BAB II
LANDASAN TEORI

2.1 Konsep Dasar Sistem

Sistem Informasi merupakan suatu istilah yang sering digunakan dalam dunia TI. Berikut ini adalah pengertian sistem, informasi dan sistem informasi

2.1.1 Pengertian Sistem

Sistem menurut McLeod & Schell (2008) merupakan sekelompok elemen-elemen yang saling terintegrasi dengan maksud yang sama untuk mencapai satu tujuan. Definisi lain dari sistem adalah sejumlah hal terkait yang bekerja sama untuk mencapai tujuan secara keseluruhan (Hanna & Rance, 2011).

2.1.2 Pengertian data dan Informasi

Data merupakan fakta-fakta dan angka-angka yang relatif tidak berarti bagi pemakainya (Mcleod & Schell, 2008). Definisi lain dari data yaitu Data merupakan fakta tentang peristiwa atau kenyataan lain yang mendukung suatu pengetahuan untuk dijadikan dasar guna penyusunan keterangan, pembuatan kesimpulan atau penetapan keputusan (Gondodiyoto dan Hendarti, 2007). Dari dua definisi tersebut dapat disimpulkan bahwa data merupakan hasil pengamatan dalam bentuk fakta-fakta atau angka-angka yang relatif tidak berarti bagi pemakainya namun dapat diolah melalui proses tertentu untuk menjadi pengetahuan yang lebih bermanfaat bagi pemakainya.

Sedangkan informasi merupakan adalah data yang telah diproses, atau data yang memiliki arti (McLeod & Schell, 2008). Definisi lain menyatakan bahwa informasi merupakan hasil pengolahan data sehingga bertambah kegunaannya dan dapat dipakai untuk suatu tujuan tertentu atau untuk analisis dan pengambilan keputusan (Gondodiyoto dan Hendarti, 2007). Dari dua definisi informasi tersebut dapat disimpulkan bahwa informasi merupakan hasil dari pemrosesan data berupa fakta-fakta atau angka-angka yang bermanfaat bagi penggunanya dalam melakukan analisis dan dasar pengambilan keputusan

2.1.3 Pengertian Sistem Informasi

Menurut Stair dan Reynolds (2016) sistem informasi merupakan kumpulan komponen-komponen yang saling terkait dalam mengumpulkan, memanipulasi, serta menyebarluaskan data dan informasi serta menyediakan *feedback* (umpan balik) yang membantu organisasi dalam mencapai tujuannya seperti meningkatkan laba perusahaan atau meningkatkan layanan kepada pelanggan. Dalam sistem informasi ada 4 elemen inti yaitu *input-process-output-feedback*. *Input* (masukkan) merupakan proses mengumpulkan data mentah dalam bentuk fakta-fakta atau angka-angka untuk selanjutnya dimasukkan ke dalam sistem.

Setelah itu adalah *process* (proses) yang merupakan tahap untuk mentransformasikan data dalam bentuk fakta atau angka menjadi *output* yang bermanfaat. Setelah *process* selesai, dihasilkanlah *output* (keluaran) berupa sebuah informasi yang bermanfaat dalam bentuk laporan atau dokumen. Dan terakhir adalah *feedback* (umpan balik) yang merupakan informasi dari sistem yang digunakan untuk membuat perubahan pada tahap input atau pada tahap pemrosesan data apabila terjadi kesalahan pada tahap input atau gangguan pada saat pemrosesan data.

2.2 Konsep Dasar Audit Sistem Informasi

Audit identik dengan proses evaluasi atau penilaian sesuatu. Di bawah ini terdapat penjelasan mengenai audit lebih rinci serta audit sistem informasi.

2.2.1 Pengertian Audit Sistem Informasi

Audit dalam aspek ITistratif menurut Gondodiyoto dan Hendarti (2007) memiliki arti pemeriksaan terhadap perencanaan organisasi, penerapan sistem dan prosedur kerja apakah efektif dan efisien suatu organisasi serta kehandalan sistem sehubungan dengan kebijakan organisasi. Kemudian dalam konteks tatakelola TI audit merupakan pemeriksaan terhadap manajemen sumber daya informasi atau terhadap kehandalan sistem informasi berbasis teknologi informasi mengenai aspek efektifitas, efisiensi, data integritas, *saveguarding asset*, *reliability*, *confidentiality*, *availability*, dan *security*. Sedangkan audit sistem informasi merupakan mekanisme yang digunakan untuk memeriksa serta mengevaluasi implementasi sistem tata kelola TI di sebuah organisasi. Proses penilaian serta pengukuran ini dilakukan oleh pemeriksa (auditor) dengan menggunakan metode tertentu seperti metode *Balanced Scorecard* (BSC) (Jogiyanto & Abdillah, 2011).

Dari pengertian diatas, dapat disimpulkan bahwa audit sistem informasi adalah proses pengumpulan bukti dan evaluasi untuk mengetahui tingkat kesesuaian sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah sistem informasi telah didesain dan diimplementasikan secara efektif, efisien, ekonomis serta memiliki mekanisme pengamanan asset yang memadai dan menjamin integritas data.

2.2.2 Tujuan Audit Sistem Informasi

Audit TI memberikan informasi yang membantu organisasi mengelola risiko, selain itu Audit TI juga mengkonfirmasi alokasi sumber daya terkait TI yang efisien, serta mencapai tujuan TI dan bisnis lainnya. Adapun alasan lainnya melakukan audit (Gantz, 2014) di antara lain adalah:

a. Mengevaluasi efektivitas kontrol yang diterapkan

b. Mengkonfirmasikan kepatuhan terhadap kebijakan, proses, dan prosedur internal

c. Memeriksa kesesuaian dengan tata kelola TI atau kerangka kerja kontrol dan standar

d. Menganalisis kerentanan dan pengaturan konfigurasi untuk mendukung pemantauan berkelanjutan

e. Mengidentifikasi kelemahan dan defisiensi sebagai bagian dari manajemen risiko awal atau berkelanjutan

f. Mengukur kinerja terhadap tolok ukur kualitas atau perjanjian tingkat layanan

g. Memverifikasi dan memvalidasi rekayasa sistem atau praktik manajemen proyek TI

h. Menilai sendiri organisasi terhadap standar atau kriteria yang akan digunakan dalam audit eksternal yang akan direncanakan

2.3 Keamanan Informasi

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dalam sebuah organisasi. Berikut ini dijelaskan mengenai definisi keamanan informasi, tujuan keamanan informasi dan aspek-aspek dalam keamanan informasi.

2.3.1 Definisi Keamanan Sistem Informasi

Keamanan informasi merupakan perlindungan terhadap informasi dari 3 aspek yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan), dan juga perlindungan terhadap sistem serta perangkat keras yang digunakan untuk menyimpan atau mentransmisikan informasi tersebut melalui penerapan kebijakan, program pelatihan dan penyadaran serta teknologi (Whitman & Mattord, 2014). Sedangkan definisi keamanan informasi menurut Arnason & Willett (2008) adalah perlindungan aset organisasi (mis., Informasi) dari pengungkapan yang tidak sah dan modifikasi yang tidak sah dan tidak disengaja, dan memastikan informasi tersebut siap digunakan saat diperlukan. Peraturan perundang-undangan dan persyaratan kepatuhan lainnya membahas privasi dan pelaporan keuangan yang akurat, dan umumnya mencakup kebutuhan akan kontrol keamanan yang baik seputar informasi.

Adapun jenis keamanan informasi dapat dibagi menjadi beberapa bagian berikut (Whitman & Mattord, 2014):

1. *Physical Security* (Keamanan Fisik)

   Keamanan yang berfokus untuk memberikan perlindungan terhadap karyawan atau staff organisasi, aset fisik, maupun tempat kerja apabila terjadi ancaman seperti insiden kebakaran kebakaran, adanya akses tanpa otorisasi/tidak sah, dan bencana alam.

2. *Operational Security*

Keamanan yang berfokus untuk memberikan perlindungan terhadap adanya gangguan yang mungkin akan mengganggu kemampuan organisasi dalam melaksanakan kegiatan operasional.

3. *Communications Security*

Keamanan yang berfokus untuk memberikan perlindungan terhadap kemampuan perusahaan dalam menggunakan media komunikasi, teknologi komunikasi, serta konten yang ada di dalamnya untuk mencapai tujuan sebuah organisasi.

4. *Network Security*

Keamanan yang berfokus untuk memberikan perlindungan terhadap kemampuan perusahaan dalam menggunakan jaringan yang terdiri dari perangkat jaringan, koneksi serta konten yang ada pada jaringan untuk mencapai fungsi komunikasi data organisasi tersebut.

2.3.2 Tujuan Keamanan Informasi

Setiap organisasi atau perusahaan menerapkan sistem informasi berbasis komputer untuk mencapai tujuan tertentu. Oleh karena itu, perusahaan dituntut untuk menciptakan sistem keamanan untuk mengamankan aset yang dimiliki berupa hardware dan software dari sistem informasi tersebut. Tujuannya adalah untuk meyakinkan kerahasisaan, ketersediaan, dan integritas dari pengolahan data. Tentu biaya yang dikeluarkan perusahaan untuk pengamanan terhadap sistem komputer harus wajar apabila ingin meminimalkan risiko serta memelihara keamanan sistem komputerisasi pada suatu tingkatan atau level yang dapat diterima. Karena reputasi organisasi akan dinilai masyarakat dari tiga aspek di atas yaitu integritas, kerahasiaan, dan ketersediaan informasi (IBISA, 2011).

Penekanan dalam manajemen keamanan informasi ada pada pemantauan terus menerus, lalu penilaian ancaman dan kerentanan, serta evaluasi terhadap implementasi dan efektivitas kontrol keamanan. Kontrol keamanan baik itu keamanan administrasi, teknis, dan fisik, merupakan fokus utama manajemen keamanan informasi dan kegiatan audit yang dilakukan berguna untuk mendukung program keamanan informasi. Manajemen keamanan informasi memerlukan pemilihan, implementasi, konfigurasi, operasi, dan pemantauan kontrol keamanan yang cukup untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem informasi dan data di dalamnya (Gantz, 2014)

2.4 COBIT 5

COBIT 5 merupakan versi paling baru dari COBIT yang dibuat oleh *Information System Audit and Control Association* (ISACA) pada tahun 2012. COBIT 5 menyediakan kerangka kerja komprehensif yang dapat membantu perusahaan untuk mencapai tujuan dalam hal tata kelola serta pengelolaan TI perusahaan. COBIT 5 juga dapat membantu perusahaan untuk menciptakan nilai optimal dari TI yang digunakan dengan mengoptimalkan tingkat risiko dengan penggunaan sumber daya yang dimiliki perusahaan (ISACA, 2012).

COBIT 5 hanya menyediakan kerangka kerja bagi perusahaan untuk mengukur serta memantau kinerja TI. Namun dalam penerapannya setiap perusahaan harus mendefinisikan sendiri bidang proses yang sesuai dengan kebutuhan perusahaan dengan mempertimbangkan situasi tertentu di dalam perusahaan terkait.

Pada COBIT 5 terdapat 37 proses tata kelola dan manajemen yang bertujuan untuk menghasilkan tujuan yang optimal. Dalam area tata kelola terdapat satu domain yaitu domain *Evaluate, Direct, and Monitor* (EDM), sedangkan pada area manajemen terdapat empat domain yaitu *Align, Plan, and Organise* (APO), *Build Acquire, and Implement* (BAI), *Deliver, Service, and Support*, dan *Monitor, Evaluate, and Assess* (MEA).

Penjelasan masing-masing domain dapat dilihat di bawah ini:

1. Evaluate, Direct and Monitor (EDM)

Proses tata kelola ini sesuai bagi pemangku kepentingan perusahaan untuk melakukan penilaian, optimasi risiko dan sumber daya, yang mencakup praktek serta kegiatan dengan tujuan untuk mengevaluasi pilihan strategis dan memberikan arahan kepada TI dan melakukan pemantauan hasil dari TI.

Berikut domain proses EDM:

a. EDM 01 Memastikan Pengaturan dan Pemeliharaan Kerangka Kerja Tata Kelola
b. EDM 02 Memastikan Keluaran yang Bermanfaat
c. EDM 03 Memastikan Pengoptimalan Risiko
d. EDM 04 Memastikan Pengoptimalan Sumber Daya
e. EDM 05 Memastikan Transparansi Pemangku Kepentingan

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

Ini termasuk dalam proses manajemen yang mencakup strategi dan taktik, dan mengidentifikasi kekhawatiran cara terbaik untuk mengoptimalkan TI agar dapat berkontribusi pada pencapaian tujuan bisnis yang ingin dicapai oleh *stakeholder* perusahaan. Di bawah ini merupakan domain proses APO:

a. APO01 Mengelola Kerangka Manajemen TI
b. APO02 Mengelola Strategi
c. APO03 Mengelola Arsitektur Bisnis
d. APO04 Mengelola Inovasi
e. APO05 Mengelola Dokumen
f. APO06 Mengelola Anggaran dan Biaya
g. APO07 Mengelola Sumber Daya Manusia
h. APO08 Mengelola Relasi
i. APO09 Mengelola Perjanjian Layanan
j. APO10 Mengelola Pemasok
k. APO11 Mengelola Kualitas
l. APO12 Mengelola Risiko
m. APO13 Mengelola Keamanan

3. *Build, Acquire and Implementation* (BAI)

Termasuk dalam proses manajemen yang bertujuan memberikan solusi dan melewatinya sehingga akan berubah menjadi layanan. Dalam mewujudkan strategi TI, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan diintegrasikan ke dalam proses bisnis. Untuk memastikan bahwa solusi terus memenuhi tujuan bisnis maka domain ini juga mencakup aspek perubahan serta pemeliharaan sistem yang ada di dalam perusahaan. Di bawah ini merupakan domain proses BAI:

a. BAI01 Mengelola Program dan Proyek
b. BAI02 Mengelola Definisi Persyaratan
c. BAI03 Mengelola Identifikasi Solusi dan Pembangunan

d. BAI04 Mengelola Ketersediaan dan Kapasitas

e. BAI05 Mengelola Pemberdayaan Perubahan Organisasi

f. BAI06 Mengelola Perubahan

g. BAI07 Mengelola Penerimaan Perubahan dan Transisi

h. BAI08 Mengelola Pengetahuan

i. BAI09 Mengelola Aset

j. BAI10 Mengelola Susunan

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

DSS merupakan proses manajemen yang 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 dan fasilitas operational. Di bawah ini merupakan domain proses DSS:

a. DSS01 Mengelola Operasi

b. DSS02 Mengelola Layanan Permohonan dan Kecelakaan

c. DSS03 Mengelola Masalah

d. DSS04 Mengelola Keberlangsungan

e. DSS05 Mengelola Jasa Keamanan

f. DSS06 Mengelola Kontrol Proses Bisnis

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

Merupakan proses manajemen untuk memonitor semua proses TI yang ada serta memastikan bahwa proses mengikuti arah yang telah disediakan. Untuk memastikan kepatuhan serta kualitas, proses TI perlu dilakukan penilaian secara teratur dalam jangka waktu tertentu. Di bawah ini merupakan domain proses dari MEA:

a. MEA01 Memantau, Evaluasi dan Menilai Kinerja dan Penyesuaian

b. MEA02 Memantau, Evaluasi dan Menilai Sistem Pengendalian Internal

c. MEA03 Memantau, Evaluasi dan Menilai Kepatuhan dengan Persyaratan Eksternal

d. Pada penelitian ini penulis hanya berfokus pada domain APO13 dan DSS05 saja yang berfokus kepada keamanan sistem informasi

2.5 ISO 27001

The International Organization for Standarization atau yang sering disebut ISO, yaitu badan penetap standar internasional di bidang industrial dan komersial dunia yang bertujuan untuk meningkatkan perdagangan antar negara di dunia. ISO sendiri terdapat beberapa jenis standar yang dikeluarkan, salah satunya adalah ISO 27001.

ISO 27001 merupakan salah satu seri yang diterbitkan oleh *The International Organization for Standarization* yang didalamnya berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat indipenden terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, serta dirancang untuk menjamin kontrol keamanan yang dipilih perusahaan dapat melindingi aset informasi dari berbagai risiko serta memberi keyakinan tangkat keamanan bagi pihak yang berkepentingan