

BAB II

Landasan Teori

2.1 Audit Sistem Informasi

Audit sistem informasi merupakan proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian intern yang memadai, semua aktivitas dilindungi dengan baik atau tidak disalahgunakan serta terjaminnya integritas data, kehandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer tersebut. Audit sistem informasi juga memiliki tujuan sebagai berikut[6].

1. Pengamatan aset

Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, *file* / data dan fasilitas lain harus dijaga dengan sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Efektifitas sistem

Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut dirancang dengan benar (*doing the right thing*), telah sesuai dengan kebutuhan *user*. Informasi yang dibutuhkan oleh para manajer dapat dipenuhi dengan baik.

3. Efisiensi sistem

Efisiensi menjadi sangat penting ketika sumber daya kapasitasnya terbatas. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya informasi yang minimal.

4. Ketersediaan

Berhubungan dengan ketersediaan dukungan/layanan teknologi informasi (TI). TI hendaknya dapat mendukung secara kontinyu terhadap proses bisnis kegiatan perusahaan.

5. Kerahasiaan

Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindungi dari akses pihak-pihak yang tidak berwenang.

6. Keandalan

Berhubungan dengan kesesuaian dan keakuratan bagi manajemen dalam pengelolaan organisasi, pelaporan, dan pertanggungjawaban.

7. Menjaga integritas data

Integritas data (*data integrity*) adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut seperti: kelengkapan, kebenaran, dan keakuratan. Jika integritas data tidak terpelihara, maka suatu perusahaan tidak akan lagi memiliki informasi/laporan yang benar, bahkan perusahaan dapat menderita kerugian karena pengawasan tidak tepat atau keputusan-keputusan yang salah. Faktor utama yang membuat data berharga bagi organisasi dan pentingnya untuk menjaga integritas data adalah :

- a. Makna penting data/informasi bagi pengambilan keputusan. Peningkatan data sehingga dapat memberikan informasi bagi para pengambil keputusan.
- b. Nilai data bagi pesaing, jika data tersebut berguna bagi pesaing maka kehilangan data akan memberikan dampak buruk bagi organisasi tersebut. Pesaing dapat menggunakan data tersebut untuk mengalahkan organisasi sehingga mengakibatkan organisasi menjadi kehilangan pasar (*market*), berkurangnya keuntungan, dan sebagainya [7]

2.2 Framework COBIT

Framework COBIT (Control Objectives for Information and Related Technology) adalah kerangka kerja tata kelola IT (*IT Governance Framework*) dan kumpulan perangkat yang mendukung dan memungkinkan para manager untuk menjembatani jarak (*gap*) yang ada antara kebutuhan yang dikendalikan (*control requirement*), masalah teknis (*technical issues*) dan resiko bisnis (*bussiness risk*). *COBIT* mempermudah perkembangan peraturan yang jelas (*clear policy development*) dan praktik baik (*good practice*) untuk mengendalikan IT dalam organisasi. *COBIT* menekankan keputusan terhadap peraturan, membantu organisasi untuk meningkatkan nilai yang ingin dicapai dengan penggunaan IT, memungkinkan untuk menyelaraskan dan menyederhanakan penerapan dari kerangka *COBIT*. *COBIT* muncul pertama kali pada tahun 1996, yaitu *COBIT* versi 1 yang menekankan pada bidang audit, *COBIT* versi 2 pada tahun 1998 yang menekankan pada tahap control, *COBIT* versi 3 pada tahun 2000 yang berorientasi kepada manajemen, *COBIT* versi 4 yang lebih mengarah pada *IT Governance*, dan terakhir dirilis adalah *COBIT* versi 5 pada tahun 2012 yang mengarah pada tata kelola dan manajemen untuk aset-aset perusahaan IT. Konsep dasar kerangka kerja *COBIT* adalah sebagai penentu kendali dalam TI berdasarkan informasi yang dibutuhkan untuk mendukung tujuan bisnis dan informasi yang dihasilkan dari gabungan penerapan proses TI dan sumber daya terkait. Dalam penerapan pengelolaan TI terdapat dua jenis model kendali, yaitu model kendali bisnis (*business controls model*) dan model kendali TI (*IT focused control model*), *COBIT* mencoba untuk menjembatani kesenjangan dari kedua jenis kendali tersebut. *Framework COBIT 5* terdiri atas 5 domain, yaitu [8]:

1. EDM (*Evaluate, Direct and Monitor*)
2. APO (*Align, Plan and Organise*)
3. BAI (*Build, Acquire and Implement*)
4. DSS (*Deliver, Service, and Support*)
5. MEA (*Monitor, Evaluate and Assess*)

COBIT dirancang terdiri dari 37 proses bisnis yang menggambarkan proses TI yang terdiri dari 5 domain. Berikut ini adalah penjelasan proses bisnis dari masing-masing domain.

1. EDM (*Evaluate, Direct and Monitor*)

Proses tata kelola ini berkaitan dengan tujuan tata kelola pemangku kepentingan dalam melakukan penilaian, optimasi risiko, dan sumber daya mencakup praktek dan kegiatan yang bertujuan untuk mengevaluasi pilihan strategis, memberikan arahan kepada TI dan pematangan hasilnya[9].

Tabel 2.1 Proses Bisnis Pada Domain EDM

| Kode Domain | Sub Domain |
|--------------------|--|
| EDM01 | <i>Ensure Governance Framework Setting and Maintenance</i> |
| EDM02 | <i>Ensure Benefits Delivery</i> |
| EDM03 | <i>Ensure Risk Optimisation</i> |
| EDM04 | <i>Ensure Resource Optimisation</i> |
| EDM05 | <i>Ensure Stakeholder Transparency</i> |

2. APO (*Align, Plan and Organise*)

Memberikan arah untuk pengiriman solusi (BAI) dan penyediaan layanan dan dukungan (DSS). Domain ini mencakup strategi dan taktik, serta mengidentifikasi kekhawatiran cara terbaik TI agar dapat berkontribusi pada pencapaian tujuan bisnis. Realisasi visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perpektif yang berbeda. Sebuah organisasi yang tepat, serta infrastruktur teknologi harus dimasukkan kedalam tempatnya[10].

Tabel 2.2 Proses Bisnis Pada Domain APO

| Kode Domain | Sub Domain |
|--------------------|---|
| APO01 | <i>Manage the IT Management Framework</i> |
| APO02 | <i>Manage Strategy</i> |
| APO03 | <i>Manage Enterprise Architecture</i> |
| APO04 | <i>Manage Innovation</i> |
| APO05 | <i>Manage Portfolio</i> |
| APO06 | <i>Manage Budget and Costs</i> |
| APO07 | <i>Manage Human Resources</i> |
| APO08 | <i>Manage Relationships</i> |
| APO09 | <i>Manage Service Agreements</i> |
| APO010 | <i>Manage Suppliers</i> |
| APO011 | <i>Manage Quality</i> |
| APO012 | <i>Manage Risk</i> |
| APO013 | <i>Manage Security</i> |

3. BAI (*Built, Acquire, and Implement*)

Memberikan solusi dan melewatinya sehingga akan berubah menjadi layanan. Untuk mewujudkan strategi TI, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan terintegrasi ke dalam proses bisnis. Perubahan dan pemeliharaan sistem yang ada juga dicakup oleh domain ini, untuk memastikan bahwa solusi terus memenuhi tujuan bisnis.

Tabel 2.3 Proses Bisnis Pada Domain BAI

| Kode Domain | Sub Domain |
|------------------------|---|
| BAI01 | <i>Manage Programmes and Projects</i> |
| BAI02 | <i>Manage Requirements Definition</i> |
| BAI03 | <i>Manage Solutions Identification and Build</i> |
| BAI04 | <i>Manage Availability and Capacity</i> |
| BAI05 | <i>Manage Organisational Change Enablement</i> |
| BAI06 | <i>Manage Changes</i> |
| BAI07 | <i>Manage Change Acceptance and Transitioning</i> |
| BAI08 | <i>Manage Knowledge</i> |
| BAI09 | <i>Manage Assets</i> |
| BAI010 | <i>Manage Configuration</i> |

4. DSS (*Deliver, Service, and Support*)

Meliputi mengirimkan, layanan, dan dukungan atau memberi pelayanan yang aktual bagi bisnis, termasuk manajemen data dan proteksi informasi yang berhubungan dengan proses bisnis.

Tabel 2.4 Proses Bisnis Pada Domain DSS

| Kode Domain | Sub Domain |
|------------------------|--|
| DSS01 | <i>Manage Operations</i> |
| DSS02 | <i>Manage Service Requests and Incidents</i> |

| | |
|--------------|---|
| DSS03 | <i>Manage Problems</i> |
| DSS04 | <i>Manage Continuity</i> |
| DSS05 | <i>Manage Security Service</i> |
| DSS06 | <i>Manage Business Process Controls</i> |

5. MEA (*Monitor, Evaluate and Assess*)

Menerima solusi dan dapat digunakan bagi pengguna akhir. Domain ini berkaitan dengan pengiriman *actual* dan dukungan layanan yang dibutuhkan, yang meliputi pelayanan, pengelolaan keamanan dan kelangsungan, dukungan layanan bagi pengguna, dan manajemen data serta fasilitas operasional.

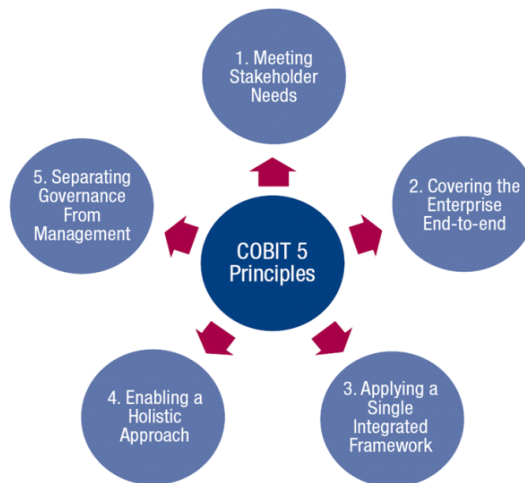
Tabel 2.5 Proses Bisnis Pada Domain MEA

| Kode Domain | Sub Domain |
|--------------------|---|
| MEA01 | <i>Monitor, Evaluate and Assess Performance and Conformance</i> |
| MEA02 | <i>Monitor, Evaluate and Assess the System of Internal Control</i> |
| MEA03 | <i>Monitor, Evaluate and Assess Compliance with External Requirements</i> |

2.3 Prinsip – Prinsip COBIT 5.0

Menurut ISACA (2012), bahwa COBIT 5 memiliki 5 prinsip dasar :

- Memenuhi kebutuhan *stakeholder*.
- Melingkupi tata kelola dan proses kerja *End-to-End Enterprise*
- Mengaplikasikan sebuah kerangka-kerja yang terintegrasi.
- Pendekatan keseluruhan untuk kemampuan tata kelola dan manajemen / pengaturan.
- Pemisahan antara tata-kelola dengan manajemen/pengaturan.



Source: COBIT®5, figure 2. © 2012 ISACA® All rights reserved.

2.4 Studi Literatur

Berikut adalah bahan studi literatur di dalam penelitian ini.

a. Audit Keamanan Sistem Informasi Pada Kantor Pemerintahan Kota Yogyakarta Menggunakan COBIT 5 [11] Masalah

Permasalahan yang dikaji dalam penelitian ini adalah perlu adanya standar operasional dan prosedur manajemen pengamanan sistem informasi dan telekomunikasi dilingkungan pemerintahan Yogyakarta dengan menggunakan *Framework* COBIT 5 sebagai metode untuk mewujudkan standar pengamanan manajemen sistem informasi dan telekomunikasi di pemerintahan kota Yogyakarta.

b. Hasil dan pembahasan

Berdasarkan hasil penilaian tingkat kapabilitas keamanan Sistem Informasi (SI) tidak dapat ditargetkan dalam jangka pendek, yaitu level 3. Berdasarkan hasil penilaian tingkat kapabilitas keamanan Sistem Informasi (SI) pada Pemerintahan Kota Yogyakarta, hasil dari lima (5) proses tingkat kapabilitas keamanan SI, yaitu semua proses berada pada tingkat kapabilitas 1 (*performed process*).

1. Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan *Framework* COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk) [12]

a. Masalah

PT Martina Berto Tbk adalah perusahaan manufaktur, pemasaran, penelitian dan pengembangan yang ada di Martha Tilaar Group. Saat ini perusahaan telah menerapkan sistem dan teknologi informasi dalam mendukung operasional perusahaan yang dilaksanakan oleh departemen *Corporate IT*. Tetapi, terdapat beberapa kekurangan dalam penerapan tersebut khususnya dalam hal keamanan seperti *security incident* yang kerap muncul serta serangan ke server perusahaan. Untuk mencegah hal-hal tersebut terjadi lagi, maka perlu diketahui sejauh mana tata kelola sistem keamanan teknologi informasi perusahaan dengan cara melakukan evaluasi, karena dengan adanya evaluasi dapat dihasilkan rekomendasi berupa tindakan-tindakan apa yang harus dilakukan agar hal-hal tersebut tidak terjadi lagi.

b. Hasil dan pembahasan

Hasil penelitian menunjukkan *Capability Level* pada domain proses APO13 dan DSS05 *Framework* COBIT 5 berada pada level 1, sedangkan *capability level* yang diinginkan pada kedua domain proses adalah level 2, sehingga menyisakan *gap* sebesar 1. Setelah mengetahui *capability level* saat ini dan yang diinginkan, maka dibuatkan rekomendasi berdasarkan analisis SWOT. Rekomendasi yang diberikan seperti pembentukan unit khusus keamanan informasi, membuat dokumen terkait pengelolaan dan peningkatan keamanan informasi dan penanganan risiko keamanan informasi, membuat dokumen standar operasional layanan keamanan serta melakukan pembaruan teknis teknologi informasi dan pemantauan secara rutin.

2. Audit Tata Kelola Teknologi Informasi Berbasis COBIT 5 (DSS05) Untuk Evaluasi Keamanan Sistem Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Kendal (Tri, 2016).

a. Masalah

Permasalahan yang dikaji dalam penelitian ini adalah pada Dinas Kominfo Kabupaten Kendal belum mendefinisikan secara jelas terkait *Standard Operasional Prosedur* (SOP) pada sistem informasi serta pada pengolahan/penyimpanan data, tidak rutin melakukan *monitoring back up* data, serta jaringan yang tidak stabil dan putusnya koneksi secara tiba-tiba juga menjadi permasalahan pada jaringan dan *server*. *Framework* yang digunakan dalam penelitian ini adalah COBIT 5 sebagai metode untuk mewujudkan standar pengamanan informasi di Dinas Kominfo Kabupaten Kendal.

b. Hasil dan pembahasan

Ditemukannya selisih *gap* sebesar 0,24 antara tingkat kapabilitas saat ini dan yang akan dicapai dengan target yang akan dicapai. Strategi perbaikan yang dapat dilakukan Dinas Kominfo Kabupaten Kendal untuk mencapai tingkat kapabilitas 3 adalah dengan memperbaiki kriteria pemenuhan dari setiap level 1 sampai 3 yang dapat dilakukan secara bertahap.

2.5 Framework ITIL

ITIL (Information Technology Infrastructure Library) adalah framework manajemen layanan TI yang fokus pada penyediaan layanan berkualitas tinggi yang berorientasi pada kebutuhan pengguna dan bisnis. ITIL menyediakan pedoman untuk mengelola layanan TI agar selaras dengan kebutuhan bisnis, meningkatkan kepuasan pengguna, dan mengoptimalkan pengelolaan sumber daya TI[13].

2.6 Siklus Layanan ITIL

Siklus layanan ITIL terbagi menjadi lima tahapan utama, yaitu:

1. *Service Strategy*: Tahapan ini mencakup perencanaan strategi untuk penyediaan layanan TI yang selaras dengan tujuan bisnis.

2. Service Design: Berfokus pada perancangan layanan TI yang sesuai dengan kebutuhan pengguna dan standar yang berlaku.
3. Service Transition: Tahapan ini mencakup proses transisi dari pengembangan layanan hingga implementasinya ke lingkungan operasional.
4. Service Operation: Berfokus pada pengelolaan operasional sehari-hari dari layanan TI yang telah diimplementasikan.
5. Continual Service Improvement: Proses ini mencakup evaluasi dan perbaikan berkelanjutan untuk meningkatkan kualitas layanan TI.

2.7 Manfaat ITIL

Penerapan ITIL memberikan beberapa manfaat, antara lain[14]:

- Meningkatkan Efisiensi Operasional: ITIL membantu perusahaan dalam mengoptimalkan penggunaan sumber daya TI dan proses layanan.
- Meningkatkan Kepuasan Pengguna: ITIL fokus pada peningkatan kualitas layanan yang diberikan kepada pengguna, sehingga meningkatkan kepuasan dan kepercayaan pengguna terhadap layanan TI.
- Pengelolaan Risiko yang Lebih Baik: Dengan panduan yang jelas, ITIL membantu perusahaan dalam mengelola risiko yang terkait dengan layanan TI.

2.8 Penggunaan COBIT 5 dan ITIL dalam Audit Sistem Informasi

Penggunaan framework COBIT 5 dan ITIL dalam audit sistem informasi memberikan pendekatan yang komprehensif untuk mengevaluasi kinerja TI dari berbagai aspek. COBIT 5 memberikan panduan dalam tata kelola dan manajemen TI, sedangkan ITIL memberikan fokus pada manajemen layanan

yang berorientasi pada pengguna. Kombinasi keduanya dapat memberikan audit yang lebih holistik, mencakup tidak hanya aspek tata kelola TI, tetapi juga kualitas layanan dan pengelolaan risiko.

Dengan menggunakan COBIT 5, auditor dapat mengevaluasi seberapa baik pengelolaan TI di PT Perkebunan Nusantara VII mendukung tujuan bisnisnya, sementara ITIL dapat digunakan untuk menilai efektivitas dan efisiensi dari layanan TI yang diberikan kepada pengguna internal dan eksternal[15]

2.9 Populasi, Sampel, Teknik Pengambilan Data, dan Teknik Pengujian Data

2.10 Populasi

“Populasi adalah wilayah generalisasi yang terdiri atas obyek/subyek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya[15]

2.11 Sampel

Sampel adalah bagian dari jumlah dan karakteristik yang dimiliki oleh populasi [5]. Pengambilan sampel dalam penelitian ini dengan teknik probability. Probability sampling adalah teknik pengambilan sampel yang memberikan peluang yang sama bagi setiap unsur (anggota) populasi untuk dipilih menjadi anggota sampel.

Jadi, sampel merupakan bagian dari populasi, data yang diperoleh tidaklah lengkap namun jika pengambilan sampel dilakukan dengan mengikuti kaidah- kaidah ilmiah maka biasanya sangat mungkin diperoleh hasil-hasil dari sampel cukup akurat untuk menggambarkan populasi yang diperlukan dalam kajian yang diperlukan.

2.12 Teknik Pengambilan Data

Arikunto (2002) “metode penelitian adalah cara yang digunakan oleh peneliti dalam pengumpulan data penelitiannya”. Berdasarkan pengertian tersebut dapat dikatakan bahwa metode penelitian adalah cara yang dipergunakan untuk mengumpulkan data yang diperlukan dalam penelitian.

Untuk memudahkan dalam pengambilan data, digunakan kuesioner / angket dan wawancara sebagai sumber data yang akan diolah. Angket menurut Sugiyono (2008) adalah “Angket atau kuisisioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawab”.