# Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)

Rusydi Umar[a], Imam Riadi[b], Eko Handoyo[c]

[ac] Program Studi Teknik Informatika, Universitas Ahmad Dahlan , Yogyakarta
[b] Program Studi Sistem Informasi, Universitas Ahmad Dahlan , Yogyakarta

*Naskah Diterima : 18 Oktober 2018; Diterima Publikasi : 19 Februari 2019*

*DOI : 10.21456/vol9iss1pp47-54*

**Abstract**

Information technology is a very important part of a company or institution. The information system itself is expected to provide better benefits for companies or institutions. However, along with technological developments are often misused by some irresponsible parties that can lead to threats of the use of technology. Information system security is very important for institutions to maintain information optimally and safely. The existence of a security problem triggers a procedure to control access rights in an information system. A good information system is an information system that can be assessed at a security level, so that it can provide comfort for users. COBIT 5 as an information technology security control standard. Whereas to achieve the standard level of achievement CMMI is needed in information technology security. The combination of the two standards in the information system is able to provide a level of achievement of information technology. The results obtained from the maturity value are 4,458 which means the institutions are at the Managed and Measurable level. This level, institutions are increasingly made aware of technological developments. Institutions have implemented the quantification concept in each process, and are always monitored and controlled for performance. Information system security at this level is good, it's just that it still needs innovation and development to be ready, fast and right in handling security threats.

***Keywords*** **:** CMMI; COBIT 5; Security; Managed and Measurable; Information Systems; Information Technology.

**Abstrak**

Teknologi informasi adalah bagian yang sangat penting bagi perusahaan atau institusi. Sistem informasi sendiri di harapkan mampu memberikan keuntungan yang baik untuk institusi. Tetapi, seiring dengan perkembangan teknologi sering kali disalah gunakan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menimbulkan terjadinya ancaman dari penggunaan teknologi. Keamanan sistem informasi menjadi sangat penting dari subuah institusi untuk menjaga informasi secara optimal dan aman. Adanya masalah keamanan memicu prosedur untuk mengendalikan hak akses pada sebuah sistem informasi. Sistem informasi yang baik adalah sistem informasi yang dapat dinilai tingkat keamananya, sehingga mampu memberikan kenyamanan bagi pengguna. *COBIT 5* sebagai standar kontrol keamanan teknologi informasi. Sedangkan untuk mencapai standar level pencapaian diperlukan *CMMI* pada keamanan teknologi informasi. Kombinasi antara kedua standar tersebut dalam sistem informasi mampu memberikan nilai tingkat pencapaian teknologi informasi. Hasil yang didapat nilai *maturity level* 4,458 yang berarti institusi berada di level *Managed and Measurable*. Level ini, institusi semakin terbuaka terhadap perkembangan teknologi. Institusi sudah menerapkan konsep kuantifikasi dalam setiap proses, dan selalu dipantau serta dikontrol kinerjanya. Keamanan sistem informasi pada level ini sudah baik, hanya saja masih membutuhakan inovasi dan pengembangan untuk siap, cepat dan tepat dalam penanganan ancaman keamanan.

***Kata kunci*****:** *CMMI; COBIT* 5; Keamanan; *Managed and Measurable*; Sistem Informasi; Teknologi informasi.

## 1. Pendahuluan

Percepatan perkembangan teknologi informasi semakin pesat dalam berbagai bidang, teknlologi informasi diharuskan semakin peka terhadap keadaan pola hidup masyarakat. Dari harapan itu teknologi informasi meghadirkan kecepatan dan efisiansi bagi kehidupan manusia (Riadi *et al*., 2019). Teknologi informasi adalah bagian yang sangat penting bagi perusahaan atau institusi. Perusahaan atau institusi menempatkan teknologi informasi sebagi hal yang bisa mendukung pencapaian rencana strategis perusahaan untuk mencapai sasaran visi, misi dan tujuan perusahaan atau institusi tersebut (Riadi *et al*., 2018). Teknologi informasi akan mendapatkan hasil yang efektif apa bila menggunakan tata kelola yang

*) Penulis korespondensi: ekokurro17@gmail.com

baik dalam penggunaannya dan mampu di nilai dan evaluasi (Umar *et al*., 2017).

Sistem informasi adalah sebuah sistem yang berisi jaringan SPD (sistem pengolahan data), yang dilengkapi dengan kanal-kanal komunikasi yang digunakan dalam sistem organisasi data (Fathoni *et al*., 2016). Sistem informasi sendiri di harapkan mampu memberikan keuntungan yang baik untuk perusahaan (Otarkhani *et al*., 2017). Tetapi, seiring dengan perkembangan teknologi sering kali disalah gunakan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menimbulkan terjadinya ancaman dari penggunaan teknologi. Sistem informasi harus memberikan keamanan, privasi dan integritas data yang diolah kinerja sistem informasi juga menjadi bagian penting yang harus diperhatikan agar sistem informasi dapat dimanfaatkan secara optimal dan aman (Kurniawan dan Riadi, 2018a).

Penerapan sistem keamanan informasi bertujuan untuk mengatasi segala masalah dan kendala baik secara teknis maupun secara non-teknis yang dapat berpengaruh dalam kinerja sistem (Rosmiati *et al*, 2016). Keamanan informasi adalah suatu keharusan dimana keamanan di maksutkan menjaga sistem dari acaman (Kurniawan dan Riadi, 2018b). Keamanan di angap penting karena jika informasi tersebut dapat diakses oleh orang-orang yang tidak bertanggung jawab maka akurasi informasi akan meragukan sehingga tidak lagi dapat di percaya informasinya (Farida dan Rahajeng, 2014). Adanya masalah keamanan memicu prosedur untuk mengendalikan hak akses pada sebuah sistem informasi (Hermaduanti dan Riadi, 2016).

Kualitas data dan informasi yang baik memnimbulkan pengaruh yang penting dalam pelayanan, produk, operasional dan keputusan bisnis sehingga diharapkan kualitas data dan informasi dapat di nilai tingkat objektifitasnya (Karami, 2017).

Penelitian ini bertujuan untuk melakukan evaluasi terkait keamanan sistem informasi yang telah diimplementasikan pada sebuah institusi untuk mendapatkan nilai maturity level keamanan sistem informasi dari sebuah institusi.

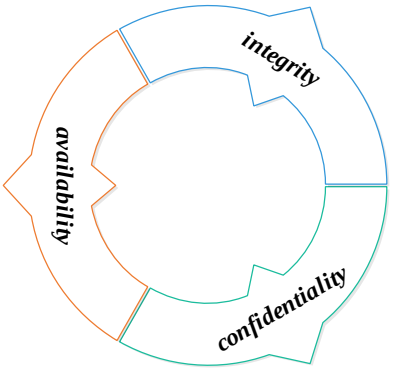
## 2. Kerangka Teori

### *2.1. Keamanan Sistem Informasi*

Keamanan sistem informasi merupakan salah satu topik dalam perkembangan teknologi informasi dan komunikasi di era digitalisasi (Umar *et al*., 2018). Untuk memecahkan masalah keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi, dan komunikasi ( Yunanri *et al*, 2016).

Keamanan informasi dapat dicapai dengan menerapkan seperangkat kontrol yang sesuai. Kontrol ini perlu ditetapkan, diterapkan, dimonitor, direview, ditingkatkan dimana yang perlu untuk memastikan bahwa tujuan bisnis dan keamanan yang spesfifik bagi organisasi dipenuhi (Raichel *et al*., 2005).

Penerapan keamanan informasi bertujuan untuk mengatasi masalah dan kendala baik secara teknis maupun non-teknis seperti faktor ketersediaan *(availability*), kerahasiaan *(confidentiality)*, dan kesatuan *(integrity)* sehingga dapat dinilai tingkat keamanan informasinya (Riadi, 2016). Keamanan informasi adalah perlindungan karakteristik informasi (*confidentiality*, *integrity*, dan *availability)* baik itu dalam memperoses informasi, menyimpan serta mengirimkanya dalam upaya untuk menjaga keberlangsungan dan memperluas kesempatan bisnis (Kurniawan *et al*., 2017). Seperti pada Gambar 1.



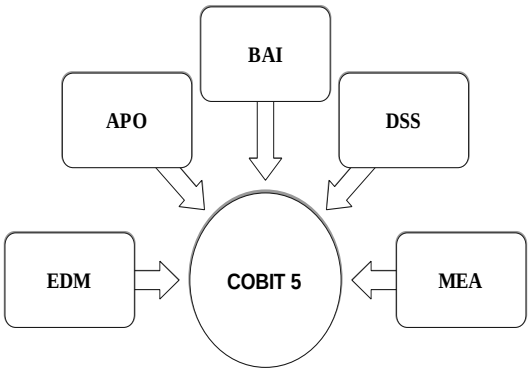

Gambar 1. Aspek keamanan informasi

Keamanan sistem informasi yang baik harus menerapkan standar *deming cycle of quality* (Hicham *et al*, 2012).Dalam area keamanan sistem informasi terdapat 4 poin *deming cycle of quality* yaitu:

- *Plan* (Merencanakan): keamanan berencana untuk pindah postur yang reaktif ke postur proaktif.
- *Develop* (Mengembangkan): serangkaian proses yang harus dilakukan dikembangkan mengikuti patokan keamanan.
- *Check* (Periksa): Keamanan dikontrol melalui tes audit dan penetrasi, dan metode yang paling umum.
- *Act* (Tindakan): Semua aktivitas kontrol dilakukan selama fase "Periksa" kemungkinan akan menyoroti sejumlah malfungsi yang perlu disediakan untuk tindakan korektif, tindakan pencegahan dan tindakan perbaikan.

### *2.2. Framework COBIT 5*

COBIT *(Control Objectives for Information and related Technology)* adalah suatu panduan standar praktek manajemen teknologi informasi dan sekumpulan dokumentasi best practices untuk tata kelola TI yang dapat membantu auditor, manajemen, dan pengguna untuk menjembatani pemisah *(gap)* antara risiko bisnis, kebutuhan pengendalian, dan permasalahan-permasalahan teknis (ISACA, 2011).



Gambar 2. Domain COBIT 5

Dalam COBIT 5 dibagi dalam 5 domain utama yaitu, Seperti pada Gambar 2.

1. EDM adalah proses evaluasi, kelangsungan, dan monitoring.
2. APO adalah proses mensejajarkan, merencanakan dan mengtur.
3. BAI adalah proses membangun, mendapatkan, dan menerapkan.
4. DSS adalah proses mengirim, melayani dan dukungan.
5. MEA adalah proses memantau, evaluasi, dan menilai.

Domain yang berhubungan dengan keamanan teknologi informasi adalah domain DSS. Domain DSS *(Deliver, Service and Support)* merupakan sebuah domain yang digunakan dalam analisa teknologi informasi dalam area menajemen yang di dalamnya terdapat beberapa proses. (Firmansyah, 2015). Dalam dosmain DSS terdapat Sub-doman DSS05 dimana sub domain ini merupakan prosedur yang lebih intensif terhadap kemanan informasi. Sub domain tersebut adalah manage security services dimana sub domain ini melaksanakan beberapa akatifitas atau pernyataan sebanyak 49 pernyatan yang di kelompokan dalam 7 proses sebagai berikut:

1. *Protect against malware* (DSS05.01) melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada diseluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak.
2. *Manage network and connectivity security* (DSS05.02) digunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas.
3. *Manage endpoint security* (DSS05.03) memberikan kepastian terhadap titik akhir keluaran (*end poin*) (missal: Laptop, desktop, dan server) dijamin tingkat yang sama atau lebih besar dari persyaratan keamanan yang disetujui.
4. *Manage user identity and logical access* (DSS05.04) memberikan kepastian terhadap semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis. Mereka dan berkoordinasi dengan devisi bisnis yang mengelola hak akses.
5. *Manage physical access to IT assets* (DSS05.05) menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut akses ke bangunan fisik. Bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses ke bangunan, bangunan dan area harus dibenarkan, disahkan, dicatat dan dipantau.
6. *Manage sensitive documents and output devices* (DSS05.06) menetapkan pengamanan fisik. Dalam segi dokumen yang berhubungan dengan istansi. Sehingga semua keluaran dokumen terstandar dalam keamanan.
7. *Monitor the infrastructure for security-related events* (DSS05.07) menggunakan alat deteksi intrusi, untuk memantau infrastruktur untuk hak akses yang tidak sah dan memastikan setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian.

### *2.3. Capability Maturity Model Integration (CMMI)*

*Capability Maturity Model Integration* (CMMI) adalah sesuatu model pendekatan untuk menilaian skala kemampuan dan kematangan sebuah organisai perangkat lunak. Sejarah CMMI pada awal mula dikenal sebagai *Capability Maturity Model* (CMM) yang dibangun dan di kembangkan oleh *Software Enginnering Institute di Pittsburgh* pada tahun 1987 (Konttinen, 2016).

CMMI memiliki aliur proses penilaian secara berjenjang. Penilaian tersebut didasarkan kuisioner dan dikembangkan secara khusus untuk mendapatkan perangkat lunak yang dapat mendukung peningkatan proses. CMMI adalah sebuah metode kematangan (*maturity model*) yang dapat digunakan untuk meningkatkan proses (*process improvement*) dalam institusi. Tujuan dari digunakannya CMMI di dalam institusi adalah untuk meningkatkan proses pengembangan dan perbaikan produk piranti perangkat lunak institusi tersebut (Syafitri, 2016).

### *2.4. Kerangka Penelitian*

Kerangka penelitian yang dilaksanakan seperti dilakukan langkah-langkah sebagai berikut:

1. Observasi adalah proses analisis terkait keamana sistem infoemasi yang sedang berjalan.
2. Pemetaan DSS05 berdasarkan feamework cobit adalah memetakan setiap aktivitas DSS05 pada framework COBIT 5.
3. Penyususnan kuesioner dengan aktivitas DSS05 pada framework COBIT 5 dengan megkombinasikan kriteria pada capability level CMMI.
4. Menghitung tingkat maturity level keamanan sistem informasi yang senag berjalan.
5. Menganalisis maturity level gap dengan menghitung maturity saat ini dengan target.

6. Menyusun rekomendasi tata kelola keamanan sistem informasi.

## 3. Metode

### *3.1. Metode Pengumpulan Data*

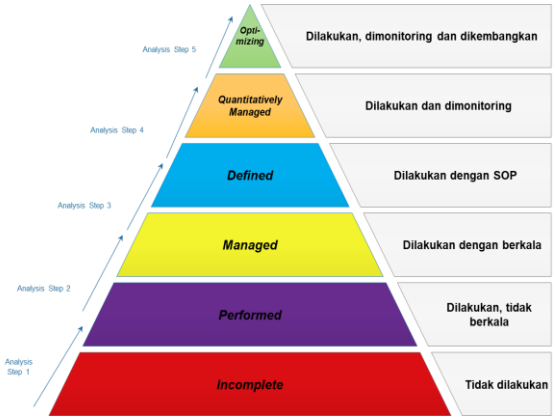
Penelitian ini, menggunakan metode teknik pengumpulan data yang digunakan dalam penelitian seperti pada Gambar 3, yaitu :

1. Studi Literatur pengambilan data dengan melakukan pencarian terhadap berbagai sumber tertulis, baik berupa buku-buku, arsip, majalah, artikel, dan jurnal, atau dokumen-dokumen yang relevan.
2. Metode Observasi pengamatan langsung menggunakan alat indera atau alat bantu untuk penginderaan suatu subjek atau objek, yaitu pelaksanaan kegiatan dan administrasi sistem informasi pada BISKOM UAD Yogyakarta.
3. Metode Wawancara yaitu mendapatkan informasi dengan cara bertanya langsung kepada responden yaitu karyawan sistem informasi di perusahan atau institusi sehingga data yang diperoleh bersifat objektif dan data dipertanggungjawabkan.
4. Metode kuesioner melakukan pembuatan kuesioner berdasarkan standar pada DSS05 Framwork COBIT 5 dengan megkombinasiakan dengan *capability level* pada standar CMMI sehingga didapatkan bentuk kuesioner yang mampu menjawab kebutuhan pada keamanan sistem informasi yang ada di instansi tersebut.

### *3.2. Metode CMMI*

Menurut (CMMI Product Team, 2010) CMMI memiliki *Capability Level* atau tingkat kemampuan. *Capability Level* berlaku untuk pencapaian kinerja institusi dan peningkatan proses di area praktik individual. Dalam area praktik tersebut dikonvensikan ke dalam kelompok praktik yang diberi label Level 0 hingga Level 5 yang menyediakan jalur evolusi untuk peningkatan kinerja. Setiap level dibangun di level sebelumnya dengan menambahkan fungsi atau kekakuan baru yang menghasilkan peningkatan kemampuan. *Capability Level* memiliki 6 level untuk setiap proses inti seperti pada Gambar 4 dan di jelaskan sebagai berikut:

- Level 0: Tidak lengkap (*Incomplete*): Pendekatan tidak lengkap untuk memenuhi maksud dari area praktek.
- Level 1: Dilakukan (*Performed*): Pendekatan awal untuk memenuhi maksud dari area praktik.
- Level 2: Dikelola (*Managed*): Berlaku praktik level 1. Praktik yang sederhana, tetapi lengkap yang membahas maksud penuh dari area praktik.
- Level 3: Ditetapkan (*Defined*): Dibangun pada praktik level 2. Menggunakan standar organisasi dan menyesuaikan untuk mengatasi karakteristik proyek dan pekerjaan. Berfokus pada pencapaian tujuan proyek dan kinerja organisasi.
- Level 4: Dikelola secara kuantitatif (*Quantitatively Managed*): Dibangun pada praktik level 3. Menggunakan teknik kuantitatif statistik dan lainnya untuk memahami variasi kinerja dan mendeteksi, memperbaiki, atau memprediksi area fokus untuk mencapai kualitas dan tujuan kinerja proses.
- Level 5: Mengoptimalkan (*Optimizing*): Dibangun pada praktik level 4. Menggunakan teknik kuantitatif statistik dan lainnya untuk mengoptimalkan kinerja dan peningkatan untuk mencapai kualitas dan tujuan kinerja proses.

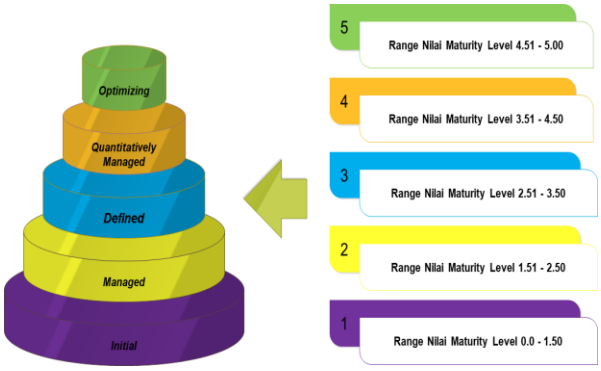



Gambar 4. *Capability Level*

Menurut (CMMI Product Team, 2010) Model CMMI menempatkan insitusi dalam 5 Maturity Level atau tinggkat kematanggan dalam CMMI seperti Gambar 5 dan di jelakan sebagai berikut:

- Level 1: *Initial* atau proses Awal. Kondisi ini institusi yang berapa pada level ini adalah institusi yang belum menjalankan CMMI.
- Level 2: *Managed* atau Dikelola. Institusi memiliki beberapa proses yang sering digunakan dalam setiap proyek pengembangan, akan tetapi tidak terdapat keseragaman secara menyeluruh.
- Level 3: *Defined* atau Ditetapkan. Institusi telah menjalankan proses yang sudah didefinisikan dan semua tim paham bagaimana proses seharusnya berjalan.
- Level 4: *Quantitatively Managed* atau Dikelola secara kuantitatif. Institusi semakin tersteruktur dan terbuka dengan sistem yang ada. Mereka mulai menerapkan konsep kuantifikasi pada setiap proses, dan selalu dimonitoring serta dikontrol dalam setiap proses kerjanya.
- Level 5: Optimizing atau Mengoptimalkan. Level ini adalah level puncak dalam model CMMI. Pada Maturity Level 5 ini suatu institusi sudah mencapai seluruh spesifik dan generik *goals* yang ada di Level 2, 3, 4, dan 5. Fokus kepada peningkatan proses secara berkesinambungan melalui inovasi teknologi dan optimasi proses

senantiasa dimonitoring dan dianalisis. Sehingga mampu memberikan sistem yang optimal.




Gambar 5. *Maturity Level*

*3.3. Validasi DSS05 dengan Aspek Keamanan*

Validasi ini merupakan analisis DSS05 pada *framework* COBIT 5 dengan parameter keamanan yaitu Kerahasiaan (*Confidentiality*), Intergritas (*Integrity*), dan Ketersediaan (*Availability*). Seperti pada Tabel 1.

Tabel 1. Validasi DSS05 dengan aspek keamanan

| No | Kode DSS | C | I | A |
|---|---|---|---|---|
| 1 | DSS05.03.1 | | √ | |
| 2 | DSS05.03.2 | | √ | √ |
| 3 | DSS05.03.3 | √ | | √ |
| 4 | DSS05.03.4 | √ | √ | |
| 5 | DSS05.03.5 | | √ | |
| 6 | DSS05.03.6 | | √ | √ |
| 7 | DSS05.03.7 | | √ | |
| 8 | DSS05.03.8 | | √ | |
| 9 | DSS05.03.9 | | √ | |

## 4. Hasil dan Pembahasan

*4.1. Metode Pengumpulan Data*

Penelitian kami menggunakan metode kuesioner dimana disesuaikan dengan standar *framework* COBIT 5 dan diadopsi dengan metode CMMI. Ukuran dalam model ini meliputi ukuran ordinal dan ukuran nominal. Ukuran ordinal adalah angka yang diberikan, angka tersebut mengandung arti tingkatan. Nomina angka l digunakan untuk mengurutkan objek dari tingkatan terendah sampai tertinggi.

Dimana dalam kuesioner ini terdapat 6 penilaian seperti pada Tabel 1.

Tabel 1. Penelitian proses TI

| Nilai | Kegitan |
|---|---|
| 0 | Tidak di lakukan |
| 1 | Dilakukan, tidak berkala |
| 2 | Dilakukan dengan berkala |
| 3 | Dilakukan dengan SOP |
| 4 | Dilakukan dan dimonitoring |
| 5 | Dilakukan, dimonitoring dan dikembangkan |

Dari penilaian kuesioner pada table 1, di kombinasikan dengan standar COBIT 5, standar yang digunakan adalah sub-domain DSS05 dimana sub-domain ini kusus untuk melakukan penilaian terkait kemanan system imformasi. Dalam standar ini terdapat 49 pertanyaan yang berhubungan dengan standar keamanan COBIT 5.

Pemilihan sampel responden menggunakan teknik *purposive sampling*, yaitu pemilihan sampel responden yang ditentukan oleh peneliti dengan alasan bahwa identifikasi sampel responden dilakukan dengan mengacu pada kompetensi personal yang berinteraksi langsung dengan tata kelola TI (Rahayu dan Sensuse, 2017).

Dalam penelitian ini kami melakukan wawancara terhadap stakeholder yang bersangkutan dengan devisi X pada instansi ABC, dimana dari wawancara itu di dapatkan 2 responden yang bersangkutan langsung dengan bidang keamanan sistem informasi yang ada dalam institusi tersebut.

*4.2. Pengolahan Data dengan CMMI*

Analisis dan interpretasi data wawancara dan kuesioner terhadap pengelola sistem informasi dapat digunakan sebagai temuan penelitian, berdasarkan perhitungan tingkat kematangan atau *maturity level*, dapat dilihat *gap* dan dapat menentukan nilai yang diharapkan yang akan dibuat.

Mengidentifikasi instansi ABC telah memenuhi standard keamanan informasi di perlukan kriteria seperti pada Tabel 2.

Tabel 2. Nilai kriteria *maturity level*

| Kriteria | Keterangan |
|---|---|
| 0 – 0.50 | *Initial* |
| 0.51 – 1.50 | *Ad Hoc* |
| 1.51 – 2.50 | *Repeatable But Invinitve* |
| 2.51 – 3.50 | *Define Process* |
| 3.51 – 4.50 | *Managed and Measurable* |
| 4.51 – 5.00 | *Optimized* |

Hasil dari kuesioner yang telah di berikan terhadap responden dan telah di isi oleh responden di dapatkan hasil seperti pada Tabel 3. Karena keterbatasan halaman data tidak ditampilkan keseluruahan.

Tabel 3. Nilai hasil kuesioner

| DSS05 | R 1 | R 2 |
|---|---|---|
| DSS05.01.1 | 5 | 5 |
| DSS05.01.2 | 5 | 5 |
| DSS05.01.3 | 5 | 5 |
| DSS05.01.4 | 5 | 5 |
| DSS05.01.5 | 5 | 5 |
| DSS05.01.6 | 5 | 5 |
| DSS05.03.8 | 5 | 4 |
| DSS05.03.9 | 0 | 0 |
| DSS05.04.1 | 5 | 5 |
| DSS05.04.2 | 5 | 5 |
| DSS05.04.3 | 5 | 5 |
| DSS05.04.4 | 5 | 5 |

Selanjutnya merelasikan antara nilai tingkatan dan nilai absolut yang dilakukan dengan perhitungan dalam bentuk indeks menggunakan formula matematika sebagai berikut (Prasetyo & Mariana, 2011):

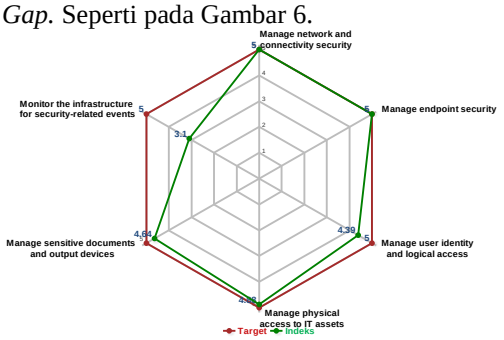
$$Indeks = \frac{\sum Jawaban\ Pertanyaan\ Terbanyak}{\sum\ Pertanyaan\ Kuesioner} \quad (1)$$

Dari perhitunggan indeks diterhadap data kuesioner didapatkan hasil seperti pada Tabel 4. Data indeks merupakan *maturity level existing*. *Maturity level existing* adalah nilai *maturity level* saat ini, nilai ini akan di gunakan untuk mendapatkan *gap maturity level.*

Tabel 4. Hasil Indeks

| DSS05 | Jumlah Jawaban | Jumlah Pertanyaan | Indeks/ *Maturity level existing* |
|---|---|---|---|
| 1 | 60 | 12 | 5 |
| 2 | 90 | 18 | 5 |
| 3 | 79 | 18 | 4,388 |
| 4 | 78 | 16 | 4,875 |
| 5 | 65 | 14 | 4,642 |
| 6 | 31 | 10 | 3,1 |
| 7 | 42 | 10 | 4,2 |

*Maturity level existing* akan dibandingkan dengan *Maturity* target sehingga akan di dapatkan *Maturity Gap.* Seperti pada Gambar 6.




Gambar 6: *Gap Maturity Level*

G*ap Maturity Level* dapat dilakukan analisis sehingga bisa di tetapkan *Maturity Level* setiap sub-domain. Seperti pada Tabel 5.

Tabel 5. *Maturity Level sub-domain DSS05*

| No | Sub-domain DSS05 | *Maturity Level* |
|---|---|---|
| 1 | DSS05.01 | *Optimized* |
| 2 | DSS05.02 | *Optimized* |
| 3 | DSS05.03 | *Managed and Measurable* |
| 4 | DSS05.04 | *Optimized* |
| 5 | DSS05.05 | *Optimized* |
| 6 | DSS05.06 | *Define Process* |
| 7 | DSS05.01 | *Managed and Measurable* |

Tingkat keamanan dapat ditetapkan dengan tingkatan *maturity level* keseluruhan aktivitas yang dilakukan dalam DSS05 dengan persamana .

$$Maturity\ Level\ DSS05 = \frac{\sum Maturity\ Level}{banyak\ proses} \quad (2)$$

$$MLDSS5 = \frac{i(DSS05.01) + i(DSS05.02) + i(DSS05.03) + i(DSS05.04) + i(DSS05.05) + i(DSS05.06) + i(DSS05.07)}{bp}$$

$$MLDSS05 = \frac{5 + 5 + 4{,}388 + 4{,}875 + 4{,}642 + 3{,}1 + 4{,}2}{7}$$

$$Maturity\ Level\ DSS05 = 4{,}458$$

Nilai ketercapaian 4,458 berarti *maturity level* pada *Managed and Measurable*. Level ini berarti institusi semakin terbuaka terhadap perkembangan teknologi. Institusi sudah menerapkan konsep kuantifikasi dalam setiap proses, dan selalu dipantau serta dikontrol kinerjanya.

*4.3. Rekomendasi*

Berdasarkan analisis *Gap* yang di dapat dari hasil level target yang ingin dicapai dan level yang tercapai pada DSS05, seperti pada Gambar 6. Rekomendasi yang dapat berikan untuk meningkatkan kualitas keamanan sistem informasi di instansi tersebut:

1. *Protect against malware* (DSS05.01) berada dalam level *Optimized* pada instansi sudah mampu melakukan prosedur dengan baik dan mampu melakukan penembangan terkait malware.
2. *Manage network and connectivity security* (DSS05.02) berada dalam level *Optimized* instansi sudah mampu melakukan prosedur dengan baik dan mampu melakukan penembangan terkait keamanan konktifitas. Menetapkan sistem yang digunakan untuk mengevaluasi ancaman – ancaman yang akan timbul, didokumentasikan dan dimonitoring.
3. *Manage endpoint security* (DSS05.03) berada dalam level *Managed and Measurable* instansi sudah mampu melakukan prosedur dengan baik, hanya saja instansi harus melakukan evaluasi yang dilakukan rutin, minimal setiap satu bulan sekali terhadap sistem informasi yang dikhawatirkan dapat timbul potensi ancaman baru.
4. *Manage user identity and logical access* (DSS05.04) berada dalam level *Optimized* instansi sudah mampu melakukan prosedur dengan baik dan mampu melakukan penembangan terkait hak akses yang dimiliki setiap pengguna.
5. *Manage physical access to IT assets* (DSS05.05) berada dalam level *Optimized* instansi sudah mampu melakukan prosedur dengan baik dan mampu melakukan pengembangan terkait keamanan fisik.
6. *Manage sensitive documents and output devices* (DSS05.06) berada dalam level *Define Process* instansi sudah mengimplementasikan keamanan pengamanan fisik, praktik akuntansi dalam segi

dokumen yang berhubungan dengan istansi. Sehingga semua keluaran dokumen terstandar dalam keamanan. Hanya saja diharapakan nantinya mampu mekukan dokumentasi dan melakukan evaluasi terhadap ancaman yang ada.

7. *Monitor the infrastructure for security-related events (DSS05.07)* berada dalam level *Managed and Measurable* instansi sudah mampu melakukan prosedur dengan baik menggunakan alat deteksi intrusi, untuk memantau infrastruktur untuk hak akses yang tidak sah dan memastikan setiap peristiwa diintegrasikan.

Penelitian yang telah dilakukan menempatkan instansi pada level *Managed and Measurable* sehingga tetersesuain rancana penelitian terah terpenuhi. Kombinasi antara *Framework* COBIT 5 dengan metode CMMI mampu memberikan hasil yang baik dalam evaluasi keamanan sehingga bisa di acuan baru dalam penilitian evaluasi keamanan.

## 5. Kesimpulan

Hasil yang dildaptkan instansi ABC tersebut di mendapatkan nilai Maturity Level 4,458 atau pada level *Managed and Measurable*. institusi semakin terbuaka terhadap perkembangan teknologi. Institusi sudah menerapkan konsep kuantifikasi dalam setiap proses, dan selalu dipantau serta dikontrol kinerjanya. Keamanan sistem informasi pada level ini sudah baik, hanya masih membutuhakan inovasi dan pengembangan untuk siap, cepat dan tepat dalam penanganan ancaman keamanan. Instansi harus aktif membaca perkembangan teknologi keamanan dan segala bentuk ancamannya. COBIT 5 memberikan standar yang baik dalam kontrol keamanan teknologi informasi dan CMMI memberikan standar level pencapain yang baik dalam penilaian keamanan teknologi informasi. Kombinasi *framework* COBIT 5 dan CMMI mampu memberikan solusi penilaian tingkat keamanan teknologi dengan optimal. Rekomendasi penelitian selanjutnya adalah melakukan kombinasi COBIT 5 dengan metode lain sehingga mampu dijadikan perbandingan.

## Ucapan Terima Kasih

Kami ucapan terima sampaikan kepada selruh staff dan pimpinan Biro Sistem Informasi dan Komunikasi (BISKOM) Universitas Ahmad Dahlan (UAD) yang sudah mendukung penelitian ini.

## Daftar Pustaka

Farida, S. I., Rahajeng, E., 2014. Usulan model tata kelola teknologi informasi pada domain monitor , evaluate and assess dengan metode framework COBIT 5.. Studi Informatika: Jurnal Sistem Informasi, (Vol. 7).

Fathoni, L. F., Firdausy, K., Yudhana, A., 2016. Application information system based health services android. Jurnal Ilmu Teknik Elektro Komputer Dan Informatika (JITEKI), 2(1), 39–48.

Firmansyah, D., 2015. Pengukuran kapabilitas pengelolaan sistem informasi sub domain deliver , service , support 01 menggunakan framework Cobit 5 Studi Kasus : Politeknik Komputer Niaga LPKIA Bandung. In *Konferensi Nasional Sistem & Informatika 2015 (pp. 689–695).*

Hermaduanti, N., Riadi, I., 2016. Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN. Journal of Theoretical and Applied Information Technology, 93(2), 287–296.

Hicham, E., Boulafdour, B., Makoudi, M., Regragui, B., 2012. Information security, 4TH wave. Journal of Theoretical and Applied Information Technology, 43(1), 1–7.

ISACA., 2011. *A* Business Framework for the Governance and Management of Enterprise IT.

Karami, A. F., 2017. Manajemen kualitas data dan informasi berbantuan sistem informasi untuk meningkatkan kinerja operasional pabrik pengolahan kelapa sawit. JSINBIS (Jurnal Sistem Informasi Bisnis), 01, 88–95.

Konttinen, V., 2016. Towards Disciplined Software Development.

Kurniawan, A. D. E., Riadi, I., Luthfi, A., 2017. Forensic Analysis and Prevent of Cross Site Scripting in Single Victim Attack Using Open Web Application Security Project (OWASP) framework. Journal of Theoretical and Applied Information Technology, 95(6), 1363–1371.

Kurniawan, E., Riadi, I., 2018a. Analisis tingkat keamanan sistem informasi akademik berdasarkan standar ISO 27002 : 2013 menggunakan SSE-CMM. Jurnal Ilmia Penelitian Teknologi Dan Penerapan Sistem Informasi, 2(1), 12–23.

Kurniawan, E., Riadi, I., 2018b. *Security level analysis of academic information systems based on standard ISO 27002:2003 using SSE-CMM*. International Journal of Computer Science and Information Security (IJCSIS), 16(1), 139–147.

Otarkhani, A., Shokouhyar, S., Pour, S., 2017. Analyzing the impact of governance of enterprise it on hospital performance. International Journal of Healthcare Information Systems and Informatics, 12(3), 1–20.

Prasetyo, A., Mariana, N., 2011. Analisis tata kelola teknologi informasi (IT governance) pada bidang akademik dengan cobit framework studi kasus pada Universitas Stikubank Semarang. Jurnal Teknologi Informasi DINAMIK, 16(2), 139–149.

Rahayu, P., Sensuse, D. I., 2017. Penilaian implementasi e-government di PUSTEKOM Kemendikbud berbasis metode PEGI. Jurnal Sistem Informasi Bisnis, 02, 139–145.

Raichel, L., Brannon, K., Fumy, W., Soete, M. De, Humphreys, E. J., Naemura, K., Ohlin, M. 2005. INTERNATIONAL STANDARD ISO / IEC.

Riadi, Imam Sunardi Firdonsyah, A. F., 2019. Forensic investigation technique on android's blackberry messenger using NIST framework. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 6, 6(4), 198–205.

Riadi, I., 2016. Analisis keamanan informasi berdasarkan kebutuhan teknikal dan operasional mengkombinasikan standar ISO 27001 : 2005 dengan maturity level (studi kasus kantor biro teknologi informasi PT . XYZ). *Seminar Nasional Teknologi Informasi Dan Multimedia 2016*, *6*(6), 6–7.

Riadi, I., Yudhana, A., Caesar, M., Putra, F., 2018. Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method, Scientific Journal of Informatics 5(2), 235–247.

Rosmiati, Riadi, I., Prayudi, Y., 2016. A Maturity level framework for measurement of information security performance. International Journal of Computer Applications, 141(8), 975–8887.

Syafitri, P. D., 2016. Penilaian kualitas pengembangan sistem informasi pada perusahaan distributor. Jurnal Sistem Informasi Bisnis, 10(01), 15–27.

Umar, R., Riadi, I., Handoyo, E., 2017. Analisis Tata kelola teknologi informasi menggunakan framework COBIT 5 Pada Domain Delivery, Service, And Support (DSS). In *Seminar Nasional Teknologi Informasi dan Komunikasi - SEMANTIKOM 2017* (pp. 41–48).

Umar, R., Riadi, I., Zamroni, G. M., 2018. Mobile Forensic tools evaluation for digital crime investigation. International Journal on Advanced Science, Engineering and Information Technology (IJASEIT), 8(3), 949. https://doi.org/10.18517/ijaseit.8.3.3591

Yunanri, W., Riadi, I., Yudhana, A., 2016. Analisis keamanan webserver menggunakan metode penetrasi testing. In *Annual Research Seminar* (Vol. 2, pp. 300–304).