

**ANALISIS PEMANFAATAN *PLATFORM E-LEARNING*
MENGUNAKAN *FRAMEWORK COBIT 5* PADA DOMAIN DSS**

Ummul Fitri Afifah¹, Ihsan Verdian²

¹Program Studi Sistem Informasi, Universitas Universal

²Program Studi Teknik Informatika, Universitas Universal

**Komplek Maha Vihara Duta Maitreya Bukit Beruntung, Sei Panas, Batam 29456
Kepulauan Riau-Indonesia**

Email: ummul.fitri@uvers.ac.id, ihsanverdian@uvers.ac.id

ABSTRACT

This study aims to determine the level of capability of using E-Learning at Universal University. In this study, the measurement of capability level uses the COBIT 5 framework which is devoted to the DSS05 (Manage Security Services) process. The data from this study were obtained from observations and interviews. The results show that the capability level in the DSS05 (Manage Security Services) process reached level 1 with a rating level of Largely achieved (57.8%). After knowing the level of capability at the E-Learning level, recommendations for improvement are made based on the acquisition of each value. The recommendations for improvement are the creation of SOPs related to E-Learning security at Universal University, the establishment of information technology asset inventory management, and the procurement of intrusion detection tools.

Keyword : *Framework COBIT 5, Manage Security Services, Universal's University*

ABSTRAK

Penelitian ini bertujuan untuk mengetahui tingkat kapabilitas dari pemanfaatan *E-Learning* di Universitas Universal. Dalam penelitian ini, pengukuran tingkat kapabilitas menggunakan kerangka kerja COBIT 5 yang dikhususkan pada proses DSS05 (*Manage Security Services*). Data dari penelitian ini didapatkan dari hasil observasi dan wawancara. Hasil penelitian menunjukkan *capability level* pada proses DSS05 (*Manage Security Services*) mencapai level 1 dengan rating level *Largely achieved* (57,8%). Setelah mengetahui tingkat kapabilitas level *E-Learning*, maka dibuatkan rekomendasi perbaikan berdasarkan perolehan masing-masing nilai. Rekomendasi perbaikan yang diberikan yaitu pembuatan SOP terkait keamanan *E-Learning* di Universitas Universal, pembentukan manajemen inventaris aset-aset teknologi informasi, dan pengadaan alat deteksi intrusi.

Kata kunci : *Kerangka Kerja COBIT 5, Mengelola Keamanan Layanan, Universitas Universal*

1. PENDAHULUAN

Pengaruh dari sebuah teknologi informasi sangatlah penting di semua aspek, terlebih pada aspek pendidikan. Dengan semakin berkembangnya teknologi informasi tersebut, hampir semua kegiatan dari bidang pendidikan saat ini telah dimasuki oleh aplikasi dan otomatisasi teknologi informasi.

Universitas Universal adalah salah satu universitas swasta di Kota Batam, Kepulauan Riau. Universitas Universal telah mengaplikasikan sistem pembelajaran berbasis *E-Learning* sejak tahun 2018. *E-Learning* adalah cara baru dalam melakukan pembelajaran dengan memanfaatkan teknologi informasi dan komunikasi sehingga proses pembelajaran menjadi lebih mudah (Andrean et al., 2020). Jadi, dengan demikian dapat dikatakan bahwa *E-Learning* merupakan sebuah platform pembelajaran berbasis web yang disediakan untuk user (dosen dan mahasiswa) yang telah memiliki akun.

Penerapan *E-Learning* di Universitas Universal sebagai suatu penunjang dalam proses pembelajaran dengan mengintegrasikan teknologi. Sebagai sebuah aset TI yang sangat penting di Universitas Universal, maka

perlu untuk memperhatikan keamanan dari sistem *E-Learning* tersebut. Keamanan informasi adalah melindungi kerahasiaan, integritas dan ketersediaan aset informasi, baik dalam penyimpanan, pengolahan, atau transmisi dan hal tersebut dicapai melalui penerapan kebijakan, pendidikan, pelatihan kesadaran, dan teknologi (Matin et al., 2018).

Di dalam sistem *E-Learning* tentunya sangat dibutuhkan *security* untuk menjaga integritas data. Integritas dan keamanan data yang tersimpan dalam sistem *E-Learning* harus dijaga keakurasiannya. Adanya koneksi sistem *E-Learning* ke jaringan internet akan berpotensi mengalami *fraud* (kecurangan) dimana akan merugikan pihak universitas.

Pemilihan kerangka kerja COBIT 5 digunakan dalam penelitian ini dikarenakan menyediakan kerangka kerja yang komprehensif dalam membantu Universitas Universal mencapai tujuan berkaitan dengan keamanan informasi. COBIT 5 tidak dimaksudkan untuk menggantikan salah satu kerangka kerja atau standar lainnya, tetapi untuk menekankan tata kelola dan manajemen serta

mengintegrasikan praktik pengelolaan terbaik pada perusahaan dengan memanfaatkan dan memaksimalkan teknologi informasi (Pasha et al., 2020).

Berikutnya salah satu domain yang dipakai dalam framework COBIT 5 terkait permasalahan diatas yaitu DSS (*Deliver, Service, Support*). Domain DSS berkaitan dengan pengiriman aktual dan dukungan layanan yang diperlukan, yang meliputi pengiriman layanan, manajemen keamanan dan kontinuitas, dukungan layanan untuk pengguna, dan pengelolaan data dan fasilitas operasional (ISACA, 2013).

Penelitian ini bertujuan untuk menilai sejauh mana tingkat kemampuan (*capability level*) pemanfaatan *E-Learning* di Universitas Universal Batam, Kepulauan Riau, yang berfokus pada proses DSS05 yaitu *Manage Security Service*. Proses DSS05 mengarah kepada meminimalisir dampak bisnis dari kerentanan keamanan informasi (Mufti & Mursityo, 2017).

2. METODE

Metode yang digunakan dalam penelitian ini, yaitu:

a. Metode Pengumpulan Data

1) Observasi

Observasi dalam penelitian ini terkait pada pengumpulan data dengan cara mengamati secara langsung aktivitas yang dilakukan di tempat dilakukannya penelitian.

2) Studi Kepustakaan

Ini dilakukan dengan cara mencari referensi terkait dengan objek penelitian, seperti buku, jurnal, dll. Hal tersebut bertujuan sebagai penunjang dalam melakukan penelitian.

3) Wawancara

Wawancara dilakukan untuk mengumpulkan data dan informasi dari narasumber. Hasil dari wawancara tersebut nantinya akan diproses sebagai data pendukung dari penelitian. Wawancara dilakukan kepada PIC (*Person In Charge*) *E-Learning* Universitas Universal.

b. Metode Analisis

Adapun metode analisis dari penelitian ini, yaitu:

1) Analisis Kondisi Saat Ini (*As Is*)

Analisis kondisi saat ini (*As Is*) merupakan hasil analisis yang didapatkan ketika melakukan

penelitian. Pada tahap ini dilakukan perhitungan *capability level* dari domain COBIT 5.

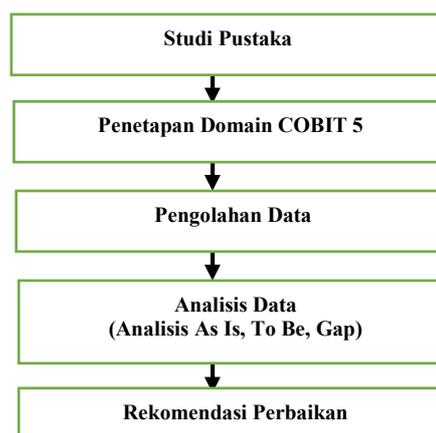
2) Analisis Kondisi Yang Diharapkan (*To Be*)

Analisis kondisi yang diharapkan merupakan target yang ingin dicapai dalam penelitian dalam bentuk level. Target didapatkan dari hasil wawancara dengan narasumber.

3) Analisis Kesenjangan (Gap)

Analisis kesenjangan didapatkan dari selisih analisis kondisi yang diharapkan (*To Be*) dengan analisis kondisi saat ini (*As Is*). Analisis Gap digunakan untuk menentukan langkah-langkah apa yang perlu diambil untuk bergeser dari kondisi saat ini ke kondisi yang diharapkan (Mufti & Mursityo, 2017).

Adapun kerangka pemikiran dari penelitian ini seperti terlihat pada Gambar 1.



Gambar 1 Kerangka Pikir Penelitian

Penjelasan mengenai kerangka penelitian, yaitu :

a. Studi Pustaka

Studi pustaka dimulai dari pengumpulan dasar-dasar teori yang berhubungan dengan COBIT 5. Dengan adanya studi pustaka diharapkan dapat membantu peneliti dalam pengerjaan tahap-tahap penelitian setelahnya (Fariz et al., 2020).

b. Penetapan Domain COBIT 5

Dalam tahap ini dilakukan pemilihan domain dalam COBIT 5, kemudian ditetapkan sebagai objek penelitian.

c. Pengolahan Data

Pengolahan data diperlukan dalam penelitian untuk mendapatkan hasil *capability level*.

d. Analisis Data

Analisis data dilakukan yaitu analisis kondisi saat ini (*As Is*), analisis

kondisi yang diharapkan (*To Be*), dan analisis kesenjangan.

e. Rekomendasi Perbaikan

Rekomendasi perbaikan digunakan sebagai solusi dari kesenjangan agar proses dapat berjalan lebih baik lagi ke depannya.

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

Tujuan dari penelitian ini yaitu mengukur sejauh mana tingkat kapabilitas proses *E-Learning* di Universitas Universal berdasarkan kerangka kerja COBIT 5 yang dikhususkan pada proses DSS05 (Mengelola Keamanan Layanan). Kapabilitas proses merupakan suatu karakteristik dari kemampuan sebuah proses untuk mencapai tujuan bisnis saat ini ataupun saat mendatang (Gunawan & Fernandes Andry, 2017). Penilaian kapabilitas proses dalam penelitian ini dilakukan berdasarkan panduan *self assessment COBIT 5*.

A. Analisis Kondisi Saat Ini (*As Is*)

Adapun hasil penilaian pencapaian level dari proses *Manage Security Service* (DSS05) lulus dari level 1. Hal ini dikarenakan proses DSS05 berada pada status *Largely*

Achieved 57,8%. Untuk hasil rincian penilaian capability level DSS05 dapat dilihat pada Tabel 1.

Tabel 1 Penilaian *Capability* DSS05

Praktik Dasar	Y/N	N	P	L	F
DSS05-1	Y			85%	
DSS05-2	Y			85%	
DSS05-3	Y			70%	
DSS05-4	Y				100%
DSS05-5	Y		55%		
DSS05-6	N	10%			
DSS05-7	N	0%			
Rata-Rata				57.8%	
Rating Levels				L	

Dari tabel diatas, dapat dilihat bahwa ada 7 praktik dasar (*base practices*) dari domain DSS05 yang dirujuk dari *COBIT 5 Process Dimension and Indicator* dengan penjelasan sebagaimana Tabel 2.

Tabel 2 Pemetaan Praktik Dasar DSS05

Praktik Dasar	Penjelasan
DSS05-1	Melakukan penerapan langkah-langkah pencegahan, detektif, dan korektif
DSS05-2	Adanya prosedur terkait langkah-langkah keamanan untuk menjaga informasi dari semua
DSS05-3	Memastikan endpoint diamankan pada tingkat yang sama dengan atau lebih besar dari persyaratan keamanan yang ditetapkan
DSS05-4	Memastikan bahwa semua user mempunyai hak akses informasi sesuai dengan persyaratan bisnis
DSS05-5	Menetapkan dan

	menerapkan prosedur untuk memberikan, membatasi, dan mencabut akses
DSS05-6	Menetapkan pengamanan fisik, praktik akuntansi, dan manajemen inventaris yang tepat atas aset TI
DSS05-07	Dengan menggunakan alat deteksi intrusi, pantau infrastruktur untuk akses yang tidak sah

Sumber: (Isaca et al., 2013)

Kemudian, untuk rating level berdasarkan panduan kerangka kerja COBIT 5 dapat dilihat pada Tabel 3.

Tabel 3 *Capability Level* COBIT 5

N	P	L	F
0-15%	>15-50%	>50%-85%	>85%-100%

Sumber : (ISACA, 2013)

Masing-masing subproses pada proses DSS05 dihitung secara bertahap. Kemudian dilihat apakah proses-proses tersebut telah memenuhi pada masing-masing levelnya. Tiap level memiliki ketentuan kategori, yaitu kategori N (*Not achieved*) dengan rentang nilai 0-15%, P (*Partially achieved*) dengan rentang nilai >15-50%, L (*Largely achieved*) dengan rentang nilai >50-85%, dan F (*Fully achieved*) dengan rentang nilai >85-100%. Untuk dapat lulus dari level 1, maka proses harus

meraih kategori L ataupun F (Bambang Gunawan, 2018).

Setelah kategori L didapatkan dari level 1, maka dapat dilakukan penilaian berikutnya. Dilakukan penurunan dari masing-masing praktik dasar menjadi beberapa *Work Product* (WP) yang digunakan untuk melakukan proses penilaian berikutnya. Adapun rincian penurunan dari praktik dasar ke *work product* menurut panduan COBIT 5 sebagaimana tertera pada Tabel 4.

Tabel 4 Pemetaan *Work Product* DSS05

<i>Work Product</i>	Penjelasan
DSS05-WP1	Konten pencegahan perangkat lunak berbahaya
DSS05-WP2	Konten evaluasi dari ancaman potensial keamanan
DSS05-WP3	Konten kebijakan keamanan pada konektivitas
DSS05-WP4	Konten hasil pengujian keamanan
DSS05-WP5	Konten kebijakan keamanan pada perangkat endpoint
DSS05-WP6	Konten persetujuan hak akses pengguna
DSS05-WP7	Konten hasil peninjauan ulang pengguna dan hak aksesnya
DSS05-WP8	Konten persetujuan permintaan hak akses
DSS05-WP9	Konten access logs pada sistem
DSS05-WP10	Konten karakteristik risiko keamanan
DSS05-WP11	Konten daftar peristiwa keamanan informasi
DSS05-WP12	Konten tiket insiden keamanan

<i>Work Product</i>	<i>Penjelasan</i>
DSS05-WP13	Konten inventarisasi dokumen dan perangkat penting
DSS05-WP14	Konten wewenang hak akses

Sumber: (ISACA, 2013)

Dari hasil penilaian *capability level* DSS05 untuk *work product*, didapatkan persentase nilai sebesar 0% dengan kategori N (*Not Achieved*). Sehingga, penilaian tidak dapat dilanjutkan ke tahap berikutnya.

Dari keseluruhan penilaian yang dilakukan didapatkan kesimpulan bahwa tingkat kapabilitas yang dicapai oleh Universitas Universal dalam pemanfaatan *Platform E-Learning* terkait proses DSS05 berada pada level 1 yaitu *Performed Process*.

B. Analisis Kondisi Yang Diharapkan

Dari hasil wawancara dengan pihak PIC (*Person In Charge*) *E-Learning* di Universitas Universal dikatakan bahwa target yang hendak dicapai dalam pemanfaatan *E-Learning* terkait proses DSS05 (*Manage Security Service*) berada di level 4 yaitu *Predictable Process*.

C. Analisis Kesenjangan (GAP)

Setelah didapatkan penilaian kapabilitas saat ini dan yang diharapkan, maka langkah selanjutnya

yaitu menghitung kesenjangan (Gap). Tabel 5 di bawah ini merincikan kesenjangan pada penilaian *capability level*.

Tabel 5 Analisis Gap DSS05

Proses	As Is	To Be	Gap
DSS05	1	4	3

3.2 Rekomendasi Perbaikan

Adapun rekomendasi perbaikan berdasarkan proses DSS05, yaitu:

- Membuat dokumen Standar Operasional Prosedur terkait keamanan *E-learning*. SOP tersebut mengatur dan memberi pedoman aktifitas dalam prosedur pemasangan perangkat lunak, prosedur permintaan hak akses, prosedur pemeliharaan perangkat lunak, dan prosedur perlindungan sistem dari malware.
- Mempersiapkan dan membentuk manajemen inventaris untuk aset-aset teknologi informasi agar lebih terarah dan terkontrol.
- Menyediakan alat deteksi intrusi untuk memantau infrastruktur *E-Learning* dari kegiatan-kegiatan yang mencurigakan.

4. SIMPULAN

Adapun kesimpulan dari penelitian ini terkait proses DSS05, yaitu:

- a. Tingkat kapabilitas dari proses *Manage Security Services (DSS05)* mencapai nilai 57,8% berada di rating L di level 1. Hal ini mengindikasikan bahwa keamanan *E-Learning* di Universitas Universal telah mencapai atau lulus level 1.
- b. Rekomendasi perbaikan untuk pengelolaan *E-Learning* Universitas Universal terkait proses *manage security services (DSS05)* yaitu pembuatan SOP terkait keamanan *E-Learning* di Universitas Universal, pembentukan manajemen inventaris aset-aset teknologi informasi, dan pengadaan alat deteksi intrusi.

5. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada **Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi** yang telah memberikan dukungan terhadap pelaksanaan penelitian ini melalui program **Hibah Penelitian Dosen Pemula (PDP) Tahun Anggaran 2021**

DAFTAR PUSTAKA

- Andrean, Z. W., Purabaya, R. H., & I Wayan Widi Pradnyana. (2020). PENGUKURAN TINGKAT KAPABILITAS TEKNOLOGI ELEARNING 4.0 DENGAN MENGGUNAKAN FRAMEWORK COBIT 5 PADA DOMAIN EDM, APO, DAN DSS (Studi Kasus: Universitas Pembangunan Nasional Veteran Jakarta). *Seminar Nasional Mahasiswa Ilmu Komputer Dan Aplikasinya (SENAMIKA)*, 5 (ISBN 978-623-93343-1-4), 187–198.
- Bambang Gunawan, D. (2018). *Perancangan Tata Kelola Teknologi Informasi* (1st ed.). ANDI.
- Fariz, M., Effendi, A., Perdanakusuma, A. R., Hayuhardhika, W., & Putra, N. (2020). *Evaluasi Kapabilitas Layanan Keamanan Teknologi Informasi Menggunakan COBIT 5 Process Assessment Model (DSS05)*. 05(May).
- Gunawan, A., & Fernandes Andry, J. (2017). Audit Aplikasi Zahir di PT Radisa Mahardi Rekatama Menggunakan Framework COBIT 5. *Audit Aplikasi Zahir Di PT Radisa Mahardi Rekatama Menggunakan Framework COBIT 5*, 2(1), 159–163. <https://fandomjapan.wordpress.com/2016/12/26/analisis-aplikasi-line-pada-penggunaan-teknologi-informasi-dan-komunikasi/>
- ISACA. (2013). *COBIT ® Process Assessment Model (PAM): Using*

COBIT® 5.

Isaca, Copy, P., & Sabilillah, R. R. (2013). *COBIT Self-assessment Guide: Using COBIT 5*.

Matin, I. M. M., Arini, A., & Wardhani, L. K. (2018). Analisis Keamanan Informasi Data Center Menggunakan Cobit 5. *Jurnal Teknik Informatika*, 10(2), 119–128.

<https://doi.org/10.15408/jti.v10i2.7026>

Mufti, R. G., & Mursityo, Y. T. (2017). Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 1(12), 1622–1631.

Pasha, D., Priandika, A. thyo, & Indonesian, Y. (2020). Analisis Tata Kelola It Dengan Domain Dss Pada Instansi Xyz Menggunakan Cobit 5. *Jurnal Ilmiah Infrastruktur Teknologi Informasi*, 1(1), 7–12.
<https://doi.org/10.33365/jiiti.v1i1.268>