BAB II
LANDASAN TEORI

Bab ini membahas teori–teori yang terkait tentang *IT Governance*(Tata kelola TI), Audit Sistem Informasi dan COBIT *4.1* sebagai pedoman yang digunakan dalam penilaian kinerja TI pada UPT komputer di STT–Nurul Fikri.

2.1 IT Governance

2.1.1 Definisi IT Governance

Menurut Weill dan Ross (2004),: "*Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT*.". Dijelaskan bahwa *IT Governance* (Tata kelola Teknologi Informasi) adalah *Framework* yang spesifik dalam pengambilan keputusan dan akuntabilitas untuk mendukung kebiasaan perusahaan dalam menggunakan TI.

Definisi tersebut menitikberatkan bahwa IT *Governance* harus mampu mengarahkan perilaku penggunaan TI sesuai dengan perilaku yang diinginkan atau ditetapkan (perilaku yang sesuai dengan visi misi, nilai-nilai, strategi dan budaya organisasi).

Menurut Sambamurthy and Zmud (1999), *IT Governance* dimaksudkan sebagai pola dari otoritas/kebijakan terhadap aktivitas TI. Pola ini diantaranya adalah: membangun kebijakan dan pengelolaan IT Infrastruktur, penggunaan TI oleh *end-user* secara efisien, efektif dan aman, serta proses *IT Project Management* yang efektif.

Lebih lanjut Oltsik mengatakan bahwa *IT Governance* yang baik harus berkualitas, *well-defined* dan bersifat "*repeatable processes*" yang terukur (*metric*). *IT Governance* yang dikembangkan dalam suatu organisasi modern berfungsi pula mendefinisikan (*outline*) kebijakan-kebijakan TI, penetapan prosedur penting *IT Process*, dokumentasi aktivitas TI, termasuk membangun *IT Plan* yang efektif berdasarkan perubahan lingkungan perusahaan dan perkembangan TI.

2.1.2 Area Fokus IT Governance

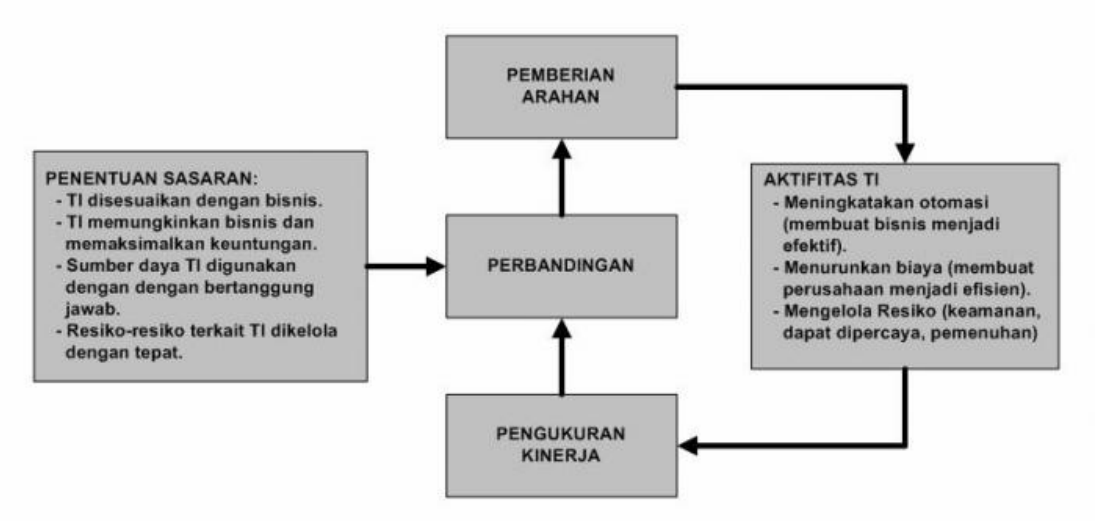
Terdapat 5 area yang menjadi fokus *IT Governance* antara lain yaitu:

1. *Strategic alignment*: berfokus pada memastikan hubungan bisnis dan rencana TI; mendefinisikan, memelihara dan memvalidasi proposisi nilai TI, dan menyelaraskan operasi TI dengan operasi perusahaan.
2. *Value delivery*: adalah tentang menjalankan proposisi nilai seluruh siklus pengiriman, memastikan bahwa TI memberikan manfaat yang dijanjikan terhadap strategi, berkonsentrasi untuk mengoptimalkan biaya dan membuktikan nilai intrinsik TI.
3. *Risk management*: membutuhkan kesadaran risiko dari pejabat perusahaan senior, pemahaman yang jelas tentang *risk appetite* perusahaan itu, pemahaman tentang persyaratan kepatuhan, transparansi tentang risiko yang signifikan untuk perusahaan dan menanamkan tanggung jawab manajemen risiko dalam organisasi.
4. *Resource management*: adalah tentang investasi yang optimal, dan pengelolaan yang tepat atas sumber daya TI yang kritis, yaitu antara lain aplikasi, informasi, infrastruktur dan orang-orang. Isu-isu kunci berkaitan dengan optimasi pengetahuan dan infrastruktur.
5. *Performance measurement*: menjalankan dan memonitor implementasi atas strategi, penyelesaian proyek, penggunaan sumber daya, kinerja proses dan pelayanan pengiriman. Misalnya, *balanced scorecard* yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan yang diharapkan.

2.1.3 Proses IT Governance

Dalam Proses *IT Governance* dimulai dengan menetapkan tujuan bagi teknologi informasi. Kemudian dari aktivitas TI yang terjadi kinerja akan diukur dan dibandingkan dengan tujuan, sehingga dihasilkan pengalihan aktivitas jika diperlukan atau melakukan perubahan tujuan yang sudah disesuaikan.

Tujuan perusahaan yang merupakan tanggung jawab utama dewan direksi dan kinerja perusahaan yang merupakan tanggung jawab pihak manajemen, tentunya menyebabkan mereka harus terus melakukan pengembangan, sehingga tujuan dapat dicapai dan pengukurannya dapat merepresentasikan tujuan yang benar.



Gambar 1 Proses IT Governance

Dalam Menanggapi tujuan yang diterima, fungsi TI perlu fokus pada pencapaian keuntungan dengan meningkatkan otomasi dan membuat organisasi / perusahaan lebih efektif dengan mengurangi biaya agar perusahaan berjalan lebih efisien, serta dengan mengelola risiko (keamanan, keandalan dan kepatuhan).

2.2 Audit Sistem Informasi

Audit sistem informasi atau *Information System Audit* disebut juga EDP Audit (*Electronic Data Processing Audit*) atau komputer audit merupakan suatu proses dikumpulkannya data dan bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi sudah diterapkan dan menerapkan sistem pengendalian internal yang sudah sepadan, seluruh aktiva dilindungi dengan baik atau disalahgunakan dan juga terjamin integritas data, keandalan dan juga efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer. Audit sistem informasi merupakan gabungan dari berbagai macam ilmu, antara lain traditional audit, manajemen sistem informasi, sistem informasi akuntansi, ilmu komputer, dan *behavioral science*. Menurut Ron Weber (2010) audit sistem informasi adalah proses pengumpulan dan penilaian bukti–bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien.

Beberapa aspek yang diperiksa pada audit sistem informasi seperti efektifitas, efisiensi, *availability system*, *reliability*, *confidentiality*, dan *integrity*, aspek *security*, audit atas proses, modifikasi program, audit atas sumber data, dan data file. Faktor-faktor yang mendorong pentingnya kontrol dan audit sistem informasi (Weber, 2006) adalah :

- Mendeteksi agar komputer tidak dikelola secara kurang terarah.
- Mendeteksi risiko kehilangan data.
- Mendeteksi risiko pengambilan keputusan yang salah akibat informasi hasil proses sistem komputerisasi salah/lambat/tidak lengkap.
- Menjaga aset perusahaan karena nilai *hardware*, *software* dan personil yang lazimnya tinggi.
- Mendeteksi risiko error komputer.
- Mendeteksi risiko penyalahgunaan komputer (*fraud*).
- Menjaga kerahasiaan.
- Meningkatkan pengendalian evolusi penggunaan komputer.

2.2.1 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Ron Weber secara garis besar yaitu:

- **Pengamanan Aset**: Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, file data harus dijaga oleh suatu sistem pengendalian internal yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan.
- **Menjaga Integritas Data**: Integritas data (*data integrity*) adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti: kelengkapan, kebenaran, dan keakuratan. Jika integritas data tidak terpelihara, maka suatu perusahaan tidak akan lagi memiliki hasil atau laporan yang benar bahkan perusahaan dapat mengalami kerugian.
- **Efektivitas Sistem**: Efektivitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan user.
- **Efisiensi Sistem**: Efisiensi menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai atau 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.

2.2.2 Pendekatan Audit

Adapun pendekatan audit terdiri dari tiga jenis yaitu :

- *Auditing Around Computer* (Audit Sekitar Komputer) yaitu dimana penggunaan komputer pada tahap proses diabaikan.
- *Auditing Through Computer* (Auditing Melalui Komputer) yaitu dimana pada tahap proses penggunaan komputer telah aktif.
- *Auditing With Computer* (Auditing Dengan Komputer) yaitu dimana input, proses dan output telah menggunakan komputer.

2.2.3 Tahapan Audit Sistem Informasi

Menurut Gallegos dalam bukunya "*Audit And Control Of Information System*" menyatakan audit sistem informasi meliputi beberapa tahapan yakni:

- **Perencanaan (*Planning*),** dalam hal ini yang perlu dilakukan adalah menentukan ruang lingkup dan tujuan dari audit itu sendiri. Penulis sudah menetapkan ruang lingkup yang hanya meneliti aktivitas dan kinerja dari UPT komputer dengan tujuan mengetahui kondisi *IT Governance* pada UPT komputer di STT-NF dengan menggunakan domain *Monitor and Evaluate* dan *Deliver and support*. Alasannya memilih domain *Monitor and Evaluate* karena UPT komputer masuk dalam implementasi TI dan memonitor keadaan jaringan dan Lab kampus.

  Sedangkan penggunaan Domain *Deliver and support* lebih ke arah pelayanan yang disediakan oleh tim UPT komputer sudah memuaskan atau belum, atau kesigapan saat dimintai pertolongan baik dosen, staf dan mahasiswa. Serta masalah apa yang harus lebih di prioritaskan.

- **Pemeriksaan lapangan (*Field Work*),** pada tahap ini yang dikerjakan yaitu mengumpulkan informasi yang dilakukan dengan cara mengumpulkan data dengan pihak–pihak yang berhubungan. Contohnya penulis membaca

literatur yang berkaitan tentang penelitian, lalu penulis juga menggunakan wawancara untuk mengetahui apa yang sebenarnya terjadi di lapangan.

- **Pelaporan (*Reporting*),** setelah pengumpulan data maka akan diperoleh data yang akan diproses untuk dihitung menurut perhitungan maturity level dimana hal ini menjadi hasil audit nantinya.
- **Tindak lanjut (*Follow Up*),** tahapan ini dilakukan dengan pemberian laporan hasil audit dalam bentuk rekomendasi tindakan perbaikan kepada pihak manajemen objek yang diteliti agar menjadi lebih baik lagi.

2.3 COBIT 4.1

2.3.1 Definisi COBIT

COBIT (*Control Objective for Information and Related Technology*) merupakan *aset best practices* (*framework*) bagi pengelolaan teknologi Informasi (TI). COBIT disusun oleh *the IT Governance Institute* (ITGI) dan *Information System Audit and Control Association* (ISACA) pada tahun 1992. Pada tahun 1996 diterbitkan COBIT edisi pertama. kemudian edisi kedua dari COBIT diterbitkan pada tahun 1998. Pada tahun 2000 dirilis COBIT 3.0 dan COBIT 4.0 pada tahun 2005. kemudian COBIT 4.1 dirilis tahun 2007 dan yang terakhir COBIT 5.0 yang dikeluarkan tahun 2012.

COBIT sendiri merupakan kombinasi dari prinsip–prinsip yang telah dibenamkan dengan *balanced scorecard* dan dapat digunakan sebagai acuan model (seperti COSO) dan disejajarkan dengan standar industri seperti ITIL, CMM, BS 779, ISO 9000. COBIT juga bermanfaat bagi manajemen untuk membantu menyeimbangkan antara risiko dan investasi pengendalian dalam sebuah lingkungan TI yang sering tidak dapat diprediksi.

Bagi seorang user ia sangat berguna untuk memperoleh keyakinan atas pelayanan keamanan dan pengendalian TI yang disediakan oleh pihak internal atau pihak ketiga. Sedang kan untuk seorang auditor ia berguna untuk mendukung atau memperkuat sebuah opini yang dihasilkan dan memberikan saran kepada manajemen atas pengendalian internal yang ada.

Menurut COBIT, keputusan dalam sebuah bisnis yang baik harus didasarkan pada Knowledge yang berasal dari informasi yang relevan, komprehensif dan tepat waktu yang dapat dihasilkan jika informasi memenuhi 7 kriteria yang ada dalam COBIT.

Demi memenuhi tujuan bisnis, Informasi perlu memenuhi kriteria tertentu, 7 kriteria informasi yang menjadi perhatian COBIT adalah sebagai berikut:

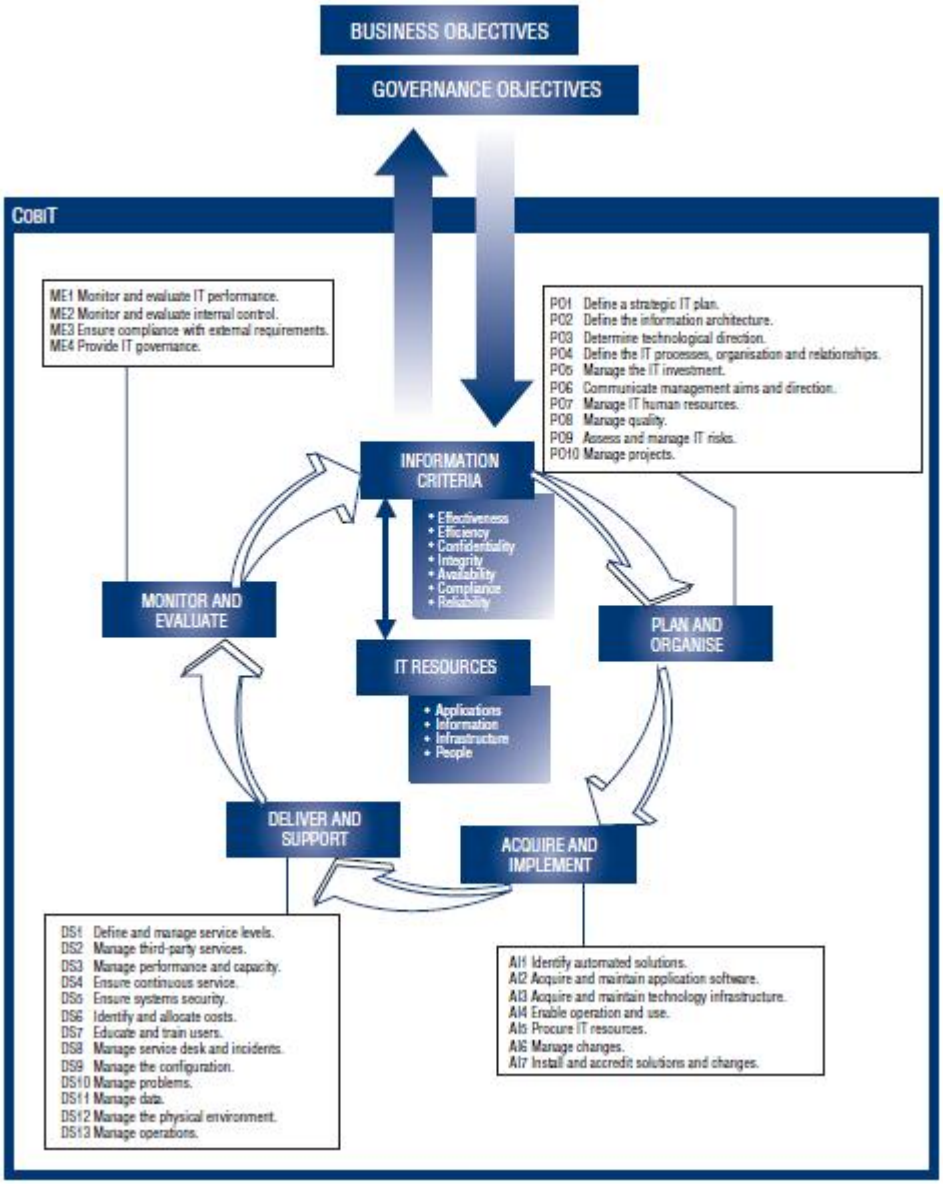
Tabel 1 Kriteria Informasi COBIT

Effectiveness (Efektifitas)	Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, konsisten, dapat dipercaya dan tepat waktu.
Efficiency (Efisiensi)	Penyediaan informasi melalui penggunaan sumber daya (yang paling produktif dan ekonomis) yang optimal.
Confidentiality (Kerahasiaan)	Berkaitan dengan proteksi pada informasi penting dari pihak–pihak yang tidak memiliki otorisasi / tidak berwenang.
Integrity (Integritas)	Berkaitan dengan keakuratan dan kelengkapan data/ informasi dan tingkat validitas yang sesuai dengan ekspektasi dan nilai bisnis.
Availability (Ketersediaan)	Fokus terhadap ketersediaan data/ informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun dimasa yang akan datang. ini juga terkait dengan pengaman atas sumber daya yang diperlukan.
Compliance (Kepatuhan)	Pemenuhan data/ informasi yang sesuai dengan ketentuan hukum, peraturan dan rencana perjanjian/ kontrak untuk proses bisnis.
Reliability (Handal)	Fokus pada pemberian informasi yang tepat bagi manajemen dan mengoperasikan perusahaan dan

	pemenuhan kewajiban mereka untuk membuat laporan keuangan.

2.3.2 COBIT Framework

Secara keseluruhan hubungan antara *Business Objectives*, *IT Governance*, *Information*, *IT Resource*, dengan 4 domain dan 34 *high level control objectives* dideskripsikan dalam gambar dibawah ini:



Gambar 2 Cobit Framework (IT Governance institute, 2007)

2.3.3 Elemen-Elemen Sumber Daya TI

Elemen–elemen sumber daya TI merupakan hal yang sangat penting di dalam pencapaian tujuan bisnis. Karena itu dibutuhkan dukungan sumber daya informasi yang memadai. Fokus terhadap pengelolaan sumber daya teknologi informasi dalam COBIT 4.1 diantaranya:

- Aplikasi

  Merupakan sistem otomatis yang digunakan dan prosedur manual mengenai proses informasi.
- Informasi

  Merupakan data dalam segala bentuk yang melalui tahap input, proses dan output / dihasilkan oleh sistem informasi dalam berbagai bentuk yang nantinya akan digunakan oleh perusahaan.
- Infrastruktur

  Merupakan teknologi dan fasilitas (*hardware, operating systems, database management system, networking*, multimedia dan lingkungan pendukung lainnya) yang dapat memproses aplikasi.
- Personil

  Personil yang dibutuhkan untuk melakukan perencanaan, mengorganisasikan, memperoleh, mengimplementasikan, menyampaikan, mendukung, mengawasi dan mengevaluasi sistem dan layanan informasi.

2.3.4 Komponen Control Objectives

Framework COBIT disusun dengan karakteristik yang berfokus pada bisnis (*business-focused*), berorientasi pada proses (*process-oriented*), berbasis pada pengendalian (*control-based)* dan terarah kepada pengukuran (*measurement-driven*). Pada edisi keempatnya ini, *Framework* COBIT terdiri dari 34 *high level control objectives* dan kemudian mengelompokan proses tersebut menjadi 4 domain, keempat domain tersebut adalah: *Planning and Organization* (10 proses), *Acquisition and Implementation* (7 proses), *Delivery and Support* (13 proses) dan *Monitoring and Evaluation* (4 proses) yang mencangkup:

Plan and Organization (perencanaan dan organisasi):
Mencakup strategi, taktik dan identifikasi kontribusi terbaik TI demi pencapaian tujuan perusahaan. Domain ini meliputi pertanyaan–pertanyaan sebagai berikut:

- Apakah proses TI dan strategi bisnis telah sesuai?
- Apakah perusahaan mencapai penggunaan yang optimum dengan sumber dayanya?
- Apakah setiap karyawan di perusahaan memahami tujuan TI?
- Apakah risiko TI dipahami dan dikelola?
- Apakah kualitas sistem TI sesuai dengan kebutuhan bisnis?

Acquire and Implement (pengadaan dan implementasi):
Untuk merealisasikan strategi ini, perlu dilakukan pengidetifikasian, pengembangan dan perolehan solusi TI, sesuai dengan yang akan diimplementasikan dan diintegrasikan ke dalam proses bisnis. Domain ini meliputi pertanyaan–pertanyaan sebagai berikut:

- Apakah proyek berkemungkinan akan memberikan solusi yang dibutuhkan?
- Apakah proyek baru kemungkinan akan dikirim tepat waktu dan sesuai dengan anggaran?
- Apakah sistem baru dapat bekerja dengan baik ketika diimplementasikan?

- Apakah perubahan dilakukan tanpa mengganggu operasi bisnis yang sedang berjalan?

Deliver and Support (pengiriman layanan dan dukungan)

Domain ini fokus terhadap penyampaian jasa yang sesungguhnya diperlukan, termasuk penyediaan layanan, manajemen keamanan dan kontinuitasnya, jasa dukungan kepada user dan manajemen data dan fasilitas operasi. Domain ini meliputi pertanyaan–pertanyaan sebagai berikut:

- Apakah jasa TI yang disampaikan dengan prioritas bisnis?
- Apakah biaya TI teroptimalisasi?
- Apakah sistem TI bekerja secara produktif dan aman?
- Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

Monitor and Evaluate (pengawasan dan evaluasi)

Berkenaan dengan manajemen kinerja, pemantauan internal control, kepatuhan terhadap regulasi dan pelaksanaan *IT Governance*. Domain ini meliputi pertanyaan–pertanyaan sebagai berikut:

- Apakah kinerja TI diukur untuk mendeteksi permasalahan sebelum terlambat?
- Apakah pihak manajemen memastikan bahwa internal control efektif dan efisien?
- Dapatkah kinerja TI dihubungkan dengan tujuan perusahaan?
- Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

2.3.5 Maturity Level

Tingkat kemampuan pengelolaan teknologi informasi pada skala *Maturity Level* dibagi menjadi 6 level antara lain:

1. Level 0 (*non- Existent)*

   Merupakan tahap awal perusahaan, organisasi pada tahap ini belum dapat mendefinisikan permasalahan–permasalahan yang harus diatasi. Organisasi merasa tidak membutuhkan adanya sebuah mekanisme proses *IT Governance* yang baku sehingga tidak ada pengawasan sama sekali.
2. Level 1 (*initial level*)

   Pada level ini organisasi mengetahui bukti bahwa adanya permasalahan yang harus diatasi. Sudah adanya kegiatan penyusunan sistem yang terkomputerisasi. Secara umum pendekatan terhadap pengelolaan proses tidak terorganisasi. Organisasi juga sudah memiliki sebuah inisiatif untuk melakukan IT Governance namun sifatnya non formal.
3. Level 2 (*repeatable level*)

   Pada level ini, organisasi sudah dapat melakukan perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Organisasi memiliki kebiasaan terpola untuk merancang *IT Governance* yang dilakukan secara berulang namun belum melibatkan dokumen formal.
4. Level 3 (*Defined level)*

   Pada level ini, sudah memiliki proses TI yang sudah terdokumentasi dengan baik kemudian dikomunikasikan melalui pelatihan, organisasi juga menyadari perlunya proses *IT Governance* sehingga adanya aturan yang menunjukan untuk organisasi secara rutin melakukan *IT Governance*.
5. Level 4 (*managed level)*

   Pada level ini, pihak manajemen organisasi dapat memonitor proses komputerisasi dengan baik, pengembangan sistem sudah terarah dan dijalankan secara terorganisir. Proses *IT Governance* sudah secara formal dilakukan dan secara terus menerus dievaluasi untuk meningkatkan layanan organisasi.

6. Level 5 (*optimized level)*

   Pada level ini, organisasi sudah mengikuti *best practice* yang ditandai dengan adanya proses otomatis pada sistem dengan metodologi yang tepat. *IT Governance* dijadikan acuan untuk pembenahan pelayanan organisasi.

Penulis menggunakan wawancara untuk menilai UPT komputer dan juga melakukan sebar kuesioner secara acak, khusus untuk kuesioner penulis menyederhanakan dengan menggunakan asumsi tersendiri untuk memudahkan hasil yang didapat. Ada lima opsi yang dibuat antara lain tidak tahu, kurang setuju, tidak setuju, setuju dan sangat setuju.

Kurang setuju dan tidak setuju masuk dalam katagori *minus*(nilainya satu) lalu setuju dan sangat setuju masuk dalam katagori *plus*(nilainya satu) dan tidak tahu itu nilai yang dipertimbangkan masuknya dalam katagori *plus* atau *minus*. Kemudian hasil keseluruhan kuesioner ini akan mewakili satu pertanyaan tentang fasilitas dan layanan yang nantinya akan menjadi nilai *Maturity Level*.

Cara menghitung agar mendapat *Maturity Level* adalah menghitung total jawaban pada satu pertanyaan, lalu dibuatkan persentase dari masing – masing jawaban yang ada. Kemudian ditentukan tingkat Maturity level berdasarkan persentase yang telah ditentukan dan setelah itu dirata – rata nilai yang didapat. Sebagai contoh jika dalam satu pertanyaan tentang UPT dan 80% responden mencentang kolom "setuju/sangat setuju" maka maturity level yang didapat adalah 4 tapi jika 80% yang mencentang adalah "tidak setuju/tidak tahu" maka maturity levelnya 2.

PERSENTASE	MATURITY LEVEL
1% s/d 19%	1
20% s/d 55%	2
56% s/d 69%	3
70% s/d 89%	4
90% s/d 100%	5

2.4 Penelitian Terkait

Tabel 2 Penelitian terkait

No	Judul penelitian	Peneliti	Objek penelitian	Metode	Tahun	kesimpulan
1	Evaluasi IT Governance berdasarkan cobit 4.1 (Studi Kasus di PT Timah (persero))	Dwi Rizki Kesumawardhani	Tata Kelola	Maturity Level	2012	Perusahaan yang diteliti mempunyai sebuah nilai rata–rata yang baik yang berarti bahwa seluruh proses telah didokumentasikan
2	Tata Kelola Teknologi Informasi (IT Governance) menggunakan Framework COBIT 5	Mega Putri Islamiah	Tata Kelola	Maturity Level	2014	Masih belum adanya proses yang belum terpenuhi karena secara umum hampir semua mengarah pada level 1
3	Audit Teknologi Informasi pada PT ASTRA International TBK (DAIHATSU) Lampung menggunakan pendekatan COBIT 4.1	Lilis Oktaviani Sirait	Audit Teknologi	Maturity Level	2017	Maturity level adalah 4,02 yang artinya TI yang dikelola sudah baik dimana prosedur dan kebijakan yang ada dilakukan secara efektif dapat dipantau dan diukur.
4	Evaluasi IT Governance menggunakan COBIT 4.1 pada UPT komputer di STT Terpadu Nurul Fikri	Muhammad Habib	Tata Kelola	Maturity Level	2019	Menilai sejauh mana dalam mengatur hal yang terkait pada COBIT 4.1