PENGUKURAN KESIAPAN MANAJEMEN KEAMANAN INFORMASI DIREKTORAT SISTEM INFORMASI UNIVERSITAS TELKOM MENGGUNAKAN ISO/IEC 20000 DAN COBIT 5

MEASURING READINESS INFORMATION SECURITY MANAGEMENT OF INFORMATION SYSTEM DIRECTORATE TELKOM UNIVERSITY USING ISO/IEC 20000 AND COBIT 5

Dwi Kurnia Putri[1], Yanuar Firdaus A.W., S.T., M.T.[2], Eko Darwiyanto S.T., M.T.[3]

[1,2,3]Prodi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom

[1]dwikurniaputri@students.telkomuniversity.ac.id [2]yanuar@telkomuniversity.ac.id

[3]ekodarwiyanto@telkomuniversity.ac.id

Abstrak

Keamanan Informasi merupakan upaya untuk melindungi komputer dan non-peralatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab [1]. Dengan menggunakan manajemen keamanan informasi, diharapkan informasi-informasi penting dalam sebuah layanan dapat terjaga keamanannya. Salah satu layanan yang membutuhkan manajemen kemanan informasi adalah Telkom University Network Engine (TUNE), yang merupakan sebuah layanan penyedia jaringan internet. Layanan TUNE ini ditujukan untuk seluruh warga Universitas Telkom. Informasi yang tersimpan dalam layanan TUNE adalah username dan password yang nantinya digunakan oleh pengguna untuk dapat login ke layanan. Untuk mengetahui kesiapan layanan TUNE dalam manajemen keamanan informasi, dibutuhkanlah sebuah kegiatan penilaian. Dalam penelitian kali ini, penilaian menggunakan framework ISO/IEC 20000 yang dipetakan dengan framework COBIT 5. Dari hasil pemetaan kedua framework, diperoleh tiga proses manajemen keamanan. Setelah melakukan penelitian, didapat penilaian kesiapan untuk ketiga proses tersebut. Untuk proses kebijakan keamanan informasi, kontrol, keamanan informasi, serta perubahan dan insiden keamanan informasi layanan TUNE berada pada level PA 1.1 (performed process) dimana hanya sedikit atau tidak ada bukti dari pencapaian sistematis atas tujuan proses. Diharapkan dapat mencapai target optimalnya pada level 4 untuk proses kebijakan keamanan informasi dan kontrol keamanan informasi, sedangkan level 5 untuk perubahan dan insiden keamanan informasi.

Kata Kunci : Cobit 5, ISO/IEC 20000, TUNE

Abstract

Information security is attempt to protect the computer and non-computer equipment, facilities, data, and information from abuse [1]. Using information security management, expected to important information in a service can be kept. One of the services that require information security management is Telkom University Network Engine (TUNE), which is a service provider of internet network. TUNE is intended for all citizens of Telkom University. Stored information in TUNE is a username and password that will be used by the user to be able to login to the service. To determine the readiness TUNE services in information security management requires an assessment. In this study, assessment using framework of ISO / IEC 20000 which is mapped to the COBIT 5. From the results of mapping the framework, acquired three security management process. After doing research, obtained readiness assessment for all three processes. For the information security policy, information security controls, and information security changes and incidents TUNE at the level PA 1.1 (performed process) where few or no evidence of systematic achievement of the purpose of the process. We wish that we can be achieve optimal targets at level 4 for the information security requirements and information security control, while level 5 for the information security changes and incidents.

Keyword*: Cobit 5, ISO/IEC 20000, TUNE*

1. Pendahuluan

Direktorat Sistem Informasi Universitas Telkom merupakan salah satu instansi yang sangat membutuhkan manajemen keamanan informasi yang baik. Hal itu dikarenakan Direktorat Sistem Informasi Universitas Telkom mengelola beberapa layanan yang berkaitan dengan banyaknya data dan informasi. Salah satu layanan yang dikelola oleh Direktorat Sistem Informasi Universitas Telkom adalah Telkom University Network Engine (TUNE).

TUNE merupakan layanan koneksi internet kampus berbasis *Single Account* dan *Single Sign On* (SSO) [2]. Layanan TUNE ini merupakan sebuah layanan koneksi internet yang hanya disediakan oleh Universitas Telkom dan ditujukan untuk warga kampus (pengelola, dosen, mahasiswa, orangtua mahasiswa dan staf tenaga kependidikan). Dalam pengaksesan layanan TUNE, seluruh warga kampus diharuskan memiliki *username* dan *password* yang nantinya digunakan untuk memeperoleh koneksi internet. Hingga tahun 2014, terdapat sekitar 21.063 account meliputi staf akademik, staf administrasi dan mahasiswa yang harus dikelola oleh Direktorat Sistem Informasi Universitas Telkom [2]. Hal inilah yang melatarbelakangi pentingnya manajemen keamanan informasi khusus untuk layanan TUNE.

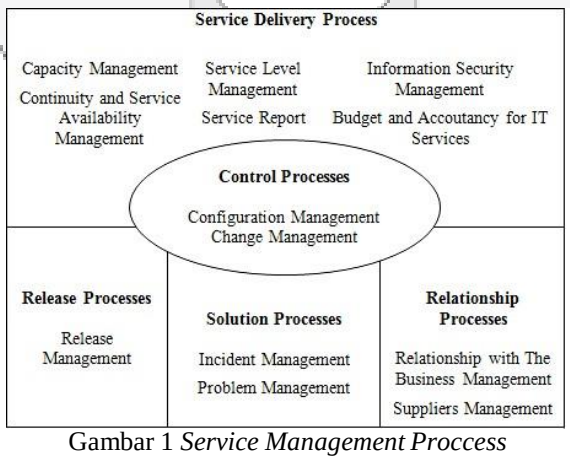
Sebagai panduan dalam pengelolaan manajemen layanan, ISO/IEC 20000 merupakan salah satu framework yang paling sering digunakan oleh instansi. Dalam jurnal yang dikarang oleh Ali Tarmuji menyebutkan bahwa ISO 20000 merupakan standar sertifikasi yang terukur untuk penyedia layanan yang terfokus secara langsung memandu pada penerapan tanpa menghiraukan ukuran perusahaan [3]. Dalam pengaplikasian standar ISO/IEC 20000, framework yang digunakan sebagai pemetaan terhadap ISO/IEC 20000 adalah COBIT 5 dengan *sub-domain Manage Security Services*. COBIT 5 merupakan pendekatan yang cocok digunakan untuk sebuah perusahaan dengan skala besar. Selain itu, COBIT 5 juga fleksibel dan mudah beradaptasi sesuai budaya, ukuran dan spesifik yang unik persyaratan setiap organisasi [4].

Oleh karena itu, dalam tugas akhir kali ini, dilakukanlah pemetaan antara ISO/IEC 20000 dengan COBIT 5. Dengan penelitian tugas akhir ini, diharapkan dapat memperoleh nilai pengukuran kesiapan proses manajemen untuk layanan TUNE. Hasil akhir dari penelitian layanan TUNE ini adalah sebuah dokumen penilaian dan rekomendasi. Rekomendasi utama diimplenetasikan dalam bentuk prototipe yang akan diimplementasikan pada layanan TUNE.

2. Dasar Teori dan Metodologi Penelitian

2.1. ISO/IEC 20000

ISO/IEC 20000 merupakan standar internasional pertama yang di rancang untuk meningkatkan model manajemen layanan TI yang memungkinkan sebuah perusahaan menyediakan layanan dengan kualitas yang memadai [6]. ISO/IEC 20000 memiliki dua bagian, bagian pertama akan membahas kebutuhan yang harus terpenuhi dan bagian kedua terkait dengan rancangan tata kelola yang harus dilakukan untuk mencapai standarisasi. ISO/IEC 20000 memiliki *Service Management Process* yang dapat digambarkan pada gambar 1 berikut:



Gambar 1 *Service Management Proccess*

Information Security Management pada ISO/IEC 20000 memiliki tujuan mengelola keamanan informasi secraa efektif dalam semua kegiatan pelayanan pada sebuah organisasi.

2.2. COBIT 5

COBIT merupakan serangkaian pedoman dan alat pendukung tata kelola perusahaan IT yang diterima di seluruh dunia. Auditor dan perusahaan menggunakannya sebagai mekanisme untuk mengintegrasikan teknologi dalam pengendalian implementasi dan memenuhi tujuan bisnis tertentu. COBIT cocok untuk perusahaan yang berfokus pada manajemen risiko dan mitigasi [8]. COBIT 5 mengidentifikasi lima prinsip dasar, tujuh kategori *enabler* untuk mengatur dan mengelola kebutuhan informasi, *Process Reference Model* yang baru, dan sejalan dengan ISO/IEC 15504 *Process Assessment Model* (PAM) [9].

Domain Deliver, Service and Support merupakan *domain* yang berfokus dengan *actual delivery and support of required services*, yang temasuk penyampaian layanan, pengelolaan atas keamanan dan kontinuitas, layanan bantuan untuk *users*, dan manajemen atas data dan fasilitas operasional. Salah satu proses yang terdapat pada *domain* DSS adalah DSS05 (Manage Security Services), yang merupakan proses yang berfokus pada upaya melindungi informasi organisasi untuk mempertahankan tingkat layanan keamanan informasi yang dapat diterima oleh organisasi sesuai dengan kebijakan keamanan. Tujuan proses ini adalah meminimalisasikan dampak bisnis dari kerentanan informasi dan insiden.

2.3. Proccess Assessment Model (PAM)

Process Assessment Model (PAM) merupakan model dua dimensi yang terdiri dari dimensi kapabilitas atau kemampuan dan dimensi proses. PAM digunakan sebagai dasr untuk penilaian kemampuan proses TI organisasi [10]. PAM memiliki dua jenis indikator penilaian, yakni:

1. Indikator proses atribut kapabilitas atau kemampuan (process capability attribute) untuk kemampuan pada tingkat 0-5 yang berupa:
    a. Praktik Umum (*Generic Practice* (GP))
    b. Hasil Kerja Umum (*Generic Work Product* (GWP))
2. Indikator proses kinerja (*process performance*) untuk kemampuan pada tingkat 1

Skala rating yang melibatkan enam level kapabilitas dijelaskan sebagai berikut [10]:

1. Level 0 *Incomplete Process* : proses belum diimplementasikan atau gagal mencapai tujuanya. Dalam level ini hanya ada sedikit atau tidak ada bukti dari pencapaian sistematis dari tujuan proses.
2. Level 1 *Performed Process* (satu atribut) : proses yang diimplementasi telah mencapai tujuannya.
3. Level 2 *Managed Process* (dua atribut) : proses yang telah dijalankan sekarang telah diimplementasikan dengan terkelola (terencana, termonitor, dan teratur) dan hasil kerjanya telah diterapkan dengan baik, terkontrol dan terpelihara.
4. Level 3 *Established Process* (dua atribut) : proses yang sudah terkelola sekarang diimplementasikan menggunakan proses terdefinisi yang mampu mencapai hasil prosesnya.
5. Level 4 *Predictable Process* (dua atribut) : proses yang telah mapan sekarang beroperasi dengan batasan yang terdefinisi untuk mencapai hasil prosesnya.
6. Level 5 *Optimizing Process* (dua atribut) : proses yang terprediksi telah diimprovisasi dengan berkelanjuran untuk mencapai tujuan bisnis perusahaan saat ini.

2.4. Diagram RACI (Responsible, Accountable, Consulted, Informed)

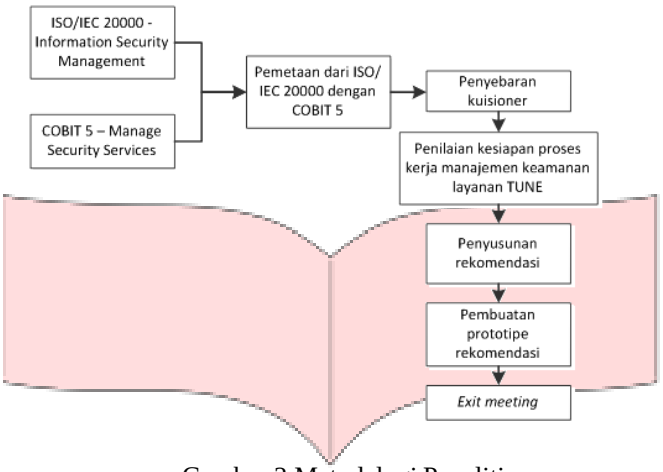
Diagram RACI merupakan matrik dari semua aktivitas dan wewenang pada organisasi yang membantu dalam mengambil keputusan. Berikut adalah penjelasan mengenai diagram RACI:

1. *Responsible*
   Responsible menjelaskan tentang siapa yang mendapatkan tugas yang harus dilakukan. Hal ini merujuk pada penanggung jawab pada kegiatan operasional.
2. *Accountable*
   Accountable menjelaskan tentang siapa yang bertanggung jawab atas keberhasilan tugas. Hal ini merujuk pada pertanggungjawaban secara keseluruhan atas tugas yang telah dilakukan.
3. *Consulted*
   Consulted menjelaskan tentang siapa yang memberikan masukan. Hal ini merujuk pada peran yang bertanggung jawab untuk memperoleh informasi dari unit lain atau mitra eksternal.
4. *Informed*
   Informed menjelaskan tentang siapa yang menerima informasi. Hal ini merujuk pada peran yang bertanggung jawab untuk menerima informasi yang tepat untuk mengawasi setiap tugas yang dilakukan.

2.5. TUNE (Telkom University Network Engine)

TUNE (Telkom University Network Engine), merupakan layanan koneksi nirkabel (*wireless*) internet kampus berbasis *Single Account* dan *Single Sign On* (SSO) yang ditujukan untuk warga kampus (pengelola, dosen, mahasiswa, orangtua mahasiswa dan staf tenaga kependidikan) dengan cakupan sinyal di seluruh kawasan kampus, baik fakultas maupun area publik, dengan total *bandwidth* 910 Mbps [2]. Akun *Single Sign On* (SSO) merupakan sebuah sistem yang memungkinkan seorang pengguna dapat menggunakan satu akun untuk mengakses beberapa aplikasi.

2.6. Metodologi Penelitian



Gambar 2 Metodelogi Penelitian

Langkah awal adalah mengetahui seluruh proses yang terdapat pada ISO/IEC 20000 dan juga proses yang terdapat pada COBIT 5. Proses-proses pada ISO/IEC 20000 dipetakan (*mapping*) terhadap proses-proses pada COBIT 5. Hasil pemetaan kedua *framework* memperoleh acuan dalam pembuatan kuesioner, dimana proses yang digunakan dalam penelitian tugas akhir ini adalah proses pada ISO/IEC 20000 dan aktifitas yang digunakan adalah aktifitas pada COBIT 5. Setelah memperoleh hasil pemetaan kedua framework, kuesioner yang telah disusun mulai disebar kepada pihak-pihak yang bertanggung jawab atas layanan TUNE Direktorat Sistem Informasi Universitas Telkom. Kuesioner yang disebar memperoleh nilai kepatuhan yang akan menentukan tingkat kapabilitas dari proses yang ada. Setelah diketahui tingkat kapabilitas, maka dilakukan analisis gap yang merupakan hasil penilaian tingkat kapabilitas dengan tingkat kapabilitas yang ingin dicapai. Dari hasil analisis gap tersebut, diperoleh beberapa rekomendasi yang akan membantu dalam peningkatan kualitas layanan TUNE Direktorat Sistem Informasi Universitas Telkom. Tahap selanjutnya adalah pembuatan prototipe salah satu rekomendasi yang diajukan. Tahap terakhir adalah penyampaian dokumen rekomendasi dan prototipe kepada pihak Direktorat Sistem Informasi Universitas Telkom disertai dengan exit meeting.

3. Pembahasan

3.1. Perencanaan Penelitian

Tahapan perencanaan dalam penelitian merupakan salah satu bagian terpenting agar penelitian berjalan dengan lancar secara baik dan benar. perencanaan penelitian ini meliputi studi pustaka yang mempelajari teori tentang ISO/IEC 20000 dan Cobit 5 serta studi lapangan tentang objek penelitian.

3.2. Pemetaan

Pada tahap ini, merupakan tahap analisis data dari objek penelitian yaitu Direktorat Sistem Informasi Universitas Telkom mulai dari analisa pemetaan ISO/IEC 20000 dengan COBIT 5, perancangan *form assesment*, pemetaan tugas dan wewenang, dan pemilihan narasumber.

Pemetaan ISO/IEC 20000 dengan COBIT 5 merupakan tiga proses yang terdapat pada *Information Security Management* ISO/IEC 20000 yang akan dipetakan dengan tujuh proses yang ada pada *Manage Security Services* COBIT 5 untuk memperoleh aktifitas-aktifitas yang berhubungan dengan kedua *framework*. Dalam pemetaan kedua *framework* ini, terlebih dahulu dilakukan eliminasi atas aktifitas-aktifitas yang mungkin tidak

sesuai dengan proses kerja pada layanan TUNE.

Pemetaan tugas dan wewenang dengan diagram RACI merupakan bagian dari struktur organisasi mempunyai definisi dan tugas yang sesuai dengan diagram RACI pada COBIT 5. Pemetaan ini diperoleh dari struktur organisasi yang ada di Direktorat Sistem Informasi Universitas Telkom yang berkaitan erat dengan pengoperasian layanan TUNE.

Tabel 1 Diagram RACI Tugas dan Wewenang

	Direktur Sistem Informasi	Manajer Komunikasi dan Layanan *Customer*	Asisten Manajer Pengembangan Infrastruktur	*System Administrator*	*Network Engineer*
Ketentuan Kemanan Informasi Layanan TUNE	C	A	R	I	R
Kontrol Keamanan Infromasi Layanan TUNE	C	A	R	I	R
Perubahan dan Insiden Keamanan Informasi Layanan TUNE	C	A	R	I	R

3.3. Pengambilan dan Pengolahan Data

Proses pengumpulan data ini dilakukan untuk mendapatkan kondisi sebenanya dari Layanan TUNE. Pengumpulan data dilakukan melalui kuisioner, interview, serta observasi (monitoring dan pemeriksaan dokumen). Kuisioner dan interview dilakukan pada sub-unit Infastruktur Direktorat Sistem Informasi Universitas Telkom. Sub-unit Infrastruktur merupakan sub-unit yang bertanggung jawab dalam proses kerja layanan TUNE.

Interview dilakukan untuk mengecek kebenaran dari tanggapan-tanggapan responden dari hasil kuisioner yang didapat dan untuk memperoleh bukti-bukti yang terkait dengan proses kebijakan keamanan informasi, kontrol keamanan informasi, serta perubahan dan insiden keamanan informasi. Kuisioner ditujukan pada satu orang asisten *manager* (asman) dan delapan orang staf pelaksana sub-unit Infrastruktur. Penyebaran kuisioner ini bertujuan untuk mendapat tanggapan dari responden mengenai keadaan terkini dari layanan TUNE dengan menggunakan ISO/IEC 20000 dan COBIT 5 untuk proses keamanan informasi. Kuisioner menggunakan skala *likert* sebagai pilihan jawaban. Skala *likert* merupakan suatu skala psikometrik yang umum digunakan dalam kuesioner. Pilihan jawaban dalam kuisioner ini memiliki skala 1 sampai dengan 5. Observasi dilakukan dengan monitoring dan pemeriksaan dokumen yang didapatkan dari hasil interview. Observasi ini dilaksanakan di sub-unit Infrastruktur.

Teknik pengolahan data yang digunakan dalam penelitian ini adalah uji validitas dan uji reliabilitas. Jenis uji validitas yang digunakan yaitu jenis validasi korelasi product moment yang dikemukakan oleh Pearson. Valid jika nilai r hitung lebih besar dari nilai r tabel product moment, atau nilai r hitung lebih besar dari nilai r kritis yang ditetapkan sebesar 0,30 [21]. Valid dalam artian data yang dihasilkan dapat dipercaya. Sedangkan, uji reliabilitas menggunakan reliabilitas alpha croanbach, dimana reliable jika koefisien reliabilitas lebih dari 0,6.

Hasil perhitungan koefisien validitas dan reliabilitas yang terkumpul dari 9 responden hasil pemetaan tugas dan wewenang menggunakan diagram RACI yang berupa rekapitulasi uji validitas dan reliabilitas masing-masing kuisioner terdapat pada tabel 2 dan tabel 3.

Tabel 2 Rekapitulasi Uji Validitas

Kuisioner	Iterasi ke-	Jumlah Pertanyaan	Jumlah Tidak Valid	Persentase Validitas
PA 1.1	1	33	11	66.67%
PA 1.1	2	34	7	79.41%

Tabel 3 Rekapitulasi Uji Reliabilitas

Kuisioner	Iterasi ke-	Koefisien Raliabilitas	Kategori Reliabilitas
PA 1.1	1	0.7882	Tinggi
PA 1.1	2	0.8682	Sangat Tinggi

3.4. Penilaian dan Pelaporan

Setelah melakukan penilaian kepada proses kebijakan keamanan informasi, kontrol keamanan informasi, serta perubahan dan insiden keamanan informasi hasil pemetaan di atas, maka didapatkan bahwa ketiga proses (kebijakan keamanan informasi, kontrol keamanan informasi, serta perubahan dan insiden keamaan informasi) berada pada level 1. Hal ini dikarenakan hasil terakhir nilai kepatuhan yang didapatkan pada masing-masing proses tidak lebih dari 85%, sehingga tidak dapat melanjutkan ke level selanjutnya.

Rekapitulasi nilai tingkat kapabilitas ini dilakukan setelah analisis hasil kuisioner di setiap proses. Berikut merupakan rekapitulasi tingkat kapabilitas pada layanan TUNE berdasarkan assessment yang sudah dilakukan.

Tabel 4 Rekapitulasi Tingkat Kapabilitas Layanan TUNE

Proses TI	Process Attribut (PA)	Hasil Penilaian (%)	Level
Kebijakan Keamanan Informasi	PA 1.1	72.1%	1
Kontrol Keamanan Informasi	PA 1.1	84.7%	1
Perubahan dan Insiden Keamanan Infromasi	PA 1.1	75%	1

4. Kesimpulan

Berdasarkan penelitian yang dilakukan terhadap penilaian tingkat kapabilitas pada layanan TUNE dengan bantuan *framework* ISO/IEC 20000 dan COBIT 5, maka diperoleh kesimpulan sebagai berikut :

1. Setelah melakukan pemetaan *framework* ISO/IEC 20000 dan Cobit 5, pada domain manajemen kemanan informasi, diperoleh 33 aktifitas yang berkaitan dengan pengoperasia layanan TUNE.
2. Tingkat kapabilitas proses kebijakan keamanan informasi, kontrol keamanan informasi, serta perubahan dan insiden keamanan informasi berada pada level PA 1.1 (*performed process*). Hal ini menunjukkan layanan TUNE masing-masing proses yang berada pada level PA 1.1 (*performed process*) hanya terdapat sedikit atau tidak ada bukti dari pencapaian sistematis atas tujuan proses.
3. Berdasarkan dengan hasil wawancara dengan sub-unit Infrastruktur Direktorat Sistem Informasi Universitas Telkom, target yang ingin dicapai untuk proses kebijakan keamanan informasi adalah level PA 4.4, sehingga setelah dilakukan analisis *gap*, terdapat *gap* sebesar 3 level. Untuk proses kontrol keamanan informasi yang telah berada level 1.1, target yang diinginkan adalah level PA 4.4, hal ini menyebabkan adanya *gap* sebesar 3 level. Sedangkan untuk proses perubahan dan insiden keamanan informasi memiliki *gap* sebesar 4 level karena target yang diinginkan adalah level PA 5.2.
4. Sesuai dengan penilaian hasil kuesioner dan analisis *gap*, rekomendasi yang berguna dalam perbaikan layanan TUNE adalah kelengkapan dokumen-dokumen dan dokumentasi dalam setiap aktifitas yang dilakukan.

Daftar Pustaka:

[1] Raymond McLeod and George P. Schell, *Management Information System*, 9th ed.: Prentice Hall Inc., 2004.

[2] Wikipedia. Universitas Telkom. [Online]. https://id.wikipedia.org/wiki/Universitas_Telkom

[3] Ali Tarmuji, "Tinjauan Umum Tentang Helpdesk dan Framework Terkait," *Jurnal Informatika*, vol. 2, pp. 146-157, Januari 2008.

[4] IT Governance Institute, *Cobit Security Baseline*.

[5] Donna Knapp, *The ITSm Process Design Guide*.: J. Ross, 2010.

[6] itSMF, *IT Service Management Global Best Practics*. UK: Van Haren Publishing, 2008, vol. 1.

[7] Charlene da Silva Leite, Jose Gabriel Peixoto Rodrigues, Tatiana da Silva Sousa, and Henrique Rego Monteiro de Hora, "IT Services Management and ISO 20000," *A Case Study in an IT Remote Support Company*, pp. 38-49, 2014.

[8] Pierre Bernard, *COBIT 5 - A Management Guide*, 1st ed., Jane Chittenden, Ed.: Van Haren Publishing, Zaltbommel, www.vanharen.net, 2012.

[9] ISACA, *A Bussines Framework for the Governance and Management of Enterprise IT*. United State of America, 2012.

[10] ISACA, *COBIT 5 Process Assessment Model*. USA: IT Governance Institute, 2013.

[11] Dr. Sugiyono, *Statistika untuk Penelitian*, 3rd ed. Bandung: CV. Alfabeta, 2000.