LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
UNIVERSITAS AHMAD DAHLAN
Jl. Condrosuli No. 3B Semaki Yogyakarta, Telp. 0274-542886, 0274-563515 ext. 1302, 1303 Fax. 0274-542886, Website : lppm.uad.ac.id, email : lppm@uad.ac.id

SURAT PERJANJIAN PELAKSANAAN PENELITIAN

Nomor: PHB-062/SP3/LPPM-UAD/IV/2019

Pada hari ini, **Senin** tanggal **Delapan** bulan **April** tahun **Dua ribu sembilan belas (08-04-2019)**, kami yang bertandatangan di bawah ini:

1. Nama : **Dr. Widodo, M.Si.**
   Jabatan : Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD), selanjutnya disebut sebagai **PIHAK PERTAMA.**
2. Nama : **IMAM RIADI, Dr., M.Kom**
   Jabatan : Dosen/Peneliti pada Program Studi **Sistem Informasi Fakultas Matematika dan Ilmu Pengetahuan Alam** Universitas Ahmad Dahlan (UAD), selaku Ketua Peneliti, selanjutnya disebut **PIHAK KEDUA.**

Kedua belah pihak menyatakan setuju dan mufakat untuk mengadakan perjanjian pelaksanaan penelitian untuk selanjutnya disebut Surat Perjanjian Pelaksanaan Penelitian (SP3) dengan ketentuan dan syarat-syarat sebagai berikut.

JUDUL PENELITIAN

Pasal 1

(1) PIHAK PERTAMA memberikan pekerjaan kepada PIHAK KEDUA dan PIHAK KEDUA menyatakan menerima pekerjaan dari PIHAK PERTAMA berupa kegiatan pada skim **Penelitian Hibah Bersaing (PHB).**

(2) Judul penelitian sebagaimana dimaksud dalam ayat (1) di atas adalah: **"PENGEMBANGAN CYBERSECURITY LAYANAN AKADEMIK PADA PERGURUAN TINGGI MENGGUNAKAN FRAMEWORK COBIT 5 ."**

PERSONALIA PELAKSANA PENELITIAN

Pasal 2

Pelaksana kegiatan ini terdiri dari:

Ketua Peneliti	: IMAM RIADI, Dr., M.Kom
Pembimbing/Konsultan	:
Anggota Peneliti 1	: Iwan Tri Riyadi Yanto, S.Si., MIT.
Anggota Peneliti 2	:

BENTUK DAN JANGKA WAKTU PERJANJIAN

Pasal 3

PIHAK KEDUA melaksanakan penelitian dalam jangka waktu paling lama **6 (enam) bulan** sejak ditandatangani SP3 ini, dan menyerahkan hasil laporan penelitian sementara kepada PIHAK PERTAMA selambat-lambatnya pada **8 Oktober 2019.**

LUARAN/*OUTPUT* PENELITIAN

Pasal 4

PIHAK KEDUA berkewajiban untuk merealisasikan luaran/*output* penelitian seperti yang dijanjikan dalam proposal penelitian di luar Laporan Hasil Penelitian.

BIAYA PENELITIAN DAN CARA PEMBAYARAN

Pasal 5

PIHAK PERTAMA menyediakan dana pelaksanaan penelitian kepada PIHAK KEDUA sejumlah **Rp 13.000.000,00 (Tiga belas juta rupiah)** yang dibebankan pada Anggaran Pendapatan dan Belanja (APB) LPPM UAD Tahun Akademik 2018/2019 dibayarkan melalui rekening bank atas nama Ketua Peneliti oleh Bidang Finansial UAD dengan tahapan sebagai berikut.

(a) **Tahap I sebesar 70% x Rp 13.000.000,00 = Rp 9.100.000,00 (Sembilan juta seratus ribu rupiah)** yang akan dibayarkan selambat-lambatnya dua minggu setelah SP3 ini ditandatangani oleh PARA PIHAK dan PIHAK KEDUA telah mengunggah file scan SP3 ini pada portal UAD.

(b) **Tahap II sebesar 30% x Rp 13.000.000,00 = Rp 3.900.000,00 (Tiga juta sembilan ratus ribu rupiah)** yang akan dibayarkan setelah PIHAK KEDUA menyelesaikan seluruh kewajibannya dalam jangka waktu seperti yang dimaksud dalam Pasal 3 serta dinyatakan benar dan lengkap.

PELAKSANAAN PEMBIMBINGAN

Pasal 6

(1) Khusus peneliti skema Penelitian Dosen Pemula (PDP) wajib melakukan pembimbingan atau konsultasi dengan dosen pembimbing penelitiannya paling sedikit 3 (tiga) kali pembimbingan.

(2) Pembimbingan sebagaimana dimaksud dalam ayat (1) yaitu pembimbingan dalam hal:
a. penyusunan angket/kuesioner dan atau teknik pengumpulan data lainnya;
b. analisis data dan interpretasinya;
b. penyusunan hasil penelitian, pembahasan, penarikan kesimpulan.

(3) Pembimbingan sebagaimana dimaksud dalam ayat (1) dan ayat (2) dituliskan dalam form pembimbingan yang ditandatangani oleh peneliti dan dosen pembimbing penelitian.

JENIS LAPORAN PENELITIAN

Pasal 7

(1) PIHAK KEDUA wajib menyusun dan menyampaikan laporan penelitian baik secara *on line* melalui portal UAD maupun *hardcopy* kepada PIHAK PERTAMA yang terdiri atas:
a. Laporan Kemajuan
b. Laporan Sementara
b. Laporan Akhir Penelitian

(2) Berkas **Laporan Kemajuan** digunakan sebagai bahan monitoring dan evaluasi (monev) internal.

(3) Berkas **Laporan Sementara** digunakan sebagai bahan kolokium laporan penelitian.

(4) Berkas **Laporan Akhir Penelitian** merupakan revisi dari Laporan Penelitian Sementara yang telah dikolokiumkan.

MONITORING DAN EVALUASI

Pasal 8

(1) PIHAK PERTAMA berhak untuk melakukan monitoring dan evaluasi (monev) internal pelaksanaan penelitian, baik secara administrasi maupun substansi.

(2) Pemantauan kemajuan penelitian dilakukan oleh Tim Monev yang dibentuk oleh PIHAK PERTAMA.

(3) PIHAK KEDUA diharuskan MENYIAPKAN SEMUA DOKUMEN/BUKTI kemajuan pelaksanaan penelitiannya guna kepentingan monev.

(4) Waktu pelaksanaan monev akan ditentukan oleh PIHAK PERTAMA.

KOLOKIUM LAPORAN PENELITIAN

Pasal 9

(1) PIHAK KEDUA wajib menyerahkan **Laporan Penelitian Sementara** sebagai bahan kolokium selambat-lambatnya **8 Oktober.**

(2) Ketua Peneliti wajib hadir dan mempresentasikan hasil penelitiannya pada kolokium **Laporan Penelitian Sementara** yang pelaksanaannya akan diatur oleh PIHAK PERTAMA.

(3) Revisi laporan penelitian yang sudah dikolokiumkan harus mendapatkan pengesahan dari *reviewer* dalam bentuk **Surat Pernyataan** dan dijilid dalam satu kesatuan laporan penelitian.

LAPORAN AKHIR PENELITIAN

Pasal 10

(1) PIHAK KEDUA wajib menyerahkan **Laporan Akhir Penelitian** selambat-lambatnya **2 (dua) pekan** setelah dikolokiumkan.

(2) Sistematika dan format laporan penelitian mengacu pada ketentuan dalam Pedoman Penelitian yang dikeluarkan oleh LPPM dan ketentuan lain yang berlaku.

(3) Berkas Laporan Akhir Penelitian yang diserahkan kepada PIHAK PERTAMA harus dilampiri:
   (a) artikel/draft publikasi ilmiah;
   (b) naskah/draft seminar (prosiding) dan sertifikat seminar;
   (c) lampiran lain yang dianggap perlu (seperti angket atau lainnya);
   (d) Profil Penelitian;
   (e) Borang Capaian Luaran Penelitian;
   (f) Form Pembimbingan (khusus skema PDP)
   (g) Daftar hadir kolokium laporan penelitian; dan
   (h) produk penelitian (naskah buku ajar, modul, naskah akademik, dan sejenisnya) atau dokumentasi/fotonya jika produk penelitian berupa barang atau perangkat keras *(hardware)* yang disertai penjelasan ringkas alat dan petunjuk pemakaiannya.

   Komponen (a) sampai dengan (g) dijilid dalam satu kesatuan sebagai berkas laporan akhir penelitian.

   Komponan (h) dijilid terpisah dari berkas laporan akhir penelitian, kecuali dokumentasi/foto produk penelitian.

(4) Laporan Akhir Penelitian sebagaimana tersebut pada ayat (1), (2), dan (3) memenuhi ketentuan sebagai berikut:
   a. bentuk/ukuran kertas A4;
   b. warna cover sesuai ketentuan;
   c. di bawah bagian cover ditulis:

PENELITIAN INI DILAKSANAKAN ATAS BIAYA
ANGGARAN DAN PENDAPATAN DAN BELANJA UNIVERSITAS AHMAD DAHLAN
TAHUN AKADEMIK 2018/2019
NOMOR KONTRAK: PHB-062/SP3/LPPM-UAD/IV/2019

(5) Berkas Laporan Akhir Penelitian sebagaimana tersebut dalam ayat (1) diserahkan kepada PIHAK PERTAMA sebagai berikut.
   1 eksemplar **ASLI** untuk PIHAK PERTAMA;
   1 eksemplar untuk PIHAK KEDUA;
   1 eksemplar untuk arsip Program Studi;

(6) PIHAK KEDUA wajib mengunggah file laporan akhir penelitian secara lengkap pada alamat *http://www.simpel.uad.ac.id* melalui akun portal ketua peneliti dengan format file PDF.

KEWAJIBAN UNGGAH LAPORAN PADA PORTAL UAD

Pasal 11

(1) PIHAK KEDUA wajib mengunggah berkas Laporan Akhir Penelitian pada *www.portal.uad.ac.id* melalui akun portal masing-masing peneliti.
(2) Berkas Laporan Akhir Penelitian sebagaimana dimaksud pada ayat (1) yang terdiri dari:
   i. Abstrak (PDF).
   ii. Laporan Akhir Final (PDF).
   iii. Profil Penelitian (PDF).
   iv. Borang Capaian Luaran Penelitian (PDF).

SANKSI DAN PEMUTUSAN PERJANJIAN PENELITIAN

Pasal 12

(1) PIHAK PERTAMA berhak memberikan peringatan dan atau teguran atas kelalaian dan atau pelanggaran yang dilakukan oleh PIHAK KEDUA yang mengakibatkan tidak dapat terpenuhinya kontrak penelitian ini.
(2) PIHAK PERTAMA berhak melakukan pemutusan perjanjian penelitian, jika PIHAK KEDUA tidak mengindahkan peringatan yang diberikan oleh PIHAK PERTAMA.
(3) Segala kerugian material maupun finansial yang disebabkan akibat kelalaian PIHAK KEDUA, maka sepenuhnya menjadi tanggungjawab PIHAK KEDUA.
(4) Jenis sanksi yang diberikan dapat berupa:
   (a) tidak diperkenankannya mengajukan proposal penelitian pada tahun anggaran berikutnya sampai kewajibannya terselesaikan; dan atau
   (b) tidak dapat mencairkan dana tahap 2; dan atau
   (c) mengambalikan dana yang telah diterima oleh PIHAK KEDUA.

KEADAAN MEMAKSA (*FORCE MAJEUR*)

Pasal 13

Ketentuan dalam Pasal 10 tersebut di atas tidak berlaku dalam keadaan sebagai berikut:

a. Keadaan Memaksa (*force majeur*)
b. PIHAK PERTAMA menyetujui atas terjadinya keterlambatan yang didasarkan pada pemberitahuan sebelumnya oleh PIHAK KEDUA kepada PIHAK PERTAMA dengan **surat pemberitahuan** mengenai kemungkinan terjadinya keterlambatan dalam penyelesaian kegiatan penelitian sebagaimana dimaksud dalam Pasal 1 dan Pasal 3; dan sebaliknya PIHAK KEDUA menyetujui terjadinya keterlambatan pembayaran sebagai akibat keterlambatan dalam penyelesaian perjanjian penelitian.

Pasal 14

(1) Keadaan Memaksa (*force majeur*) sebagaimana yang dimaksud dalam Pasal 11 ayat (1) adalah peristiwa-peristiwa yang secara langsung mempengaruhi pelaksanaan perjanjian serta terjadi di luar kekuasaan dan kemampuan PIHAK KEDUA ataupun PIHAK PERTAMA.
(2) Peristiwa yang tergolong dalam keadaan memaksa (*force majeur*) antara lain berupa bencana alam, pemogokan, wabah penyakit, huru-hara, pemberontakan, perang, waktu kerja diperpendek oleh pemerintah, kebakaran dan atau peraturan pemerintah mengenai keadaan bahaya serta hal-hal lainnya yang dipersamakan dengan itu, sehingga PIHAK KEDUA ataupun PIHAK PERTAMA terpaksa tidak dapat memenuhi kewajibannya.
(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib dibenarkan oleh penguasa setempat dan diberitahukan dengan Surat oleh PIHAK KEDUA atau PIHAK PERTAMA kepada PIHAK PERTAMA atau PIHAK KEDUA selambat-lambatnya 7 (tujuh) hari sejak terjadinya peristiwa yang dikategorikan sebagai Keadaan Memaksa (*force majeur*).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh kedua belah pihak jika keadaan *force majeur* dinyatakan telah selesai.

PENYELESAIAN PERSELISIHAN

Pasal 15

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

PENGUNDURAN DIRI

Pasal 16

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh Dekan fakultas ketua peneliti yang bersangkutan; dan bagi peneliti skim PDP ditambah persetujuan Dosen Pembimbing.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA.

LAIN-LAIN

Pasal 17

(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (*addendum*), yang merupakan kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Pemberitahuan dan/atau surat menyurat dari PIHAK KEDUA kepada PIHAK PERTAMA dialamatkan kepada Kepala Lembaga Penelitian dan Pengembangan Universitas Ahmad Dahlan.

Pasal 18

(1) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh kedua belah pihak.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini dibuat rangkap 2 (dua), bermeterai cukup pada kedua belah pihak; dan masing-masing memiliki kekuatan hukum yang sama. Biaya meterai dibebankan kepada PIHAK KEDUA.

PIHAK PERTAMA,	PIHAK KE DUA,
Dr. Widodo, M.Si.	**IMAM RIADI, Dr., M.Kom**
NIP. 196002211987091001	NIP/NIY. 60020397

Kode/Nama Rumpun Ilmu: 461 / Sistem Informasi

LAPORAN PENELITIAN

PENELITIAN HIBAH BERSAING

PENGEMBANGAN *CYBERSECURITY* LAYANAN AKADEMIK PADA PERGURUAN TINGGI MENGGUNAKAN *FRAMEWORK* COBIT 5

Disusun Oleh :

Dr. Imam Riadi, S.Pd., M.Kom (0510088001)
Iwan Tri Riyadi Yanto, S.Si., M.IT (0514068502)

`

Program Studi Sistem Informasi
FAKULTAS SAINS DAN TEKNOLOGI TERAPAN
UNIVERSITAS AHMAD DAHLAN

Oktober, 2019

PENELITIAN INI DILAKSANAKAN ATAS BIAYA
ANGGARAN PENDAPATAN DAN BELANJA UNIVERSITAS AHMAD DAHLAN

NOMOR KONTRAK : PHB-062/SP3/LPPM-UAD/IV/2019

HALAMAN PENGESAHAN

LAPORAN PENELITIAN HIBAH BERSAING
TAHUN AKADEMIK 2018/2019

Judul Penelitian	: Pengembangan *CyberSecurity* Layanan Akademik Pada Perguruan Tinggi Menggunakan *Framework* COBIT 5
Kode/Nama Rumpun Ilmu	: 461 / Sistem Informasi
Butir RIP	:
TSE Penelitian	: 20.05 *Information, computer and communication*

Ketua Peneliti

a. Nama Lengkap	: Dr. Imam Riadi, S.Pd., M.Kom.
b. NIY	: 60020397
c. Jabatan Fungsional	: Lektor Kepala
d. Program Studi	: Sistem Informasi
e. Nomor HP	: 08156854308
f. Alamat surel (e-mail)	: imam.riadi@is.uad.ac.id

Anggota Peneliti (1)

a. Nama Lengkap	: Iwan Tri Riyadi Yanto, S.Si., M.IT
b. NIY	: 60120678
c. Perguruan Tinggi	: Universitas Ahmad Dahlan

Lokasi Penelitian	: Yogyakarta
Lama Penelitian Keseluruhan	: 10 bulan
Biaya Penelitian Keseluruhan	: Rp. 13.000.000,00
Tahun 1	: Rp. 13.000.000,00
Tahun 2	: -

Mengetahui,
Dekan FAST

Imam Azhari, S.Si., M.CS.
NIY. 60010367

Yogyakarta, 30 Januari 2020

Ketua Peneliti,

Dr. Imam Riadi, S.Pd., M.Kom.
NIY. 60020397

Menyetujui,
Kepala Lembaga Penelitian dan Pengabdian Masyarakat
Universitas Ahmad Dahlan,

Dr. Widodo, M.Si.
NIP. 19600221 198709 1 001

SURAT PERNYATAAN

Dengan surat ini kami menyatakan bahwa penelitian:

1.	Judul Penelitian	:	Pengembangan *CyberSecurity* Layanan Akademik Pada Perguruan Tinggi Menggunakan *Framework* COBIT 5
2.	Ketua Peneliti		
	a. Nama Lengkap	:	Dr. Imam Riadi, S.Pd., M.Kom.
	b. Jenis Kelamin	:	Laki-Laki
	c. Pangkat dan Golongan	:	Penata / IIIc
	d. Jabatan Fungsional	:	Lektor Kepala
	e. Fakultas/Jurusan	:	Fakultas Sains dan Teknologi Terapan / Sistem Informasi
	f. Alamat	:	Gamping Lor, RT.005/12, Ambarketawang, Gamping, Sleman, Yogyakarta. 55294
	c. Nomor HP	:	08156854308
	d. Alamat surel (e-mail)	:	imam.riadi@is.uad.ac.id
3.	Jumlah Anggota Peneliti	:	1 Orang
	a. Anggota Peneliti	:	Iwan Tri Riyadi Yanto, S.Si., M.IT.
4.	Lama Penelitian	:	10 bulan
5.	Biaya Penelitian Keseluruhan		
	a. Sumber UAD	:	Rp. 13.000.000, 00
	b. Sumber Lain	:	-
	Jumlah	:	Rp. 13.000.000, 00

Telah direvisi sesuai dengan masukan dan petunjuk yang petunjuk yang disampaikan *reviewer.*

Mengetahui,
Reviewer,

Anton Yudhana, S.T., M.T., Ph.D.
NIY. 60010383

Yogyakarta, 30 Januari 2020
Ketua Peneliti,

Dr. Imam Riadi, S.Pd., M.Kom.
NIY. 60020397

KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Allah SWT yang senantiasa melimpahkan rahmat dan hidayahNya sehingga pelaksanaan penelitian dengan judul Pengembangan *Cybersecurity* Layanan Akademik Pada Perguruan Tinggi Menggunakan *Framework* Cobit 5 ini dapat terlaksana. Penelitian ini bertujuan untuk menyusun hasil analisis layanan akademik, sehingga dapat dilakukan perbaikan dan peningkatan keamanan.

Pengembangan *Cybersecurity* Layanan Akademik Pada Perguruan Tinggi Menggunakan *Framework* Cobit 5 ini telah dilaksanakan dalam kurun waktu 6 bulan. Keberhasilan dari penelitian ini tidak terlepas dari peran beberapa pihak yang telah membantu peneliti sehingga peneliti berjalan dengan lancar. Peneliti mengucapkan terimakasih yang sebesar-besar pada para pihak yang tidak dapat kami sebutkan satu persatu.

Akhirnya, kami berharap laporan penelitian ini dapat menambah khasanah pustaka dan mejadi referansi bagi para pembaca terutama bagi pada peneliti yang memiliki bidang minat yang sama.

Yogyaarta, 31 Januari 2020

Dr. Imam Riadi, S.PD., M.KOM.
Iwan Tri Riyadi Yanto, S.SI., M.IT

DAFTAR ISI

DAFTAR LAMPIRAN

DAFTAR TABEL

DAFTAR GAMBAR

PENGEMBANGAN *CYBERSECURITY* LAYANAN AKADEMIK PADA PERGURUAN TINGGI MENGGUNAKAN *FRAMEWORK* COBIT 5

Imam Riadi,Iwan Tri Riyadi Yanto

ABSTRAK

Sistem Informasi Akademik (SIA) menjadi bagian yang sangat penting bagi perguruan tinggi untuk menjaga informasi secara optimal dan aman. Teknologi sering disalahgunakan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menimbulkan terjadinya ancaman. Dalam rangka mencegah hal-hal tersebut terjadi, maka perlu diketahui tata kelola keamanan SIA perguruan tinggi dengan cara melakukan evaluasi. Penelitian ini dilakukan untuk mengetahui maturity level pada tata kelola keamanan SIA di perguruan tinggi menggunakan *NIST cybersecurity framework*.

NIST cybersecurity framework merupakan sebuah metode analisi *cybersecurity* yang dapat digunakan dalam analisis layanan akademik. Metode ini memeliki 5 fungsi, yaitu identifikasi (*identify*); perlindungan (*protect)*; deteksi (*detect)*; respon (*respond*); dan pemulihan (*recovery*). *Framework COBIT 5* akan di jadikan sebagai acuan proess aktivitas dalam fungsi *NIST cybersecurity framework.* Penelitian ini meghasilkan metode yang efektif terkait pengembangan layanan akademik di perguruan tinggi.

Penelitian ini bertujuan untuk membantu memberikan analisis evaluasi yang tepat digunakan dalam *cybersecurity* layanan akademik. Objek penelitian ini berada pada layanan akademik di perguruan tinggi, dimulai dengan penggumpulan data terkait dengan layanan akademik. Langkah selanjutnya adalah menganalisis *cybersecurity* layanan akademik berdasarkan *framework* COBIT 5. Penelitian ini diharapkan bisa menjadi kajian analisis terkait *cybersecurity* layanan akademik, sehingga dapat dijadikan rekomendasi dalam perbaikan dan juga pengembangan *cybersecurity* layanan akademik di perguruan tinggi.

Kata kunci: *COBIT 5, cybersecurity, evaluasi, framework,* SIA

ABSTRACT

The Academic Information System (SIA) is a very important part of the college to keep information optimally and securely. Technology is often misused by some irresponsible parties that can cause threats. to prevent these things from happening, it is necessary to know the security governance of SIA College by evaluating. This research was conducted to know maturity levels on SIA security governance in universities using the NIST cybersecurity framework.

The NIST cybersecurity framework is an analytic method of cybersecurity that can be used in the analysis of academic services. This method has 5 functions: identification (identify); protection; Detection (detect); Response (respond); and recovery. The COBIT Framework 5 will be about the processing activity in the NIST cybersecurity framework function. This research has been an effective method of developing academic services in colleges.

This research aims to help provide the proper evaluation analysis used in cybersecurity academic services. The object of this research is on academic service in college, starting with the complainant of data related to academic services. The next step is to analyze the cybersecurity academic service based on the COBIT framework 5. This research is expected to be a study of analysis related to cybersecurity academic services, so it can be used as a recommendation in the improvement and development of cybersecurity academic services in college.

Keywords: COBIT 5, *cybersecurity, evaluation, framework,* SIA

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang disertai perkembangan internet saling mendukung satu sama lain sehingga melahirkan konsep Teknologi Informasi (TI) berbasis internet yang perkembangannya semakin luas dan semakin meningkat telah diterapkan dalam bisnis perusahaan diberbagai bidang (Umar, Riadi, & Handoyo, 2017). TI saat ini menjadi teknologi yang banyak digunakan oleh hampir seluruh perusahaan atau lembaga dan dipercaya dapat membantu meningkatkan efisiensi proses yang berlangsung, tak terkecuali di institusi pendidikan. Untuk mencapai hal tersebut diperlukan suatu pengelolaan TI yang ada secara terstruktur.

Tata kelola TI memungkinkan perusahaan atau lembaga tersebut berupaya untuk menerapkan suatu sistem informasi yang dapat memenuhi kebutuhan perusahaan dalam mencapai tujuannya misalnya untuk meningkatkan kegiatan operasional kerja. Fungsi teknologi informasi tidak hanya untuk meningkatkan operasional kerja tetapi juga memberi nilai tambah dan keuntungan kompetitif.

Dengan berbagai keuntungan dan pentingnya TI, Perguruan Tinggi (PT) mengimplementasikan kedalam proses operasionalnya. Sistem informasi merupakan sistem yang berisi jaringan SPD (Sistem Pengolahan Data), yang dilengkapi kanal-kanal komunikasi yang digunakan dalam sistem organisasi data (Fathoni et al., 2016). Sistem informasi berbasis komputer di butuhkan oleh perguruan tinggi misalnya untuk mengelola data akademik, sumber daya manusia, promosi, pendidikan dan hiburan (Firdausy et al., 2008). Perguruan tinggi dapat memanfaatkan TI untuk pelayanan administrasi, mendukung Kegiatan Belajar Mengajar (KBM), sebagai media berkomunikasi, dan membantu untuk pengambilan keputusan. Implementasi TI yang baik pada PT maka akan meningkatkan kualitas layanan di PT tersebut.

Universitas Ahmad Dahlan (UAD) merupakan salah satu PT yang mengimplementasikan TI dalam kegiatan sehari-hari dalam hal akademik. UAD menjadi perguruan tinggi yang berperan aktif dalam perkembangan TI. UAD membentuk Biro Sistem Informasi dan Komunikasi (BISKOM) sebagai biro adminitrasi khusus terhadap pengembangan dan layanan TI dengan tujuan:

1. Menyelenggarakan layanan Teknologi Informasi dan Komunikasi (TIK) dengan tingkat kematangan yang meningkat secara berkelanjutan.
2. Menyediakan layanan sistem informasi yang handal dan terintegrasi dalam mendukung kelancaran proses akademik.
3. Menyelenggarakan layanan jaringan komunikasi dan internet dengan *Service Level Agreement* (SLA) 99%.
4. Menyelenggarakan layanan *helpdesk* dengan waktu respon keluhan maksimum 2 hari.
5. Mengelola website dan sosial media dalam mendukung pencitraan universitas serta seluruh unit di UAD.
6. Meningkatkan kerjasama bidang TIK dengan pihak eksternal dalam rangka meningkatkan daya saing UAD.

Berdasarkan tujuan di atas BISKOM UAD membuat sistem khusus yang memberikan kemudahan dalam akses akademik atau sering disebut Sistem Informasi Akademik (SIA) yang diberi nama Portal akademik. Portal akademik yang dikelola oleh BISKOM UAD mulai aktif digunakan pada tahun 2008, yang dibuat dan dikembangkan oleh vendor (Gama Techno) setelah itu pada tahun 2017 terdapat migrasi ke sistem baru yang dikembangkan sendiri oleh BISKOM UAD. Migrasi ini disebabkan karena adanya perkembangan teknlologi sistem informasi, sehingga dianggap perlu untuk dilakukan migrasi untuk menjaga stabilitas dan keamaman sistem infromasi tersebut. SIA selama berjalan 12 tahun sudah mengalami kendala, masalah dan ancaman pada sistem informasi. Masalah, kendala dan ancaman yang sering terjadi adalah sebagai berikut:

1. Beberapa sistem yang belum terintregerasi dengan baik.
2. Ketika masa KRS online terjadi *server down*.
3. Sering terjadinya lupa user name dan *password*.
4. Proses koneksi atau transmisi data yang lambat.
5. Serangan virus dan *malware*.

Kendala, masalah dan ancaman dapat ditangulangi dengan resiko seminimal mungkin dengan lebih fokus terhadap keamanan sistem informasi, maka perlu diketahui sejauh mana *cybersecurity* layanan akademik dengan cara melakukan evaluasi terhadap sistem keamanan.

Proses evaluasi BISKOM UAD menerapkan standar ISO 9000 untuk standar sistem manajemen mutu (SMM) yang teritregasi dengan semua biro di seluruh institusi. Standar dan audit yang betujuan langsung dengan keamanan sitem informasi selama ini belum ada. Banyak standar yang bisa digunakan dalam proses evaluasi dan audit terkait dengan keamanan sistem informasi seperti *Framework* COBIT, *International Standart Organisation* (ISO) 27000, *National Institute of Standards and Technology* (NIST), Indeks KAMI, *Information Technology Infrastructure Library* (ITIL), *The Open Group Architecture Framework* (TOGAF), dan lain-lain.

Evaluasi tidak hanya membutuhkan standar saja dalam prosesnya, akan tetapi membutuhkan metode untuk menilai proses standar yang sudah di jalankan dalam sistem tersebut. Beberapa metode yang bisa digunakan dalam penilaian tingkat kematangan keamanan sistem informasi seperti *Capability Maturty Model Integrated (CMMI), Balanced Scorecard*, Pemeringkatan *E-Government* Indonesia (PeGI), Metode Teknometrik dan lain-lain. Hasil penilian dalam kematangan dan kemampuan sebuah organisasi perangkat lunak itu ditunjukan dengan nilai *Maturity Level.*

Penelitian ini bertujuan untuk membantu memberikan analisis evaluasi yang tepat digunakan dalam *cybersecurity* layanan akademik. Objek penelitian ini berada pada layanan akademik BISKOM UAD, dimulai dengan penggumpulan data terkait dengan layanan akademik di UAD. Langkah selanjutnya adalah meganalisis *cybersecurity* layanan akademik berdasarkan *framework* COBIT 5. Penelitian ini diharapkan bisa menjadi kajian analisis terkait *cybersecurity* layanan akademik di BISKOM UAD sehinga dapat dijadikan rekomendasi dalam perbaikan dan juga pengembangan terkait *cybersecurity* layanan akademik.

1.2 Identifikasi Masalah

Berdasarkan latar belakang tersebut maka diidentifikasi sebagai berikut:

1. Seiring berkembangnya perkembangan teknologi memunculkan ancaman keamanan sehingga diperlukan evaluasi terkait *cybersecurity* layanan akademik.
2. Dibutuhkan standarisasi yang tepat untuk evaluasi cybersecurity layanan akademik di BISKOM UAD.
3. Tingkat kematangan (*maturity level*) dari proses layanan akademik harus di ketahui untuk dijadikan bahan analisis pada institusi.

1.3 Rumusan Masalah

Rumusan masalah dari penelitian ini yaitu:

1. Bagaimana menentukan metode yang tepat untuk evaluasi *cybersecurity* layanan akademik?
2. Bagaimana penerapan standarisasi keamanan sistem informasi dan menjaga informasi yang tersimpan dari berapa ancama yang ada?
3. Bagaimana mendapatkan nilai *maturity level* layanan akademik?

1.4 Batasan Masalah

Agar pembahasan tidak menyimpang dari permasalahan yang ada, maka penulis membuat batasan masalah dalam penelitian ini, sebagai berikut:

1. Menggunakan *framework* COBIT 5 dengan fokus pada *Domain Delivery, Service, and Support* (DSS).
2. Lingkup tata kelola TI yaitu layanan akademik UAD yang di kelola oleh BISKOM.
3. Penelitian ini tidak menghasilkan output berupa program, tepi menyajikan analisis layanan akademik dari *maturity level* yang dapatkan.

1.5 Tujuan Penelitian

Tujuan dilakukannya penelitian ini yaitu:

1. Menghasilkan rekomendasi metode audit yang tepat digunakan dalam layanan akademik.
2. Menghasilkan level standarisasi keamanan dan menjaga layanan akademik dari acaman keamanan.
3. Menyusun hasil analisis layanan akademik, sehingga dapat dilakukan perbaikan dan peningkatan keamanan.

1.6 Manfaat Penelitian

Adapun manfaat penelitian dari penelitian ini yaitu:

1. Memberikan rekomendsi motode audit yang tepat untuk layanan akademik.
2. Memberikan usulan pengelolaan layanan akademik terhadap pengelola.
3. Meningkatkan keamanan layanan akademik.

BAB 2
KAJIAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian sejenis ini sebelumnya pernah dilakukan oleh:

Michael Mylrea, Sri Nikhil Gupta Gourisetti, Andrew Nicholls, 2017 IEEE, 2016, pp. 127-136, dengan judul: HyperLink: An Introduction to Buildings Cybersecurity Framework.

Mahfizah Mazlan, Nurul Aqilah Mohd Zarani, Jamaludin Ibrahim., 2016, **International Journal of Information and Communication Technology Research**, **vol. 6, no. 12**, dengan judul: A Cyber Security Assessment of Muslim Countries.

Khosraw Salamzada, Zarina Shukur, Marini Abu Bakar, 2015 Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik Vol. 4 No. 1, dengan judul: A Framework For Cybersecurity Strategy For Developing Countries: Case Study Of Afghanistan.

Wei Wei, Arti Mann, Kewei Sha, T. Andrew Yang, 2016 IEEE, 2016, dengan judul: Design and Implementation of a Multi-Facet Hierarchical Cybersecurity Education Framework.

Muhamad Rizal, Yanyan M. Yani, Journal of ASEAN Studies, Vol. 4, No. 1, 2016, dengan judul: ForenVisor: Cybersecurity Policy and Its Implementation in Indonesia.

Penelitian-penelitian di atas digunakan sebagai rujukan dalam penelitian ini. Adapun peninjauan mengenai perbedaan dan persamaan penelitian-penelitian sebelumnya dengan penelitian yang dilakukan sekarang bisa dilihat pada tabel 2.1

Tabel 2.1. Tabel Perbedaan dan Persamaan Penelitian

Persamaan dan Perbedaan pada Penelitian Penulis	Topik	Judul - Jenis Tulisan - Sekolah/Universitas	Objek - *Platform*	Metode
Michael Mylrea, Sri Nikhil Gupta Gourisetti, Andrew Nicholls (2016)	*cybersecurity*	IEEE International Conference on Autonomic Computing (ICAC),	Building Cybersecurity Framework (BCF)	*(NIST) Cybersecurity Framework*
Mahfizah Mazlan, Nurul Aqilah Mohd Zarani, Jamaludin Ibrahim (2016)	*cybersecurity*	International Journal of Information and Communication Technology Research, vol. 6, no. 12	Cyber Security Assessment	*Cyber security assessments in muslim*
Khosraw Salamzada, Zarina Shukur, Marini Abu Bakar (2016)	*cybersecurity*	Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik Vol. 4 No. 1	Building Cybersecurity	*CSS framework*
Wei Wei, Arti Mann, Kewei Sha, T. Andrew Yang (2015)	*cybersecurity*	IEEE	Design and Implementation	*Cybersecurity Education Framework*
Muhamad Rizal, Yanyan M. Yani (2016)	*cybersecurity*	Journal of ASEAN Studies, Vol. 4, No. 1, 2016	Implementation of Cyber Security Regulations in Indonesia	*Cyber Security Regulations in Indonesia*

2.2 Dasar Teori

2.2.1 *Cyber Security*

Teknologi dilahirkan merupakan kegiatan yang oleh manusia dengan merencanakan dan menciptakan benda- benda material yang bernilai praktis, seperti mobil, pesawat, televisi adalah hasil dari pengembangan teknologi. Dilihat dari fungsi dan pentingnya teknologi, semua kalangan masyarakat dan instasi pemerintah sangat tergantung terhadap teknologi baik yang digunakan untuk hal postif maupun negatif. Kata *cyber* dan teknologi diuraikan dari asal kata *technique,* dari kata Yunani *Technikos* yang berarti kesenian atau keterampilan dalam dan *logos* adalah limo atau asas-asas utama pada *cyber (software)*. Meningkatnya pemanfaatan pada ruang siber *(cyberspace)* di seluruh lini kehidupan masyarakat pada era globalisasi saat ini secara parallel, akan menghubungkan pada pemanfaatan suatu jaringan teknologi internet pada obyek atau sektor tertentu sesuai dengan tujuan dari pengawakannya (Rahmawati, 2017).

Cyber security atau keamanan dunia maya adalah proteksi perlindungan dunia maya dari sumber-sumber bahaya. Sedangkan *Cyber defense* atau pertahanan dunia maya adalah segala bentuk usaha untuk mempertahankan keamanan *cyber* atau dunia maya. *Cyber Security* berbeda dengan security atau keamanan biasa karena ancaman *cyber* tidak bisa dimasukan begitu saja ke dalam kategori keamanan tradisional.4 Selain berasal dari dalam negeri, ancaman *cyber* atau *Cyber Threats* juga datang dari luar negeri. Namun, ancaman ini jarang mencapai taraf yang membutuhkan respon militer karena apapun yang akan dilakukan pemerintah dalam menanggapi ancaman *cyber* ini akan memiliki implikasi domestik dan internasional (Saputera, Yuliansyah, 2015).

2.2.2 Sistem Informasi Akademik

Sistem informasi adalah sekumpulan komponen yang saling berhubungan, mengumpulkan atau mendapatkan, memproses, menyimpan, dan mendistribusikan informasi untuk menunjang pengambilan keputusan dan pengawasan dalam suatu organisasi. Secara umum Sistem Informasi Akademik (SIA) sebagai sistem yang dirancang untuk memenuhi kebutuhan akademik yang menjadikan pelayanan pendidikan secara terkomputerisasi untuk meningkatkan kinerja. SIA membantu organisasi, instansi ataupun lembaga pendidikan untuk memecahkan masalah dalam pengelolaan data serta pencarian daya yang cepat, tepat, lengkap sesuai dengan kebutuhan pemakai. SIA telah banyak digunakan oleh hampir semua perguruan tinggi di Indonesia, hal ini dimaksudkan untuk memudahkan penyampaian informasi kepada

peserta didik, dan staf pengajar serta tenaga administrasi dalam manajemen(Kurniawan & Riadi, 2018).

2.2.3 (NIST) Cybersecurity Framework

NIST CSF for Improving Critical Infrastructure merupakan kerangka kerja yang dapat digunakan untuk mengarahkan organisasi pada aktivitas keamanan siber dan mempertimbangkan risiko keamanan siber sebagai bagian dari proses manajemennya. Kerangka kerja ini memberikan panduan dan tahapan dalam meningkatkan keamanan siber melalui analisis risiko keamanan siber. Untuk menerapkannya, kerangka kerja ini memerlukan kerangka kerja yang lain karena sifatnya sangat bergantung pada kerangka kerja lain. Bagian utama dalam kerangka kerja ini adalah *framework core* yang merupakan satu rangkaian aktivitas keamanan siber, outcome yang diinginkan, dan beberapa referensi informatif yang dapat digunakan untuk mencapainya. *Framework core* terdiri dari 5 fungsi, yaitu identifikasi (*identify*); perlindungan (*protect)*; deteksi (*detect)*; respon (*respond*); dan pemulihan (*recovery*), 22 kategori dan 100 subkategori yang cocok dengan contoh referensi informatifnya (Briliyant & Ashari, 2018). seperti pada Gambar 2.1 yaitu:

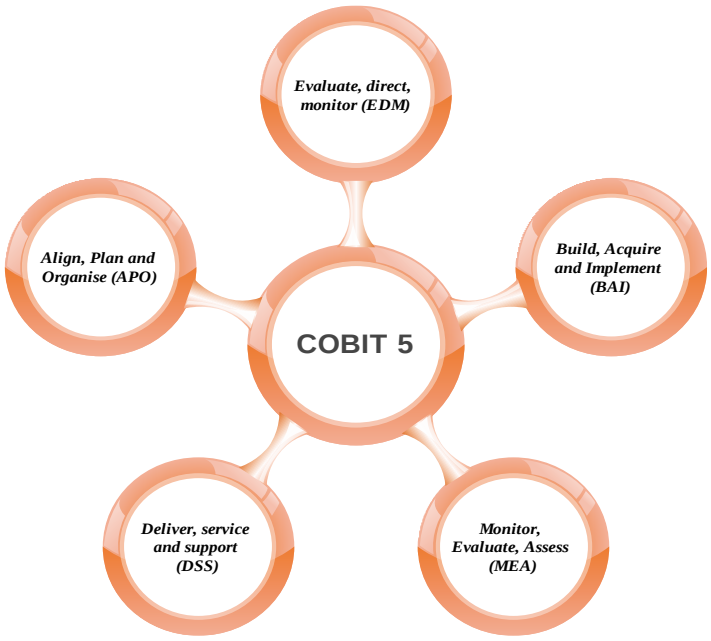
Gambar 2.1 *NIST Cybersecurity Framework*

2.2.4 Framework COBIT 5

Control Objective for Information & Related Technology (COBIT) adalah panduan standar praktek manajemen TI 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).

Menurut (Sasongko, 2009) COBIT adalah sekumpulan dokumentasi best practice untuk IT Governance yang dapat membantu auditor, pengguna (user), dan manajemen, untuk menjembatani gap antara resiko bisnis, kebutuhan kontrol dan masalah-masalah teknis IT. COBIT adalah salah satu framework yang digunakan untuk standar audit, COBIT merupakan standar yang dinilai lengkap dan cakupan yang menyeluruh sebagai framework audit. COBIT dikembangkan secara berkala oleh ISACA. Didalam COBIT ini terdapat beberapa domain yang digunakan untuk proses audit.

COBIT 5 merupakan kerangka kerja generasi terbaru dari panduan ISACA yang tata kelola dan manajemen TI. COBIT 5 menyediakan kerangka kerja yang membantu perusahaan dalam mencapai tujuan dengan tata kelola dan manajemen TI (Ferriyan, 2015). COBIT 5 terdiri 5 domain utama seperti pada Gambar 2.2 yaitu:



Gambar 2.2 *Domain COBIT 5*

1. *Evaluate, Direct, Monitor* (EDM) adalah kegitan megevaluasi, mengarahkan dan memonitoring semua kegitan TI di oraganisasi tersebut.
2. *Align, Plan and Organise* (APO) adalah kegitan merencanakan TI dalam organisasi tersebut.
3. *Build, Acquire and Implement* (BAI) adalah kegitan membangun TI di organisasi tersebut.

4. *Deliver, Service and Support* (DSS) adalah kegitan menjalankan TI di organisasi tesebut.
5. *Monitor, Evaluate, Assess* (MEA) adalah kegitan memonitoring TI yang sedang berjalan pada organisi tersebut.

Lima domain pada COBIT 5 terdiri dari 37 proses yaitu EDM 5 proses, APO 13 proses, BAI 10 proses, DSS 6 proses, dan MEA 3 proses. Proses yang terdapat pada doamain COBIT 5 harus di gunakan sesuai dengan kebutuhan dan tujuan organisasi yang ada mampu memberikan penilaian dan efiktifitas pada kegiatan implentasi COBIT 5.

BAB 3
METODOLOGI PENELITIAN

3.1 Metodologi

Penelitian ini diperlukan data dan informasi yang lengkap guna mendukung tahapan pengujian yang akan dilakukan. Metode pengumpulan data yang digunakan adalah sebagai berikut:

a. Studi Kasus

   Metode ini dilakukan dengan mengumpulkan, membaca serta mempelajari data yang berasal dari berbagai media seperti buku, jurnal, karya tulis atau artikel yang terkait dengan penelitian.

b. Observasi

   Observasi merupakan metode pengumpulan data dengan melakukan pengamatan langsung pada lapangan penelitian. Pada penelitian ini, peneliti melakukan pengamatan langsung pada SIA di perguruan tinggi untuk mengumpulkan kebutuhan pengujian.

c. Wawancara

   Peneliti melakukan wawancara secara langsung kepada narasumber yang berwenang tehadap layanan akademik di perguruan tinggi.

d. Kuesioner

   Metode kuesioner metode ini dilakukan pengumpulan data dengan *NIST Cybersecurity Framework* dan mengadopsi dari *framework COBIT 5*.

3.2 Alat dan Bahan

Untuk menyelesaikan penelitian ini, digunakan alat dan bahan seperti ditunjukkan pada tabel 3.1.

Tabel 3.1 Alat dan bahan

No.	Nama Alat dan Bahan	Deskripsi / Spesifikasi	Keterangan
1.	Leptop	Acer ES1-132	Intel Celeron, 6GB RAM.
2.	Office	Microsoft Word	2019
3.	Office	Microsoft Excel	2019
4.	Desain	Microsoft Visio	2019
5.	Desain	Edraw Max	7.9
6.	Tools	COBIT5-Tool-Kit	COBIT5-Governance-and Management-Practices-Activities_April2014
7.	Tools	Implementing the NIST Cybersecurity Framework	V.1

BAB 4
HASIL DAN PEMBAHASAN

4.1 Rencana Anggaran Biaya (RAB) Penelitian

Bagian ini akan menyajikan metode proses terstruktur. analisis implementasi dan pengukuran tingkat kematangan sistem informasi dengan kerangka kerja COBIT 5 sub-domain DSS05 dan CMMI.

4.2 Pengamatan Proses Sistem Informasi Akademik

Proses ini melakukan wawancara langsung dengan nara sumber yang memiliki wewenang dalam keamanan sistem informasi akademik di Universitas Ahmad Dahlan, di mana hasilnya adalah bahwa BISKOM UAD menggunakan sistem informasi akademik untuk menjadi aktif pada tahun 2008, awal dari sistem informasi yang dibuat dan dikembangkan oleh vendor (Gama Techno) setelah itu, pada tahun 2017 ia dapat bermigrasi ke sistem baru di mana sistem dikembangkan oleh BISKOM UAD sendiri, dimana dalam migrasi ini adalah karena perkembangan teknologi sistem informasi, sehingga dianggap perlu untuk melakukan migrasi untuk menjaga stabilitas dan keamanan sistem informasi.

Tujuan dari sistem akademik Universitas Ahmad Dahlan itu adalah:

- Untuk mengelola kegiatan akademik di Universitas Ahmad Dahlan.
- Memberikan kemudahan kepada masyarakat, yaitu dosen, mahasiswa, staf dan BAA dalam proses akademik.

Seiring berjalannya waktu penggunaan sistem informasi juga mengalami, hambatan, masalah dan ancaman terhadap sistem informasi. Masalah, hambatan dan ancaman yang sering terjadi adalah sebagai berikut:

- Ada beberapa sistem yang belum terintegrasi dengan baik.
- Ketika KRS online terjadi, server sedang down.
- Sering terjadi lupa nama pengguna dan kata sandi Anda.
- Proses koneksi data atau transmisi lambat.
- Serangan virus dan malware.

Proses standardisasi dan audit BISKOM UAD menerapkan ISO 9000 di mana standar tersebut digunakan untuk standar untuk sistem manajemen mutu (SMM) yang digabungkan dengan

semua biro di semua lembaga. Proses ini juga membahas penentuan responden yang akan memberikan informasi terperinci terkait dengan informasi tentang keamanan sistem informasi akademik yang ada. Pemilihan sampel responden menggunakan teknik purposive sampling, yang merupakan pemilihan sampel responden yang ditentukan oleh peneliti dengan alasan bahwa identifikasi sampel responden dilakukan dengan mengacu pada kompetensi pribadi yang berinteraksi langsung dengan tata kelola TI [14]. Wawancara mendapatkan 2 responden yang secara langsung peduli dengan bidang keamanan sistem informasi di dalam institusi.

4.3 Pemetaan DSS05 Berdasarkan Kerangka Kerja COBIT 5

Proses ini adalah kompilasi dari kegiatan kesesuaian domain DSS05 dengan pertanyaan yang akan dibuat dalam kuesioner. karena keterbatasan tulisan kami, kami hanya mendaftar salah satu dari 7 proses sub-domain DSS05, yaitu DSS05.01. Proses DSS05.01 terdiri dari 6 kegiatan, seperti pada tabel 1.

Tabel 4.1. Lindungi dari aktivitas *malware*

Lindungi dari *malware* (DSS05.01)	
No	Pertanyaan Aktivitas
1	Obtain information about malicious software and how to handle it..
2	Install and activate anti-virus on your PC.
3	Is anti virus on the PC always updated.
4	Regularly review and evaluate information about potential malware threats.
5	Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information.
6	Conduct periodic training on malware in the use of e-mail and the Internet.

4.4 Persiapan Kuisioner dengan kombinasi DSS05 dan Level Kemampuan

Proses ini dilakukan dengan kuesioner berdasarkan standar pada DSS05 Framework COBIT 5 dengan menggabungkan dengan tingkat kemampuan standar CMMI sehingga dapat diperoleh bentuk kuesioner yang mampu menjawab kebutuhan keamanan sistem informasi dalam instalasi . Untuk menyederhanakan proses membaca, perbedaan warna untuk setiap keputusan dibuat dalam Level Kemampuan dan Tingkat Kedewasaan seperti pada tabel 2.

Tabel 4.2. Proses Peta Warna

Color	Information	
	Capability Level	***Maturity Level***
Red	*Incomplete*	*Non-Existent Initial*
Purple	*Performed*	*Initial / Ad Hoc*
Yellow	*Managed*	*Repeatable But Invinitve*
Blue	*Defined*	*Define Process*
Orange	*Quantitatively Managed*	*Managed and Measurable*
Green	*Optimizing*	*Optimized*

Dimana dalam kuesioner ini ada 6 penilaian untuk proses dengan tingkat kemampuan CMMI seperti pada Tabel 3.

Tabel 4.3. Penilaian proses TI dengan tingkat kemampuan CMMI

Nilai	*Capability Level CMMI*	Proses TI
0	*Incomplete*	Are not done
1	*Performed*	Done, not periodically
2	*Managed*	Performed periodically
3	*Defined*	Done with SOP
4	*Quantitatively Managed*	Performed and monitored
5	*Optimizing*	Done, monitored and developed

Penilaian proses TI pada Tabel 3 dikombinasikan dengan kerangka kerja COBIT 5 DSS05 standar pada Tabel 1, seperti pada Tabel 4.

Tabel 4.4. Formulir Kuisioner

Protect against malware (DSS05.01)							
	Activity	**Answer**					
		0	**1**	**2**	**3**	**4**	**5**
1	Obtain information about malicious software and how to handle it.						
2	Install and activate anti-virus on your PC.						
3	Is anti virus on PC always updated.						
4	Regularly review and evaluate information about potential malware threats.						
5	Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information.						
6	Conduct periodic training on malware in the use of e-mail and the Internet.						

4.5 KemampuanPerhitungan Tingkat Kematangan SIA Keamanan

Bagian ini akan menjelaskan hasil analisis implementasi dan pengukuran kinerja tingkat kematangan sistem informasi akademik yang diperoleh dari hasil kuesioner dan wawancara sesuai dengan kerangka kerja 5 domain COBIT DSS05 domain. Untuk mengidentifikasi sejauh mana perusahaan atau organisasi memenuhi standar keamanan informasi yang baik, dapat menggunakan kerangka identifikasi yang diwakili pada tingkat kedewasaan yang memiliki tingkat kemampuan pengelompokan perusahaan, sebagaimana dijelaskan dalam Tabel 5.

Tabel 4.5. Nilai kriteria tingkat kematangan

Criteria	Information
0 – 0.50	*Non-Existent Initial*
0.51 – 1.50	*Initial / 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 kuesioner yang telah diberikan kepada responden dan diisi oleh responden mendapatkan hasil. Karena halaman terbatas, data yang ditampilkan hanya pada DSS05.01. Seperti pada Tabel 6.

Tabel 4.6. Hasil kuesioner

DSS05	Responden 1	Responden 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

Selanjutnya, korelasi antara nilai level dan nilai absolut yang dilakukan dengan perhitungan dalam bentuk indeks menggunakan rumus matematika. Persamaan matematika untuk menentukan nilai indeks adalah sebagai berikut [15]:

$$Indeks = \frac{\sum Most\ Question\ Answers}{\sum Questionnaire\ Questions}$$

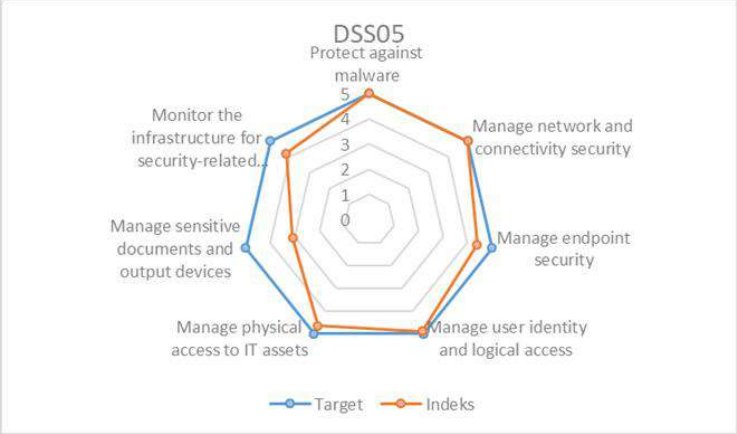
Setelah mendapatkan indeks, kita bisa mendapatkan Level Kematangan saat ini (sekarang). Nilai ini adalah nilai akumulasi dari proses yang berjalan di institusi. seperti pada tabel 6.

Tabel 4.7. Nilai Kematangan Yang Ada

DSS05	*Value of Maturity Level Existing*
Protect against malware	5,00
Manage network and connectivity security	5,00
Manage endpoint security	4,39
Manage user identity and logical access	4,88
Manage physical access to IT assets	4,64
Manage sensitive documents and output devices	3,10
Monitor the infrastructure for security-related events	4,20

4.6 Perhitungan Tingkat Kematangan Celah

Setelah nilai Level Kematangan yang ada diperoleh dan Kematangan. Tingkat rekomendasi (target) telah ditentukan, maka kesenjangan antara kondisi saat ini dan target yang akan dicapai akan dianalisis dan diidentifikasi peluang dari celah yang akan dioptimalkan. Level gap seperti pada Gambar 5.



Gambar 4.1. Kesenjangan Tingkat Kematangan

4.7 Analisis Kesenjangan Tingkat Kematangan

Berdasarkan analisis Gap diperoleh dari hasil level target yang ingin dicapai dan level yang dicapai pada DSS05, seperti pada Gambar 5., maka berikut ini adalah beberapa Analisis Level Maturity Gap. Seperti pada tabel 7 sebagai berikut.

Tabel 4.8. Analisis Tingkat Kematangan Celah

DSS05	*Maturity Level*
Protect against malware	*Optimized*
Manage network and connectivity security	*Optimized*
Manage endpoint security	*Managed and Measurable*
Manage user identity and logical access	*Optimized*
Manage physical access to IT assets	*Optimized*
Manage sensitive documents and output devices	*Define*
Monitor the infrastructure for security-related events	*Managed and Measurable*

Nilai keseluruhan Tingkat Kematangan pada DSS05 akan dihitung rata-rata sehingga akan mendapatkan tingkat Tingkat Kematangan di organisasi atau lembaga.

$$Maturity\ Level\ DSS05 = \frac{\sum Maturity\ Level}{many\ processes} \qquad (2)$$

$$MLDSS5 = \frac{\begin{array}{c} i(DSS05.01) + i(DSS05.02) + i(DSS05.03) + \\ i(DSS05.04) + i(DSS05.05) + \\ i(DSS05.06) + i(DSS05.07) \end{array}}{mp}$$

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

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

Dari hasil perhitungan diperoleh nilai pencapaian adalah 4,458 sehingga dapat diatur Tingkat Kematangan organisasi atau lembaga berada pada level Dikelola dan Terukur.

4.8 Kompilasi Rekomendasi Tata Kelola TI

Setelah Tingkat Kematangan ditentukan, proses persiapan rekomendasi akan dilakukan. Rekomendasi yang dapat diberikan untuk meningkatkan kualitas keamanan sistem informasi di lembaga:

- Protect terhadap malware (DSS05.01) berada pada tingkat Dioptimalkan di mana pada level ini BISKOM dari Universitas Ahmad Dahlan telah mampu melakukan prosedur dengan baik dan mampu mengembangkan yang terkait dengan malware. Diharapkan agensi akan dapat mengantisipasi ancaman malware dengan lebih cepat dan tepat dalam mendeteksi ancaman malware.
- Mengelola keamanan jaringan dan konektivitas (DSS05.02) berada pada tingkat Dioptimalkan di mana pada tingkat ini BISKOM Universitas Ahmad Dahlan telah mampu melaksanakan prosedur dengan baik dan mampu melaksanakan pengembangan yang terkait dengan keamanan kegiatan. Menetapkan sistem yang digunakan untuk mengevaluasi ancaman yang akan muncul, didokumentasikan dan dipantau. Diharapkan bahwa agen-agen masa depan akan lebih siap dengan ancaman konektivitas dan dapat dengan cepat memberikan tindakan pencegahan terkait dengan keamanan konektivitas.
- Mengelola keamanan titik akhir (DSS05.03) di tingkat Dikelola dan Terukur di mana pada tingkat ini BISKOM Universitas Ahmad Dahlan telah mampu melaksanakan prosedur dengan baik, hanya lembaga yang harus melakukan evaluasi rutin, setidaknya sebulan sekali pada sistem informasi yang dikhawatirkan berpotensi menjadi ancaman baru.
- Mengelola identitas pengguna dan akses logis (DSS05.04) berada pada level Dioptimalkan di mana pada level ini BISKOM Universitas Ahmad Dahlan telah mampu melaksanakan prosedur dengan benar dan mampu mengembangkan hak akses terkait masing-masing pengguna. Diharapkan bahwa perusahaan atau institusi dapat memberikan peringatan dini tentang potensi ancaman keamanan terhadap sistem dan peralatan yang dimiliki oleh semua karyawan.
- Mengelola akses fisik ke aset TI (DSS05.05) berada pada level Dioptimalkan di mana pada level ini BISKOM Universitas Ahmad Dahlan telah mampu melakukan prosedur dengan baik dan mampu melaksanakan pengembangan yang terkait dengan keamanan fisik. Diharapkan di masa depan, ia akan dapat menghasilkan dan melaporkan terkait

dengan uji coba sistem keamanan yang diterapkan dan dievaluasi dalam rana fisik berkala.

- Mengelola dokumen sensitif dan perangkat keluaran (DSS05.06) di tingkat Define Process, di BISKOM ini, Universitas Ahmad Dahlan telah menerapkan keamanan fisik, praktik akuntansi dalam hal dokumen yang berkaitan dengan situasi tersebut. Sehingga semua dokumen keluaran distandarisasi dalam keamanan. Hanya berharap nanti kelak bisa membengkokkan dokumentasi dan mengevaluasi ancaman yang ada.
- Memantau infrastruktur untuk acara yang berhubungan dengan keamanan (DSS05.07) berada pada level Dikelola dan Terukur di mana pada level ini BISKOM Universitas Ahmad Dahlan telah mampu melaksanakan prosedur dengan baik menggunakan alat deteksi intrusi, untuk memantau infrastruktur untuk akses tidak sah hak dan memastikan bahwa setiap peristiwa terintegrasi dengan kegiatan pemantauan dan manajemen acara harus melakukan evaluasi rutin, setidaknya setiap semester untuk sistem informasi yang dikhawatirkan potensi ancaman baru dapat muncul.

BAB 5
KESIMPULAN DAN SARAN

1.1 Kesimpulan

Sub-domain DSS05 Mengelola layanan keamanan adalah prosedur yang baik untuk digunakan dalam implementasi dan mega-audit terkait dengan keamanan sistem informasi akademik dan CMMI adalah metode penilaian yang baik dalam sistem audit lembaga. Berdasarkan penelitian yang dilakukan di BISKOM, Universitas Ahmad Dahlan menerima Tingkat Kematangan 4.458 sehingga menetapkan bahwa tingkat kematangan saat ini berada pada tingkat Dikelola dan Terukur. Level ini, institusi semakin disadarkan akan perkembangan teknologi. Lembaga telah menerapkan konsep kuantifikasi dalam setiap proses, dan selalu dipantau dan dikendalikan untuk kinerja.

DAFTAR PUSTAKA

Briliyant, O. C., & Ashari, R. A. (2018). Rencana Penerapan Cyber-Risk Management Menggunakan Nist Csf Dan Cobit 5. *Jurnal Sistem Informasi (Journal of Information System)*, *14*(2), 83–89.

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. *Jurnal Ilmu Teknik Elektro Komputer Dan Informatika (JITEKI)*, *2*(1), 39–48.

Ferriyan, A. (2015). Data Center Governance Information Security Compliance Assessment Based on the Cobit Framewok. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *6*(2), 34–36.

Firdausy, K., Yudhana, A., Studi, P., Elektro, T., & Ahmad, U. (2008). Sistem Informasi Perpustakaan berbasis Web dengan PHP dan MySQL. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *6.2*, 109–114.

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

Kurniawan, E., & Riadi, I. (2018). 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. https://doi.org/10.13140/RG.2.2.20925.15840

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber. *Jurnal Pertahanan & Bela Negara*, *7*(2), 51–66.

Saputera, Yuliansyah, M. (2015). Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare. *Jom FISIP*, *2*(2), 1–14.

Sasongko, N. (2009). Pengukuran Kinerja Teknologi Informasi Menggunakan Framework COBIT versi. 4.1, Ping Test dan Caat pada PT.Bank X Tbk. di Bandung. *Seminar Nasional Aplikasi Teknologi Informasi 2009*, *2009*(Snati), 108–113.

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.

LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
UNIVERSITAS AHMAD DAHLAN
Jl. Gondosuli No. 1B Semaki Yogyakarta, Telp. 0274-542886, 0274-583515 ext. 1502, 1503 Fax. 0274-542886, Website : lppm.uad.ac.id, email : lppm@uad.ac.id

SURAT PERJANJIAN PELAKSANAAN PENELITIAN

Nomor: PHB-062/SP3/LPPM-UAD/IV/2019

Pada hari ini, **Senin** tanggal **Delapan** bulan **April** tahun **Dua ribu sembilan belas (08-04-2019)**, kami yang bertandatangan di bawah ini:

1. Nama : **Dr. Widodo, M.Si.**
   Jabatan : Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD), selanjutnya disebut sebagai **PIHAK PERTAMA.**
2. Nama : **IMAM RIADI, Dr., M.Kom**
   Jabatan : Dosen/Peneliti pada Program Studi **Sistem Informasi Fakultas Matematika dan Ilmu Pengetahuan Alam** Universitas Ahmad Dahlan (UAD), selaku Ketua Peneliti, selanjutnya disebut **PIHAK KEDUA.**

Kedua belah pihak menyatakan setuju dan mufakat untuk mengadakan perjanjian pelaksanaan penelitian untuk selanjutnya disebut Surat Perjanjian Pelaksanaan Penelitian (SP3) dengan ketentuan dan syarat-syarat sebagai berikut.

JUDUL PENELITIAN

Pasal 1

(1) PIHAK PERTAMA memberikan pekerjaan kepada PIHAK KEDUA dan PIHAK KEDUA menyatakan menerima pekerjaan dari PIHAK PERTAMA berupa kegiatan pada skim **Penelitian Hibah Bersaing (PHB).**

(2) Judul penelitian sebagaimana dimaksud dalam ayat (1) di atas adalah: **"PENGEMBANGAN CYBERSECURITY LAYANAN AKADEMIK PADA PERGURUAN TINGGI MENGGUNAKAN FRAMEWORK COBIT 5 ."**

PERSONALIA PELAKSANA PENELITIAN

Pasal 2

Pelaksana kegiatan ini terdiri dari:

Ketua Peneliti	: IMAM RIADI, Dr., M.Kom
Pembimbing/Konsultan	:
Anggota Peneliti 1	: Iwan Tri Riyadi Yanto, S.Si., MIT.
Anggota Peneliti 2	:

BENTUK DAN JANGKA WAKTU PERJANJIAN

Pasal 3

PIHAK KEDUA melaksanakan penelitian dalam jangka waktu paling lama **6 (enam) bulan** sejak ditandatangani SP3 ini, dan menyerahkan hasil laporan penelitian sementara kepada PIHAK PERTAMA selambat-lambatnya pada **8 Oktober 2019.**

LUARAN/*OUTPUT* PENELITIAN

Pasal 4

PIHAK KEDUA berkewajiban untuk merealisasikan luaran/*output* penelitian seperti yang dijanjikan dalam proposal penelitian di luar Laporan Hasil Penelitian.

BIAYA PENELITIAN DAN CARA PEMBAYARAN

Pasal 5

PIHAK PERTAMA menyediakan dana pelaksanaan penelitian kepada PIHAK KEDUA sejumlah **Rp 13.000.000,00 (Tiga belas juta rupiah)** yang dibebankan pada Anggaran Pendapatan dan Belanja (APB) LPPM UAD Tahun Akademik 2018/2019 dibayarkan melalui rekening bank atas nama Ketua Peneliti oleh Bidang Finansial UAD dengan tahapan sebagai berikut.

(a) **Tahap I sebesar 70% x Rp 13.000.000,00 = Rp 9.100.000,00 (Sembilan juta seratus ribu rupiah)** yang akan dibayarkan selambat-lambatnya dua minggu setelah SP3 ini ditandatangani oleh PARA PIHAK dan PIHAK KEDUA telah mengunggah file scan SP3 ini pada portal UAD.

(b) **Tahap II sebesar 30% x Rp 13.000.000,00 = Rp 3.900.000,00 (Tiga juta sembilan ratus ribu rupiah)** yang akan dibayarkan setelah PIHAK KEDUA menyelesaikan seluruh kewajibannya dalam jangka waktu seperti yang dimaksud dalam Pasal 3 serta dinyatakan benar dan lengkap.

PELAKSANAAN PEMBIMBINGAN

Pasal 6

(1) Khusus peneliti skema Penelitian Dosen Pemula (PDP) wajib melakukan pembimbingan atau konsultasi dengan dosen pembimbing penelitiannya paling sedikit 3 (tiga) kali pembimbingan.

(2) Pembimbingan sebagaimana dimaksud dalam ayat (1) yaitu pembimbingan dalam hal:
a. penyusunan angket/kuesioner dan atau teknik pengumpulan data lainnya;
b. analisis data dan interpretasinya;
b. penyusunan hasil penelitian, pembahasan, penarikan kesimpulan.

(3) Pembimbingan sebagaimana dimaksud dalam ayat (1) dan ayat (2) dituliskan dalam form pembimbingan yang ditandatangani oleh peneliti dan dosen pembimbing penelitian.

JENIS LAPORAN PENELITIAN

Pasal 7

(1) PIHAK KEDUA wajib menyusun dan menyampaikan laporan penelitian baik secara *on line* melalui portal UAD maupun *hardcopy* kepada PIHAK PERTAMA yang terdiri atas:
a. Laporan Kemajuan
b. Laporan Sementara
b. Laporan Akhir Penelitian

(2) Berkas **Laporan Kemajuan** digunakan sebagai bahan monitoring dan evaluasi (monev) internal.

(3) Berkas **Laporan Sementara** digunakan sebagai bahan kolokium laporan penelitian.

(4) Berkas **Laporan Akhir Penelitian** merupakan revisi dari Laporan Penelitian Sementara yang telah dikolokiumkan.

MONITORING DAN EVALUASI

Pasal 8

(1) PIHAK PERTAMA berhak untuk melakukan monitoring dan evaluasi (monev) internal pelaksanaan penelitian, baik secara administrasi maupun substansi.

(2) Pemantauan kemajuan penelitian dilakukan oleh Tim Monev yang dibentuk oleh PIHAK PERTAMA.

(3) PIHAK KEDUA diharuskan MENYIAPKAN SEMUA DOKUMEN/BUKTI kemajuan pelaksanaan penelitiannya guna kepentingan monev.

(4) Waktu pelaksanaan monev akan ditentukan oleh PIHAK PERTAMA.

KOLOKIUM LAPORAN PENELITIAN
Pasal 9

(1) PIHAK KEDUA wajib menyerahkan **Laporan Penelitian Sementara** sebagai bahan kolokium selambat-lambatnya **8 Oktober.**

(2) Ketua Peneliti wajib hadir dan mempresentasikan hasil penelitiannya pada kolokium **Laporan Penelitian Sementara** yang pelaksanaannya akan diatur oleh PIHAK PERTAMA.

(3) Revisi laporan penelitian yang sudah dikolokiumkan harus mendapatkan pengesahan dari *reviewer* dalam bentuk **Surat Pernyataan** dan dijilid dalam satu kesatuan laporan penelitian.

LAPORAN AKHIR PENELITIAN
Pasal 10

(1) PIHAK KEDUA wajib menyerahkan **Laporan Akhir Penelitian** selambat-lambatnya **2 (dua) pekan** setelah dikolokiumkan.

(2) Sistematika dan format laporan penelitian mengacu pada ketentuan dalam Pedoman Penelitian yang dikeluarkan oleh LPPM dan ketentuan lain yang berlaku.

(3) Berkas Laporan Akhir Penelitian yang diserahkan kepada PIHAK PERTAMA harus dilampiri:
(a) artikel/draft publikasi ilmiah;
(b) naskah/draft seminar (prosiding) dan sertifikat seminar;
(c) lampiran lain yang dianggap perlu (seperti angket atau lainnya);
(d) Profil Penelitian;
(e) Borang Capaian Luaran Penelitian;
(f) Form Pembimbingan (khusus skema PDP)
(g) Daftar hadir kolokium laporan penelitian; dan
(h) produk penelitian (naskah buku ajar, modul, naskah akademik, dan sejenisnya) atau dokumentasi/fotonya jika produk penelitian berupa barang atau perangkat keras *(hardware)* yang disertai penjelasan ringkas alat dan petunjuk pemakaiannya.

Komponen (a) sampai dengan (g) dijilid dalam satu kesatuan sebagai berkas laporan akhir penelitian.

Komponan (h) dijilid terpisah dari berkas laporan akhir penelitian, kecuali dokumentasi/foto produk penelitian.

(4) Laporan Akhir Penelitian sebagaimana tersebut pada ayat (1), (2), dan (3) memenuhi ketentuan sebagai berikut:
a. bentuk/ukuran kertas A4;
b. warna cover sesuai ketentuan;
c. di bawah bagian cover ditulis:

PENELITIAN INI DILAKSANAKAN ATAS BIAYA
ANGGARAN DAN PENDAPATAN DAN BELANJA UNIVERSITAS AHMAD DAHLAN
TAHUN AKADEMIK 2018/2019
NOMOR KONTRAK: PHB-062/SP3/LPPM-UAD/IV/2019

(5) Berkas Laporan Akhir Penelitian sebagaimana tersebut dalam ayat (1) diserahkan kepada PIHAK PERTAMA sebagai berikut.
1 eksemplar **ASLI** untuk PIHAK PERTAMA;
1 eksemplar untuk PIHAK KEDUA;
1 eksemplar untuk arsip Program Studi;

(6) PIHAK KEDUA wajib mengunggah file laporan akhir penelitian secara lengkap pada alamat *http://www.simpel.uad.ac.id* melalui akun portal ketua peneliti dengan format file PDF.

KEWAJIBAN UNGGAH LAPORAN PADA PORTAL UAD

Pasal 11

(1) PIHAK KEDUA wajib mengunggah berkas Laporan Akhir Penelitian pada *www.portal.uad.ac.id* melalui akun portal masing-masing peneliti.
(2) Berkas Laporan Akhir Penelitian sebagaimana dimaksud pada ayat (1) yang terdiri dari:
   i. Abstrak (PDF).
   ii. Laporan Akhir Final (PDF).
   iii. Profil Penelitian (PDF).
   iv. Borang Capaian Luaran Penelitian (PDF).

SANKSI DAN PEMUTUSAN PERJANJIAN PENELITIAN

Pasal 12

(1) PIHAK PERTAMA berhak memberikan peringatan dan atau teguran atas kelalaian dan atau pelanggaran yang dilakukan oleh PIHAK KEDUA yang mengakibatkan tidak dapat terpenuhinya kontrak penelitian ini.
(2) PIHAK PERTAMA berhak melakukan pemutusan perjanjian penelitian, jika PIHAK KEDUA tidak mengindahkan peringatan yang diberikan oleh PIHAK PERTAMA.
(3) Segala kerugian material maupun finansial yang disebabkan akibat kelalaian PIHAK KEDUA, maka sepenuhnya menjadi tanggungjawab PIHAK KEDUA.
(4) Jenis sanksi yang diberikan dapat berupa:
   (a) tidak diperkenankannya mengajukan proposal penelitian pada tahun anggaran berikutnya sampai kewajibannya terselesaikan; dan atau
   (b) tidak dapat mencairkan dana tahap 2; dan atau
   (c) mengembalikan dana yang telah diterima oleh PIHAK KEDUA.

KEADAAN MEMAKSA (*FORCE MAJEUR*)

Pasal 13

Ketentuan dalam Pasal 10 tersebut di atas tidak berlaku dalam keadaan sebagai berikut:

a. Keadaan Memaksa (*force majeur*)
b. PIHAK PERTAMA menyetujui atas terjadinya keterlambatan yang didasarkan pada pemberitahuan sebelumnya oleh PIHAK KEDUA kepada PIHAK PERTAMA dengan **surat pemberitahuan** mengenai kemungkinan terjadinya keterlambatan dalam penyelesaian kegiatan penelitian sebagaimana dimaksud dalam Pasal 1 dan Pasal 3; dan sebaliknya PIHAK KEDUA menyetujui terjadinya keterlambatan pembayaran sebagai akibat keterlambatan dalam penyelesaian perjanjian penelitian.

Pasal 14

(1) Keadaan Memaksa (*force majeur*) sebagaimana yang dimaksud dalam Pasal 11 ayat (1) adalah peristiwa-peristiwa yang secara langsung mempengaruhi pelaksanaan perjanjian serta terjadi di luar kekuasaan dan kemampuan PIHAK KEDUA ataupun PIHAK PERTAMA.
(2) Peristiwa yang tergolong dalam keadaan memaksa (*force majeur*) antara lain berupa bencana alam, pemogokan, wabah penyakit, huru-hara, pemberontakan, perang, waktu kerja diperpendek oleh pemerintah, kebakaran dan atau peraturan pemerintah mengenai keadaan bahaya serta hal-hal lainnya yang dipersamakan dengan itu, sehingga PIHAK KEDUA ataupun PIHAK PERTAMA terpaksa tidak dapat memenuhi kewajibannya.
(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib dibenarkan oleh penguasa setempat dan diberitahukan dengan Surat oleh PIHAK KEDUA atau PIHAK PERTAMA kepada PIHAK PERTAMA atau PIHAK KEDUA selambat-lambatnya 7 (tujuh) hari sejak terjadinya peristiwa yang dikategorikan sebagai Keadaan Memaksa (*force majeur*).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh kedua belah pihak jika keadaan *force majeur* dinyatakan telah selesai.

PENYELESAIAN PERSELISIHAN

Pasal 15

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

PENGUNDURAN DIRI

Pasal 16

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh Dekan fakultas ketua peneliti yang bersangkutan; dan bagi peneliti skim PDP ditambah persetujuan Dosen Pembimbing.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA

LAIN-LAIN

Pasal 17

(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (*addendum*), yang merupakan kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Pemberitahuan dan/atau surat menyurat dari PIHAK KEDUA kepada PIHAK PERTAMA dialamatkan kepada Kepala Lembaga Penelitian dan Pengembangan Universitas Ahmad Dahlan.

Pasal 18

(1) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh kedua belah pihak.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini dibuat rangkap 2 (dua); bermeterai cukup pada kedua belah pihak; dan masing-masing memiliki kekuatan hukum yang sama. Biaya meterai dibebankan kepada PIHAK KEDUA.

PIHAK PERTAMA,	PIHAK KE DUA,
	METERAI TEMPEL EDBFDAFF688389931 6000 ENAM RIBU RUPIAH
Dr. Widodo, M.Si.	**IMAM RIADI, Dr., M.Kom**
NIP: 196002211987091001	NIP/NIY. 6002-0397

PERSONALIA PENELITIAN

Judul Penelitian : Pengembangan Cybersecurity Layanan Akademik Pada Perguruan Tinggi Menggunakan Framework Cobit 5

Skema : Penelitian Hibah Bersaing

1. Ketua Peneliti

a. Nama Lengkap dan Gelar : Dr. Imam Riadi, M. Kom
b. NIDN/NIY/NIP : 0510088001/60020397/19700206200501 1 001
c. Fakultas/Program Studi : Sains dan Teknologi Terapan/Sistem Informasi
d. Jabatan Akademik : TP/AA/L/LK/GB
e. Alokasi waktu untuk penelitian : 10 minggu
f. Tugas dalam penelitian : 1. .....
2. .....

2. Anggota Peneliti 1

a. Nama Lengkap dan Gelar : Iwan Tri Riyadi Yanto, S.Si., M. IT
b. NIDN/NIY/NIP : 0514068502/60120678
c. Fakultas/Program Studi : Sains dan Teknologi Terapan/Sistem Informasi
d. Jabatan Akademik : TP/AA/L/LK/GB
e. Alokasi waktu untuk penelitian : 10 jam/minggu
f. Tugas dalam penelitian : 1. .....
2. .....

3. Keterlibatan Mahasiswa

No	Nama Mahasiswa dan NIM	Program Studi	Tugas dalam Tim	Judul Tugas Akhir**)
1	..... NIM:			
2	..... NIM:			

Catatan:

*) = khusus skema PDP, nama anggota peneliti diganti dengan nama Pembimbing Penelitian

**) = jika dalam kegiatan ini, mahasiswa juga sekaligus dalam rangka menyelesaikan Tugas Akhir (skripsi/thesis).

BIODATA KETUA DAN ANGGOTA TIM PENGUSUL

A. Identitas Diri

1	Nama Lengkap dan Gelar	Dr. Imam Riadi, M.Kom
2	Jenis Kelamin	Laki-Laki
3	Jabatan Fungsional	Lektor
4	NIP/NIK/NIDN	60020397
5	Tempat dan Tanggal Lahir	0510088001
6	E-mail	Kudus, 10 Agustus 1980
7	Nomor HP	imam.riadi@mti.uad.ac.id
9	Program Studi/Fakultas	0274-3049191 / 08156854308
10	Alamat Kantor	Jln. Prof. Dr. Soepomo, Janturan, Yogyakarta
11	Nomor Telepon/Faks Kantor	0274 – 563515 / 0274 – 564604
12	Lulusan yang telah dihasilkan	S1 > 50 orang
13. Mata Kuliah yang diampu		1. Jaringan Komputer 2. Sekuritas Komputer 3. Administrasi Sistem dan Jaringan 4. Organisasi dan Arsitektur Komputer 5. Forensik Digital

A. Riwayat Pendidikan

	S-1	S-2	S-3
Nama Perguruan Tinggi	Universitas Negeri Yogyakarta	Universitas Gadjah Mada	Universitas Gadjah Mada
Bidang Ilmu	Pendidikan Teknik Komputer/Teknik Elektro	Ilmu Komputer	Ilmu Komputer

Tahun Masuk - Lulus	1997 – 2001	2001 – 2013	2008 - 2014
Judul Skripsi / Tesis / Disertasi	*Internet Gateway* Berbasis Linux	Analisis Kelemahan *Cross Site Scipting* pada PHP Nuke untuk Keamanan Website	Framework Untuk Forensik Internet *Menggunakan k-means Clustering* dan *Horizontal Partitioning*
Nama Pembimbing/Promotor	Drs. Priyanto, M.Kom	Drs. Jazi Eko Istiyanto, M.Sc., Ph.D	1. Prof. Drs. Jazi Eko Istiyanto, M.Sc., Ph.D 2. Dr.techn. Ahmad Ashari, M.Kom. 3. Prof. Drs. Subanar, Ph.D

B. Pengalaman Penelitian dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah
1	2015	Rancang Bangun Aplikasi Paket Mahasiswa Baru UAD Berbasis Android Terintegrasi Dengan Sistem	PKK UAD	18.8

		Informasi Perwalian Dan Sistem Informasi Manajemen Ruangan		
2	2015	Model Management Risiko Layanan Akademik Pada Mahasiswa yang Berbasis Pada Sistem Informasi dan Teknologi Di Universitas Ahmad Dahlan Yogyakarta	PKK UAD	17.2
3	2016	Evaluasi dan Pengembangan Aplikasi for Student's UAD Dalam Sistem Operasi Android	PKK UAD	19
4	2016	Tata Kelola IT untuk Manajemen Resiko Layanan Akademik Menggunakan COBIT 5	PKK UAD	20
5	2016	Pengembangan dan Evaluasi Sistem Notifikasi Berbasis Android Untuk Penentuan Obat Pasien Bagi Farmasi Klinik.	PHB DIKTI	50

C. Pengalaman Pengabdian Masyarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Masyarakat	Pendanaan	
			Sumber	Jumlah
1	2016	Tim Pendamping Program 1 Juta Domain	KOMINFO	25

D. Publikasi Artikel Ilmiah di Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor/Tahun
1	Forensic SIM Card Cloning Using Authentication Algorithm	IJEIE (International Journal of Electronics and Information Engineering)	Vol 4. No.2 Juni 2016 ISSN 2313-1527 ISSN 2313-1535
2	Forensics Analysis From Cloud Storage on Proprietary Operating System	IJCA (International Journal of Computer Appliacation)	Volume xx /Number x ISSN : 0975-8887 ISBN: 973-93-80886-50-0
3	A Maturity Level Framework for Measurement of Information Security Performance	IJCA (International Journal of Computer Appliacation)	Volume 141/Number 8 ISBN: 973-93-80893-10-1
4	An Analysis of Vulnerability Web Against Attack Unrestricted Image File Upload	Computer Engineering and Applications Journal	Vol 5, No 1, Februari 2016 ISSN: 2252-4274 ISSN: 2252-5459
5	Denial of Service Log Analysis Using Density K-Means Method	JATIT (*Journal of Theoretical and Applied Information Technology*)	Vol 83, No.2, Januari 2016 ISSN : 1992-8645, e-ISSN: 1817-3195
6	Merging of Vigenére cipher with XTEA Block cipher to Encryption Digital documents	IJCA (International Journal of Computer Appliacation)	Volume 132/Number 1 ISSN : 0975-8887 ISBN: 973-93-80890-46-8

7	Implementation of integration Blowfish Cryptography Methods With Blend Steganography To Improve Security Text Messages	IJCA (International Journal of Computer Appliacation)	Volume 132/Number 7 ISSN : 0975-8887 ISBN: 973-93-80890-52-3
8	Analysis of Smartphone Users Awareness Activities Cybercrime	IJCA (International Journal of Computer Appliacation)	Volume 129/Number 2 ISSN : 0975-8887 ISBN: 973-93-80889-91-2
9	Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA)	IJCA (International Journal of Computer Appliacation)	Volume 123/Number 6 ISSN : 0975-8887 ISBN: 973-93-80888-83-5
10	Implementation of Malware Analysis using Static and Dynamic Analysis Method	IJCA (International Journal of Computer Application)	Volume 117/Number 6 ISSN : 0975-8887 ISBN: 973-93-80886-50-0
11	Internet Forensics Framework Based-on Clustering	IJACSA (*International Journal of Advanced Computer Scieence and Application)*	Vol. 4 Issue 12, December 2013. ISSN: 2156-5570 ISSN: 2158-107X
12	Log Analysis Techniques using *Clustering in Network Forensics*	IJCSIS (International Journal of Computer Science & Information Security)	Vol.10 No.7, July 2012. ISSN: 1947-5500
13	A Fuzzy Topsis Multiple-Attribute Decision Making For Scholarship Selection	TELKOMNIKA (Telekomunikasi	Vol.9 No.1, April 2011 ISSN: 1693-6930

		Komputasu Elektronika Kendali)	

E. Pemakalah Seminar Ilmiah (*Oral Presentation*) dalam 5 Tahun Terakhir

No	Nama Pertemuan Ilmiah / Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
1	Confast 2016 (*Conferences on Fundamental and Applied Science and Technology)*	*An Analysis of Weakness Attack SQL Injection to Improve Security Website*	25-26 Januari 2016, UAD, Yogyakarta, Indonesia

F. Karya Buku dalam 5 Tahun Terakhir

No	Judul Buku	Tahun	Jumlah Halaman	Penerbit

G. Perolehan HKI dalam 5 Tahun Terakhir

No	Judul / Tema HKI	Tahun	Jenis	Nomor P / ID

H. Pengalaman Merumuskan KebijakanPublik / Rekayasa Sosial lainnya dalam 5 Tahun Terakhir

No	Judul / Tema / Jenis Rekayasa Sosial Lainnya yang Telah Diterapkan	Tahun	Tempat Penerapan	Respon Masyarakat

I. Penghargaan dalam 5 Tahun Terakhir (dari pemerintah, asosiasi dan institusi lainnya)

No	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila dikemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sangsi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan penelitian unggulan program studi.

BIODATA TIM PENELITI

A. Identitas Diri

1	Nama Lengkap (dengan gelar)	Iwan Tri Riyadi Yanto, S.Si., M.IT.
2	Jenis Kelamin	Laki-Laki
3	Jabatan Fungsional	Asisten Ahli
4	NIY	60120678
5	NIDN	0514068502
6	Tempat dan Tanggal Lahir	Klaten, 14 Juni 1985
7	Email	yanto.itr@is.uad.ac.id
8	Nomor Telp / HP	085729277133
9	Alamat Kantor	Jln. Prof. Dr. Soepomo, Janturan, Yogyakarta
10	Nomor Telp / Faks	0274 – 563515 / 0274 – 564604
11	Lulusan yang dihasilkan	-
12	Mata Kuliah yang diampu	1. Statistik dan probabilitas 2. Matematika diskrit 3. Matematika dasar

B. Riwayat Pendidikan

	S-1	S-2	S-3
Nama Perguruan Tinggi	Universitas Ahmad Dahlan	Tun Hussein On Malaysia	-
Bidang Ilmu	Optimasi	Data mining	
Tahun Masuk - Lulus	2003-2007	2009-2011	
Judul Skripsi / Tesis / Disertasi	*Interior Point Methods for Solving Linear Programming*	Rough set for web clustering	
Nama Pembimbing/Promotor	Dr. Julan Hernadi., M.Si.	Prof. Dr. Mustafa Mat Deris.	

C. Pengalaman Penelitian dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah
1	2013	MCLA Categorical Data Clustering Based On Maximal Cardinality	UAD	1.500.000
2	2015	Multi step chicken algorithm	UAD	15.000.000
3	2015	Reducing complexity of MAR	UAD	6.500.000
4	2016	Soft maximum Association rule for web mining	DIKTI	11.500.00

5	2016	Fuzzy Clustering menggunakan	UAD	7.500.000

		Fuzzy C-Mean dan Chicken Swarm Optimization		
6	2016	Fuzzy K Partition Based on Metaheuristic Algorithm for Categorical DataFuzzy K Partition Based on Metaheuristic Algorithm for Categorical Data	UAD	7.500.000

D. Pengalaman Pengabdian Masyarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian masyarakat	Pendanaan Sumber	Jumlah
1	2012	Wokshop Penelitian tindakan kelas	UnMuh	-
			Ponorogo	
2	2015	Pelatihan pembuatan perngkap	UAD	500.000
		nyamuk dari botol bekas di desa		
		margosuluh		
3	2015	Pelatihan macromedia flash guru	UAD	500.000
		SMP N 1 Minggir		
4	2015	Pengenalan Dan Pelatihan Internet	UAD	5.000.000
		Untuk Belajar Anak Bagi		
		Masyarakat Geneng Prambanan		
		Kabupaten Klaten		
5	2016	Pengenalan Dan Pelatihan Internet	UAD	5.000.000
		Untuk Belajar Anak Bagi Masyarakat		
		Geneng Prambanan Kabupaten Klaten		

E. Publikasi Artikel Ilmiah di Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor/ Tahun
1	Minimum Error clsification	SERSC	2013
2	Ringed seal search for global optimization via a sensitive search model	Plos One	Januari 2016
3	Automatic differentiation based for particle swarm optimization Steepest descent direction	IJAIN	Juny 2015
4	Alternative Technique reducing complexity of Maximum Attribute Relation	Telkomnika	Desember 2015

F. Pemakalah Seminar Ilmiah (*Oral Presentation*) dalam 5 Tahun Terakhir

1	SCDM 2016	A Categorical Data Clustering Technique based on Classification Quality of Variable Precision Rough Set Model	Bandung, 18-20 Agustus 2016
2	SCDM 2016	A Data Clustering Framework based on Chicken Swarm Optimization	Bandung, 18-20 Agustus 2016
3	SCDM 2016	Histogram Thresholding for Automatic Color Segmentation based on k-means Clustering	Bandung, 18-20 Agustus 2016
4	SCDM 2016	Application of Wavelet De-noising Filters in Mammogram Images Classification Using Fuzzy Soft Set	Bandung, 18-20 Agustus 2016
5	SCDM 2016	An Application of Rough Set Theory for Clustering Performance Expectancy of Indonesian e-Government Dataset.	Bandung, 18-20 Agustus 2016

G. Karya Buku dalam 5 Tahun Terakhir

No	Judul Buku	Tahun	Jumlah Halaman	Penerbit

H. Perolehan HKI dalam 5 Tahun Terakhir

No	Judul / Tema HKI	Tahun	Jenis	Nomor P / ID

I. Pengalaman Merumuskan KebijakanPublik / Rekayasa Sosial lainnya dalam 5 Tahun Terakhir

No	Judul / Tema / Jenis Rekayasa Sosial Lainnya yang Telah Diterapkan	Tahun	Tempat Penerapan	Respon Masyarakat

J. Penghargaan dalam 5 Tahun Terakhir (dari pemerintah, asosiasi dan institusi lainnya)

No	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila dikemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sangsi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan penelitian unggulan program studi.

Pengembangan Cybersecurity Layanan Akademik Pada Perguruan Tinggi Menggunakan Framework Cobit 5

Peneliti

Dr. Imam Riadi, M.Kom.

Sistem Informasi/Fakultas Sains dan Teknologi Terapan
Universitas Ahmad Dahlan
imam.riadi@is.uad.ac.id

Iwan Tri Riyadi Yanto, S.Si., MIT.

Informasi/Fakultas Sains dan Teknologi Terapan
Universitas Ahmad Dahlan
yanto.itr@is.uad.ac.id

Ringkasan Eksekutif

Sistem Informasi Akademik (SIA) menjadi bagian yang sangat penting bagi perguruan tinggi untuk menjaga informasi secara optimal dan aman. Teknologi sering disalahgunakan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menimbulkan terjadinya ancaman. Dalam rangka mencegah hal-hal tersebut terjadi, maka perlu diketahui tata kelola keamanan SIA perguruan tinggi dengan cara melakukan evaluasi. Penelitian ini dilakukan untuk mengetahui maturity level pada tata kelola keamanan SIA di perguruan tinggi menggunakan NIST cybersecurity framework.

NIST cybersecurity framework merupakan sebuah metode analisi cybersecurity yang dapat digunakan dalam analisis layanan akademik. Metode ini memeliki 5 fungsi, yaitu identifikasi (identify); perlindungan (protect); deteksi (detect); respon (respond); dan pemulihan (recovery). Framework COBIT 5 akan di jadikan sebagai acuan proess aktivitas dalam fungsi NIST cybersecurity framework. Penelitian ini meghasilkan metode yang efektif terkait pengembangan layanan akademik di perguruan tinggi.

Penelitian ini bertujuan untuk membantu memberikan analisis evaluasi yang tepat digunakan dalam cybersecurity layanan akademik. Objek penelitian ini berada pada layanan akademik di perguruan tinggi, dimulai dengan penggumpulan data terkait dengan layanan akademik. Langkah selanjutnya adalah menganalisis cybersecurity layanan akademik berdasarkan framework COBIT 5. Penelitian ini diharapkan bisa menjadi kajian analisis terkait cybersecurity layanan akademik, sehingga dapat dijadikan rekomendasi dalam perbaikan dan juga pengembangan cybersecurity layanan akademik di perguruan tinggi.

HKI dan Publikasi

1. http://iceat.ast-ptm.or.id/2019/

Latar Belakang

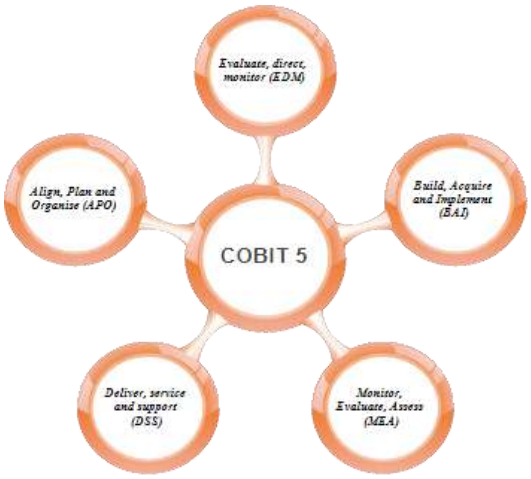
Sistem Informasi Akademik (SIA) menjadi bagian yang sangat penting bagi perguruan tinggi untuk menjaga informasi secara optimal dan aman. Teknologi sering disalahgunakan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menimbulkan terjadinya ancaman. Dalam rangka mencegah hal-hal tersebut terjadi, maka perlu diketahui tata kelola keamanan SIA perguruan tinggi dengan cara melakukan evaluasi. Penelitian ini dilakukan untuk mengetahui maturity level pada tata kelola keamanan SIA di perguruan tinggi menggunakan NIST cybersecurity framework.

Metode

Studi Kasus
Metode ini dilakukan dengan mengumpulkan, membaca serta mempelajari data yang berasal dari berbagai media seperti buku, jurnal, karya tulis atau artikel yang terkait dengan penelitian.
Observasi
Observasi merupakan metode pengumpulan data dengan melakukan pengamatan langsung pada lapangan penelitian. Pada penelitian ini, peneliti melakukan pengamatan langsung pada SIA di perguruan tinggi untuk mengumpulkan kebutuhan pengujian.
Wawancara
Peneliti melakukan wawancara secara langsung kepada narasumber yang berwenang tehadap layanan akademik di perguruan tinggi.
Kuesioner
Metode kuesioner metode ini dilakukan pengumpulan data dengan NIST Cybersecurity Framework dan mengadopsi dari framework COBIT 5.

Hasil dan Manfaat

Sub-domain DSS05 Mengelola layanan keamanan adalah prosedur yang baik untuk digunakan dalam implementasi dan mega-audit terkait dengan keamanan sistem informasi akademik dan CMMI adalah metode penilaian yang baik dalam sistem audit lembaga. Berdasarkan penelitian yang dilakukan di BISKOM, Universitas Ahmad Dahlan menerima Tingkat Kematangan 4.458 sehingga menetapkan bahwa tingkat kematangan saat ini berada pada tingkat Dikelola dan Terukur. Level ini, institusi semakin disadarkan akan perkembangan teknologi. Lembaga telah menerapkan konsep kuantifikasi dalam setiap proses, dan selalu dipantau dan dikendalikan untuk kinerja.



Gambar. Domain COBIT 5

Lima domain pada COBIT 5 terdiri dari 37 proses yaitu EDM 5 proses, APO 13 proses, BAI 10 proses, DSS 6 proses, dan MEA 3 proses. Proses yang terdapat pada doamain COBIT 5 harus di gunakan sesuai dengan kebutuhan dan tujuan organisasi yang ada mampu memberikan penilaian dan efiktifitas pada kegiatan implentasi COBIT 5.

BORANG CAPAIAN LUARAN PENELITIAN
SUMBERDANA UAD TAHUN AKADEMIK 2019/2020
SKEMA HIBAH BERSAING

I. IDENTITAS PENELITI

Judul penelitian : Pengembangan Cybersecurity Layanan Akademik Pada Perguruan Tinggi Menggunakan Framework Cobit 5
Ketua Peneliti : Dr. Imam Riadi, M. Kom
NIDN / e-mail : 0510088001/imam.riadi@is.uad.ac.id
Prodi/Fakultas : Sistem Informasi/Sains dan Teknologi Terapan
Anggota Peneliti 1 : Iwan Tri Riyadi, S. Si., MIT
Jenis/Tahap Penelitian : 1. Dasar 2. Terapan 3. Pengembangan
TKT/TRL : 1 / 2 / 3 4 / 5 / 6 7 / 8 / 9

II. CAPAIAN LUARAN PENELITIAN

A. PUBLIKASI ILMIAH

	Keterangan
ARTIKEL JURNAL KE-1*[1]	
Nama jurnal yang dituju	International Conference on Engineering and Applied Technology (ICEAT)
Level jurnal	Internasional
Status	Berputasi*
Impact factor untuk jurnal	-
Judul artikel	Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI)
Status naskah	terbit*
Alamat URL artikel	http://iceat.ast-ptm.or.id/2019/
ARTIKEL JURNAL KE-2, dst.	
Nama jurnal yang dituju	International Conference on Engineering and Applied Technology (ICEAT)
Level jurnal	Internasional
Status	Berputasi*
Impact factor untuk jurnal	-
Judul conference	Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI)
Status naskah	terbit*
Alamat URL artikel	http://iceat.ast-ptm.or.id/2019/

*[1] Jika masih ada artikel ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

B. BUKU AJAR

Buku ke-1*[2]	**Keterangan**
Judul buku	
Penulis	
Penerbit	
No. ISBN	
Buku ke-2, dst.	

*[2] Jika masih ada buku ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

C. PEMBICARA PADA PERTEMUAN ILMIAH (SEMINAR/SIMPOSIUM)

Mengikuti seminar*[3]	**Keterangan**
Pertemuan Ilmiah ke-1	
- Judul Makalah	Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI)
- Nama pertemuan ilmiah	International Conference on Engineering and Applied Technology (ICEAT)
- Tempat pelaksanaan	Sorong
- Waktu pelaksanaan	30 Oktober-1 November2019
- Jenis pertemuan	Conference
- Status naskah	Terbit*
Pertemuan Ilmiah ke-2, dst.	

*[3] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

D. PEMBICARA KUNCI/*KEYNOTE* SPEAKER PADA PERTEMUAN ILMIAH (SEMINAR/SIMPOSIUM)

	Keterangan
- Judul makalah	
- Penulis	
- Penyelenggara	
- Waktu Pelaksanaan	
- Tempat Pelaksanaan	
- Skala pertemuan	Regional/Nasional/Internasional
- Status pertemuan	Sudah dilaksanakan / belum
- Alamat URL artikel	

*[3] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

E. Menjadi Peneliti Tamu (*Visiting Scientist)*

Menjadi peneliti tamu (*visiting scientist*) pada perguruan tinggi lain*[4]	**Nasional**	**Internasional**
- Perguruan tinggi pengundang		
- Lama kegiatan		
- Kegiatan penting yang dilakukan		

*[4] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

F. Hak Kekayaan Intelektual dan Lainnya

Jenis HKI	**Uraian**
Paten	Tuliskan judul paten adan tanggal pengajuannya
Hak Cipta	Tuliskan bentuk dan atau nama/judul hak cipta dan tanggal pengajuannya
TEKNOLOGI TEPAT GUNA	Jelaskan nama TTG dan pemanfaatan serta penggunanya
REKAYASA SOSIAL	Uraikan kebijakan publik yang sedang atau sudah dapat diubah
JEJARING KERJA SAMA	Uraikan kapan jejaring dibentuk dan kegiatannya sampai saat ini, baik antarpeneliti maupun antarlembaga
PENGHARGAAN	Uraikan penghargaan yang diterima sebagai peneliti, baik dari pemerintah atau asosiasi profesi
LAINNYA	Tulis dan uraikan luaran HKI lainnya

Yogyakarta, 31 Januari 2020
Ketua Peneliti,

Dr. Imam Riadi, M. Kom

Analysis of Academic Service Cybersecurity in University Based on Framework COBIT 5 Using CMMI

Imam Riadi[1, a)] Iwan Tri Riyadi Yanto[2, b)] Eko Handoyo[3, c)]

[1]Department of Information System Universitas Ahmad Dahlan Yogyakarta,
[2]*Department of Information System Universitas Ahmad Dahlan Yogyakarta,*
[3]*Department of Computer Engineering Universitas Muhammadiyah Lamonggan,*

[a)] imam.riadi@is.uad.ac.id
[b)] yanto.itr@is.uad.ac.id
[c)] ekohandoyo@umla.ac.id

Abstract. A secure academic information system is part of the college. The security of academic information systems is very important to maintain information optimally and safely. Along with the development of technology, academic information systems are often misused by some irresponsible parties that can cause threats. To prevent these things from happening, it is necessary to know the extent to which the security of the academic information system of universities is conducted by evaluating. So the research was conducted to determine the Maturity Level on the governance of the security of University Ahmad Dahlan academic information system by using the COBIT 5 framework on the DSS05 domain. The DSS05 domain on COBIT 5 is a good framework to be used in implementing and evaluating related to the security of academic information systems. Whereas to find out the achievement of evaluation of academic information system security level, CMMI method is needed. The combination of the COBIT 5 framework on the DSS05 domain using the CMMI method in academic information system security is able to provide a level of achievement in the form of a Maturity Level value. The results of the COBIT 5 framework analysis of the DSS05 domain use the CMMI method to get a Maturity level of 4,458 so that it determines the achievement of the evaluation of academic information systems at the tertiary level is Managed and Measurable. This level, universities are increasingly open to technological developments. Universities have applied the quantification concept in each process, and are always monitored and controlled for performance in the security of academic information systems.

Keywords— CMMI, COBIT 5, Security SIA, Managed and Measurable, Maturity Level

I. INTRODUCTION

Companies or institutions place information technology as a thing that can support the achievement of the company's strategic plan to achieve the goals of the company or institution's vision, mission and goals. Information technology will get effective results if it uses good governance in its use and is able to be evaluated and evaluated [1]. Information systems are systems that contain SPD networks (systems processing data), which are equipped with communication channels used in data organization systems [2]. There are various concepts of information systems, compatibility is one of the keys to the successful implementation and acceptance of information systems [3]. Along with the development of technology, it is often misused by some irresponsible parties that can cause threats [4]. Academic information systems must provide the security, privacy and integrity of data processed, so that the performance of academic information systems is also an important part that must be considered so that academic information systems can be used optimally and safely [5]. The application of information security systems aims to overcome all problems and constraints, both technically and non-technically which can affect the performance of the system such as availability, confidentiality and integrity factors so that the level of information security can be assessed [6]. As in **Figure 1**.

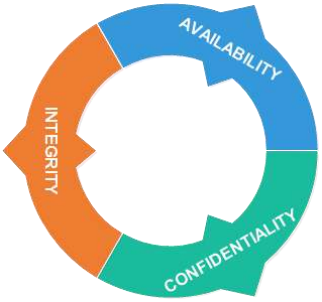


Figure 1 Information security aspects

The existence of a security problem triggers a procedure for controlling access rights to an information system [7]. A good information system security must apply the standard Deming cycle of quality [8]. The security of academic information systems can be audited with various standards such as COBIT, COSO, ITIL, CMM, BS779, ISO 9000. COBIT (Control Objectives for Information and related Technology) is a standard guide to information technology management practices and a set of best practices documentation for IT governance that can help auditors, management, and users to bridge the gap between business risk, control needs, and technical issues [8]. All organizations can adjust COBIT 5 for their various purposes, and are able to evaluate the organization in achieving its intended goals [9]. Domain DSS (Deliver, Service and Support) is related to system delivery and service support needed by the system, which includes service, security and continuity management, service support for users, and data management and operational facilities so that it is more integrated in the domain that provides services well [8]. DSS domains have sub-domain DSS05 wherein this sub-domain is a more intensive procedure for information security. The method that can be used in evaluating the achievement of evaluation is CMMI. Capability Maturity Model Integration (CMMI) is a model approach to assess the scale of capability and maturity of a software organization. The history of CMMI at the beginning was known as the Capability Maturity Model (CMM) which was built and developed by the Software Engineering Institute in Pittsburgh in 1987[10]. The CMMI method in academic information system security is able to provide a level of achievement in the form of Maturity Level values. So as to be able to give a decision on the extent to which the security process of academic information systems that have been run by universities.

This study aims to conduct an evaluation related to the security management of academic information systems that have been implemented at Ahmad Dahlan University. This study aims to obtain the value of the level of information system security of an institution, so that recommendations and innovations can be made for the security of information systems in these institutions. So that the institution can provide security and comfort for the use of the information system.

II. METHODS

A. DSS05 Framework COBIT 5

The DSS05 sub-domain is part of the DSS domain (Deliver, Service and Support). As in **Figure 2.**

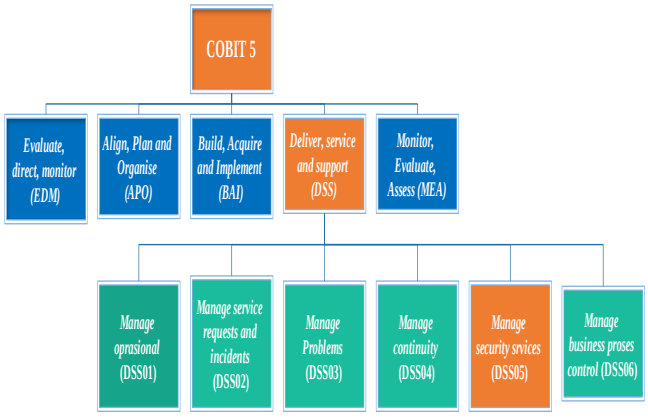


Figure 2. DSS05 scheme

The DSS05 sub-domain is managing security services where these sub-domains are grouped in 7 processes. The seven processes carry out some activities or statements of the 49 statements as follows [11]:

- Protect against malware (DSS05.01) where this process carries out and maintains existing precautions, detective and repairs (especially the latest security patches and virus controls) throughout the company to protect information systems and technology from malware (e.g., Viruses, worms, spyware, spam).
- Manage network and connectivity security (DSS05.02) where this process uses security measures and related management procedures to protect information from all methods of connectivity.
- Manage endpoint security (DSS05.03) where this process provides assurance of end points (e.g., Laptops, desktops, servers, and other cellular and cellular networks or software) guaranteed to be the same or greater than the requirements approved security.
- Manage user identity and logical access (DSS05.04) This process provides certainty for all users to have the right to access information in accordance with business needs. They and coordinate with the business division that manages access rights.
- Manage physical access to IT assets (DSS05.05) this process determines and applies procedures to give, limit and revoke access to physical buildings. Buildings and areas according to business needs, including emergencies. Access to buildings, buildings and areas must be justified, ratified, recorded and monitored.
- Manage sensitive documents and output devices (DSS05.06) where this process establishes physical security. In terms of documents relating to agencies. So that all output documents are standardized in security.
- Monitor the infrastructure for security-related events (DSS 05.07) where this process uses intrusion detection tools, to monitor infrastructure for unauthorized access rights and ensure that every event is integrated with monitoring events and managing events.

B. Capability Maturity Model Integration (CMMI)

CMMI has a streamlined assessment process. The assessment was based on questionnaires and was developed specifically to get software that could support process improvement. CMMI is a maturity method that can be used to improve processes within the institution. The purpose of using the CMMI within an institution is to improve the process of developing and improving the software product of the institution [12].

According to [13] CMMI has Capability Level. Capability Level is a model to describe how each core process runs within an institution. Capability Level has 6 levels for each core process, namely. As in **Figure 3.**

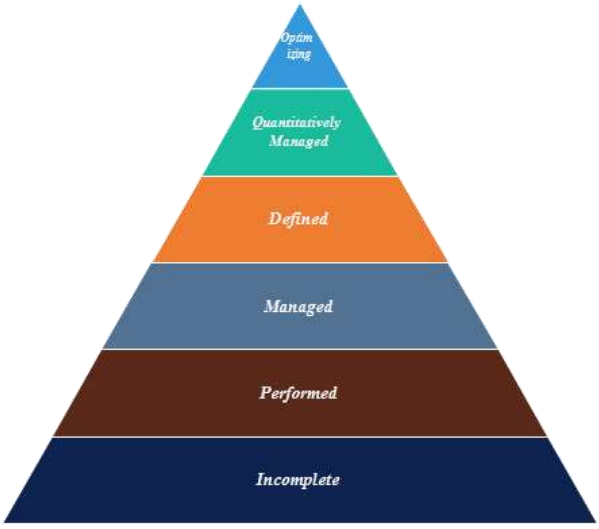


Figure 3. Capability Level CMMI

According to [13] The CMMI model places, institutions in 5 Maturity Levels or CMMI levels, namely. As in **Figure 4.**

Figure 4. Maturity Level CMMI

III. RESULT AND DISCUSSION

This section will present a structured process method. analysis of the implementation and measurement of the maturity level of the information system with the framework COBIT 5 sub-domain DSS05 and CMMI.

A. Observation of the Academic Information System Process

This process conducts interviews directly with the resource person who has authority in the security of the academic information system at University Ahmad Dahlan, where the results are that BISKOM UAD uses an academic information system to be active in 2008, the beginning of the information system created and developed by vendors (Gama Techno) after that, in 2017 it was able to migrate to a new system where the system was developed by BISKOM UAD itself. Where in this migration is due to the development of information systems technology, so it is considered necessary to do the migration to maintain the stability and security of the information system.

The purpose of the academic system of University Ahmad Dahlan it is:

- To manage academic activities in University Ahmad Dahlan.
- Providing convenience to the community, namely lecturers, students, staff and BAA in the academic process.

As time goes on the use of information systems also experiences, obstacles, problems and threats to information systems. The problems, obstacles and threats that often occur are as follows:

- There are several systems that have not been well integrated.
- When the online KRS happened the server was down.
- It often happens to forget your username and password.
- The process of data connection or transmission is slow.
- Virus and malware attacks.

The BISKOM UAD standardization and audit process applies ISO 9000 where the standard is used for standards for quality management systems (SMM) which are aggregated with all bureaus in all institutions. This process also discusses the determination of respondents who will provide detailed information related to information on the security of existing academic information systems. The selection of respondent samples using purposive sampling technique, which is the selection of respondents 'samples determined by researchers on the grounds that identification of respondents' samples is done by referring to personal competencies that interact directly with IT governance [14]. Interviews get 2 respondents who are directly concerned with the field of information system security within the institution.

B. DSS05 Mapping Based on the COBIT Framework 5

This process is a compilation of DSS05 domain conformity activities with questions to be made in the questionnaire. because of the limitations of our writing, we only list one of the 7 DSS05 sub-domain processes, namely DSS05.01. The DSS05.01 process consists of 6 activities, as in **table 1.**

Table 1 Protect against malware activity

Protect against malware (DSS05.01)	
No	**Activity Questions**
1	Obtain information about malicious software and how to handle it..
2	Install and activate anti-virus on your PC.
3	Is anti virus on the PC always updated.
4	Regularly review and evaluate information about potential malware threats.
5	Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information.
6	Conduct periodic training on malware in the use of e-mail and the Internet.

C. Preparation of Questionnaires with a combination of DSS05 and Capability Level

This process is carried out by questionnaires based on the standard on DSS05 Framework COBIT 5 by combining with the capability level of CMMI standards so that the form of a questionnaire can be obtained that is able to answer the needs of the information system security in the installation. To simplify the reading process, the color differences for each decision are made in Capability Level and Maturity Level as in **table 2.**

Table 2. Process Color Maps

Color	**Information**	
	Capability Level	***Maturity Level***
Red	*Incomplete*	*Non-Existent Initial*
Purple	*Performed*	*Initial / Ad Hoc*
Yellow	*Managed*	*Repeatable But Invinitve*
Blue	*Defined*	*Define Process*
Orange	*Quantitatively Managed*	*Managed and Measurable*
Green	*Optimizing*	*Optimized*

Where in this questionnaire there are 6 assessments for processes with capability level CMMI as in **Table 3.**

Table 3. Assessment of IT processes with CMMI capability level

Nilai	***Capability Level CMMI***	**Proses TI**
0	*Incomplete*	Are not done
1	*Performed*	Done, not periodically
2	*Managed*	Performed periodically
3	*Defined*	Done with SOP
4	*Quantitatively Managed*	Performed and monitored
5	*Optimizing*	Done, monitored and developed

The assessment of the IT process in **Table 3** is combined with the standard COBIT 5 DSS05 framework in **Table 1,** as in **Table 4.**

Table 4. Questionnaire Form

Protect against malware (DSS05.01)							
	Activity	**Answer**					
		0	**1**	**2**	**3**	**4**	**5**
1	Obtain information about malicious software and how to handle it.						
2	Install and activate anti-virus on your PC.						
3	Is anti virus on PC always updated.						

4	Regularly review and evaluate information about potential malware threats.
5	Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information.
6	Conduct periodic training on malware in the use of e-mail and the Internet.

D. Calculation of Security SIA Maturity Level

This section will explain the results of the analysis of the implementation and measurement of the performance of the maturity level of academic information systems obtained from the results of questionnaires and interviews in accordance with the framework 5 COBIT domain DSS05. To identify the extent to which the company or organization meets good information security standards, can use the framework identification represented at a level of maturity that has a level of grouping capability of the company, as described in **Table 5.**

Table 5. Value of maturity level criteria

Criteria	Information
0 – 0.50	*Non-Existent Initial*
0.51 – 1.50	*Initial / 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*

The results of the questionnaire that has been given to the respondent and filled in by the respondent get results. Because the page is limited, the data displayed is only on DSS05.01. As in **Table 6.**

Table 6. The results of the questionnaire

DSS05	Responden 1	Responden 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

Furthermore, the correlation between level values and absolute values that are done by calculation in the form of an index uses a mathematical formula. The mathematical equation to determine the index value is as follows [15]:

$$Indeks = \frac{\sum Most\ Question\ Answers}{\sum Questionnaire\ Questions}$$

After getting the index, we can get the current Maturity Level (present). This value is the accumulated value of the process that is running on the institution. as in **table 6.**

Table 6. Existing Maturity Value

DSS05	*Value of Maturity Level Existing*
Protect against malware	5,00
Manage network and connectivity security	5,00
Manage endpoint security	4,39
Manage user identity and logical access	4,88

Manage physical access to IT assets	4,64
Manage sensitive documents and output devices	3,10
Monitor the infrastructure for security-related events	4,20

E. Gap Maturity Level Calculation

Once the existing Maturity Level values are obtained and Maturity The recommendation level (target) has been determined, then the gap between the current condition and the target to be achieved will be analyzed and identified opportunities from the gap to be optimized. Level gap as in **Figure 5.**

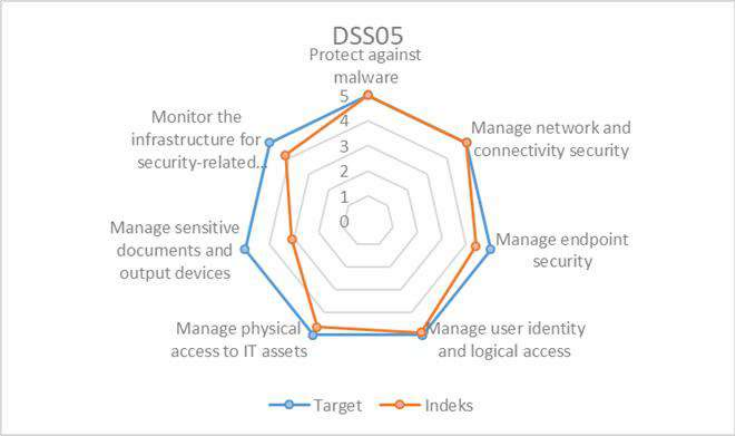


Figure 5. Maturity Level gap

F. Gap Analysis Maturity Level

Based on Gap analysis obtained from the results of the target level to be achieved and the level achieved on DSS05, as in **Figure 5.**, then here is some Gap Maturity Level Analysis. As in **table 7** as follows.

Table 7. Gap Maturity Level Analysis

DSS05	***Maturity Level***
Protect against malware	*Optimized*
Manage network and connectivity security	*Optimized*
Manage endpoint security	*Managed and Measurable*
Manage user identity and logical access	*Optimized*
Manage physical access to IT assets	*Optimized*
Manage sensitive documents and output devices	*Define*
Monitor the infrastructure for security-related events	*Managed and Measurable*

The overall value of Maturity Level on DSS05 will be calculated on average so that it will get the level of Maturity Level in the organization or institution.

$$Maturity\ Level\ DSS05 = \frac{\sum Maturity\ Level}{many\ processes} \qquad (2)$$

$$MLDSS5 = \frac{\begin{array}{c} i(DSS05.01) + i(DSS05.02) + i(DSS05.03) + \\ i(DSS05.04) + i(DSS05.05) + \\ i(DSS05.06) + i(DSS05.07) \end{array}}{mp}$$

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

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

From the calculation results obtained the value of achievement is 4,458 so that it can be set Maturity Level of organization or institution is at the Managed and Measurable level.

G. Compilation of IT Governance Recommendations

After Maturity Level has been determined, the recommendation preparation process will be carried out. Recommendations that can be given to improve the quality of information system security in the agency:

- Protect against malware (DSS05.01) is on the Optimized level where in this level the BISKOM of Ahmad Dahlan University has been able to perform procedures well and is able to develop malware related ones. It is expected that the agency will be able to anticipate the threat of malware more quickly and precisely in detecting malware threats.
- Manage network and connectivity security (DSS05.02) is at the level of Optimized wherein at this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures well and is able to carry out developments related to security of activities. Establish a system that is used to evaluate threats that will arise, documented and monitored. It is expected that the future agencies will be better prepared with the threat of connectivity and be able to quickly provide countermeasures related to connectivity security.
- Manage endpoint security (DSS05.03) in the Managed and Measurable level where in this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures well, only agencies must carry out routine evaluations, at least once a month on information systems that are feared to be potential new threats.
- Manage user identity and logical access (DSS05.04) is on the Optimized level where in this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures properly and is able to develop related access rights of each user. It is expected that companies or institutions are able to provide early warning of the potential security threats to the system and equipment that is owned by all employees.
- Manage physical access to IT assets (DSS05.05) is on the Optimized level where in this level the BISKOM of Ahmad Dahlan University has been able to perform procedures well and is able to carry out development related to physical security. It is hoped that in the future, it will be able to produce and report related to security system trials that are applied and evaluated in a periodic physical shutter.
- Manage sensitive documents and output devices (DSS05.06) in the Define Process level, in this BISKOM, Ahmad Dahlan University has implemented physical security, accounting practices in terms of documents relating to the situation. So that all output documents are standardized in security. It's just hoped that later it will be able to bend documentation and evaluate existing threats.
- Monitor the infrastructure for security-related events (DSS05.07) is in the Managed and Measurable level where in this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures properly using intrusion detection tools, to monitor infrastructure for unauthorized access rights and ensure that every event is integrated with monitoring events and management of events must carry out routine evaluations, at least every semester to the information system which is feared that potential new threats can arise.

IV. CONCLUSION

Sub-domain DSS05 Manage security services is a good procedure to be used in the implementation and mega-audit related to the security of academic information systems and CMMI is a good assessment method in an institution's audit system. Based on the research conducted at the BISKOM, Ahmad Dahlan University received a Maturity Level of 4,458 thus stipulating that the current maturity level is on 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.

REFERENCES

1. I. Riadi and E. Handoyo, “Security Analysis of GRR Rapid Response Network using COBIT 5 Framework,” vol. 10, no. 1, pp. 29–39, 2019.
2. L. F. Fathoni et al., “Application Information System Based Health Services Android,” J. Ilmu Tek. Elektro Komput. dan Inform., vol. 2, no. 1, pp. 39–48, 2016.
3. I. Muslimin, S. P. Hadi, and E. Nugroho, “An Evaluation Model Using Perceived User Technology Organization Fit Variable for Evaluating the Success of Information Systems,” vol. 4, no. 2, pp. 86–94, 2017.

4. Y. W, I. Riadi, and A. Yudhana, “Webserver Security Analysis Using the Penetration Testing Method,” in Annual Research Seminar, 2016, vol. 2, no. 1, pp. 300–304.
5. E. Kurniawan and I. Riadi, “Security level analysis of academic information systems based on standard ISO 27002:2003 using SSE-CMM,” Int. J. Comput. Sci. Inf. Secur., vol. 16, no. 1, pp. 139–147, 2018.
6. Rosmiati, I. Riadi, and Y. Prayudi, “A Maturity Level Framework for Measurement of Information Security Performance Imam Riadi,” Int. J. Comput. Appl., vol. 141, no. 8, pp. 975–8887, 2016.
7. N. Hermaduanti and I. Riadi, “Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN,” J. Theor. Appl. Inf. Technol., vol. 93, no. 2, pp. 287–296, 2016.
8. E. Hicham, B. Boulafdour, M. Makoudi, and B. Regragui, “Information security, 4TH wave,” J. Theor. Appl. Inf. Technol., vol. 43, no. 1, pp. 1–7, 2012.
9. F. Latifi and H. Zarrabi, “A COBIT5 Framework for IoT Risk Management,” Int. J. Comput. Appl., vol. 170, no. 8, pp. 40–43, 2017.
10. V. Konttinen, Towards Disciplined Software Development, no. May. 2016.
11. J. F. Andry, “Audit of IT Governance Based on COBIT 5 Assessments: A Case Study,” J. Teknol. dan Sist. Inf., vol. 2, no. 2, p. 27, 2016.
12. P. D. Syafitri, “Assessment of Quality of Information System Development at Distributor Companies,” J. Sist. Inf. Bisnis, vol. 10, no. 01, pp. 15–27, 2016.
13. CMMI Product Team, CMMI® for Development, Version 1.3. 2010.
14. P. Rahayu and D. I. Sensuse, “Assessment of e-Government Implementation in the Ministry of Education and Culture's PUSTEKOM based on the PEGI method,” J. Sist. Inf. Bisnis, vol. 02, pp. 139–145, 2017.
15. A. Prasetyo and N. Mariana, “Analysis of Information Governance (It Governance) in the Academic Field with Cobit FrameWork Case Study at Stikubank University Semarang,” J. Teknol. Inf. Din., vol. 16, no. 2, pp. 139–149, 2011.

Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI)

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan Yogyakarta
imam.riadi@is.uad.ac.id

Iwan Tri Riyadi Yanto
Department of Information System
Universitas Ahmad Dahlan Yogyakarta
yanto.itr@is.uad.ac.id

Eko Handoyo

Departmen of Computer Engineering
Universitas MuhammadiyahLamonggan
ekohandoyo@umla.ac.id

***Abstrak*— Safe academic services are the most important part of universities. The security of academic services is very important to maintain information optimally and safely. Along with the development of technology, academic information services are often misused by some irresponsible parties that can cause threats. To prevent these things from happening, it is necessary to know the extent of governance of higher education academic information system security by evaluating. So the research was conducted to determine the maturity of the security of Higher Education academic information service security by using the COBIT 5 framework in the DSS05 domain. The DSS05 domain in COBIT 5 is a good framework for use in implementing and evaluating the security of academic information services. Meanwhile, to determine the achievement of the evaluation of the security level of academic information systems, the Indonesian e-government ranking (PEGI) method is required. The combination of the COBIT 5 framework in the DSS05 domain using the PEGI method in academic information security service is able to provide a level of achievement in the form of Customer Value. The results of the COBIT 5 framework analysis of the DSS05 domain using the PEGI method get a score of 3.50 so that the quality of academic information service security evaluation achievement is at a very good level. At this level, universities are increasingly open to technological development. Higher education has applied the concept of quantification in every process, and has always been monitored and controlled for its performance in the security of academic information systems.**

Keywords*— *COBIT 5, Maturity, PEGI, Safety.

I. INTRODUCTION

Institutions place information technology as things that can support the achievement of the company's strategic plan to achieve the goals of the institution's vision, mission and goals. Information technology will get effective results if it uses good governance in its use and is able to be assessed and evaluated[1]. The information system is a system that contains an SPD network (data processing system), which is equipped with communication channels that are used in data organization systems[2]. There are various concepts of information systems, suitability is one of the keys to successful implementation and acceptance of information systems[3]. Along with the development of technology, it is often misused by some irresponsible parties that can cause threats[4]. Academic information system services must provide security, privacy and integrity of data processed, so that the performance of academic information systems is also an important part that must be considered so that academic information systems can be utilized optimally and safely[5]. The application of information security systems aims to overcome all problems and obstacles both technically and non-technically that can affect system performance, such as availability, confidentiality, and integrity so that the level of information security can be assessed[6]. As in Figure 1.

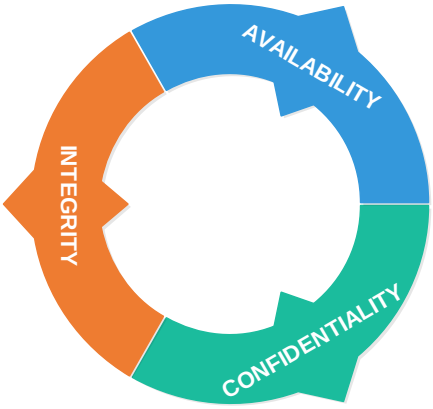


Figure 1 Aspects of information security

The existence of security problems triggers, procedures to control access rights in an information system[7]. A good information system security must apply the Deming cycle of quality standard. The security of academic information systems can be audited with various standards such as COBIT, COSO, ITIL, CMM, BS779, ISO 9000. COBIT (Control Objectives for Information and related Technology) is a standard guide to information technology management practices and a collection of documentation of best practices for IT governance that can help auditors, management, and users to bridge the gap between business risk, control needs, and technical issues[8]. All organizations can adjust COBIT 5 to their various goals, and are able to evaluate the organization in achieving its intended goals [9]. Domain DSS (Deliver, Service and Support) relates to system delivery and service support needed by the system, which includes service, security and continuity management, service support for users, and data management and operational facilities so that it is more focused on domain scopes that provide services that well[8]. DSS domain has sub-domain DSS05 which in this sub-domain is a more intensive procedure for information security. The method that can be used in evaluating achievement evaluations is PEGI. Indonesian e-government ranking (PEGI) is a model created by the Directorate of e-Government, Directorate General of Applications and Telematics, Ministry of Communication and Information (Kementerian KOMINFO) which can be used as a solution to analyze e-Government. Page has five dimensions of assessment, namely each policy, institutional, infrastructure, application and planning. Each dimension has the same weight in the assessment because all are important, interrelated and mutually supportive[10]. The PEGI method in academic information system security is able to provide a level of achievement in the form of maturity value. So as to be able to provide a decision on the extent to which the academic information system security process has been carried out by universities.

This study aims to conduct an evaluation related to the security of academic information service security that has been implemented at the University. This study aims to obtain the value of information system security from an institution, so that recommendations and innovations can be made for information system security in the institution. So that institution can provide security and comfort for the delivery of the information system services.

II. METHOD

A. *DSS05 Framework COBIT 5.*

The DSS05 sub-domain is part of the DSS (Deliver, Service and Support) domain. Like Figure 2.

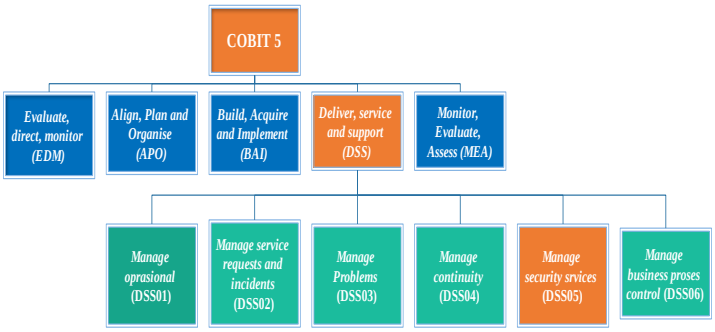


Figure 2. DSS05 schema

The DSS05 sub-domain is managed security services where the sub-domain is grouped into 7 processes. Like picture 3.

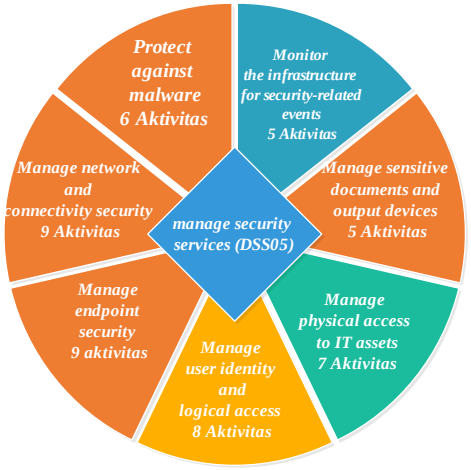


Figure 3. Metode DSS05

The seven processes carry out some 49 statements or activities as follows [11]:

1. Protect against malware (DSS05.01) where this process implements and maintains existing preventive, detective and corrective measures (especially security patches and virus control) throughout the company to protect information systems and technology from malware (e.g. Viruses, worms, spyware, spam).
2. Manage network and connectivity security (DSS05.02) where this process is used in security measures and related management procedures to protect information from all connectivity methods.
3. Manage endpoint security (DSS05.03) where this process provides certainty for endpoints (for example: Laptops, desktops, servers, and mobile devices and cellular networks or other software) guaranteed a level equal to or greater than the agreed security requirements.

4. Manage user identity and logical access (DSS05.04) This process gives certainty to all users having the right to access information according to business needs. They and coordinate with business divisions that manage access rights.
5. Manage physical access to IT assets (DSS05.05) this process determines and applies procedures to give, limit and revoke access to physical buildings. Buildings and areas according to business needs, including emergencies. Access to buildings, buildings and areas must be justified, authorized, recorded and monitored.
6. Manage sensitive documents and output devices (DSS05.06) where this process establishes physical security. In terms of documents relating to institutions. So all document output is standardized in security.
7. Monitor the infrastructure for security-related events (DSS05.07) where this process uses intrusion detection tools, to monitor infrastructure for unauthorized access rights and ensure every event is integrated with event monitoring and event management.

B. *Indonesian E-Government Ratings (PeGI)*

PeGI is a model created by the Directorate of e-Government, Directorate General of Applications and Telematics, Ministry of Communication and Information (Kementerian KOMINFO) yang dapat digunakan sebagai solusi untuk menganalisis e-Government. Pegi has five dimensions of assessment, namely each policy, institutional, infrastructure, application and planning. Each dimension has the same weight in the assessment because all are important, interrelated and mutually supportive[12].

The e-Government Directorate implemented the PeGi for the first time in 2007. All provinces in Indonesia were invited, as many as 11 provinces participated, namely Aceh, Lampung, South Sumatra, Banten, West Java, Central Java, Special Region of Yogyakarta, East Java, West Kalimantan, Sulawesi Southeast, and East Nusa Tenggara. PeGi is expected to be able to increase the development and use of ICTs in government institutions throughout Indonesia. In its implementation, KOMINFO cooperates with various groups from the ICT community, universities and related government agencies.

In general, the assessment of Indonesian e-Government governance is shown in Figure 4 and explained [13]:

a. Value 1.0-1.49 (very less): Indicator does not exist at all or very less in terms of quantity and quality.
b. Value 1.5-2.49 (less): Indicator already exists, but still needs to be added in terms of quantity and improved in quality.
c. Value 2,5-3,49 (good): Indicators of number and quality are quite good and can be seen to have a positive impact on the use of e-government, but improvements are needed to maintain the continuity of implementation in the future.
d. Value 3.5-4.0 (very good): Indicator both in terms of quantity and very good quality. The impact of implementing e-government is very real. Readiness to continue to be developed in the future is clearly visible.

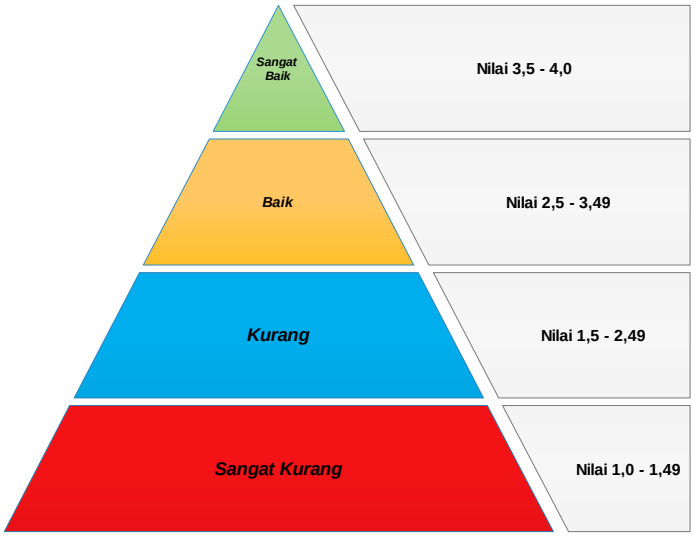


Figure 4 PeGi rating

III. RESULTS

This section will be presented in the process of methods guaranteed in a structured manner. analysis of the implementation and performance measurement of the maturity level of information systems with a framework sub-domain DSS05 framework COBIT 5 and PEGI.

A. *Academic Service Process Observation*

This process conducted interviews directly with informants authorized by the security of academic information systems in Higher Education using academic information systems began to be active in 2008, the beginning of the information system created and developed by vendors (Gama Techno) After that, in 2017 there will be migrating to a new system where the system will be developed by universities. Where in the migration is caused by the development of information system technology, so it is deemed necessary to do the migration to maintain the stability and security of the information system.

The aim of the college's academic system itself is:

1. To manage academic activities in the college environment.
2. Providing facilities for the Civitas, lecturers, students, staff and BAA in the academic process.

Over time the use of information systems is also experiencing obstacles, problems and threats to the information system. The problems, obstacles and threats that often occur are as follows:

1. There are several systems that have not been well integrated.
2. When the KRS is online the server is down.
3. Frequent occurrence of forgetting usernames and passwords.

4. The process of connecting or data transmission is slow.
5. Virus and malware attacks.

The standardization and auditing process of tertiary institutions applies ISO 9000 which is used as a standard for a quality management system (QMS) that is integrated with all bureaus in all institutions. This process also discusses the determination of respondents who will provide detailed information related to information about the security of existing academic information systems. The sample selection of respondents uses a purposive sampling technique, namely the selection of the sample of respondents determined by the researcher on the grounds that identification of the sample of respondents is done by referring to personal competencies that interact directly with IT governance[14]. The interview got 2 respondents who were directly related to the information system security sector in the institution.

B. *Mapping DSS05 Based on COBIT 5 Framework*

This process is the preparation of activity suitability in the DSS05 sub-domain with questions that will be made in the questionnaire. This process against malware consists of 6 activities, as in table 1.

Table 1. Protect against malware activity

Protect against malware (DSS05.01)	
No	Pertanyaan Aktivitas
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 meninjau 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.

C. *Questionnaire preparation with a combination of DSS05 and value PEGI*

This process is carried out by establishing a questionnaire based on the standard on DSS05 Framework COBIT 5 by combining it with the values of the PEGI standard so that a questionnaire form is obtained that is able to answer the needs of the existing information system security in the installation. To make it easier to read the process, a difference in the color of each decision is made. as in Table 2.

Tabel 2. Mapsing warna

Status	Warna	Nilai
Sangat Baik		3.5 - 4.0
Baik		2.5 - 3.49
Kurang		1.5 - 2.49
Sangat Kurang		1.0 - 1.49

Where in this questionnaire there are 4 assessments in the process with PEGI as shown in Table 3.

Table 3 criteria and values

Warna	Nilai	Kegiatan
	3.5 - 4.0	Dilakukan dengan SOP dan dievaluasi
	2.5 - 3.49	Dilakukan dangan SOP
	1.5 - 2.49	Dilakukan
	1.0 - 1.49	Tidak dilakukan

From the IT process assessment in Table 3, combined with the DSS05 COBIT 5 framework standard in Table 1, as in Table 4.

Tabel 4 Form Kuesioner

Protect against malware (DSS05.01)					
Aktivitas		**Jawaban**			
1	Memperoleh informasi tentang software berbahaya dan cara penanganannya.				
2	Instal dan aktifkan antivirus di PC anda.				
3	Apakah antivirus di PC selalu di update.				
4	Secara teratur meninjau 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.				

D. *Calculation of the maturity level of Academic service security*

This section will explain the results of the analysis of the implementation and performance measurement of the maturity level of the academic information system obtained from questionnaires and interviews in accordance with the DSS05 framework framework COBIT 5. To identify the extent to which an institution has met with good information security standards, it can use an identification framework that is represented at a level of maturity that has a level of grouping of company capabilities, as described in Table 5.

Table 5. Maturity criterion value PEGI

Kriteria	Nilai
Sangat Baik	3.5 - 4.0
Baik	2.5 - 3.49
Kurang	1.5 - 2.49
Sangat Kurang	1.0 - 1.49

The results of the questionnaire that has been given to the respondent and have been filled out by the respondent get results as in Table 6.

Table 6. Questionnaire Results

DSS	Responde 1	Responden 2
DSS05.06.1	2	2
DSS05.06.2	3	2
DSS05.06.3	3	2

DSS05.06.4	4	2
DSS05.06.5	1	2

Next correlate between the level value and absolute value which is done by calculation in the form of an index using a mathematical formula. The mathematical equation to determine the index value is as follows[15]:

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

After the index is obtained, we can get the current level of maturity (existing) this value is the value of the accumulation of processes that are running in the institution. a case in table 6.

Table 6. Current maturity value

DSS05	*Nilai Existing*
Protect against malware	3,92
Manage network and connectivity security	4,00
Manage endpoint security	3,50
Manage user identity and logical access	3,88
Manage physical access to IT assets	3,71
Manage sensitive documents and output devices	2,30
Monitor the infrastructure for security-related events	3,20

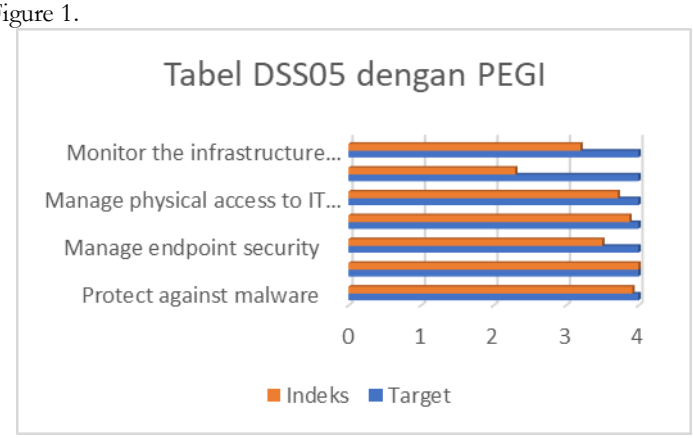
E. Gap Calculation

Once the value of the existing Maturity Level is obtained and the recommended Maturity Level (target) has been determined, the gap between the current condition and the target to be achieved will be analyzed and opportunities for the gap to be optimized will be identified, as in table 7.

Table 7. Maturity Gap value..

DSS05	Target	*Indeks Maturity Level Existing*
Protect against malware	4	**3,92**
Manage network and connectivity security	4	**4,00**
Manage endpoint security	4	**3,50**
Manage user identity and logical access	4	**3,88**
Manage physical access to IT assets	4	**3,71**
Manage sensitive documents and output devices	4	**2,30**
Monitor the infrastructure for security-related events	4	**3,20**

From table 7 is a comparison between the desired target and the achievement of the maturity value of existing information technology security processes that have been carried out so far. So that it can be drawn a maturity gap in the form of a graph like Figure 1.



Grafik 1. Gab Maturity.

IV. DISCUSSION

The discussion section provides in-depth reviews (insights) of the data obtained in the study. In this section tables or graphs can be presented which are the results of data processing.

Based on the Gap analysis obtained from the results of the target level to be achieved and the level achieved in DSS05, as in Graph 1, then here is some Gap Maturity Level Analysis. As in table 8 as follows.

Table 8. Maturity Level Gap Analysis

DSS05	*Maturity Level*
Protect against malware	*Sangat Baik*
Manage network and connectivity security	*Sangat Baik*
Manage endpoint security	*Sangat Baik*
Manage user identity and logical access	Sangat Baik
Manage physical access to IT assets	Sangat Baik
Manage sensitive documents and output devices	Baik
Monitor the infrastructure for security-related events	Baik

From the overall value of the level of death on DSS05 will be calculated on average, so that the level of maturity of the institution's security will be obtained.

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

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

MLDDSSO5 = 3.92+4+3.50+3.88+3.70+2.30+3.20/7
Level of maturity DSS05 = 3,50

From the calculation results, the achievement value is 3.50 so that the institution's kematnagn can be set at the Very Good level.

V. CONCLUSION

Sub-domain DSS05 Manage security services is a good procedure to be used in implementing and conducting megabits related to academic information system security services and PEGI is a good assessment method in an institution's audit system. Based on research conducted at the tertiary institution,

the score of the fatality level was 3.50 thus establishing that the current level of maturity is at a very good level. At this level, institutions are increasingly exposed to technological developments. Institutions have applied the concept of quantification in every process, and are always monitored and controlled for their performance.

REFERENCES

[1] R. Umar, I. Riadi, and E. Handoyo, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Pada Domain Delivery, Service, And Support (DSS)," *Semin. Nas. Teknol. Inf. dan Komun. - Semant. 2017 Anal.*, pp. 41–48, 2017.

[2] L. F. Fathoni *et al.*, "APPLICATION INFORMATION SYSTEM BASED HEALTH," vol. 2, no. 1, pp. 37–46, 2016.

[3] I. Muslimin, S. P. Hadi, and E. Nugroho, "An Evaluation Model Using Perceived User Technology Organization Fit Variable for Evaluating the Success of Information Systems," vol. 4, no. 2, pp. 86–94, 2017.

[4] A. Supriyatna, V. Maria, P. Studi, and M. Informatika, "khazanah informatika Analisis Tingkat Kepuasan Pengguna dan Tingkat Kepentingan Penerapan Sistem Informasi DJP Online dengan Kerangka PIECES," *khazanah Inform.*, vol. 3, no. 2, pp. 88–94, 2017.

[5] E. Kurniawan, "Security Level Analysis Of Academic Information Systems Based On standard iso 27002 : 2013 using sse-cmm," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. January, 2018.

[6] I. Riadi, S. Sunardi, and E. Handoyo, "Security Analysis of Grr Rapid Response Network using COBIT 5 Framework," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 10, no. 1, p. 29, 2019.

[7] M. Sumagita, I. Riadi, U. A. Dahlan, K. Yogyakarta, and D. I. Yogyakarta, "Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application," vol. 7, no. 4, pp. 373–381, 2018.

[8] E. Hicham, B. Boulafdour, M. Makoudi, and B. Regragui, "Information security, 4TH wave," *J. Theor. Appl. Inf. Technol.*, vol. 43, no. 1, pp. 1–7, 2012.

[9] F. Latifi and H. Zarrabi, "A COBIT5 Framework for IoT Risk Management," *Int. J. Comput. Appl.*, vol. 170, no. 8, pp. 40–43, 2017.

[10] R. Fadhlurrahman, M. C. Saputra, and A. D. Herlambang, "Evaluasi Penerapan E-government Di Pemerintah Kota Batu Menggunakan Kerangka Kerja Pemeringkatan E-government Indonesia (PeGI)," vol. 2, no. 12, pp. 5977–5982, 2018.

[11] J. F. Andry, "Audit of IT Governance Based on COBIT 5 Assessments : A Case Study," *TEKNOSI*, vol. 02, no. May, 2017.

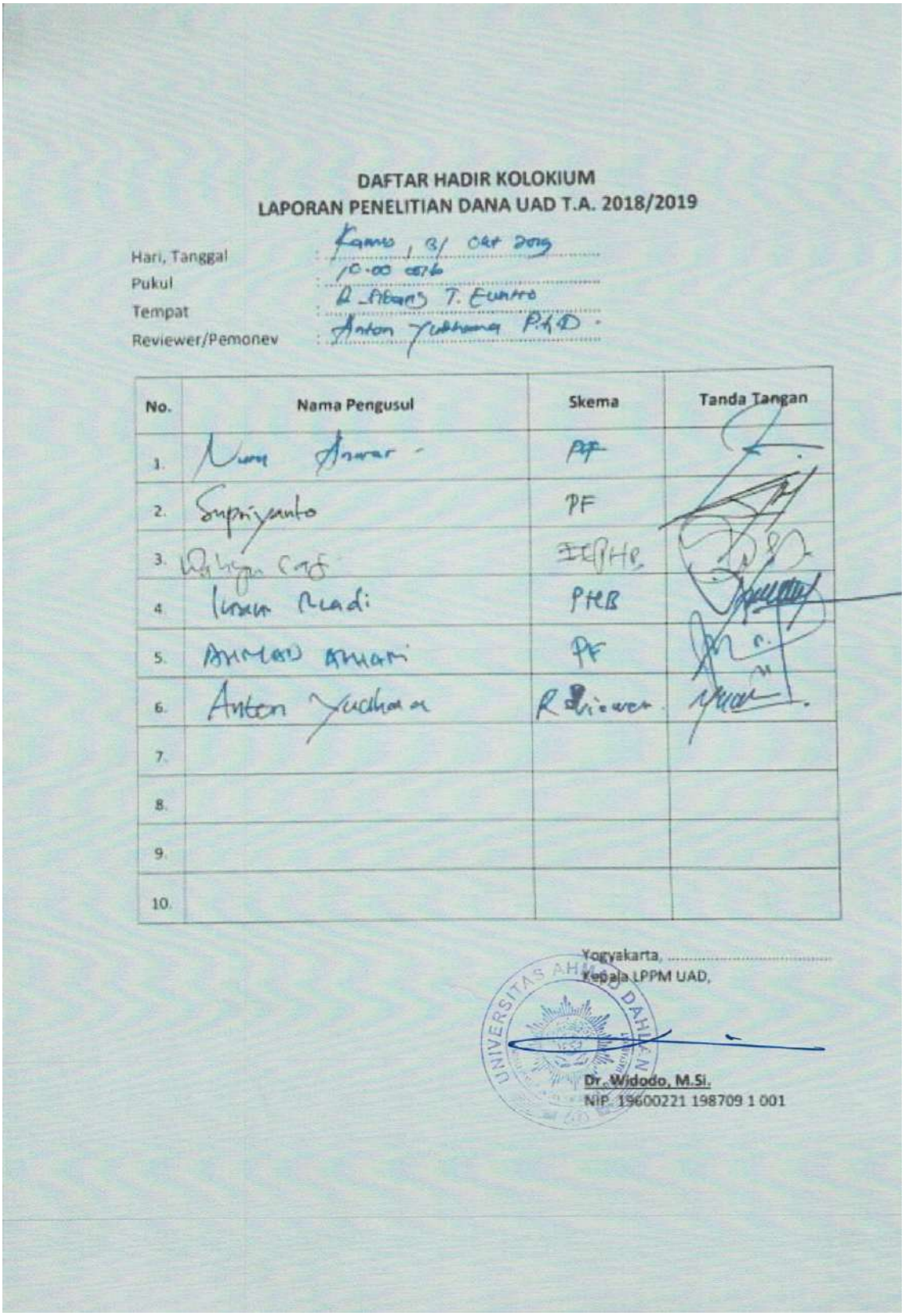
[12] A. Yudhana *et al.*, "Perancangan Sistem Informasi Menggunakan Enterprise Architecture Planning (Studi Kasus Pada Kecamatan di Kota Samarinda)," *khazanah Inform.*, vol. 4, no. 2, pp. 114–123, 2018.

[13] A. Fitriansyah, H. Budiarto, and J. Santoso, "Metode Pemeringkatan E-Government Indonesia (PeGI) Untuk Audit Tata Kelola Teknologi Informasi," *Semin. Nas. Sist. Inf. Indones.*, pp. 2–4, 2013.

[14] P. Rahayu and D. I. Sensuse, "Penilaian Implementasi e-Government di PUSTEKOM Kemendikbud berbasis metode PEGI," *J. Sist. Inf. Bisnis*, vol. 02, pp. 139–145, 2017.

[15] Rusydi Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, vol. 01, pp. 47–54, 2019.

LAMPIRAN 6. DAFTAR HADIR KOLOKIUM



DAFTAR HADIR KOLOKIUM
LAPORAN PENELITIAN DANA UAD T.A. 2018/2019

Hari, Tanggal : Kamis, 31 Okt 2019
Pukul : 10.00 s/d
Tempat : R. Sidang T. Lantai
Reviewer/Pemonev : Anton Yudhana, PhD.

No.	Nama Pengusul	Skema	Tanda Tangan
1.	Nuryanto Anwar	PF	
2.	Supriyanto	PF	
3.	Wahyu Cahyo	IEPHB	
4.	Iswan Riadi	PHB	
5.	Ahmad Ashari	PF	
6.	Anton Yudhana	Reviewer	
7.			
8.			
9.			
10.			

Yogyakarta, ...
Kepala LPPM UAD,

Dr. Widodo, M.Si.
NIP. 19600221 198709 1 001