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

By Eko Handoyo

WORD COUNT 4483 TIME SUBMITTED 18-OCT-2018 04:05PM
PAPER ID 41136028

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

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

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

Naskah Diterima : ; Diterima Publikasi :

DOI : 10.21456/vol7iss1pp

Abstract

Information technology is a very important part of a company or institution. The information system itself is expected to provide good benefits for companies or institutions. However, along with technological developments are often misused by some irresponsible parties that can lead to threats from the use of technology. Information system security is very important from 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 as 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. From this research, get institutions at the Managed and Measured level. At this level, institutions are increasingly lured into technological development. The institution has implemented the quantification concept in each process, and its performance is always monitored and controlled. Information system security at this level is good, it's just that it still needs innovation and development to be ready, fast and precise 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 perusahaan atau 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 keamanannya, 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. Dari Penelitian ini di dapatkan 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 membutuhkan inovasi dan pengembangan untuk siap, cepat dan tepat dalam penanganan ancaman keamanan.

Keywords : *CMMI; COBIT* 5; Keamanan; *Managed and Measurable*; Sistem Informasi; Tekniligi informasi;

*) Penulis korespondensi: ekokurro17@gmail.com

1. Pendahuluan

Percepatan perkembangan teknologi informasi semakin pesat dalam berbagai bidang, teknlologi informasi diharuskan semakin peka terhadap keadaan pola hidup masyarakat. Teknologi informasi di harapkan mampu memberikan kemudahan dalam kehidupan manusia. Dari harapan itu teknologi informasi meghadirkan kecepatan dan efisiansi bagi kehidupan manusia. 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. Teknologi informasi akan mendapatkan hasil yang efektif apa bila menggunakan tata kelola yang baik dalam penggunaannya dan mampu di nilai dan evaluasi. (Kurniawan, Riadi, & Handoyo, 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. . 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 & 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 & Riadi, 2018b). Keamanan di anggap 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 & Rahajeng, 2014). Adanya masalah keamanan memicu prosedur untuk mengendalikan hak akses pada sebuah sistem informasi (Hermaduanti & Riadi, 2016).

Sebuah perusahaan dan institusi harus mampu memberikan kenyamanan dan keamanan dalam memberikan layanan sistem informasi. 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). Dimana kualitas data dan informasi yang baik bermakna data tersebut tepat kebutuhannya untuk digunakan penggunanya dan dapat memberikan akurasi sesuai dengan apa yang di harapkan penggunanya.

Sebuah pengunanan teknologi informasi yang baik adalah teknologi informasi itu dapat diukur dan dinilai tingkat pencapaian teknologi informasi tersebut.sehingga teknologi itu bisa selalu berinovasi untuk menyesuaikan perkembangan zaman. Untuk mengetahui tingkat perkembangan teknologi tesebut di perlukan sebuah audit sistem teknologi informasi tersebut.

Penelitian ini bertujuan untuk melakukan evaluasi terkait manajemen keamanan sistem informasi yang telah diimplementasikan devisi X pada sebuah institusi ABC. Penelitian ini bertujuan untuk mendapatkan nilai tingkat keamanan sistem informasi dari sebuah institusi, sehingga bisa di lakukan rekomendasi dan inovasi untuk keamanan sistem informasi di institusi tesebut. Sehingga institusi dapat memberikan keamanan dan kenyamanan bagi pengunan sistem informasi tersebut.

2. Kerangka Teori

2.1 Keamanan sitem informasi

Keamanan sistem informasi merupakan salah satu topik dalam perkembangan teknologi informasi dan komunikasi di era digitalisasi. Institusi sangat penting untuk melindungi aset informasi dengan mengikuti pendekatan yang konprehensif dan terstruktur untuk memberikan perlindungan dari ancaman keamanan yang mungkin terjadi. 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 control yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi serta fungsi perangakat lunak dan perangkat keras. 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). Availability focus pada penggunaan sumber daya dalam kerangka waktu yang diinginkan. *Confidentiality* merujuk pada data tidak dapat diakses atau ditampilkan terhadap orang yang tidak berhak. I*ntegrity* fokus pada

perlindungan melawan perubahan yang tidak diinginkan. Tinda kan teknis dan administrasi keamanan dibutuhkan untuk mencapai tiga karakteristik ini. Dapat disimpulkan bahwa 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. Seperti pada Gambar 1.

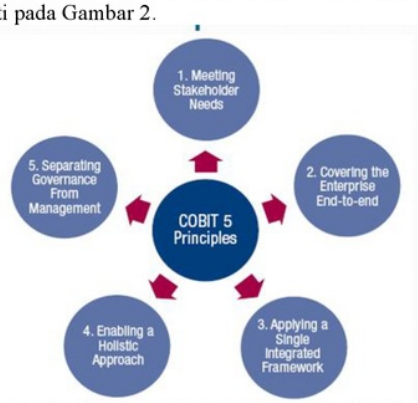
Gambar 1 Aspek keamanan informasi (*opentext.com*)

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): Keamanan adalah 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 kumpulan 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). COBIT adalah kombinasi dari prinsip-prinsip yang telah distruktur yang dilengkapi dengan balance scorecard dan dapat digunakan sebagai acuan model (seperti COSO) dan disejajarkan dengan standar industri, seperti ITIL, CMM, BS779, ISO 9000. Seperti pada Gambar 2.



Gambar 2 Prinsip COBIT 5 (ISACA, 2011)

Dalam COBIT 5 dibagi dalam 5 domain utama yaitu:

1. Evaluasi, Langsung, dan Monitor (EDM).
2. Sejajarkan, Rencanakan dan Atur (APO).
3. Bangun, Dapatkan, dan Terapkan (BAI).
4. Kirim, Layanan dan Dukungan (DSS).
5. Pantau, Evaluasi, dan Nilai (MEA).

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. Domain DSS berhubungan dengan pengiriman actual sistem dan dukungan layanan yang dibutuhkan sistem, yang meliputi pelayanan, pengelolaan keamanan dan kelangsungan, dukungan layanan bagi pengguna, dan manajemen data dan fasilitas operasional sehingga lebih terkusus dalam sekup domain yang memberikan layanan yang baik. (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) dimana proses ini melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama patch keamanan dan pengendalian virus terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (mis., Virus, worm, spyware, spam).
2. *Manage network and connectivity security* (DSS05.02) dimana proses ini digunakan langkah-

langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas.

3. *Manage endpoint security* (DSS05.03) dimana proses ini memberikan kepastian terhadap titik akhir keluaran (end poin) (missal: Laptop, desktop, server, dan perangkat seluler dan jaringan seluler atau perangkat lunak lainnya) dijamin tingkat yang sama atau lebih besar dari persyaratan keamanan yang disetujui.

4. *Manage user identity and logical access* (DSS05.04) proses ini 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) proses ini 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) dimana proses ini 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) dimana proses ini 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).

Menurut (CMMI Product Team, 2010) CMMI memiliki *Capability Level* atau tingkat kemampuan. *Capability Level* adalah suatu model untuk menggambarkan bagaimana tiap proses inti berjalan di dalam sebuah institusi. *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:

- Level 0: Tidak lengkap (*Incomplete)* : Pendekatan tidak lengkap untuk memenuhi maksud dari Area Praktek. Mungkin tidak memenuhi maksud dari praktik apa pun. Performa tidak konsisten.
- Level 1: Dilakukan (*Performed)* : Pendekatan awal untuk memenuhi maksud dari Area Praktik. Bukan satu set praktik yang lengkap untuk memenuhi maksud penuh dari Area Praktik. Mengatasi masalah kinerja.
- Level 2: Dikelola (*Managed)* : Berlaku praktik level 1. Praktik yang sederhana, tetapi lengkap yang membahas maksud penuh dari Area Praktik. Tidak memerlukan penggunaan aset organisasi. Mengidentifikasi dan memantau kemajuan menuju sasaran kinerja proyek.
- Level 3: Ditetapkan (*Defined)* : Dibangun pada praktik level 2. Menggunakan standar organisasi dan menyesuaikan untuk mengatasi karakteristik proyek dan pekerjaan. Proyek menggunakan dan berkontribusi pada aset organisasi. 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. Mengidentifikasi dan memahami variasi, dan memprediksi dan meningkatkan kemampuan 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.

Menurut (CMMI Product Team, 2010) Model CMMI menempatkan insitusi dalam 5 *Maturity Level* atau tinggkat kematanggan dalam CMMI yaitu:

1. Level 1: *Initial* atau proses Awal.
   Kondisi ini institusi yang berapa pada level ini adalah institusi yang belum menjalankan CMMI. Tidak terdapatnya proses yang standar dalam pengembangan IT, banyak perubahan yang bersifat ad-hoc (begitu terdapat defect, langsung dilakukan perbaikan tanpa melihat

penyebab utama secara menyeluruh) dan sangat sedikit kontrol.

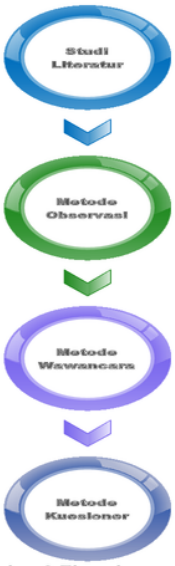
2. Level 2: *Managed* atau Dikelola.
   Level ini telah dimiliki institusi dengan beberapa proses yang sering digunakan dalam setiap proyek pengembangan, akan tetapi tidak terdapat keseragaman secara menyeluruh. Proses sudah mulai berjalan secara konsisten, akan tetapi tidak menyeluruh pada semua lini institusi.
3. Level 3: *Defined* atau Ditetapkan
   Level ini adalah yang paling umum dilaksanakan oleh hampir seluruh institusi pada saat mereka telah mengimplementasikan CMMI. Level ini, semua devisi institusi telah menjalankan proses yang sudah didefinisikan dan semua tim paham bagaimana proses seharusnya berjalan.
4. Level 4: *Quantitatively Managed* atau Dikelola secara kuantitatif.
   Level ini, Institusi semakin terstruktur dan terbuka dengan sistem yang ada. Mereka mulai menerapkan konsep kuantifikasi pada setiap proses, dan selalu dimonitoring serta dikontrol dalam setiap proses kerjanya.
5. 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. *Maturity Level* 5 fokus kepada peningkatan proses secara berkesinambungan melalui inovasi teknologi dan optimasi proses senantiasa dimonitoring dan dianalisis. Sehingga mampu memberikan sistem yang optimal.

3. Metode

Penelitian ini, menggunakan metode teknik pengumpulan data yang digunakan dalam penelitian ini 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 dengan permasalahan yang dikaji. Sehingga informasi yang didapat dari studi kepustakaan ini dijadikan rujukan untuk memperkuat argumentasi-argumentasi yang
2. Metode Observasi pengamatan langsung menggunakan alat indera atau alat bantu untuk penginderaan suatu subjek atau objek, yaitu pelaksanaan kegiatan dan administrasi sistem informasi perusahan atau institusi.
3. Metode Wawancara metode etode pengumpulan data adalah dengan jalan 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 metode ini dilakukan pengumpulan data dilakukan dengan metode kuesioner yang telah dijadikan standar dengan framework COBIT 5 dan mengadopsi dari CMMI.

Dengan langkah kegitan yang di lakuakan dalam penelitian ini yang terangkai dalam flowchat metode seperti pada Gambar 3.



Gambar 3 Flowchant metode

4. Hasil dan Pembahasan

Pada bagian ini akan disajikan hasil metode – metode yang dijanli secara tersetruktur. analisis terhadap implementasi dan pengukuran kinerja tingkat kematangan sistem informasi dengan kerangka kerja COBIT 5 dan CMMI.

4.1. Metode Kuesiner

Untuk mempermudah proses penelitian kami menggunakan metode kuesioner dimana kuesioner ini sudah di sesuaikan dengan standar framework COBIT 5 dan diadopsi dengan metode CMMI. Kuesioner penelitian ini menggunakan model pengukuran ordinal skala likert. Ukuran dalam model ini meliputi ukuran ordinal dan ukuran nominal. Ukuran ordinal adalah angka yang diberikan, angka tersebut mengandung arti tingkatan. Nomina angka 1 digunakan untuk mengurutkan obyek dari tingkatan terendah sampai tertinggi. Ukuran ini tidak memberikan nilai absolut

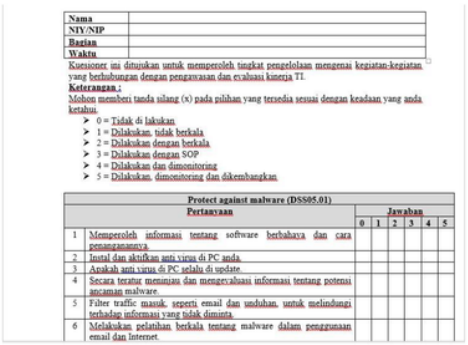
terhadap obyek sehingga hanya memberikan urutan tingkatan terendah sampai dengan tingkat tertinggi.

Dimana dalam kuesioner ini terdapat 6 penilain seperi pada Tabel 1 berikut ini:

Tabel 1 Penelian 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, dimana standar yang di gunakan adalah subdomain DSS05 dimana subdomain ini kusus untuk melakukan penilaian terkait kemanan system imformasi. Dalam standar ini terdapat 49 pertanyaan yang berhubungan dengan standar keamanan COBIT 5. Seperti pada Gambar 4:



Nama
NIY/NIP
Bagian
Waktu

Kuesioner ini ditunkan untuk memperoleh tingkat pengelolaan mengenai kegiatan-kegiatan yang berhubungan dengan pengawasan dan evaluasi kinerja TI.

Keterangan :

Mohon memberi tanda silang (x) pada pilihan yang tersedia sesuai dengan keadaan yang anda ketahui.

- 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

Protect against malware (DSS05.01)

	Pertanyaan	Jawaban					
		0	1	2	3	4	5
1	Memperoleh informasi tentang software berbahaya dan cara penanganannya						
2	Instal dan aktifkan anti virus di PC anda						
3	Apakah anti virus di PC selalu di update						
4	Secara teratur menunjau dan mengevaluasi informasi tentang potensi ancaman malware.						
5	Filter traffic masuk seperti email dan unduhan, untuk melindungi terhadap informasi yang tidak diminta						
6	Melakukan pelatihan berkala tentang malware dalam penggunaan email dan Internet						

Gambar 4. Kuesioner COBIT 5

4.2 Responden

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 & 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.

4.3 Pengolahan Data

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. rekomendasi dari masing-masing tujuan pengendalian yang perlu perbaikan. Model perhitungan yang digunakan untuk mengukur tingkat kematangan menggunakan CMMI.

Untuk mengidentifikasi sejauh mana devisi X pada instansi ABC telah memenuhi standard keamanan informasi yang baik untuk itu ditetapkan tingkat kematangan kapabilitas instansi, sebagaimana dijelaskan dalam Tabel 2 berikut :

Tabel 2 Nilai kriteria maturity level

Kriteria	Keterangan
0 – 0.50	*Initial* (Prose awal)
0.51 – 1.50	*Ad Hoc*
1.51 – 2.50	*Repeatable But Invinitve* (Berulang)
2.51 – 3.50	*Define Process* (di tentukan SOP)
3.51 – 4.50	*Managed and Measurable* (dikelola dan diukur)
4.51 – 5.00	*Optimized* (dioptimalisasi)

Hasil dari kuesioner yang telah di berikan terhadap responden dan telah di isi oleh responden di dapatkan hasil seperti pada Tabel 3:

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
DSS05.02.1	5	5
DSS05.02.2	5	5
DSS05.02.3	5	5
DSS05.02.4	5	5
DSS05.02.5	5	5
DSS05.02.6	5	5
DSS05.02.7	5	5
DSS05.02.8	5	5
DSS05.02.9	5	5
DSS05.03.1	5	5
DSS05.03.2	5	5
DSS05.03.3	5	5
DSS05.03.4	5	5
DSS05.03.5	5	5
DSS05.03.6	5	5
DSS05.03.7	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

DSS05	R 1	R 2
DSS05.04.5	5	5
DSS05.04.6	4	5
DSS05.04.7	4	5
DSS05.04.8	5	5
DSS05.05.1	5	5
DSS05.05.2	5	5
DSS05.05.3	5	5
DSS05.05.5	5	5
DSS05.05.6	5	4
DSS05.05.7	4	4
DSS05.06.1	3	3
DSS05.06.2	4	3
DSS05.06.3	4	3
DSS05.06.4	3	3
DSS05.06.5	2	3
DSS05.07.1	4	5
DSS05.07.2	4	5
DSS05.07.3	4	5
DSS05.07.4	3	5
DSS05.07.5	2	5

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

$$Indeks = \frac{\sum Jawaban\ Pertanyaan\ Terbanyak}{\sum\ Pertanyaan\ Kuesioner}$$

Dari perhitunggan indeks di terhadap data kuesioner di dapatkan hasil seperti pada Tabel 4 sebagai berikut ini:

Tabel 4 Hasil Indeks

DSS05	Jumlah Jawaban	Jumlah Pertanyaan	Indeks
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

4.4 Analisis dan Rekomendasi

Setelah tingkat indeks kematangan proses saat ini ditetapkan dan target kematangan proses sudah ditentukan, maka *gap* antara kondisi saat ini dan target yang akan dicapai akan dianalisis dan diidentifikasi peluang dari *gap* yang akan dioptimalkan. Untuk mempermudah dalam proses penjelasan di buat dengan ukuran nominal untuk mengurutkan nilai dari yang paling rendah sampai yang tertinggi. Seperti pada Grafik 1:

Gafik 1: *Gap Maturity Level*

Berdasarkan analisis *Gap* yang di dapat dari hasil level target yang ingin dicapai dan level yang tercapai pada DSS05, seperti pada grafik 1, maka berikut adalah beberapa analisis dan rekomendasi yang dapat berikan untuk meningkatkan kualitas keamanan sistem informasi di instansi tersebut:

1. *Protect against malware* (DSS05.01) berada dalam level *Optimized* dimana dalan level ini devisi X pada instansi ABC sudah mampu melakukan prosedur dengan baik dan mampu melakukan penembangan terkait maleware. Diharapkan selanjutnya instansi mampu meberikan antisipasi terhadap ancaman maleware lebih cepat dan tepat dalam mendeteksi ancaman malware.
2. *Manage network and connectivity security* (DSS05.02) berada dalam level *Optimized* dimana dalan level devisi X pada instansi ABC 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. Diharapkan instansi kedepanya semakin siap dengan adanya acaman terkait konektifitas dan mampu dengan cepat memberikan tindakan penanggulangan terkait keamanan konektivitas.
3. *Manage endpoint security* (DSS05.03) berada dalam level *Managed and Measurable* dimana dalan level ini devisi X pada instansi ABC 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* dimana dalan level ini devisi X pada instansi

ABC sudah mampu melakukan prosedur dengan baik dan mampu melakukan penembangan terkait hak akses yang dimiliki setiap pengguna. Diharapkan perusahaan atau institusi mampu memberikan peringatan dini terhadaap potensi ancaman keamanan terhadap sistem dan perangkat yang dimiliki kepada seluruh pegawai.

5. *Manage physical access to IT assets* (DSS05.05) berada dalam level *Optimized* dimana dalan level ini devisi X pada instansi ABC sudah mampu melakukan prosedur dengan baik dan mampu melakukan pengembangan terkait keamanan fisik. Di harapkan untuk kedepanya mampu membuat dan laporan terkait ujicoba sistem keamanan yang diterapkan dan dievaluasi dalam rana fisik secara berkala.
6. *Manage sensitive documents and output devices* (DSS05.06) berada dalam level *Define Process* dalam ini devisi X pada instansi ABC 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* dimana dalan level ini devisi X pada instansi ABC sudah mampu melakukan prosedur dengan baik menggunakan alat deteksi intrusi, untuk memantau infrastruktur untuk hak akses yang tidak sah dan memastikan setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian hanya saja perusaan atau instansi harus melakukan evaluasi yang rutin, minimal tiap semester terhadap sistem informasi yang dikhawatirkan dapat timbul potensi ancaman baru.

5. Kesimpulan

Berdasarkan penelitian yang dilakukan pada devisi X pada instansi ABC tersebut di dapatkan hasil bahwa dari hasil tingkat kematangan keamanan sistem informasi yang dihasilkan diketahui bahwa tingkat kematangan saat ini *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. 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.

Ucapan Terima Kasih

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

Daftar Pustaka

CMMI Product Team. (2010). CMMI® for Development, Version 1.3, (November). https://doi.org/CMU/SEI-2010-TR-034

Farida, S. I., & Rahajeng, E. (2014). *Usulan Model Tata Kelola Teknologi Informasi Pada Domain Monitor , Evaluate And Assess Dengan Metode Framework COBIT 5* (Vol. 7).

Fathoni, L. F., Firdausy, K., Yudhana, A., Studi, P., Elektro, T., Industri, F. T., & Dahlan, U. A. (2016). Application Information System Based Health Services Android, *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. *Konferensi Nasional Sistem & Informatika 2015*, 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. https://doi.org/10.1016/j.cose.2006.03.004

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, 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)*, 1), 139–147. http://doi.org/10.13140/RG.2.2.20925.15840

Prasetyo, A., & Mariana, N. (2011). Analisis Tata Kelola Teknologi Informasi (It Governance) pada Bidang Akademik dengan Cobit Frame Work Studi Kasus pada Universitas Stikubank Semarang, *16*(2), 139–141.

Rahayu, P., & Sensuse, D. I. (2017). Penilaian Implementasi e-Government di PUSTEKOM Kemendikbud berbasis metode PEGI, *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, 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*(2016), 6–7.

Rosmiati, Riadi, I., & Prayudi, Y. (2016). A Maturity Level Framework for Measurement of Information Security Performance Imam Riadi. *International Journal of Computer Applications*, *141*(8), 975–8887. https://doi.org/10.5120/ijca2016907930

Syafitri, P. D. (2016). Penilaian Kualitas Pengembangan Sistem Informasi Pada Perusahaan Distributor, *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). Seminar Nasional Teknologi Informasi dan Komunikasi - SEMANTIKOM 2017 ANALISIS.

W, Y., Riadi, I., & Yudhana, A. (2016). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing. In *Annual Research Seminar* (Vol. 2, pp. 300–304).

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

ORIGINALITY REPORT

25%

SIMILARITY INDEX

PRIMARY SOURCES

1	ejournal.undip.ac.id Internet	168 words — 4%
2	ojs.unpkediri.ac.id Internet	165 words — 3%
3	media.neliti.com Internet	165 words — 3%
4	ekokusuma.blogspot.com Internet	60 words — 1%
5	repository.upi.edu Internet	56 words — 1%
6	www.scribd.com Internet	45 words — 1%
7	mti.uad.ac.id Internet	43 words — 1%
8	www.senaski.unikom.ac.id Internet	39 words — 1%
9	kemenpora.go.id Internet	37 words — 1%
10	es.scribd.com Internet	34 words — 1%

11	Endang Kurniawan, Imam Riadi. "Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM", INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, 2018 Crossref	32 words — 1%
12	digilib.uinsby.ac.id Internet	29 words — 1%
13	repository.uinjkt.ac.id Internet	29 words — 1%
14	xxx.unizar.es Internet	25 words — 1%
15	scholar.uad.ac.id Internet	24 words — 1%
16	www.unisbank.ac.id Internet	24 words — 1%
17	journal.stth-medan.ac.id Internet	23 words — < 1%
18	media.proquest.com Internet	21 words — < 1%
19	journal.uad.ac.id Internet	21 words — < 1%
20	semantikom.unira.ac.id Internet	17 words — < 1%
21	andynuriman.files.wordpress.com Internet	16 words — < 1%
22	armanibrahim.blogspot.com Internet	16 words — < 1%
23	"10-Q: PSI INTERNATIONAL, INC.", EDGAR Online-Glimpse,	

	March 13 2018 Issue Publications	13 words — < 1%
24	www.coursehero.com Internet	12 words — < 1%
25	riadi.staff.uad.ac.id Internet	11 words — < 1%
26	stikes-yogyakarta.ac.id Internet	11 words — < 1%
27	vdocuments.site Internet	11 words — < 1%
28	ranmaryani.blogspot.com Internet	10 words — < 1%
29	www.sciencedirect.com Internet	9 words — < 1%
30	elib.unikom.ac.id Internet	9 words — < 1%
31	heri49e.blogstudent.mb.ipb.ac.id Internet	9 words — < 1%
32	ejournal.bsi.ac.id Internet	8 words — < 1%
33	jbioleng.biomedcentral.com Internet	8 words — < 1%

EXCLUDE QUOTES OFF
EXCLUDE MATCHES OFF
EXCLUDE BIBLIOGRAPHY OFF