihan dan aktivitas pengujian* sebagaimana ditentukan dalam rencana kontinuitas.	✓								✓			

5	Lakukan pembekalan dan analisis pasca latihan untuk mempertimbangkan pencapaiannya.	✓								✓				
6	Berdasarkan hasil review, susun rekomendasi untuk perbaikan rencana kontinuitas saat ini.	✓								✓				

DSS04.05 Review, maintain and improve the continuity plans

Melakukan tinjauan manajemen atas kemampuan kontinuitas secara berkala interval untuk memastikan kesesuaian, kecukupan, dan efektivitasnya yang berkelanjutan. Kelola perubahan rencana sesuai dengan kontrol perubahan proses untuk memastikan bahwa rencana esinambungan selalu diperbarui dan mencerminkan kebutuhan bisnis yang sebenarnya.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Secara teratur, tinjau rencana kesinambungan dan kapabilitas terhadap asumsi yang dibuat dan tujuan strategis.		✓							✓			
2	Secara teratur, tinjau rencana kesinambungan untuk mempertimbangkan dampak perubahan baru terhadap organisasi perusahaan.	✓								✓			
3	Pertimbangkan apakah penilaian dampak bisnis yang direvisi mungkin diperlukan.		✓							✓			
4	Merekomendasikan perubahan dalam kebijakan, rencana, prosedur, infrastruktur, serta peran dan tanggung jawab melalui proses manajemen perubahan TI.		✓							✓			

DSS04.06 Conduct continuity plan training

Memberikan pelatihan rutin kepada semua pihak internal dan eksternal terkait sesi mengenai prosedur dan peran serta tanggung jawab mereka dalam kasus gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Merencanakan pelatihan BCP dan DRP	✓								✓			
2	Pastikan bahwa rencana pelatihan mempertimbangkan frekuensi pelatihan dan mekanisme penyampaian pelatihan	✓								✓			
3	Mengembangkan kompetensi berdasarkan		✓							✓			

	pelatihan praktik, termasuk keikutsertaan dalam latihan dan tes.												
4	Berdasarkan hasil latihan dan tes, pantau keterampilan dan kompetensi	✓								✓			

DSS04.07 Manage backup arrangements.

Menjaga ketersediaan informasi penting bisnis.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mencadangkan sistem, aplikasi, data, dan dokumentasi sesuai jadwal yang ditentukan. Pertimbangkan juga pencadangan online otomatis dan tentukan sumber data, serta keamanan dan hak akses.		✓							✓			
2	Tetapkan persyaratan untuk penyimpanan data cadangan di tempat dan di luar situs yang memenuhi persyaratan bisnis.		✓							✓			
3	Mengelola data arsip dan cadangan secara berkala.		✓							✓			
4	Memastikan bahwa sistem, aplikasi, data, dan dokumentasi yang dikelola atau diproses oleh pihak ketiga dicadangkan secara memadai atau diamankan.	✓								✓			

DSS04.08 Conduct post-resumption review.

Menilai kecukupan rencana kesinambungan bisnis (BCP) dan rencana respon bencana (DRP) setelah bisnis berhasil dilanjutkan proses dan layanan setelah gangguan.

NO	Aktivitas Tata Kelola	As – is (saat ini)						To be (target)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Mendokumentasikan kepatuhan terhadap BCP dan DRP.	✓								✓			
2	Menentukan efektivitas renstra dalam korelasi keberlangsungan proses bisnis.		✓							✓			
3	Mengidentifikasi kelemahan rencana dan membuat rekomendasi untuk perbaikan, libatkan puncak pimpinan.		✓							✓			

KUESIONER SURVEY

Penilaian Capability Level DSS 05 Cobit 2019

Perkenalkan nama saya Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Anton Kurniadi, S.Kom
Email	
Seksi	Senior Pranata Komputer
Organisasi / Perusahaan	BSML Regional II
Paraf	

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

Deskripsi:

Lindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan 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.

DSS05.01 Protect against malicious software.

Menerapkan dan memelihara tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan kontrol virus) di file perusahaan untuk melindungi sistem informasi dan teknologi dari kejahatan perangkat lunak (mis., ransomware, malware, virus, worm, spyware, 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	✓								✓			

DSS05.03 Manage endpoint security.

Pastikan titik akhir (mis., Laptop, desktop, server, dan seluler lainnya dan perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi tersebut diproses, 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.		✓						✓				

DSS05.04 Manage user identity and logical access

Memastikan bahwa semua pengguna memiliki hak akses 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 secera rutin pada semua akun dan hak istimewa terkait.	✓								✓			

DSS05.05 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 dibenarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, sementara staf, klien, 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 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 IT (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)	✓								✓			

DSS05.06 Manage sensitive documents and output devices.

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset I&T sensitif, seperti khusus formulir, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau 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 askes istimewa kepada jabatan tertentu berdasarkan keputusan manajemen		✓							✓				
3	Buat inventarisasi dokumen sensitif perusahaan.	✓								✓				
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.	✓								✓				

DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.

Menggunakan portofolio alat dan teknologi (mis., Deteksi intruksi 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	AGUNG DWI YULIANTA, S.T., M.Eng.
Email	agungdy@gmail.com
Seksi	PELAYANAN METROLOGI LAN
Organisasi / Perusahaan	BSML Regional II
Paraf	

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

Deskripsi:

Lindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan 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.

DSS05.01 Protect against malicious software.

Menerapkan dan memelihara tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan kontrol virus) di file perusahaan untuk melindungi sistem informasi dan teknologi dari kejahatan perangkat lunak (mis., ransomware, malware, virus, worm, spyware, 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	✓								✓			

DSS05.03 Manage endpoint security.

Pastikan titik akhir (mis., Laptop, desktop, server, dan seluler lainnya dan perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi tersebut diproses, 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.		✓						✓				

DSS05.04 Manage user identity and logical access.
Memastikan bahwa semua pengguna memiliki hak akses 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.		✓							✓			

DSS05.05 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 dibenarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, sementara staf, klien, 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 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 IT (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)	✓								✓			

DSS05.06 Manage sensitive documents and output devices.

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset I&T sensitif, seperti khusus formulir, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau 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 askes istimewa kepada jabatan tertentu berdasarkan keputusan manajemen		✓							✓			
3	Buat inventarisasi dokumen sensitif perusahaan.	✓								✓			
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.	✓								✓			

DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.
Menggunakan portofolio alat dan teknologi (mis., Deteksi intruksi 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Farida Nur Rofi, S.Si., M.Sc.
Email	farida3021@yahoo.com.sg
Seksi	Bimbingan Kemasyarakatan
Organisasi / Perusahaan	BSML Regional II
Paraf	

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

Deskripsi:

Lindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan 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.

DSS05.01 Protect against malicious software.

Menerapkan dan memelihara tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan kontrol virus) di file perusahaan untuk melindungi sistem informasi dan teknologi dari kejahatan perangkat lunak (mis., ransomware, malware, virus, worm, spyware, 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	✓								✓			

DSS05.03 Manage endpoint security

Pastikan titik akhir (mis., Laptop, desktop, server, dan seluler lainnya dan perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi tersebut diproses, 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.		✓							✓			

DSS05.04 Manage user identity and logical access.

Memastikan bahwa semua pengguna memiliki hak akses 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 secera rutin pada semua akun dan hak istimewa terkait.	✓								✓			

DSS05.05 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 dibenarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, sementara staf, klien, 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 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 IT (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)	✓								✓			

DSS05.06 Manage sensitive documents and output devices.

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset I&T sensitif, seperti khusus formulir, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau 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 askes istimewa kepada jabatan tertentu berdasarkan keputusan manajemen		✓							✓			
3	Buat inventarisasi dokumen sensitif perusahaan.		✓							✓			
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.	✓								✓			

DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.
Menggunakan portofolio alat dan teknologi (mis., Deteksi intruksi 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	[illegible], SE, MPPM
Email	
Seksi	Senior Perencana Ahli
Organisasi / Perusahaan	BSML Regional II
Paraf	

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

Deskripsi:

Lindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan 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.

DSS05.01 Protect against malicious software.

Menerapkan dan memelihara tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan kontrol virus) di file perusahaan untuk melindungi sistem informasi dan teknologi dari kejahatan perangkat lunak (mis., ransomware, malware, virus, worm, spyware, 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	✓								✓			

DSS05.03 Manage endpoint security.

Pastikan titik akhir (mis., Laptop, desktop, server, dan seluler lainnya dan perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi tersebut diproses, 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.	✓								✓			

DSS05.04 Manage user identity and logical access.
Memastikan bahwa semua pengguna memiliki hak akses 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 secera rutin pada semua akun dan hak istimewa terkait.		✓							✓			

DSS05.05 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 dibenarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, sementara staf, klien, 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 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 IT (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)	✓								✓			

DSS05.06 Manage sensitive documents and output devices.

Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset I&T sensitif, seperti khusus formulir, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau 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 askes istimewa kepada jabatan tertentu berdasarkan keputusan manajemen		✓						✓				
3	Buat inventarisasi dokumen sensitif perusahaan.	✓							✓				
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.	✓							✓				

DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.

Menggunakan portofolio alat dan teknologi (mis., Deteksi intruksi 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 Angga Wijaya Narwa Putra 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 Aktivitas yang dilakukan kurang lebih telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap, yang dapat dikategorikan sebagai kegiatan awal atau kegiatan yang bersifat intuitif - tidak terlalu terorganisir.
- 2 Aktivitas yang dilakukan telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional.
- 3 Aktivitas yang dilakukan telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Aktivitas biasanya telah didefinisikan dengan baik.
- 4 Aktivitas yang dilakukan telah mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
- 5 Proses telah mencapai tujuan, terdefinisi dengan baik dan terukur, dan dilakukan perbaikan berkelanjutan

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

Identitas Responden	
Nama Responden	Eko Wachyudiono, ST.MT
Email	
Seksi	Sub. Koord. Tata Usaha
Organisasi / Perusahaan	BSML Regional II
Paraf	

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

Deskripsi:

Lindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan 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.

DSS05.01 Protect against malicious software.

Menerapkan dan memelihara tindakan pencegahan, detektif, dan korektif (terutama patch keamanan terbaru dan kontrol virus) di file perusahaan untuk melindungi sistem informasi dan teknologi dari kejahatan perangkat lunak (mis., ransomware, malware, virus, worm, spyware, 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	✓								✓			

DSS05.03 Manage endpoint security.

Pastikan titik akhir (mis., Laptop, desktop, server, dan seluler lainnya dan perangkat jaringan atau perangkat lunak) diamankan pada tingkat yang setara atau lebih besar dari persyaratan keamanan yang ditetapkan untuk informasi tersebut diproses, 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.		✓							✓			

DSS05.04 Manage user identity and logical access

Memastikan bahwa semua pengguna memiliki hak akses 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 secera rutin pada semua akun dan hak istimewa terkait.	✓								✓			

DSS05.05 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 dibenarkan, diotorisasi, dicatat dan dipantau. Persyaratan ini berlaku untuk semua orang yang memasuki lokasi, termasuk staf, sementara staf, klien, 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 saat berada di lokasi.		✓							✓			
4	Batasi dan pantau akses ke situs IT 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 IT (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)	✓								✓			

DSS05.06 Manage sensitive documents and output devices.
Tetapkan pengamanan fisik yang sesuai, praktik akuntansi dan manajemen inventaris terkait aset I&T sensitif, seperti khusus formulir, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau 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 askes istimewa kepada jabatan tertentu berdasarkan keputusan manajemen		✓							✓			
3	Buat inventarisasi dokumen sensitif perusahaan.		✓							✓			
4	Menetapkan perlindungan fisik yang sesuai atas dokumen sensitif perusahaan.		✓							✓			

DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.
Menggunakan portofolio alat dan teknologi (mis., Deteksi intruksi 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		✓							✓			