# ANALISIS TATA KELOLA TI BERDASARKAN DOMAIN *DELIVERY AND SUPPORT* 5 (DS5) UNTUK MEMASTIKAN KEAMANAN SISTEM MENGGUNAKAN FRAMEWORK COBIT 4.1 PADA UNIVERSITAS DIAN NUSWANTORO SEMARANG

Eka Mahardika

Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang

Jl. Nakula I No. 5-11 Semarang 50131

ekamahar1992@gmail.com

**ABSTRAK**

Oleh karena penyelenggaraan aktivitas pendidikan tidak dapat lepas dari TI perlu diperhatikan pula tinggkat keamanannya. Keamanan TI adalah hal yang paling krusial atau penting. Tingkat keamanan data yang ada di dalam sistem adalah harta paling penting. Pada penelitian ini dilakukan analisis terhadap tata kelola proses untuk memastikan keamanan sistem (DS 5) menggunkanan framework COBIT 4.1. Data diperoleh dengan mengumpulkan data secara study dokumen, wawancara dan kuisioner. Berdasarkan perhitungan maturity level, Udinus berada pada level 2 yakni Repeatable but Intuitive. Pada level tersebut praktek memastikan keamanan sistem telah bermunculan hanya tingkat insiden masih tinggi dan terulang karena belum dilakukan secara berkelanjutan dan tidak ada dokumen prosedur. Rekomendasi perbaikan telah diberikan dengan memanfaatkan 6 atribut maturity level pada level 3 (defined process) dan sesuai dengan control objective proses untuk memastikan keamanan sistem (DS 5).

**Kata Kunci** : *Control Objective, Framework COBIT 4.1, Maturity Level, Memastikan Keamanan Sistem, Repeatable but Intuitive.*

## 1. PENDAHULUAN

### 1.1. Latar Belakang Masalah

Bagaimana tingkat kematangan *(maturity level)* memastikan keamanan sistem (DS5) di Universitas Dian Nuswantoro berdasarkan *Framework COBIT 4.1*, serta bagaimana perumusan strategi yang tepat untuk menentukan skala prioritas pengelolaan dan memastikan keamanan sistem yang sesuai dengan strategi bisnis dan tujuan Universitas Dian Nuswantoro Semarang berdasarkan tingkat kematangan *(maturity level)* proses tersebut.

### 1.2. Tinjauan Pustaka

Objek yang menjadi penelitian adalah pada Universitas Dian Nuswantoro Semarang.

### 1.3. Tujuan

Tujuan yang akan dicapai dalam penelitian ini adalah untuk mengetahui pengelolaan proses memastikan keamanan sistem (DS5) di Universitas Dian Nuswantoro saat ini. Serta untuk mengetahui perbaikan berkaitan dengan pengelolaan proses memastikan tingkat keamanan sistem (DS5) di Universitas Dian Nuswantoro saat ini.

### 1.4. Manfaat

Manfaat yang diharapkan dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Sebagai pertimbangan kebijakan manajemen dalam menerapkan TI di Universitas Dian Nuswantoro terutama pada domain DS5 proses memastikan keamanan sistem.
1. Sebagai bahan untuk memperkaya ilmu pengetahuan di Bidang Tata Kelola IT pada lembaga bersifat non profit salah satunya yaitu Lembaga Perguruan Tinggi.

## 2. RUANG LINGKUP, TAHAPAN ANALISIS DAN METODE

### 2.1 Tata Kelola IT

Tata kelola TI adalah suatu struktur dan proses yang saling berhubungan serta mengarahkan dan mengendalikan perusahaan dalam pencapaian tujuan perusahaan melalui nilai tambah dan penyeimbangan antara risiko dan manfaat dari teknologi informasi serta prosesnya.

*IT Governance* merupakan satu kesatuan dengan sukses dari enterprise governance melalui peningkatan dalam efektivitas dan efisiensi dalam proses perusahaan yang berhubungan.

### 2.2 Ruang Lingkup Tata Kelola IT

Pada saat ini TI dirasakan berperan penting dalam meningkatkan keunggulan bersaing. Teknologi informasi terbukti telah menciptakan value bagi organisasi. Organisasi semakin tergantung terhadap teknologi informasi agar tetap dapat bersaing. Dengan semakin meningkatnya penggunaan teknologi informasi dalam bisnis, tata kelola teknologi informasi (*IT governance*) menjadi konsep yang penting dibicarakan.

### 2.3 *COBIT (Control Objectives For Information And Related Technology)*

Alat yang komprehensif untuk menciptakan adanya IT Governance di organisasi adalah penggunaan COBIT (*Control Objectives For Information And Related Technology*) yang mempertemukan kebutuhan beragam manajemen dengan menjembatani celah antara risiko bisnis, kebutuhan kontrol, dan masalah-masalah teknis TI.

### 2.4 *Framework Cobit*

Konsep dasar kerangka kerja *COBIT* adalah bahwa penentuan 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.

*COBIT* di rancang terdiri dari 34 *high level control objectives* yang menggambarkan proses TI yang terdiri dari 4 domain yaitu: *Plan and Organise, Acquire and Implement, Deliver and Support dan Monitor and Evaluate*. Berikut kerangka kerja *COBIT* yang terdiri dari 34 proses TI yang terbagi ke dalam 4 domain pengelolaan, yaitu :

a. *Plan and Organise* (PO), mencakup masalah mengidentifikasikan cara terbaik TI untuk memberikan kontribusi yang maksimal terhadap pencapaian tujuan bisnis organisasi. Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI

dengan strategi organisasi. Domain PO terdiri dari 10 *control objectives*, yaitu :

PO1 – Define a strategic IT plan
PO2 – Define the information architechture
PO3 – Determine technological direction
PO4 – Define IT processes, organisation and relationships
PO5 – Manage the IT investment
PO6 – Communicate management ains and direction
PO7 – Manage IT human resource
PO8 – Manage quality
PO9 – Asses and manage IT risks
PO10 – Manage projects

b. *Acquire and Implement* (AI), domain ini menitikberatkan pada proses pemilihan, pengadaaan dan penerapan TI yang digunakan. Pelaksanaan strategi yang telah ditetapkan, harus disertai solusi-solusi TI yang sesuai dan solusi TI tersebut diadakan, diimplementasikan dan diintegrasikan ke dalam proses bisnis organisasi. Domain AI terdiri dari 7 *control objectives*, yaitu :

AI1 – Identify automated solutions
AI2 – Acquire and maintain application software
AI3 – Acquire and maintain technology infrastructure
AI4 – Enable operation and use
AI5 – Procure IT resources
AI6 – Manage changes
AI7 – Install and accredit solutions and changes

c. *Deliver and Support* (DS), domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan. Domain DS terdiri dari 13 control objectives, yaitu :

DS1 – Define and manage service levels.
DS2 – Manage third-party services.
DS3 – Manage performance and capacity.
DS4 – Ensure continuous service.
DS5 – Ensure systems security.
DS6 – Identify and allocate costs.
DS7 – Educate and train users.
DS8 – Manage service desk and incidents.
DS9 – Manage the configuration.
DS10 – Manage problems.
DS11 – Manage data.
DS12 – Manage the physical environment.
DS13 – Manage operations.

d. *Monitor and Evaluate* (ME), domain ini menitikberatkan pada proses pengawasan pengelolaan TI pada organisasi seluruh kendali-kendali yang diterapkan setiap proses TI harus diawasi dan dinilai kelayakannya secara berkala. Domain ini fokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan *internal* dan *eksternal*. Berikut proses-proses TI pada domain *monitoring and evaluate* :

ME1 – Monitor and evaluate IT performance.
ME2 – Monitor and evaluate internal control.
ME3 – Ensure regulatory compliance.
ME4 – Provide IT Governance. 17

Dengan melakukan kontrol terhadap ke 34 obyektif tersebut, organisasi dapat memperoleh keyakinan akan kelayakan tata kelola dan kontrol yang diperlukan untuk lingkungan TI. Untuk mendukung proses TI tersebut tersedia lagi sekitar 215 tujuan kontrol yang lebih detil untuk menjamin kelengkapan dan efektifitas implementasi.

**2.5 Model Maturity**

*COBIT* mempunyai model kematangan (*maturity models*) untuk mengontrol proses-proses TI dengan menggunakan metode penilaian (*scoring*) sehingga suatu organisasi dapat menilai proses-proses TI yang dimilikinya dari skala *non-existent* sampai dengan *optimised* (dari 0 sampai 5).

Tabel 1. Maturity Model COBIT 4.1

| | |
|---|---|
| *0 – Existent* | Perusahaan sama sekali tidak perduli terhadap pentingnya teknologi informasi untuk dikelola secara baik oleh manajemen |
| *1 Initial* | Perusahaan secara reaktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya. |
| *2 Repeatable* | Perusahaan telah memiliki pola yang berulangkali dilakukan dalam melakukan manajemen aktivitas terkait dengan tata kelola teknologi informasi, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidakkonsistenan. |
| *3 Define* | Perusahaan telah memiliki prosedur baku formal dan tertulis yang telah disosialkan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. |
| *4 Manage* | Perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan aplikasi teknologi informasi yang ada. |
| *5 Optimised* | Perusahaan telah mengimplementasikan tata kelola teknologi informasi yang mengacu pada "*best practice*" |


Dengan adanya *maturity level model*, maka organisasi dapat mengetahui posisi kematangannya saat ini, dan secara terus menerus serta berkesinambungan harus berusaha untuk meningkatkan levelnya sampai tingkat tertinggi agar aspek *governance* terhadap teknologi informasi dapat berjalan secara efektif. Salah satu cara menghitung tingkat kematangan adalah sebagai berikut :

1. Mengembangkan kuisioner dengan mengacu pada tingkat kematangan proses tata kelola TI berdasarkan *framework COBIT 4.1*.
2. Menghitung bobot semua proses tata kelola berdasarkan hasil kuisioner.
3. Menghitung tingkat kematangan berdasarkan proses-proses tata kelola terkait.
4. Menentukan nilai kontribusi tiap tingkat kematangan dengan cara membagi nilai tingkat kematangan dengan total tingkat kematangan.
5. Mengalikan nilai kontribusi dengan masing-masing tingkat kematangan.
6. Menjumlahkan semua nilai kontribusi yang didapat.
7. Total Nilai Kontribusi = Tingkat Kematangan Proses.

### 2.6 Memastikan Keamanan Sistem (DS5)

Kontrol atas proses TI untuk memastikan keamanan sistem :

1. **Tujuan DS 5**

   Menjaga integritas informasi dan infrastruktur pengolahan dan meminimalkan dampak kerentanan keamanan dan insiden.

2. **DS 5 berfokus pada**

   Mendefinisikan kebijakan keamanan IT, prosedur dan standar, dan pemantauan, mendeteksi, pelaporan dan menyelesaikan kerentanan keamanan dan insiden.

3. **DS 5 dicapai dengan**
   a. Memahami persyaratan keamanan, kerentanan dan ancaman.
   b. Mengelola identitas pengguna dan otorisasi dengan cara standar.
   c. Keamanan Pengujian secara teratur.
4. **Dan diukur dengan**
   a. Jumlah insiden merusak reputasi dengan masyarakat.
   b. Jumlah sistem di mana persyaratan keamanan tidak terpenuhi.
   c. Jumlah pelanggaran dalam pemisahan tugas.

### 2.7 *Maturity Model DS 5*

Pengelolaan proses untuk memastikan keamanan sistem yang memenuhi kebutuhan bisnis untuk TI mempertahankan integritas informasi dan infrastruktur pengolahan dan

meminimalkan dampak dari kerentanan keamanan dan insiden adalah :

a. 0 *Non-existent*
Organisasi tidak menyadari kebutuhan untuk keamanan IT .

b. 1 *Initial / Ad Hoc*
Organisasi mengakui kebutuhan untuk keamanan IT.

c. 2 *Repeatable but Intuitive*
Tanggung jawab dan akuntabilitas untuk keamanan IT ditugaskan ke koordinator keamanan IT, meskipun kewenangan manajemen koordinator terbatas.

d. 3 Proses Ditetapkan
Kesadaran keamanan ada dan dipromosikan oleh manajemen.

e. 4 Managed and Measurable
Tanggung jawab untuk keamanan IT ditugaskan jelas, dikelola dan ditegakkan.

f. 5 Optimised
Keamanan IT adalah tanggung jawab bersama bisnis dan manajemen IT dan terintegrasi dengan tujuan bisnis keamanan perusahaan.

### 2.8 Tahapan Analisis

a. Metode *Trianggulasi*

Metode *trianggulasi* merupakan teknik analisi dari penilaian pengelolaan proses memastikan keamanan sistem di Universitas Dian Nuswantoro Semarang.

b. Metode Analisis Data

Metode analisis data yang digunakan dalam penelitian ini meliputi:

*1. Editing*

Meneliti kelengkapan dalam pengisian kuisioner yang sudah diberikan kepada responden, bila ada jawaban yang tidak di jawab, peneliti menghubungi responden yang bersangkutan untuk di sempurnakan jawabannya agar kuisioner tersebut sah.

2. Perhitungan *Maturity Level*

Dalam Mengola kuisioner, peneliti akan melakukan analisis data menggunakan software *Microsoft excel*. Adapun langkah-langkah untuk perhitungan *Maturity Level* sebagai berikut :

a. Perhitungan tiap pertanyaan *Maturity Level* (ML).

$$\bar{x} = \frac{\sum fx}{\sum f}$$

$\bar{x}$ = pertanyaan, $fx$ = hasil bobot dari jawaban, $f$ = responden

b. Perhitungan tiap *Maturity Level* (ML).

$$= \frac{\bar{x}P_1 + \bar{x}P_2 + \bar{x}P_3 + \bar{x}P..n}{\sum(Pn)}$$

$\bar{x}P$ = hasil perhitungan tiap pertanyaan, $Pn$ = jumlah pertanyaan

c. Menentukan nilai normalisasii tiap tingkat kematangan dengan cara membagi rata-rata tiap *Maturity Level* dengan total tingkat *Meturity Level*.

d. Menghitung nilai kontribusi dengan cara mengalikan nilai normalisasi dengan masing-masing tingkat *Maturity*.

e. Menjumlahkan semua nilai kontribusi yang didapat.

f. Total Nilai Kontribusi = Tingkat Kematangan / *Maturuty Level Proses*.

## 3. HASIL PEMBAHASAN

### 3.1 Hasil Penelitian

#### 3.1.1 Studi Dokumen

Berdasarkan dokumen *Standart Operation Procedures* (SOP) yang mengacu pada *Audit*

*Guideline* dari UPT Dinustech dan PSI didapat hasil sebagai berikut :

1. Tidak ditemukan dokumen mengenai prosedur berkaitan dengan *managemen user account* (pengaturan identitas).
2. Tidak ditemukan kebijakan dan prosedural untuk mempersiapkan dan mempertahankan strategi teknologi dan rencana keamanan.
3. Tidak ditemukan kebijakan dan presedural mengenai manajemen kunci kriptografi.
4. Tidak ditemukan dokumen mengenai pelatihan berkaitan dengan keamanan sistem informasi.
5. Tidak ditemukan dokumentasi log insiden berkaitan dengan keamanan sistem.
6. Tidak ditemukan dokumentasi berkaitan dengan inventaris kebutuhan alat bantu.
7. Tidak ditemukan dokumentasi berkaitan dengan pengujian sistem.

### 3.1.2 Wawancara

Berdasarkan hasil wawancara telah disimpulkan hasilnya sebagai berikut :

1. Kepedulian untuk memastikan keamanan sistem sudah ada dan dilakukan di seluruh bagian UDINUS. Komunikasi terhadap pihak yang bertanggung jawab mengenai keamanan sistem tidak dilakukan secara rutin. Hanya bila ada insiden atau masalah berkaitan dengan keamanan sistem. Komunikasi yang dilakukan saat ini adalah jika unit mengalami insiden berkaitan dengan sistem unit tersebut menghubungi unit PSI atau dinustech via *telepone* untuk selanjutnya pihak PSI atau Dinustech akan menganalisis inseden tersebut kemudian melakukan tindakan sesuai dengan hasil analisis yang telah dilakukan.
2. Kebijakan dan prosedural ada dibeberapa aspek mengenai keamanan sistem, prosesnya dilakukan secara berulang karena keahlian individu, namun kebijakan dan procedural tersebut tidak terdokumentasi.
3. Alat bantu berkaitan dengan keamanan sistem yang ada di UDINUS hanya ada rooter.
4. Pengembangan kemampuan dan pelatihan staf hanya diberikan kepada unit terkait. Namun perencanaan pelatihan tidak ada dan tidak ada pelatihan secara formal yang terjadi.
5. Jaminan pihak ketiga dalam memberikan pelayanan untuk memastikan keamanan sistem tidak ada.
6. Tanggung jawab dan wewenang berkaitan dengan kemananan jaringan dan internet diberikan kepada UPT Dinustch, dan tanggung jawab mengenai kemananan software diberikan kepada PSI.
7. Pengukuran, pengujian berkaitan dengan pencapaian tujuan keamanan sistem tidak dilakukan secara periodik.

### 3.1.3 Kuisioner

Berikut ini adalah tabel hasil akhir perhitungan maturity level yang telah dihitung menggunakan software bantu *Microsoft Excel* :

Table 2. Perhitungan *Maturity Level*

| Maturity Level | Rata-rata | Normalisasi | Kontribusi |
|---|---|---|---|
| 0 | 0,35 | 0,21 | 0,00 |
| 1 | 0,41 | 0,24 | 0,24 |
| 2 | 0,31 | 0,18 | 0,36 |
| 3 | 0,32 | 0,19 | 0,56 |
| 4 | 0,16 | 0,09 | 0,36 |
| 5 | 0,18 | 0,10 | 0,51 |

| | | | |
|---|---|---|---|
| **Total** | **1,73** | **1,00** | **2,03** |

Keterangan :

* Nilai normalisasi adalah hasil dari nilai rata-rata tiap *maturity level* di bagi dengan jumlah nilai rata-rata.

* Nilai kontribusi adalah hasil dari nilai normalisasi di kali dengan *maturity level*.

* Total Nilai Kontribusi adalah Hasil dari perhitungan *Matuity Level*.

* Hasil keseluruhan perhitungan *maturity level* ada di bagian lampiran.

## 4. KESIMPULAN DAN SARAN

### 4.1 Kesimpulan

1. Berdasarkan uraian yang telah di jelaskan pada bab penjelasan dapat di simpulkan bahwa tingkat kematangan (*maturity level*) pengelolaan proses untuk memastikan keamanan sistem yang ada di Udinus menurut domain DS 5 Cobit 4.1 ada di level 2,03 yang termasuk dalam skala *repeatable but intuitive* atau tingkat kematangan 2.
2. Kepedulian mengenai keamanan sistem masih di nilai kurang dan komunikasi belum berlangsung secara konsisten dan tidak terdokumentasi.
3. Kebijakan,standart dan prosedur berkaikatan dengan keamanan sistem telah ada namun belum terdokumentasi.
4. Perencanaan mengenai pelatihan belum ada, pelatihan dilakukan hanya pada unit tertentu saja.
5. Tanggung jawab berkaitan dengan keamanan sistem diberikan pada unit PSI dan unit Dinustech.
6. Pendekatan alat bantu masih tergantung pada individu kunci.
7. Kegiatan pengukuran manajemen keamanan sistem belum dilakukan secara berkala dan tidak terdokumentasi.
8. Rekomendasi perbaikan di masing-masing detail proses berdasarkan domain DS 5 telah di berikan berdasarkan standart yang diberikan pada Cobit 4.1 pada level 3 (defined process).

### 4.2. Saran

Beberapa saran yang dapat disampaikan pada laporan tugas akhir ini adalah sebagai berikut:

1. Meningkatkan tingkat kematangan proses ke level yang lebih tinggi dengan mengacu pada standart proses yang ada pada *COBIT* Analisis terhadap tata kelola TI untuk selanjutnya dapat dilakukan pada semua proses yang ada pada 4 domain dalam *COBIT*, yaitu *Plan and Organise* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS) dan *Monitor and Evaluate* (ME), untuk mendapatkan hasil evaluasi yang lebih lengkap.
2. Analisis serta evaluasi tata kelola TI ini disarankan dapat dilakukan secara rutin setiap periode waktu tertentu serta menjadi bagian yang terintegrasi dengan *Audit Mutu Internal*, agar peningkatan kematangan proses pengelolaan TI dapat berkontribusi pada peningkatan kinerja organisasi secara keseluruhan.
3. Saran juga diberikan pada 6 atribut *maturity level* sebagai berikut:

Tabel 2. Atribut *Maturity Level*

| Atribut | Saran Jangka Pendek | Saran Jangka Panjang |
|---|---|---|
| **Kesadaran dan** | Melakukan komunikasi yang | Menerapkan teknis komunikasi secara |

| | | |
|---|---|---|
| **Komunikasi** | lebih formal dan terstruktur | terukur dan dikomunikasikan mengenai standarisasi proses berkaitan dengan keamanan sistem dan peralatan yang digunakan didalamnya |
| **Kebijakan, standart dan prosedur** | Melakukan koordinasi untuk menetapkan kebijakan dan prosedur berkaitan dengan keamanan sistem | - Melakukan dokumentasi untuk seluruh proses berkaitan dengan keaman sistem<br>- Kebijakan yang telah dirancang untuk dapat disetujui dan tetapkan, didokumentasikan, dan dikomunikasikan sebagai standar prosedur untuk dapat dilakukan di semua aspek beriaktan dengan keamanan sistem yang telah ditetapkan |
| **Perangkat bantu** | Medokumentasikan inventaris seluruh alat bantu yang ada berkaitan dengan keamanan sistem, apakah ada alat bantu yang rusak ataupun membutuhkan alat bantu yang lain | - Melakukan perencanaan berkaitan dengan alat bantu apa saja yang dibutuhkan untuk kedepannya<br>- Alat bantu dapat digunakan dalam bidang utama ke sistem utama yang kritis untuk dapat mengautomatisai pengelolaan proses monitoring dan control kegiatan kritis |
| **Keterampilan dan keahlian** | Melakukan pelatihan keterampilan berkaitan dengan keamanan sistem untuk seluruh unit yang lebih formal dan terstruktur | - Pelatihan untuk dapat diperbarui secara rutin untuk semua aspek berkaitan dengan keamanan sistem, dan mendorong untuk dapat melakukan sertivikasi pada unit yang bertanggung jawab penuh berkaitan dengan keamanan sistem |
| **Tanggung jawab dan wewenang** | Mengkomunikasikan kepada seluruh bagian bahwa tanggung jawab berkaitantan dengan keamanan sistem tidak sepenuhnya ada pada unit PSI dan Dinustech saja. Seluruh bagian harus bertanggung jawab kerbakaitan dengan keamanan sistem yang digunakan itu sendiri | Pemilik proses berkaitan dengan keamanan sistem ditugaskan untuk membuat keputusan dan tindakan, persetujuan dari tanggung jawab telah diberikan kebawah pada keseluruhan unit secara konsisten |
| **Penentuan tujuan dan pengukuran** | Melakukan perencanaan berkaitan dengan manajemen jadwal untuk dapat melakukan pengukuran, pengujian berkaitan dengan keamanan sistem untuk dapat dilakukan secara berkala | Melakukan pengukuran kinerja,efektivitas dan efisiensi sistem yang diselaraskan dengan tujuan bisnis |

## 5. DAFTAR PUSTAKA


[1] Budi Widjajanto, Nova Rijati, 2011. Analisis Maturity Level Tata Kelola Teknologi Informasi UDINUS Berdasarkan Domain DS dan ME COBIT 4.0, LP2M Universitas Dian Nuswantoro

[2] IT Governance Institute, 2000, IT Governance Executive Summary

[3] Weill, P. & Ross, 2004 J.W., "IT Governance, How Top Performers Manage IT Decision Rights for Superior Results", Harvard Business School Press, Boston

[4] IT Governance Institute, 2007, IT Governance Implementation Guide 2nd Edition

Guidelines 3nd Edition

[5] IT Governance Institute, 2005, COBIT 4.0 Control Objectives, Management Guidelines, Maturity Models , IT Governance Institute

[6] ISACA, 2006, Integrating COBIT into the IT Audit Process (Planning, Scope Development, Practisee) , IT Governance Institute

[7] ISACA, 2004, COBIT Student Book, IT Governance Institute

[8] Andrea Pederiva, 2003, The COBIT Maturity Model In Verndor Evaluation Case, Information System Control Journal, Vol 3, ISACA

[9] IT Governance Institute, 2000, Audit