TUGAS AKHIR – KS141501

PEMBUATAN DOKUMEN SOP (STADARD OPERATING PROCEDURE) KEAMANAN DATA YANG MENGACU PADA KONTROL KERANGKA KERJA COBIT 5 DAN ISO27002:2013 (STUDI KASUS : STIE PERBANAS)

Aulia Nur Fatimah
NRP 5212100058

Dosen Pembimbing
Dr. Apol Pribadi S., S.T, M.T

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

FINAL PROJECT – KS141501

DEVELOPING STANDARD OPERATING PROCEDURE (SOP) FOR DATA SECURITY REFER TO CONTROL COBIT 5 AND ISO27002:2013 FRAMEWORK (CASE STUDY : STIE PERBANAS)

Aulia Nur Fatimah
NRP 5212100058

Supervisor
Dr. Apol Pribadi S., S.T, M.T

INFORMATION SYSTEMS DEPARTMENT
Information Technology Faculty
Institute of Technology Sepuluh Nopember
Surabaya 2016

KATA PENGANTAR

Syukur Alhamdulillah terucap atas segala petunjuk, pertolongan, kasih sayang dan kekuatan yang diberikan oleh Allah SWT. Hanya karena ridho-Nya, peneliti dapat menyelesaikan laporan Tugas Akhir, dengan judul ***Pembuatan Dokumen SOP (Standard Operating Procedure) Keamanan Data yang Mengacu pada Kontrol Kerangka Kerja Cobit 5 dan ISO27002:2013 (Studi Kasus : STIE Perbanas).*** Tugas akhir ini dibuat dalam rangka menyelesaikan gelar sarjana di Jurusan Sistem Informasi Fakultas Teknologi Informasi Institut Teknologi Sepuluh Nopember Surabaya.

Terima kasih tiada henti terucap untuk seluruh pihak yang sangat luar biasa dalam membantu penelitian ini, yaitu:

- Untuk Dosen Pembimbing, Dr. Apol Pribadi, S.T., M.T., terima kasih atas segala bimbingan, ilmu serta motivasi yang sangat bermanfaat untuk peneliti.
- Untuk Bapak Dr. Ir. Aris Tjahyanto, M.Kom., selaku Ketua Jurusan Sistem Informasi ITS, yang telah menyediakan fasilitas terbaik untuk kebutuhan penelitian mahasiswa.
- Untuk Bapak Dr. Drs. Emanuel Kritijadi, MM., selaku Pembantu Ketua 1 Bidang Akademik STIE Perbanas yang selalu memberikan informasi, pengetahuan serta dukungan yang sangat baik selama penelitian.
- Untuk Bapak Hariadi Yutanto, S.Kom., M.Kom., selaku Kasie Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas yang selalu memberikan informasi, pengetahuan serta dukungan yang sangat baik selama peneitian.
- Untuk Bapak Lutfi SE., M.Fin., selaku ketua STIE Perbanas dan Ibu Meliza Silvi SE., M.Si., selaku Pembantu Ketua Bidang Keuangan dan Administrasi Umum yang selalu memberikan informasi dan pengetahuan selama penelitian.
- Untuk Ibu Hamin Maria Astuti, S.Kom., M.Sc., dan Ibu Annisah Herdiyanti S.Kom., M.Sc., sebagai dosen penguji

peneliti, terima kasih atas kritikan dan masukan yang bersifat membangun untuk peningkatan kualitas penelitian ini.

- Untuk Ibu Renny Pradina S.T., M.T., selaku dosen wali yang selalu membimbing dan memberikan dukungan serta motivasi yang berarti bagi peneliti.
- Untuk sahabat seperjuangan yang selalu memberi dukungan dan motivasi, yang selalu membantu selama proses perkualiahan, selalu memberikan semangat yang luar biasa kepada peneliti, terima kasih teman-teman terbaik, Sabrina Leviana Putri, Ika Aningdityas, Prasanti Asriningpuri, Ameilia TP, Agnesia Anggun K, Laras Aristiani untuk segala inspirasinya yang berarti bagi peneliti.
- Untuk teman-teman satu penelitian Ardhana, Danar, Adrianto terima kasih telah menjadi teman yang selalu mendukung dan membantu segala proses penelitian di STIE Perbanas.
- Untuk seluruh teman-teman Laboratorium MSI, teman-teman SOLA12IS, terima kasih untuk kebersamaannya dan dukungannya dalam penelitian ini serta seluruh pihak yang tidak bisa disebutkan satu-persatu di buku ini.

LEMBAR PENGESAHAN

PEMBUATAN DOKUMEN SOP *(STANDARD OPERATING PROCEDURE)* KEAMANAN DATA YANG MENGACU PADA KONTROL KERANGKA KERJA COBIT 5 DAN ISO27002:2013 *(STUDI KASUS : STIE PERBANAS)*

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

AULIA NUR FATIMAH
5212 100 058

Surabaya, Januari 2016

KETUA
JURUSAN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom
NIP.19650310 199102 1 001

LEMBAR PERSETUJUAN

PEMBUATAN DOKUMEN SOP *(STANDARD OPERATING PROCEDURE)* KEAMANAN DATA YANG MENGACU PADA KONTROL KERANGKA KERJA COBIT 5 DAN ISO27002:2013 *(STUDI KASUS : STIE PERBANAS)*

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

AULI A NUR FATIMAH
5212 100 058

Disetujui Tim Penguji : Tanggal Ujian : Januari 2016
Periode Wisuda : Maret 2016

Dr. Apol Pribadi S., S.T, M.T **(Pembimbing)**

Hanim Maria Astuti S.Kom., M.Sc **(Penguji 1)**

Annisah Herdiyanti, S.Kom., M.Sc., ITIL **(Penguji 2)**

PEMBUATAN DOKUMEN SOP (*STANDARD OPERATING PROCEDURE*) KEAMANAN DATA YANG MENGACU PADA KONTROL KERANGKA KERJA COBIT 5 DAN ISO27002:2013 (STUDI KASUS : STIE PERBANAS)

Nama Mahasiswa : AULIA NUR FATIMAH
NRP : 5212 100 058
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing : Dr. Apol Pribadi S., S.T, M.T

ABSTRAK

Dalam mendukung proses bisnis utamanya, perguruan tinggi membutuhkan adanya dukungan sebuah teknologi informasi. Pengimplementasian teknologi informasi dianggap mampu memberikan value dan keunggulan kompetitif tersendiri bagi organisasi. STIE Perbanas telah menggunakan teknologi informasi dalam pemenuhan proses bisnisnya yaitu dengan mengimplementasikan sebuah sistem informasi akademik, sistem informasi kepegawaian dan sistem informasi keuangan. Sistem informasi ini dibangun untuk mendukung efisiensi dan efektivitas proses bisnis utama pada STIE Perbanas. Sejalan dengan kondisi tersebut, dukungan terhadap keamanan data dalam sistem informasi tersebut sangat dibutuhkan untuk memastikan data yang ada dapat terjamin kerahasiaannya (confidentiality), keutuhannya (integrity) dan ketersediaannya (availability). Dalam memenuhi kebutuhan keamanan data tersebut maka diperlukan adanya sebuah tata kelola TI yaitu dalam bentuk dokumen SOP (Standard Operating Procedure) untuk mengurangi adanya ancaman dan risiko dari keamanan data serta untuk mendukung

penyelarasan pencapaian tujuan organisasi dalam mengadopsi TI pada proses bisnisnya.

Dalam penelitian ini, hasil akhir yang diharapkan adalah sebuah dokumen SOP yang berdasarkan pada kontrol kerangka kerja Cobit 5 dan ISO27002:2013. Pembuatan dokumen SOP akan didasarkan pada hasil analisis risiko pada aset informasi yang memiliki nilai risiko tinggi pada nilai dampak (severity) dan nilai kemungkinan terjadinya (occurrence). Sedangkan penilaian Risiko dalam penelitian didasarkan pada pendekatan risk assessment dan risk treatment ISO27002:2013.

Kata kunci: Keamanan Data, Standard Operating Procedure, Risiko, Manajemen Risiko, Cobit 5, ISO27002:2013

DEVELOPING STANDARD OPERATING PROCEDURE (SOP) FOR DATA SECURITY REFER TO CONTROL COBIT 5 AND ISO27002:2013 FRAMEWORK (CASE STUDY : STIE PERBANAS)

Name	**: AULIA NUR FATIMAH**
NRP	**: 5212 100 058**
Department	**: Information Systems FTIF -ITS**
Supervisor	**: Dr. Apol Pribadi S., S.T, M.T**

ABSTRACT

In supporting the core business processes, the college requires the support of an information technology. Implementation of information technology is considered capable of providing its own value and competitive advantage for organizations. STIE Perbanas been using information technology in the fulfillment of its business processes by implementing an academic information system, personnel information system and financial information system. This information system is built to support the efficiency and effectiveness of key business processes in Perbanas. In line with these conditions, support for data security in the information system is needed to ensure the existing data can be confidential (confidentiality), integrity (integrity) and availability (availability). In meeting the needs of data security it is necessary for an IT governance, namely in the form of documents SOP (Standard Operating Procedure) to reduce the threat and risk of data security as well as to support the alignment to organizational objectives in adopting IT on business processes.

In this study, the expected end result is an SOP document that is based on the control of COBIT 5 and ISO27002: 2013 framework. SOP document creation will be based on the results

of the risk analysis on the value of information assets that have high risk on the value impact (severity) and the possibility of (occurence). While the risk assessment in the study are based on risk assessment and risk approach to treatment ISO27002: 2013.

Keywords: Data Security, Standard Operating Procedure, Risk, Risk Mangement, Cobit 5, ISO27002:2013

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Pada bab ini dijelaskan beberapa hal mendasar pada penulisan tugas akhir, yang meliputi latar belakang, rumusan permasalahan, batasan masalah, tujuan, dan manfaat yang diperoleh dari penelitian tugas akhir ini.

1.1 Latar Belakang

Dewasa ini, penggunaan teknologi informasi telah menjadi salah satu faktor kunci keberhasilan suatu perusahaan ataupun organisasi. Teknologi informasi dianggap mampu memberikan *value* tersendiri dan mampu untuk menciptakan keunggulan kompetitif. Banyak perusahaan maupun organisasi kini semakin bergantung pada penggunaan teknologi informasi, tak terkecuali dalam sektor pendidikan salah satunya adalah penerapan teknologi informasi pada STIE Perbanas. STIE Perbanas telah mengimplementasikan beberapa teknologi informasi yang dapat mendukung proses bisnis utamanya. Sejalan dengan kondisi tersebut, dukungan terhadap kebutuhan informasi yang akurat, cepat serta *reliable* mengharuskan pihak manajemen untuk melakukan tindakan dalam menjaga keamanan informasinya, khususnya dalam keamanan data. Sebuah sistem akan kehilangan integritasnya apabila data yang diterima pada saat terjadinya proses tidak memiliki integritas, sehingga data yang diproses akan diubah kedalam informasi yang tidak dapat dipastikan kebenarannya. Proteksi terhadap data dibutuhkan untuk memastikan data yang ada dalam lingkup akademik dapat terjamin kerahasiaannya (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*).

STIE Perbanas telah mengimplementasikan teknologi informasi untuk membantu proses akademiknya namun belum memiliki sebuah penatakelolaan yang baik untuk memastikan apakah dukungan teknologi informasi yang berjalan selama ini telah

mendukung proses bisnis yang ingin dicapai dan belum dapat pula dipastikan apakah proses TI yang berjalan selama ini telah mendukung pencapaian dari tujuan STIE Perbanas. Salah satu permasalahan yang sering terjadi adalah mengenai integritas data pada sistem informasi akademiknya, dimana hal ini menjadi permasalahan bagi STIE Perbanas disetiap semester baru. Permasalahan tersebut adalah seperti hilangnya konten dalam kartu rencana studi mahasiswa yang terjadi hampir disetiap semester. Hal ini menunjukan bahwa risiko kehilangan data menjadi salah satu perhatian yang harus segera diatasi. Dengan adanya permasalahan tersebut, keamanan data harus dapat dikelola dengan baik sehingga dapat memperkecil risiko yang menyebabkan terganggunya proses bisnis.

Menurut ISO27001:2013, sistem manajemen keamanan informasi adalah bagian terintegrasi dari sebuah proses organisasi dan keseluruhan manajemen keamanan informasi dalam menjaga kerahasiaan (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*) informasi yang mengaplikasikan proses manajemen risiko untuk memberikan kepercayaan bagi organisasi bahwa risiko telah dikelola dengan cukup baik (ISO/IEC27001, 2013). Dimana dalam hal ini, data merupakan bagian dasar pembentuk sebuah informasi. Sehingga dalam meginisiasi sebuah keamanan informasi, perlu bagi sebuah organisasi untuk memastikan keamanan datanya tetap terjaga. Karena pada dasarnya, sebuah informasi merupakan hasil masukan dari sebuah data, modifikasi data dan hasil proses data yang akan menghasilkan luaran berupa sebuah informasi. Pengelolaan risiko pada ketiga aspek keamanan yaitu kerahasiaan (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*) membutuhkan adanya sebuah kontrol dan aksi mitigasi terhadap risiko tesebut. Kontrol mitigasi pada risiko dapat dilakukan dengan membuat sebuah prosedur yang baik untuk memastikan tidak adanya risiko yang berulang kembali dan dapat menyebabkan terganggunya proses bisnis yang berjalan.

Dengan demikian, salah satu bentuk dukungan dalam menjaga keamanan data yang dapat diimplementasikan pada STIE Perbanas adalah dengan membuat sebuah prosedur yang terdokumentasi dengan baik dalam bentuk sebuah dokumen SOP (*Standard Operating Procedure*) mengenai kemanan data agar risiko dari keamanan informasi khususnya dalam segi keamanan data dapat dikurangi atau dihindari. SOP berguna dalam mendefinisikan seluruh konsep, teknik, dan persyaratan dalam melakukan suatu proses yang dituliskan ke dalam suatu bentuk yang langsung dapat digunakan oleh pegawai yang bersangkutan dalam melaksanakan tugas proses bisnisnya (R Stup, 2002).

Dalam proses pembuatan sebuah dokumen SOP dibutuhkan adanya standard yang akan menjadi sebuah acuan. Dalam penelitian ini, kerangka kerja yang akan digunakan adalah Cobit 5 dan standard ISO27002:2013. Dimana Cobit 5 dan ISO 27002 akan digunakan sebagai penentuan kontrol yang harus ada dalam penyusunan dokumen SOP terutama kontrol yang berkaitan dengan keamanan data pada aspek kerahasian (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Pada kerangka kerja Cobit 5 domain yang digunakan adalah pada domain *Deliver Service and Support* (DSS) yaitu pada proses *DSS05.01 Protect Against Malware, DSS05.03 Manage Endpoint Security , DSS05.04 Manage User, Identity and Logical Access,* dan *DSS05.05 Manage Physical Access to IT*. Dan pada standard ISO 27002 kontrol yang akan digunakan adalah *9.4.3 Password Management System, 11.1.2 Physical Entry Controls, 12.2.1 Controls Against Malware, 12.3.1 Information Backup* dan *16.1 Management of Information Security Incidents and Improvements*.

1.2 Rumusan Permasalahan

Bedasarkan latar belakang diatas, maka rumusan masalah yang akan diteliti pada Tugas Akhir ini adalah sebagai berikut:

1. Apakah hasil analisis risiko untuk keamanan data pada STIE Perbanas untuk aspek keamanan data yaitu kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*)?
2. Bagaimana hasil pembuatan dokumen SOP (*Standard Operating Procedure*) untuk keamanan data pada STIE Perbanas yang mengacu pada kontrol kerangka kerja Cobit 5 dan ISO27002:2013?
3. Bagaimana hasil verifikasi dan validasi dari dokumen SOP keamanan data dengan kebutuhan keamanan pada STIE Perbanas?

1.3 Batasan Masalah

Bedasarakan permasalahan diatas, maka batasan masalah dari Tugas Akhir ini adalah sebagai berikut:

1. Peneilitian ini dilakukan pada bagian Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas.
2. Penelitian ini berfokus pada aspek keamanan data yaitu aspek kerahasiaan data (*confidentiality*), integritas data (*integrity*) dan ketersediaan data (*availability*).
3. Penelitian ini menggunakan kontrol dalam kerangka kerja Cobit 5 yaitu pada domain *Deliver Service and Support* (DSS) yaitu pada proses *DSS05.01 Protect Against Malware, DSS05.03 Manage Endpoint Security , DSS05.04 Manage User, Identity and Logical Access,* dan *DSS05.05 Manage Physical Access to IT Assets.*
4. Penelitian ini menggunakan kontrol dalam standard ISO27002:2013 yaitu pada kontrol *9.4.3 Password Management System, , 11.1.2 Physical Entry Controls, 12.2.1 Controls Against Malware, 12.3.1 Information Backup* dan *16.1 Management of Information Security Incidents and Improvements.*
5. Justifikasi dari analisis risiko dilakukan berdasarkan hasil wawancara dan interview langsung dengan Wakil Ketua

1 bidang Akademik dan Ketua Sie (Kasie) TIK STIE Perbanas.

6. Pendekatan yang digunakan untuk analisis risiko dengan menggunakan pendekatan proses penilaian risiko (*risk assessment*) dan perlakuan risiko (*risk treatment*) keamanan informasi pada ISO27001:2013.
7. Metode penilaian risiko dilakukan dengan menggunakan pendekatan metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability*) dan FMEA (*Failure Modes and Effecs Analysis*).
8. Penelitian ini berfokus pada pembuatan dokumen SOP (*Standard Operating Procedure*) keamanan data yang mengacu pada kerangka kerja Cobit 5 dan standard ISO27002:2013.

1.4 Tujuan Tugas Akhir

Berdasarkan rumusan permasalahan yang telah disusun, maka tujuan yang diharapkan dari penelitian Tugas Akhir ini sebagai berikut:

1. Menghasilkan analisis risiko terkait keamanan data pada STIE Perbanas untuk aspek keamanan data yaitu kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).
2. Menghasilkan dokumen SOP (*Standard Operating Procedure*) keamanan data pada STIE Perbanas yang berdasarkan hasil analisis risiko dan sesuai dengan kerangka kerja Cobit 5 dan ISO27002:2013.
3. Mengetahui hasil verifikasi dan validasi dari dokumen SOP sehingga dapat digunakan oleh STIE Perbanas untuk mendukung pengelolaan keamanan data.

1.5 Manfaat Tugas Akhir

Manfaat yang didapat dengan Tugas Akhir ini adalah sebagai berikut:

Bagi akademis

1. Memberikan kontribusi mengenai implementasi analisis risiko berdasarkan pendekatan identifikasi risiko keamanan informasi pada ISO27001:2013 dan metode penilaian risiko dengan OCTAVE dan FMEA.
2. Memberikan kontribusi mengenai penyusunan dokumen SOP (*Standard Operating Procedure*) terkait keamanan data yang mengacu pada kerangka kerja Cobit 5 dan standard ISO27002:2013.

Bagi Organisasi

1. Mengetahui risiko risiko yang dapat muncul pada bagian Teknologi Informasi STIE Perbanas
2. Dokumen SOP (*Standard Operating Procedure*) yang dihasilkan dapat digunakan sebagai panduan atau langkah dasar untuk melakukan proses keamanan data.

1.6 Relevansi

Topik yang diangkat pada tugas akhir ini mengenai Pembuatan Dokumen SOP (*Standard Operating Procedure*) Keamanan Data Mengacu pada Kontrol Kerangka Kerja Cobit 5 dan ISO27002:2013 (*Studi Kasus : STIE Perbanas*). Topik yang diangkat dalam tugas akhir ini berkaitan dengan mata Kuliah Manajemen Risiko dan Tata Kelola TI. Topik penelitian ini mengikuti bidang *roadmap* laboratorium Perencanaan dan Pengembangan Sistem Informasi (PPSI) pada Jurusan Sistem Informasi.

BAB II
TINJAUAN PUSTAKA

Bab ini akan menjelaskan pustaka atau literatur dan teori pendukung yang digunakan selama penelitian ini.

2.1 Penelitian Sebelumnya

Dalam mengerjakan tugas akhir ini terdapat beberapa penelitian terkait yang digunakan sebagai referensi, berikut merupakan informasi singkat mengenai penelitian-penelitian tersebut:

Tabel 2.1. Daftar Penelitian Sebelumnya

Judul : Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I	
Nama Peneliti	Margo Utomo
Tahun Penelitian	2012
Hasil Penelitian	Penelitian ini menghasilkan sebuah dokumen tata kelola yang terdiri dari dokumen manual, dokumen prosedur, instruksi kerja dan formulir yang berhubungan dengan keamanan kontrol akses. Dimana kontrol yang didapatkan ditentukan berdasarkan hasil penilaian risiko pada aset informasi teringgi
Hubungan dengan Tugas Akhir	Keterkaitan dengan penelitian adalah pada metodologi penelitiannya dimana penentuan kontrol dari standard atau kerangka kerja dipetakan

	terlebih dahulu berdasarkan pada hasil penilaian risiko tertinggi
Judul : Pembuatan Standard Operating Procedure (SOP) Layanan TI Berdasarkan GAP Analysis dan ITIL 2011 Level Service Operation Pada Jurusan Sistem Informasi ITS	
Nama Peneliti	Sella Wahyu Restiana
Tahun Penelitian	2015
Hasil Penelitian	Penelitian ini menghasilkan sebuah dokumen *standard operating procedure* (SOP) untuk mengelola *service operation* pada Jurusan Sistem Informasi. Dokoumen SOP yang dihasilkan berbasiskan kerangka kerja ITIL (*Information Technology Infrastructure Library*) yang berfokus pada level *service operation.*
Hubungan dengan Tugas Akhir	Keterkaitan dengan penelitian adalah hasil luaran yang akan dihasilkan pada penelitian adalah berupa dokumen produk SOP dan dalam penelitian ini juga metodologi penyusunan SOP hingga skenario pengujian dokumen SOP sama dengan penelitian tugas akhir.
Judul : *Designing Data Governance*	
Nama Peneliti	Vijay Khatri & Carol V. Brown

Tahun Penelitian	2010
Hasil Penelitian	Penelitian ini menghasilkan sebuah kerangka berfikir mengenai penelitian tata kelola pengelolaan data yang terdiri dari lima domain yaitu *data principles, data quality, metadata, data access* dan *data lifecycle*
Hubungan penelitian dengan Tugas Akhir	Keterkaitan dengan penelitian adalah luaran dari penelitian ini yang berhubungan dengan perancangan tata kelola data, hanya saja dalam penelitian tata kelola lebih mengutamakan pengelolaan data sedangkan dalam penelitian pengelolan lebih berfokus pada keamanan

2.2 Dasar Teori

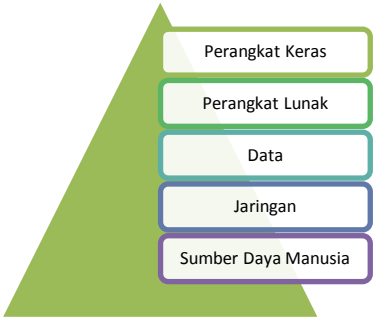
Pada bagian ini, akan dijelaskan mengenai teori-teori yang digunakan untuk mendukung pengerjaan tugas akhir. Teori tersebut yaitu mengenai : aset, keamanan data, risiko, metode manajemen risiko yaitu OCTAVE dan FMEA, kerangka kerja Cobit dan ISO27002:2013 serta SOP (*Standard Operating Procedure*).

2.2.1 Aset

Aset adalah sumber daya yang dikuasai dan/atau dimiliki oleh pemerintah sebagai dari peristiwa masalalu dan dari mana manfaat dimasa depan diharapkan dapat diperoleh, baik oleh pemerintah maupun masyarakat. Sebuag aset dapat diukur dengan satuan uang, termasuk sumber daya non keuangan yang diperlukan untuk penyediaan jasa bagi masyarakat umum dan sumber-sumber daya dipelihara karena alasan sejarah dan budaya.

2.2.2 Aset Informasi

Aset informasi adalah gabungan dari pengetahuan yang diatur dan dikelola sebagai satu kesatuan oleh organisasi sehingga dapat dipahami, dibagikan, dilindungi dan dapat dimanfaatkan dengan baik. Aset informasi pada penelitian ini akan mengacu pada definisi komponen Sistem Informasi. Komponen sistem informasi dibangun berdasarkan komponen-komponen pendukung yang meliputi : sumber daya manusia (people), perangkat keras (hardware), perangkat lunak (software), data dan jaringan (network). Dimana kelima komponen tersebut saling menyatu dan berineraksi sehingga dapat berfungsi sebagai pendukung dan *enabler* dalam meningkatkan operasi kesehariaan bisnis, serta penyedia kebutuhan informasi dalam rangka pengambilan keputusan yang baik.



Gambar 2.1. Komponen Aset Informasi

Pada gambar diatas diibaratkan sebuah sistem informasi yang terdiri dari beberapa komponen penyusunannya. Komponen tersebut yaitu sebagai berikut :

a. Perangkat Keras (Hardware)

Perang keras mencakup piranti fisik seperti: komputer, printer, monitor dan server. Berperan penting sebagai media penyimpanan vital dalam dunis sistem informasi. Dimana setiap perusahaan yang memiliki teknologi informasi memiliki hardware yang komplek dan berjumlah banyak.

b. Perangkat Lunak (Software)
Perangkat lunak merupakan sekumpulan intruksi yang dapat mempengaruhi kinerja peragkat keras dan memproses data. Tujuan adanya perangkat ini adalah untuk mengolah, menghitung dan memanipulasi data agar menghasilkan informasi yang berguna.

c. Data
Data dalam dunia teknologi informasi adalah sebuah bagian dari database, yang disimpan dalam basis data sebagai penyedia informasi dalam tujuannya untuk mendukung perusahaan melakukan kegiatan operasional.

d. Jaringan (Network)
Jaringan merupakan sebuah sistem penghubung yang memungkinkan suatu sumber (utamanya perangkat keras dan perangkat lunak) digunakan secara bersamaan dalam waktu yang berbeda.

e. Sumber Daya Manusia (People)
Sumber daya manusia atau orang dalam penelitian ini adalah civitas akademika dalam STIE Perbanas baik dalam bagian TI maupun Non TI dan yang berhubungan dengan sistem informasi maupun tidak. Sumber daya manusia tersebut antara lain staf TI dan Non TI serta Dosen dan Mahasiswa.

2.2.3 Keamanan Data

Keamanan data dapat diklasifikasikan kedalam tiga ketegori yaitu keamanan akses data, kemanan modifikasi data, dan ketersedian data (Bertino & Ferrari). Data merupakan bagian dari infromasi, dimana sekumpulan data diproses dan diolah menjadi sebuah informasi yang berguna. Menurut ISO27002, keamanan informasi merupakan pemeliharaan terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) (ISO/IEC, 2005). Dalam penelitian ini, aspek keamanan data akan difokuskan pada ketiga kategori keamanan data yaitu kerahasiaan

data, integritas data dan ketersediaan data. Ketiga faktor keamanan data tersebut mencakup mengenai akurasi dan keutuhan selama penginputan data, pemrosesan data, penyimpanan data dan validasi dari keluaran data.

2.2.3.1 Kerahasiaan Data

Kerahasiaan (*confidentiality*) berdasarkan kerangka kerja Cobit adalah proteksi pada informasi yang sensitif dari akses yang tidak terautorisasi (ITGI, 2007). Data yang tidak terautorisasi akan mengakibatkan tersingkapnya informasi pada pengguna yang tidak memiliki hak untuk mengakses informasi. Memastikan kerahasiaan data berarti mencegah keluarnya informasi dengan cara yang tidak tepat. Autorisasi yang tepat, dapat memastikan akses pengguna telah pada objek yang tepat. Dengan kata lain autorisasi haruslah berdasarkan pada kebijakan keamanan yang dimiliki oleh organisasi.

2.2.3.2 Integritas Data

Integritas (*integrity*) berdasarkan kerangka kerja Cobit adalah akurasi dan keutuhan dari sebuah informasi yang validasinya sesuai dengan nilai bisnis dan ekspektasi (ITGI, 2007). Data merupakan sebuah materi dasar yang digunakan untuk membentuk sebuah informasi, dimana data dan informasi memiliki ketergantungan pada integritas sebuah sistem (Woodroof & Searcy, 2001). Integritas adalah mengenai kebenaran modifikasi beberapa data, berdasarkan mekanisme kontrol akses untuk memverifikasi kebenaran akses pengguna dalam memodifikasi data dan batasan integritas yang berkaitan akan memverifikasi kebenaran pembaharuan data. Sebuah sistem akan kehilangan integritasnya apabila data yang diterima pada saat terjadinya proses tidak memiliki integritas, sehingga data yang diproses akan diubah kedalam informasi yang tidak dapat dipastikan kebenarannya. Dengan demikian, untuk memastikan bahwa sebuah sistem menghasilkan sebuah informasi yang memiliki integritas, hal mendasar yang perlu dipastikan adalah

mengenai integritas dari data yang diterimanya, dan selanjutnya mengenai proteksi terhadap proses yang terjadi didalamnya.

2.2.3.3 Ketersediaan Data

Ketersediaan (*availability*) berdasarkan kerangka kerja Cobit adalah ketersediaan informasi pada saat dibutuhkan dalam proses bisnis sekarang dan yang akan datang, dimana ketersediaan juga berfokus pada usaha perlindungan kebutuhan sumber daya (ITGI, 2007). Ketika sebuah data tidak tersedia, maka informasi yang penting untuk beberapa fungsi dalam organisasi mungkin tidak dapat terbaca dan terakses saat dibutuhkan. Memastikan ketersediaan data berarti memastikan pencegahan (*preventing*) dan tidakan pemulihan (*recovery*) perangkat keras dan perangkat lunak dari kesalahan yang mengakibatkan sistem database tidak tersedia (Bertino & Ferrari).

2.2.4 Risiko

Risiko adalah suatu efek dari ketidakpastian dalam pencapaian suatu tujuan yang dapat bersifat positif maupun negative (ISO3100:2009). Menurut PMBOK (*Project Management Body of Knowledge*) risiko adalah adalah sebuah kejadian yang tidak pasti dan tidak dapat diprediksi, atau sebuah kondisi yang apabila terjadi akan meninbulkan dampak setidaknya pada satu tujuan proyek. Sehingga dapat disimpulkan bahwa risiko merupakan efek yang muncul dari adanya ketidakpastian dalam sebuah tujuan.

2.2.5 Risiko Teknologi Informasi

Risiko TI meningkat sebanding dengan perkembangan penggunaan teknologi informasi. Penggunaan TI yang meningkat mengakibatkan dependesi bagi organisasi maupun perusahaan yang mengadopsi TI pada proses bisnisnya, sehingga risiko yang ditimbulkan dari pengimplementasian TI tersebut pun meningkat. Risiko TI adalah sebuah kejadian yang tidak dapat direncanakan dan berdampak pada keagalan atau penyalahgunaan TI yang mengancam tujuan bisnis (George & Hunter, 2007).

Menurut ISACA (*Information Systems Audit and Control Association*) risiko TI merupakan sebuah risiko bisnis yang berkaitan dengan aspek teknologi informasi yang tidak direncanakan dan dapat menimbulkan dampak pada perusahaan. Sehingga risiko TI perlu dianalisis dan dimitigasi untuk mencegah terhambatnya proses bisnis yang dapat menghambat kegiatan opersional perusahaan ataupun organisasi.

2.2.6 Manajemen Risiko

Menurut *Institute of Risk Management* (IRM) manajemen risiko sebagai suatu proses yang bertujuan untuk membantu organisasi atau perusahaan dalam memahami, mengevaluasi dan mengambil tindakan untuk risiko-risiko yang muncul, dengan meningkatkan kemungkinan untuk berhasil dan mengurangi kemungkinan kegagalan. Dan menurut Djohanputro dalam penelitiannya *Manajemen Risiko Korporat* dikatakan bahwa manajemen risiko merupakan suatu proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternative penanganan risiko dan monitor serta pengendalian penanganan risiko (Djohanputro, 2008). Sehingga dapat disimpulkan bahwa manajemen risiko adalah sebuah proses yang didalamnya terdapat aktifitas pengelolaan risiko untuk meminimalisir kerugian atau dampak bagi organisasi atau perusahaan.

2.2.7 Manajemen Risiko Teknologi Informasi

Menurut *National Institute Risk Technology* (NIST) dalam publikasinya, manajemen risiko teknologi informasi adalah suatu rangkaian proses yang meliputi penilaian risiko, mitigasi risiko dan evaluasi dari komponen TI sebuah organisasi atau perusahaan. Manajemen risiko TI merupakan sebuah proses pengidentifikasian, penilaian dan mitigasi risiko yang terjadi dalam organisasi pada aspek teknologi informasi.

Sehingga dapat disimpulkan bahwa manajemen risiko TI merupakan bagian dari proses pengelolaan risiko TI. Dimana manajemen risiko TI dilakukan dengan tujuan untuk melindungi aset TI dan meminimalisir risiko serta dampak dari risiko yang berkaitan pada teknologi informasi yang diadopsi pada organisasi. Dalam manajemen risiko TI pada umumnya akan diikuti dengan penentuan risiko mana yang membawa dampak atau kerugian yang paling besar dan yang akan ditangani terlebih dahulu. Berikut adalah kategori penentuan tindakan terhadap risiko atau mitigasi risiko yang dibagi kedalam 4 kategori : *avoid, transfer, mitigate, accept.*

- Avoid

Strategi mitigasi risiko *avoidance* digunakan untuk menghindari risiko tersebut terjadi bagaimananpun caranya. Strategi ini biasanya memerlukan biaya yang tinggi dan dilakukan apabila dampak dari risiko yang akan terhadi cukup merugikan organisasi atau perusahaan.

- Transfer

Stratego mitigasi risiko *mitigation* adalah strategi dimana organisasi atau perusahaan memerlukan pergeseran beberapa atau semua dampak negative dari ancaman, bersama dengan kepemilikan respon, kepada pihak ketiga.

- Mitigate

Strategi mitigasi risiko *transference* adalah strategi dimana organisasi atau perusahaa n melakukan beberapa kegiatan untuk mengurangi atau membatasi dampak dari risiko ini. Pembatasan risiko ini adalah gabungan dari penerimaan risiko (*risk acceptance*) dab penghindaran risiko (*risk avoidance*).

- Accept

Strategi mitigasi *acceptance* biasanya dilakukan apabila efekt dari risiko dinilai cukup besar dan tidak dapat dihindari, seperti contoh risiko alamih berupa bencana alam. Strategi ini dilakukan karena biaya untuk mengatasi maupun menghindari risiko lebih besar dibandingkan dengan memilih strategi

menerima risiko tersebut. Startegi ini digunakan apabila risiko memiliki kemungkinan terjadi yang kecil.

2.2.8 Kaitan antara Risiko TI dan Keamanan Data (CIA)

Menurut ISRMC dalam penelitiannya mengenai *Operational Risk Framework*, sebuah risiko TI yang berhubungan dalam bidang operasional disebut dengan risiko operasional. Dan risiko operasional adalah hal hal operasional yang mungkin terjadi dan berdampak pada informasi organisasi ataupun aset kritisnya (ISRMC, 2009). Dimana risiko TI dalam bidang operasional tersebut erat hubungannya dengan ketiga aspek keamanan yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability)*. ISRMC menggambarkan sebuah kerangka kerja *Operational Risk Framework* sebagai berikut (Gambar 2-1).

Gambar 2.2. Operational Risk Framework Model (ISRMC, 2009)

Dalam *Operational Risk Framework* dijelaskan bahwa sebuah risiko dilihat berdasarkan aset yang ada. Dimana risiko tersebut diidentifikasikan berdasarkan kategori kemanan yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability)* dari masing masing aset yang ada. Dalam penelitian ini, aset yang dimaksud adalah berupa data. Sehingga keamanan data adalah sebuah bentuk proteksi keamanan terhadap aset organisasi yaitu data terhadap ketiga risiko yang mungkin dapat muncul dilihat dari segi kerahasiaan (*confidentiality*), keutuhan

(*integrity*) dan ketersediaan (*availability)*. Risiko tersebut merupakan risiko TI yang dilihat dari segi operasional yang dapat menganggu berjalannya operasional proses bisnis. Sehingga kaitan antara keamanan data dalam aspek CIA (*confidentiality, integrity, availability*) dan risiko TI adalah bahwa sebuah keamanan data dapat tercapai dengan melakukan pengelolaan terhadap risiko TI yang mungkin muncul pada aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability)* data yang akan mengakibatkan terganggungnya proses bisnis khususnya dalam bidang operasional.

2.2.9 Manajemen Risiko dengan Pendekatan *Risk Assessment* dan *Risk Treatment* ISO27001:2013

ISO27001:2013 menyediakan sebuah standard dalam menspesifikasikan kebutuhan untuk membentuk, mengimplementasikan, mengelola dan melakukan peningkatan terus menerus dalam sistem manajemen keamanan informasinya pada konteks organisasi. Dimana dalam standard tersebut juga terdapat sebuah fase yaitu *planning* yang menyediakan pendekatan untuk megidentifikasi kebutuhan dalam menilai dan cara memperlakukan risiko keamanan informasi sesuai kebutuhan organisasi. Pendekatan tahap *planning* tersebut terdiri dari *actions to address risks and opportunities* dan *security objectives and planning to achieve them.* Pada penelitian ini, dalam melakukan manajemen risiko dilakukan pendekatan dengan ISO27001:2013 yaitu pada tahap *action to address risks and opportunities* .

Tahap *action to address risks and opportunities* terdiri dari dua tahapan utama yaitu *information security risk assessment* (penilaian risiko keamanan informasi) dan *information security risk treatment* (perlakukan terhadap risiko keamanan informasi).

a) Penilaian Risiko Keamanan Informasi

Tahapan penilaian risiko keamanan informasi merupakan tahapan dalam mengelola dan mengaplikasikan proses penilaian risiko keamanan informasi yang teridi dari proses :

- Menetapkan dan mengelola kriteria keamanan informasi yang termasuk didalamnya yaitu :
  - Menentukan kriteria penerimaan risiko (*risk acceptance criteria*).
  - Menentukan kriteria untuk melakukan penilaian risiko keamanan informasi.
- Memastikan bahwa penilaian risiko keamanan informasi akan menghasilkan hasil yang konsisten, valid dan sebanding.
- Mengidentifikasi risiko keamanan informasi yang teridiri dari tahap yaitu :
  - Mengaplikasikan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang berhubungan dengan kehilangan kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) sebuah informasi dalam cakupan sistem manajemen keamanan informasi.
  - Mengidentifikasi pemilik risiko.
- Menganalisa risiko keamanan informasi yang terdiri dari tahap yaitu :
  - Menilai konsekuensi potensial yang mungkin terjadi jika risiko telah teridentifikasi.
  - Menilai frekuensi kemungkinan terjadinya risiko yang teridentifikasi.
  - Menentukan tingkatan atau level risiko.
- Mengevaluasi risiko keamanan informasi yang teridiri dari tahap yaitu :
  - Membandingkan hasil analisis risiko dengan kriteria risiko yang telah ditetapkan
  - Memprioritaskan hasil analisis risiko untuk selanjutnya ditentukan perlakuan terhadap risiko tersebut.

b) Perlakuan terhadap risiko keamanan informasi

Tahapan selanjutnya adalah tahapan menentukan perlakuan terhadap risiko yang telah dihasilkan pada tahapan sebelumnya

yaitu tahapan penilaian risiko keamanan informasi. Tahapan dalam perlakuan risiko keamanan informasi terdiri dari proses :

- Memilih opsi perlakuan risiko keamanan informasi yang sesuai berdasarkan hasil penilaian risiko.
- Menentukan seluruh kontrol yang dibutuhkan untuk mengimplementasikan opsi perlakuan risiko keamanan informasi yang dipilih.
- Membandingkan kontrol yang telah ditentukan dengan kontrol yang ada pada kerangka kerja dan memverifikasi bahwa kontrol yang tidak dibutuhkan telah dihilangkan
- Membuat sebuah pernyataan yang menjelaskan kebutuhan dari kontrol dalam bentuk justifikasi kebutuhan kontrol.
- Memformulasikan rencana perlakuan terhadap risiko keamanan informasi.
- Memvalidasi formulasi rencanan perlakuan keamanan kepada pemilik risiko untuk mendapatkan persetujuan terhadap rencana tersebut.

Dalam penelitian ini, secara garis besar ISO27001:2013 merupakan kerangka yang digunakan untuk melakukan manajemen risiko, sedangkan metode yang digunakan dalam melakukan analisis risiko dan penilaian risiko adalah metode FMEA.

2.2.10 OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability*)

OCTAVE untuk membuat pendekatan standarisasi untuk pengendalian risiko dan *practice based* untuk evaluasi keamanan informasi. Metode Octave merpakan sebuah *framework* yang ditujukan untuk melakukan manajemen risiko terkait dengan keamanan aset perusahaan. Octave digunakan dalam mengidentifikasi dan mengatur risiko keamanan informasi. Dalam melakukan manajemen risiko, Octave menggunakan metode evaluasi secara komprehensif yang memungkinkan organisai

untuk mengidentifikasi aset informasi yang penting untuk misi pada perusahaan (Christopher J. Alberts, 1999).

Gambar 2.3. Framework Octave (Sumber : Octave)

Octave menggunakan pendekatan tiga tahapan dalam menguji isu organisasi terhadap penyusunan masalah yang komprehensif dan berhubungan dengan kebutuhan keamanan sebuah organisasi. Berikut merupakan penjelasan dari masing masing tahapan dalam Octave :

a. Tahap 1 : Membangun Aset berbasis Ancaman Profil
   Tahapan ini merupakan bagian dari *organisational view* yang melihat dari sisi internal organisasi, sehingga luaran dari tahapan ini adalah aset penting organisasi, kebutuhan keamanan organisasi, praktek keamanan terkini yang telah atau sedang dilakukan organisasi dan kelemahan kebijakan yang dimiliki organisasi saat ini.

b. Tahap 2 : Identifikasi Infrastruktur *Vulnerabilities*
   Tahapan ini akan melihat dari sisi teknologi yaitu melakukan evaluasi terhadap infrastruktur TI yang dimiliki organisasi. Sehingga luaran dari tahapan ini

adalah berupa komponen penting dalam aset kritis dan kelemahan infrastruktur TI yang ada saat ini.

c. Tahap 3 : Mengembangkan Strategi Keamanan dan Perencanaan
   Tahapan ini merupakan tahapan penilaian risiko dan mitigasi risiko dengan melakukan pengembangan strategi keamanan dan perencanaannya.Sehingga luaran dari tahapan ini adalah berupa analisis risiko, pengukuran tingkat risiko dan strategi proteksi.

2.2.11 FMEA (*Failure Modes and Effects Analysis*)

FMEA adalah suatu prosedur terstruktur untuk mengidentifikasi akibat atau konsekuensi dari kegagalan sistem atau proses, serta mengurangi atau mengeliminasi peluang terjadinya kegagalan. FMEA merupakan metode yang dapat digunakan untuk mengurangi kerugian yang terjadi akibat kegagalan tersebut. Metode FMEA mampu mengidentifikasi tiga hal yaitu penyebab kegagalan dari sistem, desain produk, dan proses, efek dari kegagalan dan tingkatan kritikal efek dari suatu kegagalan.

Metode FMEA memiliki 9 elemen yang dibangun berdasarkan informasi yang mendukung analisis yaitu fungsi proses, mode kegagalan, efek potensial dari kegagalan, dampak, penyebab potensial, kemungkinan (*occurence*), deteksi (*detection*), level risiko (RPN), dan tindakan mitigasi yang direkomendasikan. Selain itu, dalam pendekatannya FMEA juga memiliki langkah langkah terstruktur. Langkah langkah dalam FMEA adalah sebagai berikut :

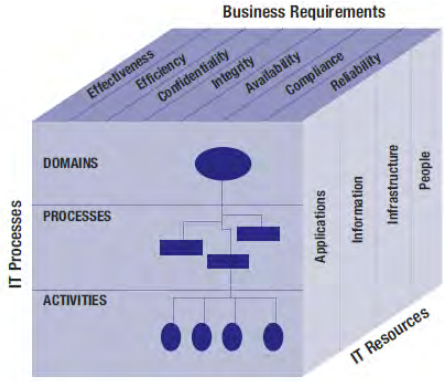
1. Mengidentifikasi komponen komponen dan fungsi yang terkait
2. Mengidentifikasi mode kegagalan (*failure modes)*
3. Mengidentifikasi dampak dari mode kegagalan (*failure mode)*
4. Menentukan nilai keparahan (*severity)* dari kegagalan

5. Mengidentifikasi penyebab dari kegagalan
6. Menentukan nilai frekuensi sering terjadinya (*occurence)* kegagalan
7. Mengidentifikasi kontrol yang diperlukan
8. Menentukan nilai keefektifan kontrol yang sedang berjalan (*detection)*
9. Melakukan kalkulasi nilai RPN (*risk priority number)*
10. Menentukan tindakan untuk mengurangi kegagalan

Dalam penelitian ini, penyusunan dokumen SOP akan berdasarkan pada kontrol dari kerangka kerja Cobit 5 dan standard ISO27002:2013, dimana penetuan kontrol yang dibutuhkan untuk penyusunan SOP tersebut akan berdasarkan pad a kebutuhan keamanan data yang kritis dilihat dari segi analisis nilai atau level risiko yang *very high* dan *high* dalam aspek operasional.

2.2.12 Kerangka Kerja Cobit 5

COBIT (*Control Objective for Information and Related Technology*) merupakan sebuah kerangka kerja tata kelola teknologi informasi (TI). Cobit dikembangkan oleh *IT Governance Institute* (ITGI) yang merupakan bagian *dari Information Systems Audit and Control Association* (ISACA). Cobit menyediakan sebuah *control objective* terkait dengan TI untuk mendefinisikan rencana strategis teknologi informasi, mendefinisikan informasi arsitektur, mendapatkan teknologi informasi yang diperlukan oleh *hardware* dan *software* dalam menjalankan proses TI dan menjamin layanan yang berkesinambungan serta pemantauan kinerja TI. Cobit berada pada level atas (*high level*) yang dikendalikan oleh kebutuhan bisnis, yang mencakupi seluruh aktifitas teknologi informasi, dan mengutamakan pada apa yang seharusnya dicapai dari pada bagaimana untuk mencapai tata kelola, manajemen dan kontrol yang efektif (Setiawan, 2008).



Gambar 2.4. Kendali Cobit (ITGI, 2007)

Pada Cobit 5 sebuah kendali dibagi kedalam tiga dimensi berbeda yaitu sumber TI, proses TI dan kebutuhan bisnis. Dimensi sumber TI mencakup semua aset TI yang termasuk didalamnya adalah sumber daya manusia, data, sistem aplikasi, teknologi informasi seperti hardware, sistem operasi, manajemen database, jaringan serta infrastruktur teknologi informasi. Proses TI sebagai dimensi kedua yaitu sebuah domain yang terdiri dari kumpulan proses dan aktifitas. Dan dimensi ketiga yaitu kebutuhan bisnis yang berguna dalam mendukung tercapainya tujuan bisnis dengan merujuk pada efektifitas, efisiensi, kerahasiaan, integritas, ketersediaan, kepatuhan dan keakuratan informasi. Dapat disimpulkan bahwa hubungan antara ketiga kendali tersebut yaitu sebuah sumber TI dikelola oleh proses TI untuk mencapai sebuah tujuan TI yang merupakan bagian dari kebutuhan bisnis.

Penggunaan pendekatan kerangka kerja Cobit 5 digunakan dalam penelitian sebagai kerangka kerja dalam penyusunan dokumen SOP. Dimana hasil yang diharapkan adalah untuk memastikan tujuan bisnis dari STIE Perbanas yang didukung oleh implementasi TI telah didukung dengan tepat oleh proses TI yang selama ini berjalan.

2.2.11.1 Domain Kerangka Kerja Cobit 5

Kerangka kerja Cobit 5 memiliki 5 domain yang dibagi kedalam 37 proses. Masing masing domain tesebut berorientasi pada proses yang terdiri dari *Evaluate Direct and Monitor* (EDM), *Align Plan and Organise* (APO), *Build Acquire and Implement* (BAI), *Deliver Service and Support* (DSS) dan *Monitor Evaluate and Assess* (MEA). Proses dalam Cobit 5 dibagi kedalam 2 area utama yaitu *management and governance.* Dimana area utama tersebut ditentukan berdasarkan aktivitas proses yang ada didalamnya. Dalam area *management* proses yang masuk didalamnya adalah EDM sedangkan pada area *governance* proses yang masuk didalamnya adalah APO, BAI, DSS dan MEA. Dalam penelitian ini, domain yang akan digunakan adalah domain *Deliver Service and Support* (DSS).

a. Deliver Service and Support (DSS)

Domain Deliver Service and Support (DSS) menerima solusi dan menggunakannya untuk memberikan layanan pada *end users* (ITGI, 2007). Domain DSS berfokus pada penyampaian secara aktual dari kebutuhan layanan, pengelolaan keamanan dan keberlangsungan bisnis, penyediaan layanan bagi pengguna dan pengelolaan data serta fasilitas operasional.

Proses dalam domain *Deliver Service and Support* yang digunakan dalam penelitian adalah sebagai berikut :

- DSS05.01 Protect Against Malware
  Kontrol dalam mengimplementasi dan mengelola aksi pencegahan, pendeteksian dan pembenaran terhadap proteksi sistem informasi dalam organisasi terhadap *malware*.
- DSS05.03 Manage Endpoint Security
  Kontrol dalam memastikan keamanan terhadap *endpoint system* yaitu laptop, server dan perangkat jaringan sesuai dengan kebutuhan keamanan untuk melakukan proses, penyimpanan dan transmisi data.

- DSS05.04 Manage User, Identity and Logical Access
  Kontrol dalam memastikan seluruh pengguna memiliki hak akses yang sesuai dengan kebutuhan bisnis dan telah terkoordinasi dengan unit bisnis yang mengelola pemberian hak akses selama proses bisnis.
- DSS05.05 Manage Physical Access to IT Assets
  Kontrol dalam membatasi akses pada area penting dalam organisasi. Kontrol ini memastikan seluruh akses terhadap area penting terautorisasi, memiliki sebuah *log* dan termonitor dengan baik.
- DSS06.02 Control the Processing of Information
  Kontrol untuk memastikan pegeksekusian dari operasional proses bisnis khususnya dalam pemrosesan informasi telah benar, lengkap, akurat, tepat waktu dan aman.

2.2.13 Standard ISO27002:2013

ISO27002:2013 merupakan standard mengenai keamanan informasi yang dikeluarkan oleh International Organization for Standardization (ISO) dan International Electronical Commision (IEC). ISO 27002 memiliki keterkaitan dengan ISO 27001, dimana dalam dokumen ISO 27001 berisikan kebutuhan mandatory dari sistem manajemen keamanan informasi sedangkan ISO 27002 melengkapinya dengan *code of practice* atau kontrol keamanan informasi untuk risiko keamanan pada kerahasian, keutuhan dan ketersediaan informasi. ISO 27002 memberikan *best practice* bagi organisasi dalam mengembangkan dan mengelola standard keamanan dan bagi manajemen untuk meningkatkan keamanan informasi dalam organisasi (IT Governance Institute & Office of Government Commerce, 2008). ISO/IEC 27002 memiliki 11 klausul utama kontrol yang masing masingnya terdiri dari kategori utama keamanan (*main security categories*) dan kontrol . Kategori utama keamanan terdiri dari 14 area berdasarkan ISO27002:2013 yaitu :

a) *Security Policy* (Kebijakan Keamanan)
b) *Organizing Information Security* (Keamanan Informasi Organisasi)
c) *Human Resources Security* (Keamanan Sumber Daya Manusia)
d) *Asset Management* (Pengelolaan Aset)
e) *Access Control* (Kontrol Akses)
f) *Cryptography* (Kriptografi)
g) *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan)
h) *Operations Security* (Keamanan Operasional)
i) *Communication Security* (Keamanan Komunikasi)
j) *System Acquisition, Development and Maintenance* (Akuisisi, Pengembangan dan Pengelolaan Sistem)
k) *Supplier Relationship* (Hubungan dengan *Supplier*)
l) *Information Security Incident Management* (Pengelolaan Insiden Keamanan Informasi)
m) *Information Security Aspects of Business Continuity Management* (Keamanan Informasi dari Aspek Pengelolaan Keberlangsungan Bisnis)
n) *Compliance* (Kepatuhan)

2.2.12.1 Kontrol Standard ISO27002:2013

Kategori utama keamanan meiliki kontrol (*control*) dan pedoman pengimplementasian (*implementation guidance*). Kontrol merupakan pendefinisian dari pernyataan mengenai kontrol untuk menjawab kontrol objektif dari setiap kategori utama keamanan dan pedoman pengimplementasian menyediakan detail informasi untuk mendukung pengimplementasian kontrol. Berikut ini merupakan kontrol ISO27002:2013 yang digunakan dalam penelitian :

- 9.4.3 Password Management System
  Kontrol dalam melakukan pengelolaan *password* dan memastikan kualitas dari setiap *password*.

- 11.1.2 Physical Entry Controls
  Kontrol untuk memastikan hanya pegawai yang memiliki autorisasi yang dapat mengakses area penting.
- 12.2.1 Controls Against Malware
  Kontrol untuk mengimplementasikan deteksi, pencegahan dan pemulihan terhadap *malware.*
- 12.3.1 Information Backup
  Kontrol untuk melakukan *backup* data penting secara berkala.
- 16.1 Management of Information Security Incidents and Improvements
  Kontrol untuk memastikan konsistensi dan efektifitas pendekatan pengelolaan gangguan terkait keamanan informasi

2.2.14 SOP (Standard Operating Procedure)

Tata kelola TI diartikan sebagai pengaturan yang dilaksanakan secara terpadu dan tidak terpisahkan dengan sumber daya organisasi. Menurut Weill dan Ross, Tata kelola TI adalah pengaturan pengaturan yang terkait dengan pengambilan keputusan. Pengaturan dijalankan untuk mendorong tercapainya perilaku pemakaian teknologi informasi yang mendukung tercapainya tujuan organisasi (Ross & Weill, 2004). Tata kelola TI memiliki struktur hirarki dokumen

SOP (*Standard Operating Procedure*) merupakan dokumen proses yang menjelaskan secara terperinci mengenai bagaimana cara melakukan sesuatu dalam sebuh kegiatan operasional (Akyar, 2012). SOP adalah kumpulan dari intruksi mengenai aktifitas yang didokumentasikan secara berulang pada sebuah organisasi. SOP digunakan untuk menjaga konsistensi kegiatan operasional serta sebagai tolak ukur keberhasilan suatu kegiatan operasional (KPRS, 2013). Dengan menyusun SOP, organisasi dapat mendefinisikan tujuan dari kegiatan operasionalnya, dan seluruh komponen terkait seperti alat atau data terkait

operasional, aktifitas terkait kegiatan operasional maupun aktor yang terlibat dalam kegiatan operasional tersebut. Salah satu manfaat dari implementasi SOP yaitu meminimalkan variasi pelaksanaan suatu kegiatan operasional, dan juga untuk menjaga konsistensi dalam meningkatkan kualitas dari suatu operasional, bahkan apabila terjadi pergantian aktor dalam kegiatan operasional tersebut, kegiatan masih dapat berjalan karena telah memiliki suatu standard proses yang jelas (Akyar, 2012).

Standard dokumen SOP menurut Akyar yaitu harus disusun dengan ringkas namun telah memuat seluruh aktifitas secara berurutan dengan format yang mudah dimengerti (Akyar, 2012). Berikut adalah beberapa kriteria penulisan SOP yang baik.

1. Spesifik dan Lengkap

Sebuah SOP disusun dengan menspesifikasikan seluruh aktifitas yang terkait dalam proses, termasuk memasukan seluruh unsur terkait proses tersebut yaitu melibatkan seluruh aktifitas, aktor hingga data yang terkait dalam kegiatan operasional. Dokumen SOP juga harus mencantumkan keterangkan lengkap mengenai nomor SOP, versi SOP, judul SOP serta status SOP.

2. Dapat Dipahami

Sebuah SOP disusun dengan jelas dan spesifik dengan menggunakan bahasa formal dan format penulisan yang baik untuk mudah dipahami.

3. Dapat Diaplikasikan

Sebuah SOP disusun dengan beracuan pada dokumen terkait yang ada pada organisasi sehingga dapat diaplikasikan pada proses operasional yang sesungguhnya. Dokumen terkait yang dapat menjadi acuan dari pembuatan SOP adalah seperti kebijakan pendukung SOP hingga dokumen teknis lainnya.

4. Dapat Diaudit

Sebuah SOP disusun dengan lengkap dan spesifik untuk memudahkan proses audit internal dalam organisasi. Dimana sebuah SOP merupakan proses yang periodic sehingga harus dapat diaudit untuk memastikan penjelasan alur proses yang ada didalamnya masih sesuai dengan kondisi organisasi.

5. Dapat Diubah

Sebuah SOP disusun dengan mengikuti kondisi organisasi dan harus mampu menyesuaikan perubahan kegiatan operasional yang terjadi pada proses operasional yang terkait.

Dalam penyusunan dokumen SOP tidak terdapat suatu format baku yang dapat dijadikan acuan, hal ini dikarenakan SOP merupakan dokumen internal yang kebiijakan pembuatannya disesuaikan oleh masing masing organisasi, begitu pula dengan penyunan format dari dokumen SOP tersebut. Namun sebuah SOP juga memiliki kriteria yang harus dipenuhi untuk memastikan bahwa dokumen yang disusun mudah dimengerti secara spesifik, efisien serta mudah diaplikasikan dalam organisasi (Akyar, 2012).

2.3.15 Format Dokumen SOP

Format penyusunan dokumen SOP akan digunakan untuk memudahkan dalam penyusunan SOP dan juga sebagai acuan pembuatan dokumen SOP keamanan data pada STIE Perbanas. Berikut merupakan format umum penyusunan dokumen SOP yang harus memenuhi unsur dokumentasi dan unsur prosedur.

1. Unsur Dokumentasi

Unsur dokumentasi merupakan unsur yang terkait dengan proses pendokumentasian SOP sebagai sebuah dokumen. Unsur dokumentasi yaitu halaman judul, keputusan pimpinan terkait, dan deskripsi singkat penggunaan dokumen.

a) Halaman Judul (*Cover*)
Halaman judul merupakan halaman yang menjadi sampul dari dokumen SOP dan harus mampu memberikan informasi mengenai isi dokumen. Sehingga dalam halam judul beberapa hal yang harus ada adalah judul SOP, instansi/satuan kerja, tahun pembuatan dan keterangan informasi lain sesuai persetujuan organisasi terkait.

b) Daftar Isi Dokumen SOP
Daftar isi digunakan untuk mempercepat pencarian informasi dan menulis perubahan atau revisi dari bagian tertentu pada SOP.

c) Deskripsi Penggunaan Dokumen
Dalam diskripsi singkat penggunaan dokumen, perlu dijelaskan mengenai ruang lingkup yang membahas mengenai tujuan disusunya prosedur, tingkasan mengenai prosedur yang disusun dan definisi kata yang terkait didalam dokumen SOP.

2. Unsur Prosedur

Unsur proedur merupakan bagian identitas dan bagian alur prosedur atau *flowchart*. Berikut adalah masing masing penjelasannya.

a) Bagian Identitas
Bagian identitas dalam dokumen SOP berisikan logo dan nama instanasi terkait, nomor SOP, tanggal pembuatan, tanggal revisi, tanggal efektif, pengesahan dokumen, judul SOP, dasar hukum dan identitas lainnya sesuai dengan kebijakan dan persetujuan organisasi terkait.

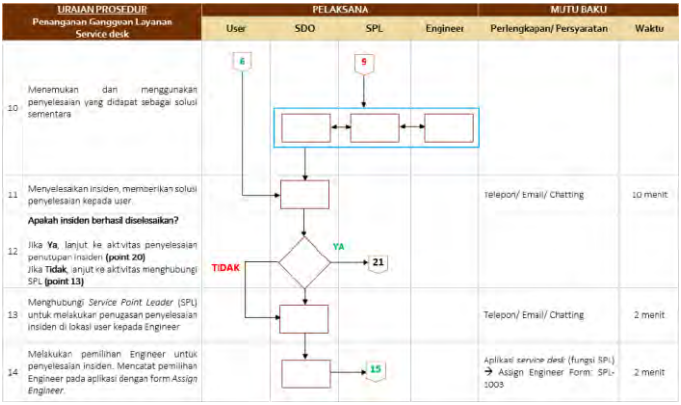
KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI DEPUTI BIDANG TATALAKSANA ASISTEN DEPUTI PENGEMBANGAN SISTEM DAN PROSEDUR PEMERINTAHAN	NOMOR SOP	KPANRB/D.IV/4.001/2011
	TGL. PEMBUATAN	6 Juli 2011
	TGL. REVISI	
	TGL. EFEKTIF	8 Agustus 2011
	DISAHKAN OLEH	Asisten Deputi Pengembangan Sistem dan Prosedur Pemerintahan Nama NIP
	NAMA SOP	PEMBUATAN LAPORAN KONSINYERING
DASAR HUKUM:	KUALIFIKASI PELAKSANA:	
1. Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2009 tentang Pembentukan dan Organisasi Kementerian Negara 2. Peraturan Presiden Republik Indonesia Nomor 24 Tahun 2010 tentang Kedudukan, Tugas, dan Fungsi Kementerian Negara serta Susunan Organisasi, Tugas, dan Fungsi Eselon I Kementerian Negara 3. Peraturan Menteri Negara PAN dan RB Nomor 12 Tahun 2010 tentang Organisasi Dan Tata Kerja Kementerian PAN dan RB	1. Memiliki kemampuan pengolahan data sederhana 2. Mengetahui tugas dan fungsi Sistem dan Prosedur Pemerintahan 3. Mengetahui tugas dan fungsi mekanisme pembuatan laporan	
KETERKAITAN:	PERALATAN/PERLENGKAPAN:	
1. SOP Pelaksanaan Konsinyering 2. SOP Pendokumentasian Laporan Konsinyering 3. SOP Pencairan Anggaran Konsinyering	1. Lembar Kerja / Rencana Kerja dan Anggaran 2. Term of Reference 3. Komputer/Printer/Scanner 4. Jaringan internet	
PERINGATAN:	PENCATATAN DAN PENDATAAN:	
Apabila Laporan Konsinyering terlambat dibuat maka pelaksanaan kegiatan Konsinyering berikutnya akan tertunda.	1. Di simpan sebagai data elektronik dan manual	

Gambar 2.5. Contoh bagian Identitas Prosedur

b) Alur Prosedur

Bagian alur prosedur merupakan bagian yang berisikan penjelasan langkah langkah prosedur kegiatan beserta mutu baku dan keterangan yang diperlukan. Alur prosedur dibentuk dalam sebuah *flowchart* yang menjelaskan langkah dari kegiatan secara berurutan dan sistemastis. Bagan alur atau *flowchart* adalah salah satu unsur dari sebuah prosedur. *Flowchart* merupakan bagian yang berisi penjelasan langkah langkah sebuah prosedur atau kegiatan beserta standard baku dan keterangan yang diperlukan.

Berikut merupakan contoh bagian *flowchart* yang sistematis dan memenuhi standard isi bagan alur yang terdiri dari nomor kegiata, uraian kegiatan yang berisi langkah-langkah (prosedur), pelaksana yang merupakan pelaku kegiatan, mutu baku yang berisi kelengkapan, waktu, output dan keterangan.

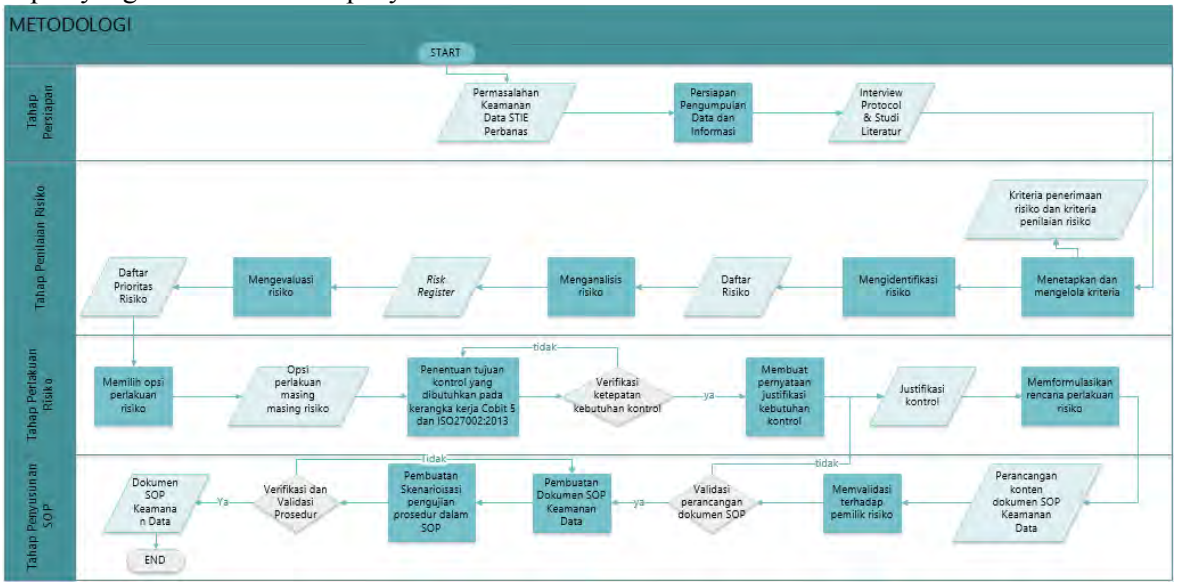


Gambar 2.6 Contoh Bagan Alur Prosedur

Berdasarkan penjabaran diatas maka dalam penyusunan dokumen SOP terhadap penelitian ini akan digunakan dengan bagan alur untuk menggambarkan alur prosedur yang ada dan disesuaikan pula berdasarkan kriteria dan sturktur atau format yang telah dijelaskan pada subbab sebelumnya. Dokumen SOP yang akan disusun yaitu dokumen SOP untuk keamanan data pada STIE Perbanas yang akan digunakan sebagai prosedur yang telah distandarisasi.

BAB III
METODOLOGI PENELITIAN

Bab ini menggambarkan metodologi yang akan digunakan selama penelitian berlangsung, termasuk tahapan yang dilakukan dalam penyusunan dokumen SOP Keamanan Data.



Gambar 3.1. Metodologi Penelitian Tugas Akhir

3.1 Tahap Persiapan

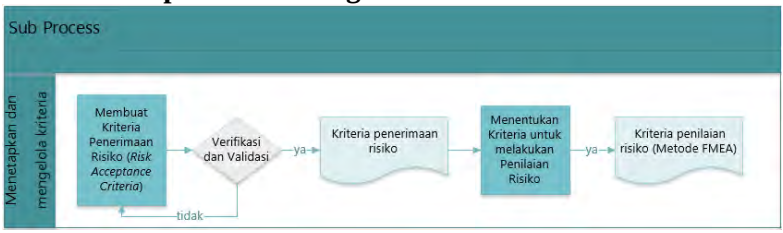
Tahap persiapan merupakan langkah awal untuk memulai penyusunan tugas akhir. Masukan dalam tahapan ini adalah permasalahan mengenai keamanan data yang ada pada STIE Perbanas. Dimana masukan dari permasalahan yang ada datang dari permintaan manajemen STIE Perbanas, untuk meninjau permasalahan keamanan informasi yang ada di STIE Perbanas. Dalam tahap persiapan dilakukan proses pengumpulan data dan informasi, dimana hasil luaran dari proses tersebut adalah berupa hasil studi literatur dan *interview protocol* yang akan digunakan sebagai media penggalian risiko keamanan informasi lebih lanjut.

Interview protocol tersebut berisikan daftar pertanyaan mengenai kemungkinan risiko opersional dalam STIE Perbanas khususnya untuk menjaga keamanan data yang berhubungan pada ketiga aspek yaitu kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*). Penggalian informasi akan dilakukan kepada pihak manajemen STIE Perbanas yaitu kepada Wakil Ketua 1 STIE Perbanas (Pembantu Ketua Bidang Akademik) dan Ketua SIE TIK (Manajemen Jaringan dan Technical Support).

3.2 Tahap Penilaian Risiko

Tahap penilaian risiko didasarkan pada pendekatan *risk assessment* pada ISO27002:2013 yang dibagi kedalam empat sub proses utama yaitu menentapkan dan mengelola kriteria, mengidentifikasi risiko, menganalisa risiko, dan mengevaluasi risiko. Masing masing dari sub proses tersebut memiliki beberapa proses dan luaran. Berikut ini adalah penjelasan dari masing masing proses dalam tahap penilaian risiko.

3.2.1 Menetapkan dan Mengelola Kriteria



Gambar 3.2. Sub Proses Menetapkan dan Mengelola

Dalam sub proses menetapkan dan mengelola kriteria terdapat dua proses yaitu menetapkan kriteria penerimaan risiko (*risk acceptance criteria*) dan menetapkan kriteria untuk melakukan penilaian risiko keamanan informasi. Luaran dari masing masing proses tersebut adalah sebuah kriteria penerimaan risiko dan kriteria penilaian risiko yang akan menjadi masukan dalam proses evaluasi risiko. Penentuan kriteria penerimaan risiko akan didasarkan pada hasil studi literatur dan akan divalidasi pula terhadap pihak manajemen STIE Perbanas untuk memastikan kesesuaian kriteria penerimaan risiko (*risk acceptance criteria*) dengan kondisi STIE Perbanas.

3.2.1.1 Menetapkan Kriteria Penerimaan Risiko (*Risk Acceptance Criteria*)

Proses membuat kriteria penerimaan risiko (*risk acceptance criteria*) didasarkan pada matriks risiko yang terdiri dari dua dimensi utama yaitu frekuensi kemungkinan terjadi risiko (*occurence*) dan dampak keparahan dari risiko (*severity*). Karena risiko dalam penelitian akan lebih mengarah pada risiko operasional maka kedua dimensi tersebut digunakan sebagai dasar dari kriteria penerimaan risiko (*risk acceptance criteria*).

3.2.1.2 Menetapkan Kriteria untuk Melakukan Penilaian Risiko

Proses menetapkan kriteria untuk melakukan penilaian risiko merupakan proses dalam menentukan metode penilaian risiko yang

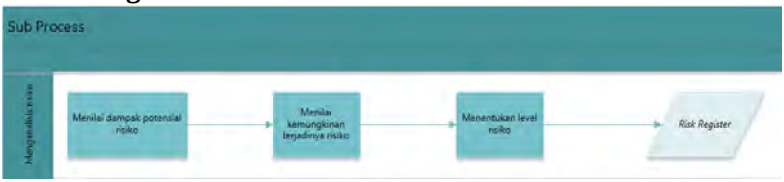
akan digunakan dalam melakukan penilaian risiko. Dalam penelitian ini, metode yang akan digunakan adalah metode penilaian dengan FMEA (*Failure Modes and Effecs Analysis*). Penetapan kriteria untuk melakukan penilaian risiko akan berdasarkan pada metode FMEA. Dalam proses ini, hasil luaran adalah sebuah studi literatur berupa kriteria penilaian risiko yang didasarkan pada metode FMEA.

3.2.2 Mengidentifikasi Risiko

Gambar 3.3. Sub Proses Mengidentifikasi Risiko

Dalam sub proses mengidentifikasi risiko, terdapat dua proses utama yang dilakukan yaitu mengidentifikasi risiko yang berhubungan dengan kehilangan aspek kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) dari sebuah data dan mengdentifikasi pemilik risiko. Identifikasi risiko akan dilakukan dengan penggalian informasi dari pihak manajemen STIE Perbanas melalui teknik interview. Identifikasi risiko tersebut akan didasarkan pada metode pada *framework* Octave yaitu dengan mengidentifikasi terlebih dahulu aset penting organisasi, kebutuhan keamanan organisasi, praktek keamanan terkini yang telah atau sedang dilakukan, aset kritis dan kelemahan infrastruktur TI yang ada saat ini. Hasil dari identifikasi risiko kemudian akan dilanjutkan pada proses identifikasi pemilik risiko. Hasil luaran dari proses mengidentifikasi risiko adalah sebuah daftar risiko. Daftar risiko tersebut selanjutnya akan menjadi masukan untuk proses analisis risiko.

3.2.3 Menganalisis Risiko



Gambar 3.4. Sub Proses Menganalisa Risiko

Dalam sub proses menganalisa risiko terdapat tiga proses yaitu menilai potensial dampak risiko, menilai kemungkinan terjadinya risiko dan menentukan level risiko. Dalam proses menganalisa risiko akan digunakan metode FMEA (*Failure Modes and Effecs Analysis*). Dalam metode FMEA analisis yang akan dilakukan yaitu pada mode kegagalan, efek potensial dari kegagalan, penyebab potensial risiko, dampak potensial risiko, kemungkinan terjadinya risiko (*occurence*), deteksi (*detection*), nilai level risiko (RPN). Dan dalam proses menganalisis risiko dengan metode FMEA ini hasil luarannya adalah sebuah *risk register*.

3.2.4 Mengevaluasi Risiko

Gambar 3.5. Sub Proses Mengavaluasi Risiko

Dalam proses mengevaluasi risiko terdapat dua proses yaitu membandingkan hasil analisis risiko dengan kriteria penerimaan risiko (*risk acceptance criteria*) dan selanjutnya memproritaskan risiko untuk menentukan perlakuan risiko yang tepat. Dalam hal ini proses memprioritaskan risiko akan dilakukan verifikasi dan validasi terhadap pihak manajemen STIE Perbanas untuk memastikan prioritas risiko telah benar dan sesuai dengan kondisi yang ada pada STIE Perbanas. Hasil luaran dari proses

mengevaluasi risiko adalah sebuah daftar prioritas risiko. Dimana daftar prioritas risiko tersebut nantinya akan menjadi masukan pada tahap perlakuan risiko untuk penentuan tujuan kontrol.

3.3 Tahap Perlakuan Risiko

Tahap perlakuan risiko dibagi kedalam lima proses yaitu penentuan perlakuan risiko, penentuan tujuan kontrol, verifikasi kebutuhan kontrol, justifikasi kebutuhan kontrol dan perencanaan perlakuan risiko. Berikut merupakan penjelasan dari masing masing proses dalam tahap perlakuan risiko.

3.3.1 Penentuan Perlakuan Risiko

Dalam proses penentuan perlakuan risiko akan ditentukan opsi mitigasi atau perlakuan risiko yang sesuai dengan hasil prioritasi risiko. Opsi perlakuan risiko akan didasarkan pada hasil penilaian risiko. Hasil luaran dari proses ini adalah berupa daftar risiko beserta masing masing opsi perlauan risikonya. Dimana daftar tersebut akan menjadi masukan bagi proses selanjutnya untuk menentukan tujuan kontrol yang sesuai dengan risiko.

3.3.2 Penentuan Tujuan Kontrol

Dalam proses penentuan tujuan kontrol akan ditentukan seluruh kontrol yang dibutuhkan untuk mengimplementasikan opsi perlakuan risiko yang telah ditentukan. Penentuan tujuan kontrol akan didasarkan pada kontrol yang ada pada kerangka kerja Cobit 5 dan kontrol yang ada pada kerangka kerja ISO27002:2013. Dalam proses penentuan tujuan kontrol, setiap risiko akan dipetakan langsung kedalam kontrol yang relevan dan dibutuhkan.

3.3.3 Verifikasi Kebutuhan Kontrol

Proses verifikasi kebutuhan kontrol merupakan proses dalam memastikan kebutuhan kontrol yang dipilih telah relevan dengan opsi perlakuan risiko yang ditentukan pada tahap sebelumnya. Dalam melakukan verifikasi kebutuhan kontrol akan dibuat sebuah daftar risiko, opsi perlakuan risiko dan kontrol yang dibutuhkan.

Hal ini akan memudahkan penelitian dalam melakukan validasi ketepatan kebutuhan kontrol.

3.3.4 Justifikasi Kebutuhan Kontrol

Proses justifikasi kebutuhan kontrol merupakan proses membuat sebuah pernyataan dari kebutuhan kontrol yang telah dipilih. Dalam penelitian ini justifikasi kebutuhan kontrol diperlukan untuk memastikan kebenaran kontrol. Dan dalam jstifikasi kebutuhan kontrol juga akan dipetakan dengan jelas kontrol yang diambil termasuk dalam kontrol ISO 27002:2013 atau Cobit 5. Dalam proses ini, akan dibuat sebuah daftar risiko, opsi perlakuan risiko, kontrol kerangka kerja dan justifikasi dari masing masing kontrol. Hasil luaran tersebut adalah sebuah tabel yang berisikan justifikasi kontrol.

3.3.5 Perencanaan Perlakuan Risiko

Proses perencanaan perlakuan risiko adalah proses pembuatan perencanaan perlakuan risiko. Dalam penelitian ini, perencanaan perlakuan risiko yang ditetapkan adalah dengan melakukan pembuatan dokumen SOP (*Standard Operating Procedure*). Dan dalam proses perencanaan pembuatan dokumen SOP akan terlebih dahulu dilakukan perancangan dokumen SOP yang dibutuhkan. Luaran dalam proses perencanaan perlakuan risiko ini adalah sebuah perancangan konten dokumen SOP keamanan data. Dimana perancangan tersebut akan terlebih dahulu di verifikasi dan validasi terhadap masing masing pemilik risiko untuk menentukan kesesuaian dan kebenarannya. Selanjutnya hasil perancangan konten dokumen SOP tersebut akan dikembangkan dalam tahap penyusunan SOP.

3.4 Tahap Penyusunan SOP

Tahap penyusunan SOP terdiri dari tiga proses utama yaitu pembuatan dokumen SOP, pembuatan skenarioisasi pengujian prosedur dalam SOP serta verifikasi dan validasi dokumen SOP.

Berikut adalah penjelasan dari masing masing proses dalam tahap penyusunan SOP.

3.4.1 Pembuatan Dokumen SOP

Proses pembuatan dokumen SOP adalah proses pengembangan dari perancangan konten dokumen SOP. Dokumen SOP yang dibuat akan disesuaikan dengan konten dokumen yang sudah divalidasi terhadap pihak manajemen STIE Perbanas. Pembuatan dokumen SOP akan didasarkan pada standard pembuatan dokumen SOP dan kontrol yang ada didalamnya merupakan kontrol yang mengacu pada kerangka kerja ISO27002:2013 dan Cobit 5.

3.4.2 Pembuatan Skenarioisasi Pengujian Prosedur dalam SOP

Pembuatan skenarioisasi pengujian prosedur dalam SOP adalah proses pembuatan tahapan pengujian prosedur dalam SOP. Dalam hal ini, skenarioisasi pengujian dibutuhkan untuk memastikan bahwa prosedur yang dikembangkan sesuai dengan kondisi STIE Perbanas dan dapat diimplementasikan dengan baik. Proses pengujian akan melibatkan pihak manajemen STIE Perbanas yang berkaitan dengan prosedur. Skenarioisasi pengujian akan berisikan seluruh prosedur yang ada, proses pengujiannya, keterangan pihak yang berhubungan dengan prosedur SOP dan hasil dari pengujian serta status untuk menunjukan penerimaan atau ketepatan prosedur. Apabila terdapat kesalahan dalam prosedur makan akan dilakukan kembali perbaikan pada prosedur. Dan apabila seluruh prosedur telah sesuai maka akan dilanjutkanpada proses selanjutnya yaitu verifikasi dan validasi dokumen SOP.

3.4.3 Verifikasi dan Validasi Dokumen SOP

Proses verifikasi dan validasi dokumen SOP merupakan tahapan yang dilakukan setelah seluruh pengujian prosedur SOP telah sesuai. Proses verifikasi dan validasi akan dilakukan oleh pihak manajemen STIE Perbanas. Hasil luaran dari proses verifikasi dan validasi adalah berupa keseluruhan dokumen SOP keamanan data untuk STIE Perbanas.

BAB IV
PERANCANGAN KONSEPTUAL

Bab ini menjelaskan tentang perancangan konseptual dalam pengerjaan tugas akhir ini, yaitu perancangan secara detail dari setiap tahapan pengerjaan yang telah dijerlaskan pada Bab III. Dalam tahap perancangan, terdapat tiga proses utama yaitu penentuan subjek dan objek penelitian, pembuatan daftar pertanyaan dalam bentuk *interview protocol* untuk wawancara pengalian data dan perancangan penilaian risiko serta perancangan SOP.

4.1 Objek Penelitian

Penelitian ini dilakukan pada STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas (Perhimpunan Bank Nasional Swasra) yang merupakan sebuah lembaga pendidikan tinggi dalam bidang perbankan. Objek yang akan diteliti adalah keamanan data pada STIE Perbanas. Objek keamanan data dalam STIE Perbanas merupakan salah satu bagian dari keamanan informasi yang sedang dikembangkan. Dimana dengan terkelolanya keamanan data dengan baik pada STIE Perbanas dapat meningkatkan keefektifan proses bisnis yang berjalan.

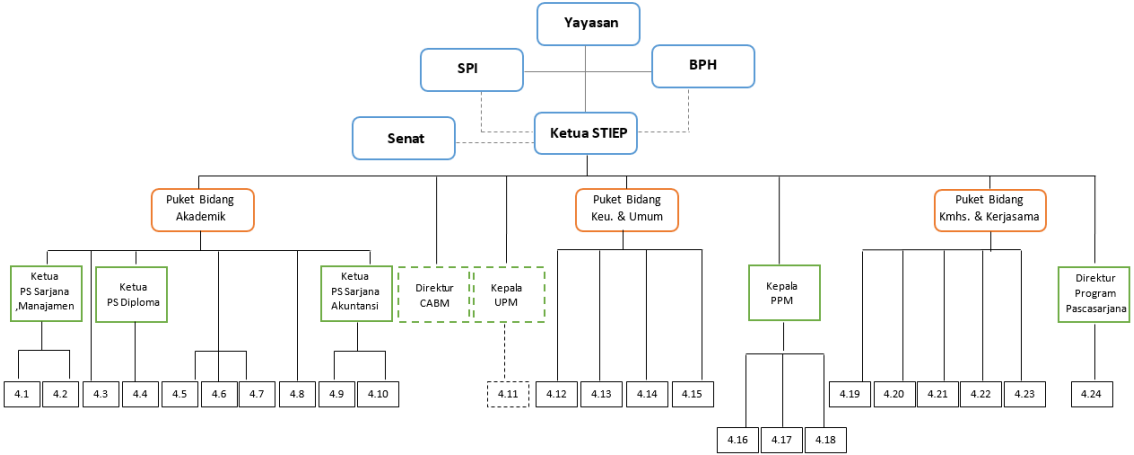
Proses perbaikan keamanan data untuk STIE Perbanas dalam penelitian ini akan dikembangkan dari segi manajamen yaitu dengan membuat sebuah prosedur berdasarkan kerangka kerja Cobit 5 dan ISO27002:2013. Selama melakukan penelitian ini, peneliti mendapat dukungan dari pihak manajemen STIE Perbanas khususnya Bagian TIK dan Bidang Akademik yang merupakan narasumber utama dalam proses penggalian kebutuhan. Narasumber utama tersebut adalah Pembantu Ketua Bidang Akademik dan Kasie TIK (Manajemen Jaringan dan Technical Support).

4.1.1 Profil dan Sejarah STIE Perbanas

STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas (Perhimpunan Bank Nasional Swasta) Jawa Timur merupakan sebuah lembaga pendidikan tinggi dalam bidang perbankan. Berikut ini adalah penjelasan lebih lanjut mengenai STIE Perbanas Surabaya. STIE Perbanas mendirikan Kursus Kader Bank Tingkat "A" untuk lulusan SLTP dan Kursus Kader Bank Tingkat "B" untuk lulusan SLTA. Dan pada tahun akademik 1967/1968 Perbanas menyelenggarakan pendidikan Kader Bank "B" Lisan untuk karyawan dan karyawati bank di Surabaya, baik untuk bank pemerintah maupun bank swasta. Penyelenggaraan lembaga tersebut bertempat di Aula PT. Bank Amerta. Pengembangan dari lembaga pendidikan Kader Bank "B" Lisan kemudian menjadi Akademi Ilmu Perbankan Perbanas Surabaya (AIP Perbanas Surabaya) yang dilaksanakan pada 29 Januari 1970 sesuai dengan Surat Keputusan Perbanas Pusat No. 25/Perbanas/1970. STIE Perbanas memiliki sebuah lambang yang menjadi identitas dengan mengusung makna "Segenap Sivitas Akademika STIE Perbanas Bersatu Di Dalam Pengabdian Yang Teguh Dan Tak Kunjung Padam, Di Dalam Menuntut Ilmu Menuju Kesejahteraan Dan Kemakmuran Nusa Dan Bangsa, Sesuai Dengan Cita Cita Proklamasi Kemerdekaan Bangsa Indoneisa Tanggal 17 Agustus 1945".

4.1.2 Struktur Organisasi Yayasan STIE Perbanas

Funsional bisnis dalam STIE Perbanas digambarkan dalam sebuah struktur organisasi Yayasan STIE Perbanas yang akan dijelaskan pada subab struktur organisasi dan proses bisnis yang berjalan dalam STIE Perbanas yang akan dijelaskan adalah proses bisnis yang berkaitan dalam penelitian pada subab proses bisnis yang terlibat dalam penelitian.



Gambar 4.1. Struktur Organisasai STIE Perbanas

Berikut adalah keterangan Struktur Organisasi Yayasan Pendidikan STIE Perbanas:

1.1 Sekretaris Program Studi (PS) Sarjana Manajemen
1.2 Kepala Laboratorium Manajemen
1.3 Kepala Bagian Akademik
1.4 Sekretaris PS Diploma
1.5 Kepala Laboratorium Komputer & PTP
1.6 Kepala Laboratorium Bahasa
1.7 Kepala Laboratorium Bank STIE
1.8 Kepala Bagian Perpustakaan
1.9 Sekretaris PS Sarjana Akuntansi
1.10 Kepala Laboratorium Akuntansi
1.11 Wakil Ketuan Unit Penjaminan Mutu (UPM)
1.12 Kepala Bagian SDM
1.13 Kepala Bagian Keuangan
1.14 Kepala Bagian Umum
1.15 Kepala Bagian Teknologi Informasi dan Komunikasi (TIK)
1.16 Kepala Bidang Abdimas
1.17 Kepala Bidang Penelitian
1.18 Kepala Pengelolaan Jurnal dan Penerbitan Buku
1.19 Kepala Bagian Humas
1.20 Kepala Bagian Kerjasama
1.21 Kepala Perbanas Career Center
1.22 Kepala Bagian Kemahasiswaan
1.23 Kepala Student Advisory Center
1.24 Sekretaris Program Pascasarjana

4.1.3 Proses Bisnis yang Terlibat dalam Penelitian

Proses Bisnis berdasarkan Pedoman Mutu STIE Perbanas dibagi kedalam tiga proses utama yaitu pada proses *upstream*, *midstream* dan *downstream*. Dalam masing masing proses tersebut terdapat pula beberapa aktivitas atau kegiatan lainnya. Berikut adalah gambaran proses bisnis inti yang ada pada STIE Perbanas.

Tabel 4. 1. Proses Bisnis Inti STIE Perbanas

UPSTREAM	MIDSTREAM	DOWNSTREAM
		
CABM, Penelitian dan Pengabdian Masyarakat, Unit Kerjasama		
Kemahasiswaan dan Alumni, PCC dan SAC		
Perpustakaan		
Laboratorium		
Layanan Administrasi Umum, Keuangan, Akademik dan SDM, Kehumasan, Sekretariat		
Teknologi Informasi dan Komunikasi		

Dalam proses bisnis diatas, hampir seluruh proses utama dalam *upstream* dan *midstream* didukung oleh adanya teknologi informasi. Sehingga aktivitas dalam proses bisnis utama dalam *upstream* dan *downstream* secara tidak langsung berkaitan dengan penelitian. Dimana Bagian TIK harus memastikan keamanan data yang mengalir selama proses bisnis utama dalam *upstream* dan *downstream* berlangsung.

4.2 Pengumpulan Data dan Informasi

Pengumpulan data dengan teknik *in-dept interview* atau wawancara, yang akan dilaksanakan terhadap Bagian TIK dan Bidang Akademik STIE Perbanas selaku perwakilan yang memiliki wewenang dalam teknologi informasi. Berikut ini adalah perancangan proses dari pengumpulan data dan informasi.

Tabel 4. 2. Deskripsi perancangan proses pengumpulan data dan informasi

Nama Proses	Pengumpulan Data dan Informassi
Teknik	**Wawancara** Wawancara sebuah kegiatan penggalian informasi melalui percakapan secara langsung kepada pihak yang berkaitan dengan objek penelitian. Wawancara umumnya menggunakan format Tanya jawab yang terencana. Dalam penelitian ini, jenis wawancara yang digunakan adalah wawancara terstruktur, yaitu dengan mempersiapkan pertanyaan.
Objek	Keamanan Data pada Komponen Sistem Informasi STIE Perbanas
Kebutuhan proses	*Interview protocol*
Strategi pelaksanaan	Untuk mengumpulkan data melalui wawancara perlu dirumuskan strategi pelaksanaan agar pada saat wawancara berlangsung tidak ditemui hambatan. Strategi tersebut dapat berupa urutan tahapan yang

Nama Proses	Pengumpulan Data dan Informassi
	akan dilakukan untuk memperisapkan wawancara. Tahapan wawancara tresebut adalah sebagai berikut : • Menetapkan tujuan wawancara • Membuat Interview Protocol • Menentukan narasumber

1. Tujuan Wawancara

Tujuan wawancara ditetapkan untuk menjadi acuan dalam perumusan pertanyaan wawancara, sehingga proses penggalian data dapat berjalan sesuai dengan tujuan yang diinginkan dan mendapatakan data serta informasi yang dibutukan dalam penelitian.

Tabel 4. 3. Tujuan Wawancara

Wawancara Ke-	Narasumber	Tujuan Wawancara
1	Pembantu Ketua 1 Bidang Akademik	Penggalian informasi mengenai proses bisnis dalam STIE Perbanas dan fungsi fungsi yang ada didalamnya, gambaran umum penggunaan teknologi informasi, kebutuhan keamanan data, pengelolaan aset sistem informasi, risiko keamanan yang pernah terjadi dan sering terjadi.
2	Bagian TIK	Penggalian informasi mengenai implementasi teknologi infomasi dalam STIE Perbanas termasuk didalamnya teknis mengenai penggunaan hardware, software, database dan jaringam, kelemahan teknologi informasi dari sudut pandang TIK, risiko

Wawancara Ke-	Narasumber	Tujuan Wawancara
		keamanan yang pernah terjadi dan sering terjadi.

2. Membuat *Interview Protocol*

Interview Protocol adalah daftar pertanyaan yang akan diajukan pada saat wawancara dengan narasumber. Dalam penelitian ini, *interview protocol* akan dibuat dengan berdasarkan pada tujuan wawancara yang sudah ditentukan. Berikut merupakan *interview protocol* dan detail ringkas pertanyaan yang akan diajukan pada saat wawancara.

Tabel 4. 4. Detail Ringkas Pertanyaan dalam Interview Protocol

No	Tujuan pertanyaan	Detail ringkas pertanyaan
1	Penggalian informasi mengenai proses bisnis dalam STIE Perbanas dan fungsi fungsi yang ada didalamnya, gambaran umum penggunaan teknologi informasi, kebutuhan keamanan data, pengelolaan aset sistem informasi, risiko keamanan yang pernah terjadi dan sering terjadi.	• Aktivitas utama dalam proses bisnis akademik di STIE Perbanas • Data struktur organisasi dan peran fungsi yang terlibat dalam proses bisnis • Data yang kritikal dalam operasional • Hak akases terhadap data kritikal • Praktek pengamanan yang telah dilakukan • Identifikasi risiko keamanan data dari segi kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availabilit*) • Seberapa sering risiko terjadi beserta penyebab dan dampaknya

No	Tujuan pertanyaan	Detail ringkas pertanyaan
2	Penggalian informasi mengenai implementasi teknologi infomasi dalam STIE Perbanas termasuk didalamnya teknis mengenai penggunaan hardware, software, database dan jaringam, kelemahan teknologi informasi dari sudut pandang TIK, risiko keamanan yang pernah terjadi dan sering terjadi.	• Aktivitas utama bagian TIK • Proses bisnis penerapan TI di STIE Perbanas • Data yang kritikal dalam operasional • Hak akases terhadap data kritikal • Praktek pengamanan yang telah dilakukan • Identifikasi risiko keamanan data dari segi kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availabilit*) • Seberapa sering risiko terjadi beserta penyebab dan dampaknya

3. Menentukan Narasumber

Penentuan narasumber dilakukan untuk memudahkan proses pengumpulan data. Dalam penetapan pihak narasumber, yang harus diperahtikan adalah kapasitas objek dalam kewenangannya memberi informasi yang valid, dan apakah pertanyaan yang dirumuskan relevan dengan pengetahuan pihak narasumber. Berikut adalah profil narasumber dalam penelitian.

Tabel 4. 5. Narasumber Penelitian

Nama	Jabatan
Dr. Drs. Emanuel Kritijadi, MM	Pembantu ketua Bidang Akademik
Hariadi Yutanto, S.Kom, M.Kom	Kasie TIK (Manajemen Jaringan dan Technical Support)

4.3 Perancangan Penilaian Risiko

Dalam melakukan penilaian risiko, penelitian menggunakan pendekatan *risk assessment* kerangka kerja ISO27002:2013 dengan metode FMEA (*Failure Modes and Effecs Analysis*). Dimana dalam pendekatan *risk assessment* tersebut terdapat beberapa proses dalam melakukan penilaian risiko yaitu menetapkan dan mengelola kriteria, mengidentifikasi risiko, menganalisa risiko dan mengevaluasi risiko.

4.3.1 Kriteria dalam Melakuan Penilaian Risiko

Dalam melakukan penilaian risiko, metode yang digunakan dalampenelitian adalah metode FMEA. Dalam metode FMEA terdapat keiteria dalan melakukan penilaian risiko yaitu berdasarkan pada nilai dampak (*severity*), nilai kemungkinan (*occurence*) dan nilai deteksi (*detection*). Berikut adalah kriteria perhitungan untuk masing masing nilai.

a. Penentuan Nilai Dampak (*Severity* = S)

Pengukuran nilai dampak akan dilihat dari seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek aspek penting dalam organisasi. Dalam menentukan penilaian tingkat dampak, perlu dibuat parameter untuk setiap nilainya. Berikut merupakan penjelasan dari masing masing nilai dampak.

Tabel 4. 6. Kriteria Nilai Dampak

Dampak	Dampak dari Efek	Ranking
Akibat Berbahaya	Melukai Pelanggan atau Karyawan	10
Akibat Serius	Aktivitas yang illegal	9
Akibat Ekstrim	Mengubah Produk atau Jasa menjadi tidak layak digunakan	8
Akibat Major	Menyebabkan ketidakpuasan pelanggan secara ekstrim	7

Dampak	Dampak dari Efek	Ranking
Akibat Signifikan	Menghasilkan kerusakan parsial secara moderat	6
Akibat Moderat	Menyebabkan penurunan kinerja dan mengakibatkan keluhan	5
Akibat Minor	Menyebabkan sedikit kerugian	4
Akibat Ringan	Menyebabkan gangguan kecil yang dapat diatas tanpa kehilangan sesuatu	3
Akibat Sangat Ringan	Tanpa disadari: terjadi gangguan kecil pad kinerja	2
Tidak Ada Akibat	Tanpa disadari dan tidak mempengaruhi kinerja	1

b. Penentuan Nilai Kemungkinan (*Occurrence* = O)

Pengukuran nilai kemungkinan adalah kemungkinan bahwa penyebab kegagalan akan terjadi dan menghasilkan bentuk kegagalan proses. Nilai kemungkinan merupakan pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat menghasilkan kegagalan. Berikut merupakan penjelasan dari nilai kemungkinan.

Tabel 4. 7. Kriteria Nilai Kemungkinan

Kemungkinan Kegagalan	Probablitas	Ranking
Very High: Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya	10
Very High: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari	9
High: Kegagalan terjadi berulang kali	Satu kali dalam seminggu	8
High: Kegagalan sering terjadi	Satu kali dalam sebulan	7

Kemungkinan Kegagalan	Probablitas	Ranking
Moderatly High : Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate : Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low : Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relative kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relative kecil dan sangat jarang	Satu kali dalam 3 - 6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6 - 50 tahun	1

c. Penentuan Nilai Deteksi (*Detection* = D)

Pengkuruan nilai deteksi merupakan penilaian terhadap kemampuan organisasi dalam melakukan kontrol dan kendali terhadap terjadinya suatu gangguan atau kegagalan yang akan terjadi. Berikut adalah penjelasan nilai deteksi dan metode deteksi terhadap risiko.

Tabel 4. 8. Kriteria Nilai Deteksi

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode detensi	10
Sangat Kecil	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi	9
Kecil	Metode deteksi tidak terbukti untuk mendeteksi tepat waktu	8

Deteksi	Kriteria Deteksi	Ranking
Sangat Rendah	Metode deteksi tidak andal dalam mendeteksi tepat waktu	7
Rendah	Metode deteksi memiliki tingkat efektifitas yang rendah	6
Sedang	Metode deteksi memiliki tingkat efektifitas yang rata-rata	5
Cukup Tinggi	Metode deteksi memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan	4
Tinggi	Metode deteksi memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan	3
Sangat Tinggi	Metode deteksi sangat efektif untuk dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	2
Hampir Pasti	Metode deteksi hampir pasti dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	1

Setelah melakukan penetuan nilai dampak (*severity*), nilai kemungkinan (*occurence*) dan nilai deteksi (*detection*) selanjutnya adalah melakukan kalkulasi nilai prioritasi risiko (Risk Priority Number) yang didapatkan dari formulasi berikut :

RPN = S x O x D

RPN : *Risk Priority Number*, perhitungan nilai risiko
S : *Severity*, nilai dampak
O : *Occurrence*, niai kemungkinan
D: *Detection*, nilai deteksi

4.3.2 Kriteria dalam Penerimaan Risiko

Penentuan kriteria penerimaan risiko didasarkan pada hasil penilaian risiko, dimana setelah ditentukan nilai RPN dari masing masing risiko, selanjutnya ditentukan level risiko berdasarkan skala RPN. Risiko dengan tingkat *very high* dan *high* kemudian akan dialakukan analisis lebih lanjut untuk menentukan perlakuan risiko. Berikut ini adalah skala penentuan nilai RPN berdasarkan pada metode FMEA.

Tabel 4. 9. Penerimaan Risiko (sumber: FMEA)

Level Risiko	Skala Nilai RPN
Very High	> 200
High	< 200
Medium	< 120
Low	< 80
Very Low	< 20

4.4 Perencanaan Perlakuan Risiko

Hasil dari analisis dan penilaian risiko serta penerimaan risiko kemudian akan menjadi masukan dalam tahap perencanaan perlakuan risiko. Dalam perencanaan perlakuan risiko dilakukan terlebih dahulu penentuan tujuan kontrol berdasarkan kerangka kerja Cobit 5dan ISO27002:2013. Penentuan tujuan kontrol tersebut dilakukan dalam dua tahap yaitu pemetaan risiko dengan kategori keamanan data dengan kontrol pada kerangka kerja Cobit 5 dan selanjutnya melakukan pemetaan kontrol Cobit 5 dengan kontrol pada ISO27002:2013.

4.4.1 Pemetaan Risiko dengan Kontrol Cobit 5

Dalam melakukan pemetaan kategori keamanan data masukan yang dibutuhkan adalah hasil dari penilaian risiko. Pemetaan ini dilakukan dengan tujuan untuk menentukan tujuan kontrol yang dibutuhkan dalam melakukan mitigasi terhadap risiko. Selain itu,

dalam penentuan tujuan kontrol juga akan ditambahkan justifikasi untuk memastikan kontrol yang digunakan telah sesuai dengan kebutuhan. Berikut adalah tabel pemetaan risiko dengan kategori keamanan data dan kontrol Cobit 5.

No	Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Level Risiko	Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Poetensial Dampak	Kontrol Cobit 4.1	Justifikasi

Gambar 4. 2. Contoh Pemetaan Risiko dengan Kontrol Cobit 5

4.4.2 Pemetaan Risiko dan Kontrol ISO27002:2013

Pemetaan ini dilakukan dengan tujuan untuk menentukan tujuan kontrol ISO27002:2013 yang dibutuhkan dalam melakukan mitigasi terhadap risiko. Berikut adalah tabel pemetaan risiko dengan kategori keamanan data dan kontrol ISO27002:2013.

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi

Gambar 4. 3. Contoh Pemetaan Risiko dengan Kontrol ISO27002:2013

Dan setelah pemetaan kontrol dengan kerangka kerja Cobit 5dan ISO27002:2013 kemudian dibuat daftar rekomendasi mitigasi risiko. Hasil rekomendasi mitigasi risiko inilah yang akan menjadi bahan pertimbangan untuk usulan perancangan prosedur.

4.4.3 Rekomendasi Mitigasi Risiko

Setelah memetakan risiko dan kontrol Cobit dan ISO27002:2013 selanjutnya adalah menentukan mitigasi risiko. Mitigasi risiko didasarkan pada kontrol kedua standard. Luaran yang didapatkan dari penentuan mitigasi risiko adalah identifikasi sebuah prosedur yang diperlukan untuk memastikan risiko tidak berulang. Berikut ini adalah tabel rekomendasi mitigasi risiko.

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Rekomendasi mitigasi risiko	Prosedur yang dihasilkan
					Kontrol keamanan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013		

Gambar 4. 4. Contoh Rekomendasi Mitigasi Risiko

4.4 Perancangan SOP

Dalam penyusunan dokumen SOP tidak terdapat suatu format baku yang dapat dijadikan acuan, hal ini dikarenakan SOP merupakan dokumen internal yang kebiijakan pembuatannya disesuaikan oleh masing masing organisasi, begitu pula dengan penyunan format dari dokumen SOP tersebut. Format langkah-langkah dalam SOP akan dibuat dalam bentuk *flowchart* untuk memudahkan penggambaran aktivitas. Berikut merupakan penjelasan dari format SOP yang akan dikembangkan dan juga *flowchart* penggambaran aktivitas prosedur.

Format SOP akan dikembangkan sesuai dengan struktur standard dengan acuan dari peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia mengenai pedoman penyusunan standar operasional prosedur nomor 35 tahun 2012. Berdasarkan panduan tersebut, berikut penjelasan struktur dan konten yang akan dimasukkan dalam dokumen SOP penelitian.

Tabel 4. 10. Format Konten SOP

Struktur Bab	Sub-Bab	Deskripsi
Pendahuluan	Tujuan	Berisi tujuan dari dibuatnya dokumen SOP
	Ruang Lingkup	Merupakan ruang lingkup dari prosedur-prosedur yang akan dimuat dalam dokumen
	Overview Keamanan Data	Berisi penjelasan singkat mengenai keamanan data dan aspek kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*)

Struktur Bab	Sub-Bab	Deskripsi
	Evaluasi Penilaian Risiko	Berisikan penjelasan dan hasil dari penilaian risiko
Prosedur	Deskripsi Umum	Merupakan pendefinisian tujuan, ruang lingkup, referensi kontrol dan pendefinisian istilah lain yang terkait dalam prosedur
	Rincian Prosedur	Berisi penjabaran aktivitas-aktivitas yang perlu dilakukan dan ditampilkan dalam bentuk *flowchart*
	Bagan Alur SOP	Semua formulir yang diperlukan untuk menjalankan prosedur akan dijelaskan cara penggunaannya

4.5 Perancangan Pengujian SOP

Pengujian SOP dilakukan melalui dua cara yakni verifikasi dan validasi. Verifikasi dilakukan dengan cara wawancara untuk memastikan kebenaran informasi yang terkandung dalam SOP, sedangkan validasi dilakukan dengan simulasi untuk mengetahui ketepatan SOP ketika implementasi dalam kasus nyata.

Tabel 4. 11. Metode Pengujian SOP

	Tujuan	Metode	Sasaran
Verifikasi	Untuk melakukan verifikasi terhadap dokumen untuk memastikan kebenaran dari informasi-informasi yang didefinisikan dan termuat di dalam dokumen SOP	Wawancara	*Key User (*pihak yang memiliki kedudukan penting dalam Bagian TIK STIE Perbanas dan memiliki kewenangan untuk mendefinisikan kebutuhan keamanan) yaitu *Kasie TIK STIE Perbanas*
Validasi	Untuk melakukan validasi dokumen dengan melihat apakah SOP dapat berjalan sesuai dengan kondisi yang ada dan untuk menemukan kekurangan dari SOP yang telah dibuat sehingga dapat dilakukan koreksi dan selanjutnya dapat diterapkan	Simulasi Pengujian dokumen SOP	Pelaksana SOP, yakni : Pegawai Bagian TIK (administrator aplikasi dan jaringan)

4.5.1 Verifikasi

Verifikasi dilakukan dengan tujuan memastikan kebenaran dari informasi yang termuat dalam dokumen SOP dan kesesuaiannya ddengan kondisi STIE Perbanas. Metode yang digunakan dalam melakukan verifikasi adalah dengan wawancara dengan bagian TIK STIE Perbanas sebagai pihak yang memiliki kewenangan dalam keamanan teknologi informasi. Berikut adalah tahapan yang dilakukan dalam melakukan verifikasi pengujian SOP.

1. Penulis menyerahkan dokumen SOP kepada bagian TIK dan menjelaskan isi dokumen dengan detil.
2. Bagian TIK melakukan review dokumen SOP.
3. Penulis mengadakan wawancara secara langsung setelah Bagian TIK selesai mereview dokumen. Pertanyaan yang dilontarkan terkait struktur SOP, konten SOP, serta istilah yang digunakan dalam SOP.
4. Bagian TIK memberikan review dan revisi dokumen jika ada
5. Penulis melakukan pembenahan dokumen SOP sesuai saran dari Bagian TIK.
6. Penulis menyerahkan ulang hasil revisi pada bagian TIK.
7. Bagian TIK menyetujui dokumen SOP yang telah diperbaiki.

4.5.2 Validasi

Validasi dilakukan untuk memastikan dokumen SOP dapat berjalan sesuai dengan kondisi yang ada pada STIE Perbanas dan untuk menemukan ketidaksesuaian dan kekurangan SOP sehingga dapat dibenahi sesuai kondisi yang ada. Metode yang digunakan adalah dengan pengujian SOP dengan pelaksana SOP yaitu bagian TIK. Berikut merupakan tahapan yang dilakukan dalam melakukan validasi pengujian SOP.

1. Penulis menyerahkan dokumen SOP yang telah diperbaiki pada tahap verifikasi.
2. Penulis memberikan arahan penggunaan dokumen SOP dan menjelaskan beberapa skenario yang akan diuji.
3. Pelaksana SOP mensimulasikan SOP dengan menggunakan case yang masuk pada service desk, termasuk mengisi form-form yang tersedia.
4. Setelah simulasi selesai, penulis meminta *feedback* dan *review* dari pelaksana.
5. Penulis melakukan perbaikan dokumen jika terdapat ketidaksesuaian pada proses simulasi
6. Setelah selesai, dokumen SOP dapat dinyatakan valid dan dapat diterapkan.

Halaman ini sengaja dikosongkan

BAB V
IMPLEMENTASI

Bab ini menjelaskan tentang implementasi setiap tahapan dan proses-proses di dalam metodologi tugas akhir yang dapat berupa hasil, waktu pelaksanaan dan lampiran terkait yang memuat pencatatan tertentu dengan implementasi proses.

5.1 Proses Pengumpulan Data

Pengumpulan data yang dilakukan dalam penelitian bertujuan untuk mengidentifikasi dan menganalisa risiko yang berkaitan dengan keamanan data pada STIE Perbanas. Dalam melakukan pengumpulan data, dilakukan wawancara menggunakan *interview protocol* dengan Pembantu Ketua Bidang Akademik dan Kepala SIE TIK STIE Perbanas. Hasil dari wawancara dapat dilihat pada Lampiran A. Berikut adalah hasil analisis risiko yang dapat ditarik dari hasil wawancara mengenai identifikasi risiko keamanan data.

5.1.1 Identifikasi Aset Kritis

Penentuan aset kritis dilakukan melalui pengumpulan informasi berdasarkan sudut pandang pihak manajemen STIE Perbanas yaitu Pembantu Ketua 1 Bidang Akdemik dan Ketua SIE TIK. Dari hasil wawancara yang terlampir pada Lampiran A dan Lampiran B maka dapat disimpulkan bahwa dalam masing masing kategori Aset TI terdapat aset kritis yang dijelaskan dalam tabel berikut ini.

Tabel 5. 1. Daftar Aset Kritis

Daftar Aset Kritis		Alasan/Sebab
Hardware	Server	Server dan PC menjadi pendukung dalam proses bisnis akademik. Server menjadi aset penting untuk memastikan data selalu dapat diakses dan komputer digunakan untuk proses operasional Bagian TIK
	PC	

Daftar Aset Kritis		Alasan/Sebab
		dan juga sebagai media untuk mengakses data.
Software	SISFO	Aplikasi SISFO, E-Learning, dan perpustakaan merupakan pendukung kegiatan akademik. Dalam SISFO yang datanya saling terintegrasi, salah modul yang paling penting adalah SIMAS sebagai sistem informasi akademik mahasiswa yang berisikan data akademik dan demografi mahasiswa. Dalam E-Learning Data penting yang terkait adalah mengenai materi ajar dosen. Sedangkan dalam Sistem Informasi Perpustakaan data penting yang terkait adalah mengenai keseluruhan penelitian yang dilakukan pada STIE Perbanas.
	E-Learning (kuliah.perbanas.ac.id)	
	Sistem Informasi Perpustakaan	
Data	Data Demografi Mahasiswa	Data terkait akademik, demografi mahasiswa penting dalam proses kegiatan akademik dan data file server penting dalam kegiatan/proses perkuliahan pada STIE Perbanas. Seluruh data hampir dibutuhkan oleh semua komponen.
	Data Akademik	
	Data File Server	
Jaringan	Wifi	Jaringan digunakan untuk mengakses informasi, seperti mengakses database dan mengakses internet.
	Kabel	
	Router	

Daftar Aset Kritis		Alasan/Sebab
Sumber Daya Manusia	Dosen	Suatu aset yang penting dalam sebuah organisasi karena SDM yang memiliki kompetensi dapat mendukung proses bisnis berjalan dengan lancer.
	Mahasiswa	
	Pegawai	

5.1.2 Identifikasi Kebutuhan Kemanan Aset Kritis

Kebutuhan keamanan merupakan bentuk perlindungan terhadap ancaman yang mungkin terjadi dalam upaya untuk memastikan keberlangsungan proses bisnis, meminimalisir risiko bisnis. Sedangkan aspek keamanan data yaitu kerahasisaan (*confidentiaityl*), integritas (*integrity*) dan ketersediaan (*availability*) merupakan aspek dasar yang digunakan sebagai dasar keamanan data didalam tugas kahir ini. Aspek keamanan data tersebut akan menjadi kategori dalam mengidentifikasi kebutuhan keamanan aset kritis. Berikut adalah daftar kebutuhan keamanan aset kritis pada STIE Perbanas.

Tabel 5. 2. Daftar Kebutuhan Keamanan Aset Kritis

Aset Kritis	Kebutuhan Kemanan	Penjelasan	Narasumber
Server	Ketersediaan (availability)	Dapat diakses 24 jam dalam 7 hari	Bagian TIK
	Ketersediaan (availability)	Konfigurasi server dilakukan dengan benar	Bagian TIK
	Ketersediaan (availability)	Adanya sumber listrik cadangan	Bagian TIK
	Kerahasiaan (confidentiality)	Adanya kontrol keamanan untuk ruang fisik server	Bagian TIK
	Kerahasiaan (confidentiality)	Adanya pembatasan hak akses	Bagian TIK

Aset Kritis	Kebutuhan Kemanan	Penjelasan	Narasumber
	Integritas (integrity)	Server tidak boleh diakses oleh usb atau pihak yang tidak berwenang yang dapat mengubah konten	Bagian TIK
PC	Ketersediaan (availability)	Dapat berfungsi selama jam kerja organisasi	Bagian TIK
	Ketersediaan (availability)	Adanya sumber listrik cadanagn	Bagian TIK
	Ketersediaan (availability)	Adanya Antivirus	Bagian TIK
	Kerahasiaan (confidentiality)	Adanya pembatasan hak akses	Bagian TIK
	Integritas (integrity)	Data-data yang terdapat didalam pc harus lengkap dan harus lengkap dan harus memiliki login agar kerahasiaan terjaga	Bagian TIK
SISFO	Ketersediaan (availability)	Dapat diakses 24 jam dalam 7 hari	Bagian TIK
E-Learning	Ketersediaan (availability)	Data dapat diakses 24 jam dalam 7 hari	Bagian TIK
Perpustakaan	Ketersediaan (availability)	Adanya backup data secara rutin	Bagian TIK

Aset Kritis	Kebutuhan Kemanan	Penjelasan	Narasumber
	Integritas (integrity)	Data-data terkait dalam aplikasi harus lengkap dan akurat	Bidang Akademik
Data Demografi Mahasiswa	Kerahasiaan (confidentiality)	Adanya pembatasan hak akses	Bagian TIK
	Kerahasiaan (confidentiality)	Adanya pengamanan terhadap data	Bidang Akademik
Data Akademik	Kerahasiaan (confidentiality)	Adanya pengamanan terhadap data	Bidang Akademik
Data File Server	Kerahasiaan (confidentiality)	Adanya pembatasan hak akses pegawai pada data	Bagian TIK
	Integritas (integrity)	Data-data harus lengkap dan akurat	Bidang Akademik
Wifi	Ketersediaan (availability)	Tersedia selama jam operasional kerja organisasi	Bagian TIK
	Ketersediaan (availability)	Terdapat sumber listrik cadangan	Bagian TIK
	Ketersediaan (availability)	Adanya kontrol rutin	Bagian TIK
	Ketersediaan (availability)	Adanya anti netcut	Bagian TIK
Kabel	Ketersediaan (availability)	Tersedia selama jam operasional kerja organisasi	Bagian TIK

Aset Kritis	Kebutuhan Kemanan	Penjelasan	Narasumber
	Ketersediaan (availability)	Adanya kontrol rutin	Bagian TIK
	Ketersediaan (availability)	Kabel dilakukan pelabelan untuk mempermudah pengorganisasian	Bagian TIK
Router	Ketersediaan (availability)	Tersedia selama jam operasional kerja organisasi	Bagian TIK
	Ketersediaan (availability)	Adanya kontrol rutin	Bagian TIK
	Integritas (integrity)	Memonitoring jaringan untuk memastikan keaslian data	Bagian TIK

5.1.3 Identifikasi Ancaman Aset Kritis

Ancaman aset kritis merupakan hal yang mungkin terjadi dan pernah terjadi pada aset dan mengakibatkan terganggung proses bisnis. Identifikasi ancaman pada aset kritis dikategorikan kedalam ancaman dari lingkungan, ancaman dari manusia dan anacaman dari infrastruktur. Daftar Ancaman berikut ini didapatkan dari hasil wawancara kepada narasumber. Berikut adalah daftar ancaman aset kritis pada STIE Perbanas.

Tabel 5. 3. Daftar Ancaman Aset Kritis

Ancaman dari Lingkungan	
1.	Gempa Bumi
2.	Tsunami dan Badai
3.	Banjir
4.	Kebakaran
5.	Kebocoran dan Kerusakan Pada Bangunan

6.	Perubahan Regulasi
Ancaman dari Manusia	
7.	Kesalahan input data
8.	Data Corrupt/Rusak
9.	Pencurian Data
10.	Sharing Password
11.	Sabotase Jaringan Internet
12.	Penurunan Kompetensi Karyawan
Ancaman dari Infrastruktur	
Hardware	
13.	Kerusakan Komputer
14.	Kerusakan Server
15.	Kerusakan pada Genset dan UPS
16.	Kesalahan Konfigurasi Hardware
17.	Pencurian Peralatan Hadware
Software	
18.	Bug pada Software
19.	Virus/Worm
20.	Kesalahan Konfigurasi Sistem
21.	Pembobolan sistem
Jaringan	
22.	Gangguan pada Router
23.	Kerusakan Kabel
24.	Gangguan Koneksi Internet

5.1.4 Identifikasi Praktik Keamanan yang telah dilakukan Organisasi

Berikut ini merupakan daftar praktik keamanan yang telah dilakukan STIE Perbanas dalam memastikan keamanan teknologi informasi dapat mendukung berjalannya proses bisnis.

Tabel 5. 4. Daftar Praktik Keamanan yang telah dilakukan Organisasi

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
Adanya antivirus (e-scan) dan diupdate terus menerus	Bagian TIK
Adanya update patch dan firewall secara berkala	Bagian TIK
Telah dipasang anti netcut untuk keamanan Wifi	Bagian TIK
Pada Lab tidak bisa memasang USB	Bagian TIK
Pada Lab tidak bisa menginstall aplikasi dari luar	Bagian TIK
Telah dipasang Smoke Detector pada ruang server untuk memberi peringatan apabila terjadi kebakaran	Bidang Umum
Telah ada fire extinguisher untuk memadamkan api saat terjadi kebakaran	Bidang Umum
Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI	Bagian TIK
Telah dilakukan backup server dan NAS setiap hari pukul 19.00	Bagian TIK
Ada penguncian/penggembokan pada ruang server sehingga tidak dapat sembarang orang bisa masuk	Bagian TIK
Data hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja	Bagian TIK
Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk kelas dan lab	Bagian TIK
Dilakukan maintenance setiap sebelum UTS dan UAS hanya untuk lab saja	Bagian TIK
Dilakukan maintenance Wifi setiap 2 minggu sekali	Bagian TIK

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan fungsinya	Bagian TIK
Pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabel	Bagian TIK
Pembuatan dan pelaksanaan beberapa SOP mengenai SI/TI di organisasi	Bagian TIK
Adanya log setiap aktivitas dalam sistem informasi SISFO	Bagian TIK

5.1.5 Identifikasi Kerentanan pada Teknologi

Berikut merupakan daftar kerentanan pada teknologi yang dibagi kedalam masing masing aset kritis.

Tabel 5. 5. Daftar Kerentanan pada Teknologi

Server	
System of Interest	Server yang menyimpan Data Penting
Komponen Utama	**Kemungkinan Ancaman**
• Sistem Operasi • Processor • RAM • Harddisk • Listrik • Keamanan Jaringan • Genset • UPS • Kabel • Smoke Detector • Ruang Server	• Tidak dapat mendapatkan aliran listrik karena terjadi pmadaman pada PLN • Genset tidak dapat berfungsi karena mengalami kerusakan • RAM mengalami kelebihan memori • Kinerja Procesor menurun akibat terlalu banyak kapasitas data • Tempat penyimpanan (Harddisk) penuh • Keamanan jaringan dapat ditembus • UPS tidak berfungsi

	• Ruang Server kurang diberi pengamanan
PC	
System of Interest	PC yang ada pada kampus I dan II STIE Perbanas
Komponen Utama	**Kemungkinan Ancaman**
• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • Antivirus • Sistem Operasi • Software • Listrik • UPS • Genset • Firewall	• Monitor, Keyboard ataupun mouse mengalami kerusakan karena pemakian berlebih • Firewall ditembus oleh bagian yang tidak berwenang • Kabel LAN putus akibat hewan pengerat • Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • UPS tidak berfungsi • Virus yang menyerang tidak dapat tertangani oleh antivirus
Data	
System of Interest	Data Demografi Mahasiswa, Data Akademik dan Data File Server
Komponen Utama	**Kemungkinan Ancaman**
• Database • Server • Listrik • PC • Firewall • Database Administrator (DBA)	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Firewall ditembus oleh bagian yang tidak berwenang • PC berhenti beroperasi karena terserang virus • Database Admnistrator salah dalah melakukan pengolahan data (ubah dan hapus)

	• Data dicuri karena Database Administrator kurang melakukan kontrol keamanan
Perangkat Lunak	
System of Interest	SIMAS, E-learning dan Perpustakaan
Komponen Utama	**Kemungkinan Ancaman**
• Firewall • Server • Antivirus	• Firewall ditembus oleh bagian yang tidak berwenang • Virus yang menyerang tidak dapat tertangani oleh antivirus • Server mengalami kerusakan sehingga sistem tidak dapat diakses
Wifi	
System of Interest	18 Wifi yang terpasang pada kampus I STIE Perbanas dan 3 Wifi yang terpasang pada kampus II STIE Perbanas
Komponen Utama	**Kemungkinan Ancaman**
• Listrik • Kabel • Keamanan Jaringan	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Kabel rusak akibat digigit hewan pengerat • Keamanan jaringan dapat ditembus oleh pihak yang tidak berwenang
Router	
System of Interest	Router
Komponen Utama	**Kemungkinan Ancaman**
• Listrik • Kabel • Keamanan Jaringan	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Kabel rusak akibat digigit hewan pengerat

5.1.6 Hubungan antara Aset Kritis, Kebutuhan Kemanan, Ancaman dan Praktik Keamanan Organisasi

Berdasarkan hasil analisis terkait aset kritis, kebutuhan keamanan, ancaman untuk masing masing aset dan juga praktik keamanan yang telah dilakukan oleh STIE Perbanas. Maka perlu dilakukan pemetaan hubungan antara masing masing aset dengan identifikasi kebutuhan keamanan dan ancaman serta praktik keamanan yang telah dilakukan. Pemetaan hubungan tersebut berfugsi untuk menganalisis lebih dalam kondisi kekinian dari praktik keamanan yang telah dilakukan oleh STIE Perbanas untuk mengatasi adanya ancaman untuk setiap aset kritis. Berikut ini adalah hubungan antara aset kritis dan masing masing kebutuhan keamanan, ancaman serta praktik keamanan yang telah diimplementasikan.

Tabel 5. 6. Hubungan aset kritis, kebutuhan keamanan, ancaman dan praktik keamanan organsiasi

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
Hardware	Server	Dapat diakses 24 jam dalam 7 hari Konfigurasi server dilakukan dengan benar Adanya sumber listrik cadangan Adanya kontrol keamanan untuk ruang fisik server	• Kerusakan Komputer • Kerusakan Server • Kerusakan Genset dan UPS • Kesalahan konfigurasi	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk perangkat TI pada setiap kelas dan lab • Dilakukan maintenance setiap sebelum UTS dan UAS hanya

		Adanya pembatasan hak akses	• Pencurian hardware	untuk perangkat TI pada Lab saja • Pada ruang server telah dipasang smoke detector untuk memberikan peringatan apabila terhadi kebakaran • Telah ada fire extinguisher untuk memadamkan api saat terjadi kebakaran • Ada penguncian pada ruang server dan kunci selalu dipegang oleh Bagian TIK • Pembuatan dan pelaksanaan beberapa SOP tekait pengelolaan perangkat TI oleh Bagian TIK
		Server tidak boleh diakses oleh usb atau pihak yang tidak berwenang yang dapat mengubah konten		
	PC	Dapat berfungsi selama jam kerja organisasi		
		Adanya sumber listrik cadanagn		
		Adanya Antivirus		
		Adanya pembatasan hak akses		
		Data-data yang terdapat didalam pc harus lengkap dan harus lengkap dan harus memiliki login agar kerahasiaan terjaga		
Software	SISFO	Dapat diakses 24 jam dalam 7 hari	• Bug pada software	

	E-Learning	Data dapat diakses 24 jam dalam 7 hari	• Virus/worm • Kesalahan konfigurasi sistem • Pembobolan sistem	• Adanya antivirus (e-scan) dan telah di update terus menerus setiap hari • Pada lab tidak dapat dipasang USB • Pada lab tidak dapat di install aplikasi dari luar • Telah dilakukan sosialisasi keapda mahasiswa dan dosen untuk praktik keamanan TI • Membedakan role dan hak akses untuk masing masing pegawai sesuai dengan unit kerja
	Sistem Informasi Perpustakaan	Adanya backup data secara rutin		
		Data-data terkait dalam aplikasi harus lengkap dan akurat		
Data	Data Demografi Mahasiswa	Adanya pembatasan hak akses	• Kesalahan input data • Data corrupt/rusak • Pencurian data • Sharing password	• Telah dilakukan back up server dan NAS setiap hari secara berkala dan terjadwal • Data hanya dapat dimasukkan, diganti dan dihapus oleh database administrator saja
		Adanya pengamanan terhadap data		
	Data Akaemik	Adanya pengamanan terhadap data		
	Data file server	Adanya pembatasan hak akses pegawai pada data		

		Data-data harus lengkap dan akurat		• Adanya perbedaan role atau hak akses pada data untuk masing masing fungsi
Jaringan	Wifi	Tersedia selama jam operasional kerja organisasi	• Gangguan pada router • Kerusakan kabel • Gangguan koneksi internet • Sabotase jaringan internet	• Telah dipasang anti netcut untuk keamanan wifi • Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk setiap perangkat TI • Dilakukan maintenance WIFI setiao 2 minggu sekali • Pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabell • Pembuatan dan pelaksanaan beberapa SOP mengenai SI/TI oleh Bagian TIK
		Terdapat sumber listrik cadangan		
		Adanya kontrol rutin		
		Adanya anti netcut		
	Kabel	Tersedia selama jam operasional kerja organisasi		
		Adanya kontrol rutin		
		Kabel dilakukan pelabelan untuk mempermudah pengorganisasian		
	Router	Tersedia selama jam operasional kerja organisasi		
		Adanya kontrol rutin		
		Memonitoring jaringan untuk memastikan keaslian data		

Berdasarkan dari hasil identifikasi aset kritis, kebutuhan keamanan, ancaman dari masing masing aset dan praktik keamanan yang telah dilakukan oleh organisasi, maka selanjutnya adalah menganalisa risiko yang mungkin timbul dari masing masing aset. Risiko tersebut dianalisis untuk setiap aset TI yaitu perangkat keras (*hardware),* perangkat lunak *(software)*, data, jaringan dan sumber daya manusia.

5.2 Analisis Risiko

Analisis risiko didasarkan pada hasil identifikasi kebutuhan keamanan, ancaman dan juga praktik keamanan dari masing masing aset kritis yang telah diidentifikasikan sebelumnya. Analisis risiko dilakukan dengan berdasarkan pada metode FMEA. Dimana sebelum melakukan analisis risiko terdapat dua proses utama yang akan dilakukan yaitu identifikasi risiko dan penilaian risiko. Dalam melakukan analisis risiko, terlebih dahulu dilakukan identifikasi potensi penyebab kegagalan dan potensi dampak kegagalan untuk setiap risiko. Setalah daftar risiko beserta penyebab dan dampak diidentifikasi, selanjutnya adalah melakukan penilaian risiko berdaarkan kriteria penilaian risiko pada metode FMEA. Penilaian risiko yang dilakukan secara meyeluruh dan didasarkan pada seluruh komponen sistem informasi yaitu *hardware, software*, jaringan, data dan sumber daya manusia. Sehingga dalam tahap analisis risiko akan dihasilkan luaran sebuah *risk register* beserta hasil penilaian risiko.

5.2.1 Risk Register

Dalam penelitian ini, risiko dititik beratkan pada risiko terhadap kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*). Berikut merupakan *risk register* untuk risiko keamanan data yang didasarkan pada risiko yang mungkin timbul pada kelima aset kritis terkait pada hilangnya kerahasiaan, integritas dan keutuhan data. Dan untuk keseluruhan daftar risiko dapat dilihat pada lampiran C.

Tabel 5. 7. Risk Register untuk Keamanan Data

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
Data	Data demografi mahasiswa, Data akademik dan Data file server	R13	Manipulasi data	Username dan password diketahui oleh pengguna lain	Komplain dari civitas akademika dan berkurangnya kepercayaan civitas akdemika	*Pengguna SISFO*
		R13	Manipulasi data	Terdapat hacker yang memanipulasi data	Komplain dari civitas akademika dan berkurangnya kepercayaan civitas akdemika	*Bagian TIK*

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
		R12	Pencurian data	Terdapat hacker yang mencuri data	Berkurangnya kepercayaan civitas akdemika	*Bagian TIK*
		R15	Data Hilang	Server rusak	Berkurangnya keperacayaan civitas kademika, komplain dari civitas akademika dan proses bisnis terhambat	*Bagian TIK*
Hardware	Server	R05	Data Hilang	Virus	Berkurangnya kepercayaan civitas akdemika dan proses bisnis terhambat	*Bagian TIK*
		R5	Data Hilang	Kesalahan DBA	Berkurangnya keperacayaan civitas kademika dan proses bisnis terhambat	*Bagian TIK*

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
		04	Pencurian data	Ruang server kurang diberi pengamanan	Penuruan citra organisasi dan penyalagunaan data	*Bagian TIK*
		R04	Pencurian data	Kesalahan konfigurasi server	Penuruan citra organisasi dan penyalagunaan data	*Bagian TIK*
Sumber Daya Manusia	Pegawai TI	R20	Data yang ada tidak valid	Kesalahan dalam input data	Komplain dari civitas akademika	*Pengguna SISFO*

5.2.2 Penilaian Risiko dengan Metode FMEA

Sesuai dengan kriteria penilaian risiko berdasarkan metode FMEA. Berikut ini merupakan hasil penilaian untuk risiko keamanan data dengan tingkat level *very high* hingga *medium*. Sedangkan untuk keseluruhan penilaian risiko dapat dilihat pada lampiran C.

Tabel 5. 8. Hasil Penilaian Risiko

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN	Jumlah
Very High	Manipulasi Data	Sharing password oleh Mahasiswa/i	210	3
		Username dan password diketahui oleh pengguna lain	200	
	Kerusakan pada Server	Kebocoran dan kerusakan pada bangunan	200	
High	Manipulasi Data	Terdapat hacker yang memanipulasi data	160	4
	Data Hilang	Virus/bug	160	
	Pencurian Data	Terdapat hacker yang mencuri data	140	
	Kerusakan pada server	Gempa bumi	120	
Medium	Data Hilang	Virus	112	11
		Server rusak	96	
		Kesalahan DBA	84	

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN	Jumlah
	Pencurian Data	Ruang server kurang diberi pengamanan	100	
		Kesalahan konfigurasi server	100	
	Kerusakan pada Server	Badai dan Petir	80	
		Banjir	80	
	Kerusakan pada PC	Kebocoran dan Kerusakan pada Bangunan	80	
	Pihak diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses	108	
	Akses internet lambat	Kesalahan Konfigurasi	100	
	Internet mati	Genset mati	80	
Low	Kerusakan pada Server	Kebakaran	48	31
	Kinerja Server Menurun	RAM mengalami kelebihan memori	48	

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN	Jumlah
		Kinerja Procesor menurun akibat terlalu banyak kapasitas data	36	
		Tempat penyimpanan (*Harddisk)* penuh	48	
	Kerusakan pada PC	Gempa Bumi	60	
		Badai dan Petir	40	
		Banjir	40	
		Kebakaran	24	
		Keyboard, mouse atau monitor mengalami kerusakan karena pemakaian berlebih	24	
	PC tidak dapat menyala	Kerusakan pada Genset dan UPS	48	
		Listrik Mati	42	
	PC terkena virus	antivirus tidak update	60	
	Aplikasi tidak dapat diakses	Listrik Mati	70	
		Server Down	75	
	Data tidak dapat diakses	Listrik Mati	70	
		Server Down	75	

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN	Jumlah
	Backup data gagal	Kapasitas media penyimpanan *overload*	48	
	Kurangnya kontrol pengamanan kabel	Kabel rusak	50	
	Internet mati	Listrik Mati	70	
		Wifi rusak	30	
		Kabel rusak	50	
	Akses internet lambat	Ada yang melakukan netcut	70	
	Penyalahgunaan data organisasi	Penurunan Kompetensi Karyawan Pegawai Non-TI	60	
		Adanya praktik KKN di perusahaan	30	
	Pelanggaran regulasi hak akses	Penyalahgunaan akses regulasi	27	
	Penyalahgunaan data organisasi	Penurunan Kompetensi Pegawai TI	60	
		Adanya praktik KKN di perusahaan	45	

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN	Jumlah
	Pelanggaran regulasi	Penyalahgunaan akses regulasi	36	
	Penyalahgunaan data organisasi	Penurunan Kompetensi Dosen	60	
		Adanya praktik KKN di perusahaan	30	
	Data yang ada tidak valid	kesalahan dalam Input	75	

5.3 Evaluasi Risiko

Dalam evaluasi risiko akan dibuat sebuah daftar prioritas risiko yang didasarkan pada level risiko yaitu berdasarkan nilai RPN untuk risiko yang berkaitan dengan hilangnya kerahasiaan (*confidentiality*), integritas (*integrity*) dan keutuhan (*availability*) data. Level risiko yang akan diprioritaskan merupakan yang berada pada level risiko *very high, high* dan *medium.* Berikut ini merupakan tabel daftar prioritas risiko dimana terdapat 9 risiko keamanan data dengan tingkat prioritas tertinggi dilihat dari nilai RPN yang tinggi.

Tabel 5. 9. Daftar Prioritas Risiko

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Level Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan
Data	Data demografi mahasiswa, Data akademik dan Data file server	R13	Very High	Manipulasi data	Username dan password diketahui oleh pengguna lain
		R13	High	Manipulasi data	Terdapat hacker yang memanipulasi data
		R12	High	Pencurian data	Terdapat hacker yang mencuri data
		R15	Medium	Data Hilang	Server rusak
Hardware	Server	R5	Medium	Data Hilang	Virus
		R5	Medium	Data Hilang	Kesalahan DBA
		R4	Medium	Pencurian data	Ruang server kurang diberi pengamanan
		R4	Medium	Pencurian data	Kesalahan konfigurasi server
Sumber Daya Manusia	Pegawai TI	R20	Medium	Data yang ada tidak valid	Kesalahan dalam input data

Berdasarkan hasil evaluasi penilaian risiko tersebut, maka dapat diketahui bahwa STIE Perbanas memiliki beberapa kemungkinan risiko yang dapat timbul terkait keamanan data yaitu manipulasi data, pencurian data, kehilangan data dan data yang tidak valid. Risiko keamanan data yang dimasud adalah untuk data yang berupa data elektronik. Risiko-risiko tersebut muncul dikarenakan oleh berbagai macam penyebab seperti *hacker, virus, human error*, kurangnya kontrol keamanan fisik dan lainnya. Hasil dari evaluasi risiko berikut ini yang nantinya akan dilakukan analisis lebih dalam untuk menentukan langkah mitigasi risiko yang harus dikelola. Dan beradasarkan hasil evaluasi risiko tersebut, selanjutnya dilakukan analisis kebutuhan mitigasi risiko yang berupa sebuah pengimplementasian kontrol kebijakan, praktek dan prosedur.

5.4 Perlakuan Risiko

Tahap perlakuan risiko merupakan tahap dalam menentukan tindakan mitigasi risiko yang tepat. Tahap perlakuan risiko dilakukan dengan melakukan pemetaan risiko terhadap masing masing kontrol yang dibutuhkan dalam kerangka kerja Cobit 5 dan ISO27002:2013 serta menganalisis rekomendasi mitigasi risiko.

Risiko dengan prioritas tertinggi dipetakan kedalam kontrol kerangka kerja Cobit 5 dan ISO27002:2013. Tujuan dari pemetaan risiko kedalam kontrol kerangka kerja adalah untuk memastikan perlakuan risiko telah tepat dan sesuai dengan *control objective* dari setiap kontrol kerangka kerja. Selain pemetaan risiko dan kontrol pada kerangka kerja, dilakukan pula justifikasi kebutuhan kontrol. Justifikasi kebutuhan kontrol tersebut memiliki fungsi untuk memastikan bahwa kontrol yang ada sesuai dengan risiko yang akan dimitigasi.

Setelah melakukan pemetaan risiko terhadap kontrol Cobit 5 dan ISO27002:2013, selanjutnya akan ditentukan rekomendasi mitigasi risiko berdasarkan kontrol yang telah ditentukan. Rekomendasi mitigasi risiko yang telah dipetakan sesuai dengan

risiko dan kebutuhan kontrolnya nantinya akan mendefinisikan usulan-usulan perbaikan dalam sistem informasi SISFO STIE Perbanas dan juga sebagai input untuk membuat dokumen *Standard Operating Procedure* (SOP) Keamanan Data pada STIE Perbanas.

5.4.1 Pemetaan Risiko dengan Kontrol Cobit 5

Dalam pemetaan kontrol dengan kerangka kerja Cobit 5 fokus domain yang digunakan adalah domain DSS (*Deliver Service and Support*). Proses dari domain DSS yang digunakan yaitu *DSS05.01 Protect Against Malware, DSS05.03 Manage Endpoint Security , DSS05.04 Manage User, Identity and Logical Access, DSS05.05 Manage Physical Access to IT Assets* dan *DSS06.02 Control the Processing of Information*. Berikut adalah pemetaan risiko dan kontrol Cobit 5, untuk pemetaan risiko dan justifikasi kebutuhan kontrol dapat dilihat pada Lampiran D.

Tabel 5. 10. Pemetaan Risiko dan Kebutuhan Kontrol pada Cobit 5

Kategori Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol Cobit 5
Data	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	DSS05.04 Manage user identity and logical access
	13	Manipulasi data	Terdapat hacker yang memanipulasi data	DSS05.01 Protect Against Malware
	15	Data Hilang	Virus/bug	DSS05.01 Protect Against Malware

Kategori Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol Cobit 5
	12	Pencurian data	Terdapat hacker yang mencuri data	DSS05.01 Protect Against Malware
Data	15	Data Hilang	Server rusak	DSS05.03 Manage Endpoint Security
Hardware	5	Data Hilang	Virus	DSS05.01 Protect Against Malware
Hardware	5	Data Hilang	Kesalahan DBA	DSS05.03 Manage Endpoint Security
Hardware	4	Pencurian data	Ruang server kurang diberi pengamanan	DSS05.05 Manage physical access to IT assets
Hardware	4	Pencurian data	Kesalahan konfigurasi server	DSS05.03 Manage Endpoint Security
Sumber Daya Manusia	20	Data yang ada tidak valid	Kesalahan dalam input data	DSS06.02 Control The Processsing of Information

5.4.2 Pemetaan Risiko dengan Kontrol ISO27002:2013

Dalam pemetaan kontrol dengan kerangka kerja ISO27002:2013 terdapat 11 klausul yang digunakan yaitu *9.4.3 Password Management System, , 11.1.2 Physical Entry Controls, 12.2.1 Controls Against Malware, 12.3.1 Information Backup* dan *16.1 Information Security Incidents Management*. Berikut adalah pemetaan risiko dan kontrol ISO27002:2013, untuk justifikasi kebutuhan kontrol dapat dilihat pada Lampiran E.

Tabel 5. 11. Pemetaan Risiko dan Kebutuhan Kontrol pada ISO27002:2013

Kategori Aset Informasi Kritis	ID Risiko	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013
Data	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	9.3.1 Use of Secrets Authentication Information
				9.4.3 Password Management System
	13	Manipulasi data	Terdapat hacker yang memanipulasi data	16.1 Management of Information security incidents and improvements
	15	Data Hilang	Virus/bug	12.2.1 Control Against Malware
				12.3.1 Information Backup

Kategori Aset Informasi Kritis	ID Risiko	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013
	12	Pencurian data	Terdapat hacker yang mencuri data	10.1.1 Policy on the Use of Crypthographic Control
				10.1.2 Key Management
				7.2.3 Disciplinary Process
	15	Data Hilang	Server rusak	12.3.1 Information Backup
Hardware	5	Data Hilang	Virus	12.2.1 Control Against Malware
Hardware	5	Data Hilang	Kesalahan DBA	12.4.3 Administrator & Operator Logs
Hardware	4	Pencurian data	Ruang server kurang diberi pengamanan	11.1.2 Physical Entry Controls
Hardware	4	Pencurian data	Kesalahan konfigurasi server	12.4.3 Administrator & Operator Logs
Sumber Daya Manusia	20	Data yang ada tidak valid	Kesalahan dalam input data	14.1.2 Securing Application Services on Public Networks

5.4.3 Rekomendasi Mitigasi Risiko

Rekomendasi mitigasi risiko yang dihasilkan akan didasarkan pada kontrol objektif dan petunjuk pelaksanaan pada kerangka kerja Cobit 5 dan ISO27002:2013. Selain itu, rekomendasi risiko juga didasarkan identifikasi praktik keamanan yang telah diimplementasikan risiko, hal ini berfungsi untuk memastikan tidak ada redundansi tindakan mitigasi risiko dalam mengelola risiko yang muncul. Dalam rekomendasi mitigasi risiko akan didefinisikan input untuk membuat dokumen *Standard Operating Procedure* (SOP) Keamanan Data pada STIE Perbanas dan juga usulan-usulan perbaikan dalam sistem informasi SISFO STIE Perbanas. Pemetaan rekomendasi mitigasi risiko dari kontrol objektif kerangka kerja Cobit 5 dan ISO27002:2013 dapat dilihat pada Lampriran F.

5.5 Prosedur Yang Dihasilkan Berdasarkan Hasil Rekomendasi Mitigasi Risiko

Berdasarkan hasil rekomendasi mitigasi risiko yang ada pada Lampiran F, maka dapat dianalisis bahwa untuk mengelola risiko keamanan data yang memiliki priotitas tertinggi pada STIE Perbanas diperlukan beberapa prosedur. Prosedur tersebut berfungsi untuk memastikan bahwa risiko yang ada tidak berulang dengan menstandarisasikan proses dan meminimalkan variasi pelaksanaan suatu kegiatan operasional. Tabel 5.12 berikut ini merupakan prosedur yang dihasilkan berdasarkan pada hasil rekomendasi mitigasi risiko pada Lampiran F.

Tabel 5. 12. Prosedur yang dihasilkan berdasarkan hasil Rekomendasi Mitigasi Risiko

ID Risiko	Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol Kerangka Kerja		Prosedur yang dihasilkan
			COBIT 5	ISO27002:2013	
R13	Manipulasi data	Username dan password diketahui oleh pengguna lain		9.4.3 *Password Management System*	SOP Manajemen Password
R13	Manipulasi data	Terdapat hacker yang memanipulasi data		16.1 *Management of Information Security Incidents and Improvements*	SOP Pengelolaan Gangguan Sistem Informasi
R12	Pencurian data	Terdapat hacker yang mencuri data		16.1 *Management of Information Security Incidents and Improvements*	

ID Risiko	Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol Kerangka Kerja		Prosedur yang dihasilkan
			COBIT 5	ISO27002:2013	
R15	Data Hilang	Server rusak	DSS05.03 *Manage Endpoint Security*		SOP Proteksi Lingkungan Server
R5	Data Hilang	Virus	DSS05.01 *Protect Against Malware*	12.2.1 Controls Against Malware	SOP Pengelolaan dan Pencegahan Malware
R5	Data Hilang	Kesalahan DBA	12.3.1 *Information Backup*		SOP Back Up dan Restore
R4	Pencurian data	Ruang server kurang diberi pengamanan	DSS05.05 *Manage Physical Access to IT Assets*	11.1.2 *Physical Entry Control*	SOP Akses Ruang Server
R4	Pencurian data	Kesalahan konfigurasi server	DSS05.03 *Manage Endpoint Security*		SOP Proteksi Lingkungan Server

ID Risiko	Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol Kerangka Kerja		Prosedur yang dihasilkan
			COBIT 5	ISO27002:2013	
R20	Data yang ada tidak valid	Kesalahan dalam input data		12.3.1 *Information Backup*	SOP Back Up dan Restore

BAB VI
HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

6.1 Dokumen Prosedur Mutu Bagian TIK STIE Perbanas

Bagian TIK STIE Perbanas telah memiliki beberapa prosedur yang terdokumentasi terdiri dari dokumen mengenai standard prosedur suatu aktivitas yang dilakukan oleh bagian TIK disebut dengan prosedur mutu dan juga beberapa instruksi kerja. Berikut merupakan penjelasan singkat mengenai masing masing prosedur mutu dan intruksi kerja yang telah diimplementasikan.

Tabel 6. 1. Daftar Dokumen Prosedur Mutu Bagian TIK

No Dokumen	Prosedur Mutu	Penjelasan
QP-ICT-01	Prosedur Perbaikan Sistem Informasi	Prosedur teknis perbaikan sistem informasi yang telah dikembangkan oleh pihak ketiga
QP-ICT-02	Prosedur Pemeliharaan Perangkat & Infrastruktur Komputer	Prosedur teknis pemeliharaan perangkat keras dan infrastruktur jaringan yang dilakukan setiap semester
QP-ICT-03	Prosedur Penanganan Komplain	Prosedur teknis dalam menangani komplani perangkat keras dan perangkat jaringan
QP-ICT-04	Prosedur Website & Email	Prosedur teknis permintaan unit kerja untuk dibuatkan website dan email STIE Perbanas
QP-ICT-	Prosedur Video	Prosedur teknis

No Dokumen	Prosedur Mutu	Penjelasan
05	Conference	pelaksanaan *video conference* melalui jaringan Inherent
QP-ICT-06	Prosedur Pelaporan EPSBED	Prosedur teknis penyusunan data dan laporan EPSBED
QP-ICT-07	Prosedur Audit Trail	Prosedur teknis audit trail terhadap transaksi data yang tersimpan dalam sistem informasi

Tabel 6. 2. Daftar Dokumen Instruksi Kerja Bagian TIK

No Dokumen	Instruksi Kerja	Penjelasan
WI-ICT-01	Instruksi Kerja Instalasi Jaringan	Instruksi kerja untuk melakukan instalasi jaringan dan koneksi jaringan
WI-ICT-02	Instruksi Kerja Software & Antivirus	Intruksi kerja untuk melakukan instalasi aplikasi atau antivirus pada setiap PC pada unit kerja dengan melalui *master software*
WI-ICT-03	Instruksi Kerja Bandwith Manajemen	Instruksi kerja untuk melakukan pengelolaan dan pengecekan bandwith jaringan
WI-ICT-04	Instruksi Kerja Reset Password User Domain	Instruksi kerja untuk melakukan *reset password* pengguna SISFO
WI-ICT-05	Instruksi Kerja Melihat Password Hotspot User Mahasiswa	Instruksi Kerja untuk melihat *password* mahasiswa melalui alamat IP

WI-ICT-06	Instruksi Kerja Membuat User Hotspot Civitas	Instruksi kerj auntuk menambahkan pengguna pada hostpot
WI-ICT-07	Instruksi Kerja Cek Koneksi Web	Instruksi kerja untuk melakukan pengecekan koneksi website dari luar lingkungan STIE Perbanas
WI-ICT-08	Instruksi Kerja Perbaikan Blue Print TI	Instruksi kerja untuk melakukan perbaikan Blue Print TIK

6.1.1 Hubungan antara Prosedur yang telah ada dan Praktik Keamanan Organisasi

Dalam membangun sebuah prosedur, perlu diperhatikan praktik praktik keamanan yang telah diimplementasikan dalam organisasi. Tujuan dari memetakan hubungan antara prosedur yang ada dengan praktik keamanan yang telah diimplementasikan oleh organisasi adalah untuk memastikan bahwa prosedur yang ada secara efektif telah mencakup praktik keamanan yang berjalan dalam organisasi. Berdasarkan hasil identifikasi praktik keamanan dalam organisasi yang telah dijabarkan dalam bab sebelumnya, maka berikut ini adalah hubungan antara prosedur mutu yang telah diimplementasikan oleh STIE Perbanas dengan praktik keamanan organisasi yang telah berjalan selama ini.

Tabel 6. 3. Hubungan antara Prosedur yang ada dan Praktik Keamanan Organisaasi

No Dokumen	Prosedur Mutu	Praktik Keamanan Organisasi
QP-ICT-01	Prosedur Perbaikan Sistem Informasi	• Pelaksanaan SOP terkait mengenai SI/TI di organisasi
QP-ICT-02	Prosedur Pemeliharaan Perangkat &	• Dilakukan maintenance setiap sebelum UTS dan UAS hanya untuk lab saja

No Dokumen	Prosedur Mutu	Praktik Keamanan Organisasi
	Infrastruktur Komputer	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk kelas dan lab • Dilakukan maintenance Wifi setiap 2 minggu sekali • Pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabel • Pada Lab tidak bisa menginstall aplikasi dari luar • Pada Lab tidak bisa memasang USB
QP-ICT-03	Prosedur Penanganan Komplain	• Adanya antivirus (e-scan) dan diupdate terus menerus • Adanya update patch dan firewall secara berkala • Telah dipasang anti netcut untuk keamanan Wifi
QP-ICT-04	Prosedur Website & Email	• Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan fungsinya
QP-ICT-05	Prosedur Video Conference	• Pelaksanaan SOP terkait mengenai SI/TI di organisasi
QP-ICT-06	Prosedur Pelaporan	• Pelaksanaan SOP terkait mengenai SI/TI di

No Dokumen	Prosedur Mutu	Praktik Keamanan Organisasi
	EPSBED	organisasi
QP-ICT-07	Prosedur Audit Trail	• Adanya log setiap aktivitas dalam sistem informasi SISFO

6.2 Prosedur yang Dihasilkan dalam Penelitian

Berdasarkan hasil rekomendasi mitigasi risiko, didefinisikan beberapa prosedur yang dapat diusulkan dalam penelitian. Selain itu, prosedur yang dihasilkan berikut ini juga telah disinkronisasikan dengan prosedur mutu yang ada pada Bagian TIK STIE Perbanas sehingga telah dapat diverifikasi bahwa tidak ada prosedur yang memiliki fungsi dan proses yang redundan. Berikut ini adalah prosedur yang diusulkan dalam penelitian.

Tabel 6. 4. Prosedur yang Diusulkan

Kontrol Objektif	Prosedur	Rung Lingkup	Aspek Keamanan
9.4.3 Password Management System	SOP Manajemen Password	Pemeliharaan (*maintenance*) Sistem Informasi	*data confidentiality and integrity*
DSS05.01 Protect Against Malware	SOP Pengelolaan dan Pencegahan Malware	Pemeliharaan (*maintenance*) Sistem Informasi	*data availability*
16.1 Management of information security incidents and improvements	SOP Pengelolaan Gangguan Sistem Informasi	Pemeliharaan (*maintenance*) Sistem Informasi	*data confidentiality and availability*

Kontrol Objektif	Prosedur	Rung Lingkup	Aspek Keamanan
12.3.1 Information Backup	SOP Backup dan Restore	Pemeliharaan (*maintenance*) Sistem Informasi	*data availability*
DSS05.03 Management Endpoint Security	SOP Proteksi Lingkungan Server	Pemeliharaan (*maintenance*) perangkat TIK	*data availability*
DSS05.05 Manage Physical Access to IT Assets	SOP Akses Ruang Server	Pemeliharaan (*maintenance*) perangkat TIK	*data confidentiality*
11.1.2 Physical Entry Controls			

Berikut ini merupakan penelasan dari masing masing prosedur yang akan dibuat untuk mendukung keamanan data pada STIE Perbanas. Jumlah prosedur yang akan dihasilkan adalah sebanyak enam prosedur. Penjelasan untuk masing-masing prosedur keterkaitannya dengan proses kekinian akan dijelaskan pada Tabel 24 dibawah ini

Tabel 6. 5. Deskripsi Prosedur

Prosedur	Penjelasan
SOP Manajemen Password	Prosedur Manajemen password merupakan prosedur untuk memastikan pengelolaan penggunaan password telah memenuhi kualitas standard *strong* password. Seluruh sistem informasi yang ada dalam STIE Perbanas yang disebut dengan SISFO mengklasifikasikan penggunanya berdasarkan *login* pengguna pada sistem, sehingga penting untuk memastikan password setiap pengguna telah sesuai dengan syarat kualitas password. Prosedur ini juga bertujuan untuk memastikan risiko manipulasi data yang disebabkan oleh username dan password diketahui oleh pengguna lain karena lemahnya kualitas password pengguna dapat diminimalisir kemungkinan terjadinya.
SOP Backup dan Restore	Prosedur Backup dan Restore Data merupakan prosedur yang bertujuan untuk memastikan backup data yang dilakukans secara berkala telah sesuai dan data yang di backup telah lengkap. Tujuan dari pembuatan prosedur ini adalah untuk memastikan

Prosedur	Penjelasan
	ketersediaan data pada setiap layanan sistem informasi yang dikelola oleh Bagian TIK.
SOP Pengelolaan dan Pencegahan Malware	Prosedur Pencegahan Malware merupakan prosedur untuk menjadi acuan bagi pegawai Bagian TIK dalam upaya melakukan pencegahan terhadap bahaya malware serta melindungi perangkat dan aset informasi milik STIE Perbanas. Prosedur ini bertujuan untuk memastikan bahwa risiko kehilangan data akibat adanya serangan hacker dapat diminimalisir kemungkinann terjadinya.
SOP Pengelolaan Gangguang Sistem Informasi	Prosedur Pengelolaan Gangguan Sistem Informas merupakan prosedur untuk menangani adanya gangguan atau insiden dalam bentuk serangan malware pada sistem informasi yang ada dalam STIE Perbanas. Prosedur ini bertujuan untuk memastikan adanya tahapan proses yang jelas bagi pegawai Bagian TIK dalam menangani serangan malware dan menyelesaikan insiden atau gangguan tersebut. Prosedur Pengelolaan Serangan Malware juga bertujuan untuk memastikan bahwa risiko kehilangan data akibat adanya virus dan malware lainnya dapat diminimalisir kemungkinan terjadinya.
SOP Proteksi Lingkungan Server	Prosedur proteksi lingkungan server merupakan prosedur untuk memastikan bahwa server telah memiliki proteksi secara fisik untuk menghindari timbulnya risiko kerusakan server yang dapat

Prosedur	Penjelasan
	berdampak pada hilangnya data akibat kondisi lingkungan sekiar server yang tidak dikelola dengan baik. Dalam prosedur ini cakupan proteksi lingkungan server yang dimaksud adalah mengenai pengelolaan lokasi penyimpanan server pada ruang server.
SOP Akses Ruang Server	Prosedur Akses Ruang Server merupakan prosedur untuk memastikan bahwa akses pada area penting seperti ruang server terkontrol dengan baik dan memastikan seluruh akses terhadap area tersebut telah terautorisasi dan memiliki sebuah *log* aktivitas yang dapat dimonitor dengan baik. Prosedur ini bertujuan untuk menghindari adanya risiko pencurian data akibat akses langsung pada server yang tidak terautorisasi kaerna kurangnya pengamanan pada ruang server.

6.3 Pemetaan SOP yang dihasilkan dengan Prosedur Mutu yang dimiliki STIE Perbanas

Pada bagian ini, akan dijelaskan mengenai hubungan antara enam prosedur yang dihasilkan dengan *existing procedure* atau prosedur mutu yang telah dimiliki oleh STIE Perbanas. Berdasarkan hasil pembelajaran terhadap prosedur mutu yang telah diimplementasikan, maka terdapat beberapa tiga SOP yang berhubungan dengan prosedur mutu yang ada yaitu SOP Pengelolaan dan Pencegahan Malware, SOP Pengelolaan Gangguan Sistem Informasi, dan SOP Proteksi Lingkungan Sever. Sehingga SOP yang dihasilkan akan menjadi dokumen terkait dalam prosedur mutu yang telah ada. Berikut ini

Tabel 6. 6. Hubungan SOP yang diusulkan dan antara Prosedur Mutu STIE Perbanas

Prosedur	Hubungan dengan *Existing Procedure*	Penjelasan
SOP Pengelolaan dan Pencegahan Malware	Prosedur Penanganan Komplain	Dalam prosedur yang telah ada terdapat prosedur yang menjelaskan mengenai proses penanganan komplain terkait perangkat keras dan perangkat jaringan. Namun kekurangan dari prosedur tersebut adalah tidak secara spesifik dijelaskan bagaimana prosedur tindak lanjut dari komplain tersebutt yang spesifik untuk pengelolan dan pencegahan terhadap risiko adanya *malware*. Sehingga dalam SOP yang akan dikembangkan yaitu SOP Pengelolaan dan Pencegahan Malware akan dilengkapi

		dengan pengelolaan dan pencegahan terhadap komplain terkait *malware.*
SOP Pengelolaan Gangguan Sistem Informasi	Prosedur Penanganan Komplain	Dalam prosedur yang telah ada terdapat prosedur yang menjelaskan mengenai proses penanganan komplain terkait perangkat keras dan perangkat jaringan. Namun kekurangan dari prosedur tersebut adalah tidak secara spesifik dijelaskan bagaimana prosedur tindak lanjut dari komplain tersebutt yang spesifik untuk pengelolan dan pencegahan terhadap risiko adanya serangan *hacker*. Sehingga dalam SOP yang akan dikembangkan yaitu SOP Pengelolaan Gangguan Sistem Informasi akan dilengkapi dengan proses pengelolaan dan pencegahan terhadap komplain terkait keamanan dalam Sistem Informasi khususnya dalam penanganan serangan *hacker.*
SOP Proteksi Lingkungan Server	Prosedur Pemeliharaan Perangkat & Infrastruktur Komputer	Dalam prosedur yang telah ada terdapat prosedur yang menjelaskan mengenai proses pengelolaan perangkat keras dan perangkat jaringan. Namun kekurangan dari prosedur tersebut adalah tidak secara rinci dijelaskan bagaimana proteksi keamanan pada lingkungan server yang membutuhkan

		pemeliharaan yang berbeda ari perangkat lainnya. Sehingga dalam SOP yang akan dikembangkan yaitu SOP Proteksi Lingkungan Sever akan melengkapi prosedur yang telah ada dengan menambahkan prosedur yang secara spesifik akan mengelola proteksi terhadap server khususnya untuk proteksi terhadap lingkungan server.

6.4 Perancangan Struktur dan Isi SOP

Pada sub-bab ini akan dijelaskan mengenai perancangan SOP yang akan dibuat. Perancangan SOP ini mengacu pada peraturan pemerintah (Menteri Pedahayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia nomo 35 tahun 2012) terkait dengan pedoman penyusunan standar operasional prosedur administrasi pemerintah. Namun, dalam perancangan struksur dan isi SOP tidak keseluruhan struktur kontn akan mengacu pada standard tersebut karena akan disesuaikan dengan kebutuhan. Struktur dokumen SOP yang akan disusun ini akan dihasilkan ke dalam sebuah buku produk yang akan diberikan kepada pihak STIE Perbanas sebagai rekomendasi tata kelola keamanan data.

Adapun struktur atau konten yang akan dimasukkan ke dalam kerangka dokumen *Standard Operating Procedure* (SOP) Keamanan Data STIE Perbanas adalah sebagai berikut.

Tabel 6. 7. Hasil Perancangan Dokumen SOP

Sturktur Bab	Sub-Bab	Konten
Pendahuluan	Tujuan	Deskripsi umum dokumen SOP Keamanan Data
	Ruang Lingkup	
	Overview Keamanan Data	Asapek Keamanan Data
	Evaluasi Penilaian Risiko Keamanan Data pada STIE Perbanas	Tabel Daftar Prioritas Risiko Keamanan Data
Prosedur	Tujuan	Deskripsi umum SOP

Sturktur Bab	Sub-Bab	Konten
Manajemen Password	Ruang Lingkup	
	Definisi	Pendefinisian istilah yang digunakan
	Rincian Prosedur	Proses pengelolaan password Proses permintaan pergantian password
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Pengelolaan dan Pencegahan Malware	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Pendefinisian istiliah yang digunakan
	Rincian Prosedur	Proses pencegahan malware Proses penggunaan perangkat/fasilitas anti malware
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Gangguan Sistem Informasi	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Pendefinisian istiliah yang digunakan
	Rincian Prosedur	Proses penanganan gangguan sistem informasi Proses evaluasi gangguan sistem informasi
	Bagan Alur SOP	Tabel Bagan Alur SOP

Sturktur Bab	Sub-Bab	Konten
Prosedur Backup dan Restore	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Pendefinisian istilah Pendefinisian klasifikasi data Pendefinisian kritikalitas data Pendefinisian tipe backup
	Rincian Prosedur	Proses backup data secara berkala Proses uji backup data Proses restore
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Proteksi Lingkungan Server	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Pendefinisian istilah yang digunakan
	Rincian Prosedur	Proses pengamanan lingkungan server
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Akses Raung Server	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Pendifinisian istilah yang digunakan
	Rincian Prosedur	Proses akses ke dalam ruang server
	Bagan Alur SOP	Tabel Bagan Alur SOP
Instruksi	Instruksi kerja Pemindaian Sistem	Rincian Instruksi

Sturktur Bab	Sub-Bab	Konten
	Informasi	
	Instruksi kerja Back up	Rincian Instruksi
	Instruksi kerja Restore	Rincian Instruksi
Formulir	Formulir Permintaan Pergantian Password	
	Formulir Laporan Gangguan Keamanan Informasi	
	Formulir Laporan Evaluasi Sistem Informasi	
	Formulir Klasifikasi Data	
	Formulir Log Backup Data	
	Formulir Pemeliharaan server	
	Formulir Log Pegawai	
	Formulir Log Daftar Pengunjung	

6.5 Hasil Perancangan SOP

Pada sub-bab ini akan dijelaskan mengenai hasil akhir dari perencanaan dan perancangan SOP yang telah diinisasi berdasarkan dari sub-bab sebelumnya. Berikut menampilkan pemetaan dari perancangan SOP dengan formulir dan instruksi yang digunakan pada setiap prosedur.

Tabel 6. 8. Pemetaan Dokumen SOP dan Formulir serta Instruksi

No Dokumen	Nama Dokumen SOP	No Dokumen	Dokumen Terkait
PS-01	Prosedur Manajemen Password	FM-01	Formulir Perbaikan Sistem Informasi
		FM-02	Formulir Permintaan Pergantian Password
PS-02	Prosedur Pengelolaan dan Pencegahan Malware	FM-04	Formulir Laporan Gangguan Keamanan Informasi
PS-03	Prosedur Pengelolaan Gangguan Sistem Informasi	FM-03	Formulir Evaluasi Sistem Informasi
		IN-01	Instruksi kerja Pemindaian Sistem Informasi
PS-04	Prosedur Backup dan Restore	FM-04	Formulir Klasifikasi Data
		FM-05	Formulir Log Backup Data
		IN-02	Instruksi Kerja Back Up
		IN-03	Instruksi Kerja Restore
PS-05	Prosedur Proteksi	FM-06	Formulir

	Lingkungan Server		Pemeliharaan server
PS-06	Prosedur Akses Ruang Server	FM-07	Formulir Log Pegawai
		FM-08	Formulir Log Daftar Pengunjung

Beirkut adalah penjelasan dari setiap prosedur dan formulir beserta dokumen pendukung yaitu formulir dan instruksi yang dibutuhkan pada setiap proses didalamnya.

6.5.1 Prosedur Manajemen Password

Sesuai dengan kontrol dalam ISO27002:2013 sub klausul 9.4.3 *password management system*, prosedur ini berisi 2 proses utama yang didefinisikan dalam beberapa aktivitas yang berurutan.

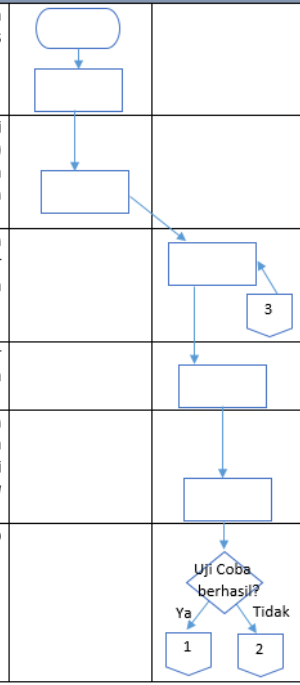
SEKOLAH TINGGI ILMU EKONOMI PERBANAS		
	Nomor SOP	PS-01
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	MANAJEMEN PASSWORD
	Disahkan oleh	(.....)

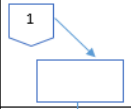
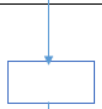
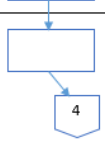
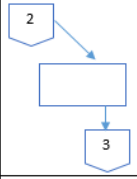
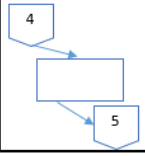
DESKRIPSI SOP	KUALIFIKASI DAN DAFTAR PELAKSANA
Prosedur Manajemen password merupakan prosedur untuk memastikan pengelolaan penggunaan password telah memenuhi kualitas standard *strong* password dan memastikan password setiap pengguna telah sesuai dengan syarat kualitas password	**DAFTAR PELAKSANA** - Kepala Bagian TIK - Pegawai Bagian TIK (programmer) - Pengguna Sistem **KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis dan kemampuan mengenai pemrograman - Memiliki kemampuan pemahaman proses bisnis yang baik - Memiliki kemampuan komunikasi yang baik
KETERKAITAN	
- Kebijakan Penggunaan Akun dan Kata Sandi - Kebijakan Ketentuan Pengguan	
REFERENSI	**PERLENGKAPAN / PERSYARATAN**
ISO27002:2013 – Sub klasusul *Password Management System*	- Media komunikasi : telepon dan email - Formulir Perbaikan Sistem Informasi (FM-01) - Formulir Pergantian Password (FM-02)
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan, maka pengelolaan password pada sistem informasi tidak sesuai dengan standard keamanan sehingga dapat mengakibatkan risiko hilangnya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) data	- Mencatat perbaikan sistem informasi pada formulir Perbaikan Sistem Informasi (FM-01) - Mencatat permintaan pergantian password pegawai dan mahasiswa pada formulir Pergantian Password (FM-02)

Melaksanakan pemilihan password yang berkualitas *(Enforce a choice of quality passwords*)

Melaksanakan penggunaan password pribadi untuk mengelola akuntabilitas *(Enforce the use of individual passwords to maintain accountability*)

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
1.	Proses Pengelolaan Password					
1.1	Menentukan standar penggunaan password sesuai dengan kualitas standard *strong password*					KJ-03 Kebijakan Penggunaan Akun dan Kata Sandi
1.2	Menginstruksikan kepada Pegawai Bagian TIK (administrator aplikasi) untuk melakukan penambahan fitur *strong password* dalam sistem informasi					
1.3	Menganalisis kebutuhan sistem informasi untuk penambahan fitur *strong password* dan menentukan waktu pengerjaan					
1.4	Mengerjakan penambahan fitur *strong password* sesuai dengan waktu yang ditentukan					
1.5	Memastikan seluruh sistem informasi yang membutuhkan prosedur *log in* telah memiliki ketentuan inputan *strong password*					
1.6	Melakukan pengujian terhadap fitur baru *strong password*					



	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
a.1	**Uji coba berhasil** Melakukan pelaporan kepada Kepala Bagian TIK					
a.2	Melakukan validasi dan persetujuan hasil penambahan fitur					
a.3	Mengisi laporan perbaikan fitur pada sistem informasi pada formulir Perbaikan Sistem Informasi					FM – 01 Formulir Perbaikan Sistem Informasi
b.1	**Uji coba gagal** Melakukakan kembali melakukan prosedur pada sub proses 1.3					
1.7	Mempersiapkan prosedur perubahan *password* lama dan melakukan *set up* pada seluruh sistem					

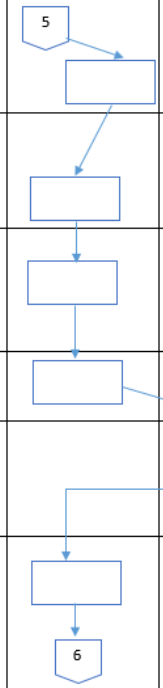
Melaksanakan penggunaan password pribadi untuk mengelola akuntabilitas *(Enforce the use of individual passwords to maintain accountability*)

Melaksanakan penggunaan password pribadi untuk mengelola akuntabilitas *(Enforce the use of individual passwords to maintain accountability*)

Menyimpan dan mentransmisikan password dengan prosedur/media yang aman *(Store and transmit passwords in protect form*)

Mengijinkan pengguna memilih *password* pribadi dan memaksa pengguna untuk mengganti *password default* di awal log in. *(Allow user to select and change their own passwords. Force user to change their passwords at the first log-on*)

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
1.8	Menyediakan *password default* sementara untuk masing pengguna sistem					
1.9	Mensosialisasikan penambahan fitur baru kepada seluruh civitas akademika melalui website resmi					
1.10	Mengirimkan *email* yang berisikan *password default* sementara untuk seluruh civitas akademika mengenai ketentuan penggunaan *strong password*					
1.11	Melakukan *login* dengan menggunakan *password default*					
1.12	Mengeluarkan notifikasi untuk melakukan pergantian *password default* dengan password baru yang sesuai dengan ketentuan kualitas standard *strong password*					
1.13	Memastikan seluruh civitas akademika mengganti *password default* dalam kurun waktu selama satu bulan					



Mengelola data penggunaan *password* lama dan memastikan tidak ada pengulangan penggunaan *password default/ password* lama *(Maintain a record of previously used password and prevent re-use*)

Mengijinkan pengguna memilih *password* pribadi dan memaksa pengguna untuk mengganti *password default* di awal log in. *(Allow user to select and change their own passwords. Force user to change their passwords at the first log-on*)

	URAIAN PROSEDUR	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
1.14	Mengelola data penggunaan password lama dan memastikan tidak ada penggunaan kembali *password default*		6			
2.	Proses Permintaan pergantian password					
2.1	Melakukan permintaan pergantian password					
a.1	**Mahasiswa** Mengajukan permintaan pergantian password dengan mengisi formulir permintaan pergantian password					
a.2	Mengisikan formulir permintaan pergantian password dan menyertakan alasan pengajuan permintaan password					FM-01 Formulir Permintaan Pergantian Password
2.2	Melakukan validasi pada formulir permintaan pergantian password			7		FM-01 Formulir Permintaan Pergantian Password

Menyimpan dan mentransmisikan password dengan prosedur/media yang aman *(Store and transmit passwords in protect form*)

	URAIAN PROSEDUR	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
2.3	Mengirimkan *email* yang berisikan link untuk menginputkan password baru kepada civitas akademika yang melakukan permintaan pergantian password		7			
2.4	Mengakses *link* dan menginputkan *password* baru					
2.5	Melakukan verifikasi dan validasi inputan password baru					

Gambar 6.1. Standard Operating Procedure Manajemen Password

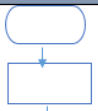
6.5.2 Prosedur Pengelolaan dan Pencegahan Malware

Prosedur ini menjelaskan mengenai langkah-langkah dalam melakukan pengelolaan dan pencegahan malware sesuai dengan kontrol pada Cobit 5, DSS05.01 *protect against malware*. Prosedur ini berisi 2 proses utama yang didefinisikan dalam beberapa aktivitas yang berurutan..

SEKOLAH TINGGI ILMU EKONOMI PERBANAS		
	Nomor SOP	PS-02
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	PENCEGAHAN MALWARE
	Disahkan oleh	(.....)
DESKRIPSI SOP	**KUALIFIKASI DAN DAFTAR PELAKSANA**	
Prosedur Pengelolaan dan Pencegahan Malware merupakan prosedur untuk menjadi acuan bagi pegawai Bagian TIK dalam upaya melakukan pencegahan terhadap bahaya malware serta melindungi perangkat dan aset informasi milik STIE Perbanas dan pengelolaan penanganan terhadap ancaman malware	**DAFTAR PELAKSANA** - Pegawai Bagian TIK - Administrator - Kasie TIK	
KETERKAITAN	**KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis mengenai malware yang baik - Memiliki kemampuan teknis instalasi perangkat anti malware - Memiliki kemampuan pemahaman teknologi informasi - Memiliki kemampuan komunikasi yang baik	
-		
REFERENSI	**PERLENGKAPAN / PERSYARATAN**	
COBIT 5 – Kontrol DSS05.01 *Protect Against Malware*	- Perangkat anti malware : *anti virus, anti spyware, spam filtering* dan *web contect filtering* - Formulir Laporan Gangguan Keamanan Informasi (FM-04)	
PERINGATAN	**PENCATATAN DAN PENDATAAN**	
Jika SOP ini tidak dijalankan, maka pencegahan malware tertunda sehingga dapat mengakibatkan risiko hilangnya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) data	- Mencatat gangguan keamanan informasi dalam bentuk *malware* pada formulir Laporan Gangguan Keamanan Informasi (FM-04)	

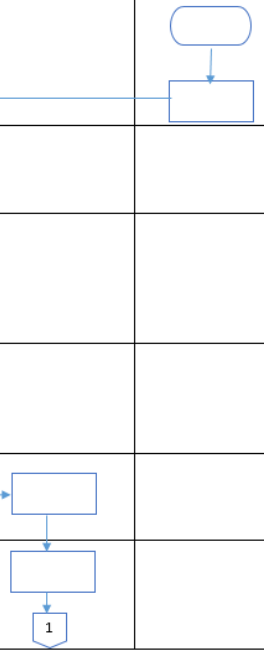
Mengkomunikasikan software anti malware dan melaksanakan tindakan / prosedur preventif dan menentukan tanggung jawab kerja *(Communicate malicious software and enforce prevention procedure and responsibilities*)

Menginstal dan mengaktifkan software anti malware pada seluruh perangkat pengolah informasi *(Install and activate malicious software on all processing facilities*) Dan mendistribusikan seluruh software proteksi keamanan pada setiap perangkat (*distribute all protection software*)

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Pegawai Bagian TIK	Administrator	Sistem	Kasie TIK	
1.	**Proses pencegahan malware**					
1.1	Melakukan *upgrade* dan *patch* sistem operasi dan aplikasi					
1.2	Menyediakan perangkat/fasilitas anti malware • Anti virus • Anti Spyware • Spam Filtering • Web Content Filtering					
	Memastikan kesesuaian spesifikasi anti virus yang digunakan					
	Memastikan keesuaian spesifikasi anti spyware (*spyware detection*) yang diguanakan					
1.3	Memastikan bahwa perangkat lunak *anti malware* segera diinstalasi pada setiap perangkat komputer dan *server*					
1.4	Memastikan anti virus selalu ter-upadte pada sistem pusat dan juga pada setiap perangkat komputer dan *server*					

Secara berkala melakukan peninjauan dan evalasi terhadap ancaman yang potensial pada sistem informasi *(regularly review and evaluate potential threats*)

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Pegawai Bagian TIK	Administrator	Sistem	Kasie TIK	
	2. Proses penanganan gangguan malware					
2.1	Menampilkan beberapa indikasi umum terjadinya gangguan malware, yang termasuk didalamnya meliputi : - *Alert* pada sistem - Perubahan konfigurasi - Firewall tidak aktif (*disabled*)					
2.2	Melakukan pelaporan insiden/gangguan keamanan informasi dalam formulir Laporan Gangguan Keamanan Informasi					FM-04 Formulir Laporan Gangguan Keamanan Informasi
2.3	Mengkomunikasikan insiden/gangguan dengan administrator baik sistem, jaringan maupun aplikasi terkait untuk menentukan rencana penanggulangan insiden/gangguan					
a	Mencatat insiden pada *log* insiden dengan mencantumkan tanggal dan waktu terjadinya insiden dan semua aktifitas yang dilakukan untuk menindaklanjutinya					
b	Mengamankan data elektronik yang terkait dengan insiden paling lambat 1 jam setelah insiden tersebut dilaporkan					
c	Mengidentifikasi risiko dan dampak indsiden terhadap aset informasi					



	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Pegawai Bagian TIK	Administrator	Sistem	Kasie TIK	
d	Menerapkan rencana penanggulangan insiden paling lambat 24 jam setelah insiden tersebut dilaporkan		1			
2.4	Menyediakan sarana penangan malware yang meliputi : - Packet Sniffer dan protocol analyzer - Daftar port - Perangkat/fasilitas anti malware - Network diagram dan daftar perangkat TIK yang bersifat kritikal - *Update security patch* - Media lain sepeti *operating system media, boot disk/CD, backup data,* atau *installer* yang dibutuhkan					
2.5	Melaporkan status penyelesaian insiden/gangguan kepada pihak terkait					
2.6	Melakukan pembaharuan pelaporan pada formulir Laporan Gangguan Kemanan Informasi					FM-04Formulir Laporan Gangguan Keamanan Informasi
2.7	Melakukan validasi formulir Laporan Gangguan Keamanan Informasi					

Secara berkala melakukan peninjauan dan evalasi terhadap ancaman yang potensial pada sistem informasi *(regularly review and evaluate potential threats*)

Gambar 6.2. Standard Operating Procedure Pengelolaan dan Pencegahan Malware

6.5.3 Prosedur Pengelolaan Gangguan Sistem Informasi

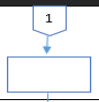
Prosedur ini menjelaskan tahapan dalam aktivitas pengelolaan gangguan pada sistem informaasi yang mengacu pada kontrol ISO27002:2013, klausul 16.1 *management of information security incidentis and improvements*. Dalam prosedur ini hanya terdapat satu proses utama yaitu proses penanganan gangguan sistem informasi khususnya terkait serangan *hacker*.

SEKOLAH TINGGI ILMU EKONOMI PERBANAS		
	Nomor SOP	PS-03
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	PENGELOLAAN GANGGUAN SISTEM INFORMASI
	Disahkan oleh	(.....)
DESKRIPSI SOP	**KUALIFIKASI DAN DAFTAR PELAKSANA**	
Prosedur Pengelolaan Gangguan Sistem Informasi ini merupakan prosedur yang menjelaskan mengenai pengelolaan terhadap gangguan atau insiden dalam bentuk serangan *hacker* pada layanan sistem informasi.	**DAFTAR PELAKSANA** - Pegawai Bagian TIK - Administrator - Kasie TIK **KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis mengenai malware yang baik. - Memiliki kemampuan pemahaman terhadap berbagai ancaman sistem informasi (*hacker, cracker*) - Memiliki kemampuan dan pemahaman teknis jaringan yang baik	
KETERKAITAN		
-		
REFERENSI	**PERLENGKAPAN / PERSYARATAN**	
SO270022013 – Klausul 16.1 *Management of Information Security Incidents and Improvements*	- Perangkan penanganan gangguan : Packet Sniffer, Protocol Analyzer, daftar port, perangkat anti malware, Network diagram, - Instruksi Kerja Pemindaian Sistem Informasi - Formulir Laporan Gangguan Keamanan Informasi (FM-04) - Formulir Evaluasi Sistem Informasi (FM-03)	
PERINGATAN	**PENCATATAN DAN PENDATAAN**	
Jika SOP ini tidak dijalankan, maka pengelolaan gangguan sistem informasi akan tertunda sehingga dapat mengakibatkan risiko hilangnya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) data serta terganggunya proses bisnis	- Mencatat gangguan sistem informasi mengenai serangan *hacker* pada formulir Laporan Gangguan Kemanan Informasi (FM-04) - Mencatat hasil evaluasi sistem informasi pada formulir evaluasi sistem informasi (FM-03)	

Melaporkan gangguan pada keamanan informasi *(reporting information security events*)

Melakukan penilaian dan pengambilan keputusan terkait penangan untuk gangguan keamanan informasi *(assessment of and decision on information security events*)

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Sistem	Administrator	Pegawai Bagian TIK	Kasie TIK	
1.	Proses penanganan gangguan serangan *hacker*					
1.1	Menampilkan beberapa indikasi umum terjadinya gangguang serangan *hacker*					
1.2	Melakukan pelaporan insiden/gangguan keamanan informasi dalam formulir Laporan Gangguan Keamanan Sistem Informasi dan melaporkan langsung kepada Kepala Bagian TIK					FM-04 Formulir Laporan Gangguan Keamanan Informasi
1.3	Mengamankan data elektronik yang terkait dengan insiden paling lambat 1 jam setelah insiden/gangguan dilaporkan					
1.4	Mengkomunikasikan insiden/gangguan dengan administrator baik sistem, jaringan maupun aplikasi terkait untuk menentukan rencana penanggulangan insiden/gangguan					
a.	Mencatat insiden pada *log* insiden dengan mencantumkan tanggal dan waktu terjadinya insiden dan semua aktifitas yang dilakukan untuk menindaklanjutinya		1			

		SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
			Sistem	Administrator	Pegawai Bagian TIK	Kasie TIK	
Melakukan penanganan/bentuk respon terhadap insiden/gangguan keamanan informasi *(response to information security incidents)*	b.	Mengganti *passoword* pada sistem yang di indikasi terkena serangan *hacker*					
	c.	Melakukan *restore* data pada sistem yang di indikasi terkena serangan *hacker*					PS-04 Prosedur Back Up dan Restore
	d.	Memperkuat jaringan *firewall* dan melakukan *block mac address*					
	e.	Melakukan analisis pada log sistem					
	f.	Mengidentifikasi risiko dan dampak indisden terhadap aset informasi					
	1.5	Melakukan analisis keamaan sistem informasi dengan melakukan pemindaian/*scanning* secara berkala terhadap perangkat pengolah informasi untuk menemukan kelemahan sistem sesuai dengan instruksi kerja pemindaian perangkat pengolah informasi					IN-01 Instruksi Kerja Pemindaian Sistem Informasi
	1.6	Mencatat hasil analisis gangguan sistem informasi yang terdiri dari dua aktivitas					

Melaporkan gangguan pada keamanan informasi *(reporting information security events*)

Melakukan pembelajaran berdasarkan gangguan/insiden keamanan informasi yang terjadi *(learning from information security incidents*)

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Sistem	Administrator	Pegawai Bagian TIK	Kasie TIK	
a.	Analisis dan penyusunan tindakan perbaikan (*corrective*) lanjutan yang perlu diterapkan untuk menghindari terulangnya kejadian serupa		2			FM-03 Formulir Evaluasi Sistem Informasi
b.	Penerapan inisiatif tindakan pencegahan (*preventive*) terhadap area yang memiliki potensi rentan terhadap gangguan/insiden sejenis					FM-03 Formulir Evaluasi Sistem Informasi
1.7	Melakukan peloporan status penyelesaian insiden/gangguan keamanan informasi					
	Apakah penyelesaian insiden/gangguan berhasil?		Berhasil / Tidak Berhasil			
a1.	**Berhasil** Melaporkan status penyelesaian insiden/gangguan keamanan sistem informasi kepada pihak terkait					
a2.	Melakukan pembaharuan pelaporan pada formulir Laporan Gangguan Kemanan Sistem Informasi					FM-04 Formulir Laporan Gangguan Keamanan Informasi
b1.	**Tidak Berhasil** Melaporkan kepada Kasie TIK untuk melakukan penanganan lebih lanjut					
1.8	Mengkaji hasil evaluasi sistem informasi secara berkala					

Gambar 6.3. Standard Operating Pengelolaan Gangguan Sistem Informasi

6.5.4 Prosedur Back Up dan Restore

Prosedur ini menjelaskan langkah langkah dalam aktivitas backup yang sesuai dengan kontrol ISO27002:2013, sub klausul 12.3.1 *information backup*. Prosedur Back up dan restore dibagi kedalam empat proses utama yang terdiri dari beberapa aktivitas yang berurutan. Namun, sebelum mendeskripsikan prosedur penangan secara terstruktur, terlebih dahulu didefinisikan informasi pendukung yang dibutuhkan untuk menunjang aktivitas didalam prosedur tersebut. Pendefinisan tesebut berguna untuk menentukan strategi back up yang sesuai dengan kebutuhan bisnis. Pendefinisan dalam prosedur Back up dibagi kedalam tiga yaitu pendefinisian klasifikasi data, pendefinisian kritikalitas data dan pendefinisian tipe back up.

1. **Pendefinisian Klasifikasi Data**
   Dalam penelitian ini, diusulkan pendefinisian klasifikasi data berdasarkan tingkat sensitivtas data. pendefinisian klasifikasi data berguna bagi manajemen untuk menentukan tipe back up yang sesuai. Berikut ini adalah klasifikasi data yang terdiri dari 4 tingkatan klasifikasi.

Tabel 6. 9. Klasifikasi Data

Klasifikasi Data	Keterangan
Sangat Rahasia (*Strictly Confidential*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian bagi STIE Perbanas
Rahasia (*Confidential*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan atau menurunkan citra dan reputasi STIE Perbanas
Terbatas	Data yang apabila didistribusikan

Klasifikasi Data	Keterangan
(*Internal Use Only*)	secara tidak sah atau jatuh ke tangan yang tidak sah atau tidak berhak akan mengganggu kelancaran kegiatan tetapi tidak akan mengganggu citra dan reputasi STIE Perbanas
Umum (*Public*)	Data yang secara sengaja disediakan untuk dapat diketahui umum dan tidak akan menggangu privasi atau keamanan organsiasi apabila jatuh ke tangan yang tidak berhak

2. Pendefinisian Kritikalitas Data

Dalam penelitian ini, diusulkan pendefinisian klasifikasi data yang didasarkan pada tingkat kritikalitas data. pengklasifikasian kritikalitas data ini berguna untuk menentukan prosedur backup yang sesuai. Berikut ini adalah pendefinisian dari kritikalitas data yang dibagi kedalam tiga tingkatan kritikalitas data.

Tabel 6. 10. Kritikalitas Data

Tingkatan Kritikalitas Data	RPO	MTD	Penanganan	
			Full Backup	Differential/Incremental Backup
Tinggi	Maks 24 jam	Maks 24 jam	1 x Seminggu	Maks 24 jam
Sedang	Maks 1 minggu	Maks 1 minggu	1 x Sebulan	Maks 1 Minggu
Rendah	> 1 Minggu	> 1 Minggu	Min 1 x 3 Bulan	> 1 Minggu

Kritikaslitas data didasarkan pada RPO (*Recovery Point Object*) dan MTD (*Maximum Tolerable Downtime*). Berikut adalah masing masing penjelasannya.

- RPO (*Recovery Point Object*)
  RPO adalah jumlah waktu maksimal yang dapat ditoleransi perusahaan terhadap kehilangan data akibat risiko yang terjadi.
- MTD (*Maximum Tolerable Downtime*)
  MTD adalah jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan terhadap kegagalan proses bisnis.

3. Pendefinisian Tipe Back Up

Dalam penelitian ini juga didefinisikan tipe backup pada server yang dapat dilakukan secara bekala dengan kurun waktu setiap hari setelah jam kerja aktif. Tipe backup yang umum diimplementasikan yaitu *full backup* dan *differential/incremental backup*. Berikut adalah penjelasan dari masing masing tipe back up.

Tabel 6. 11. Tipe Back Up

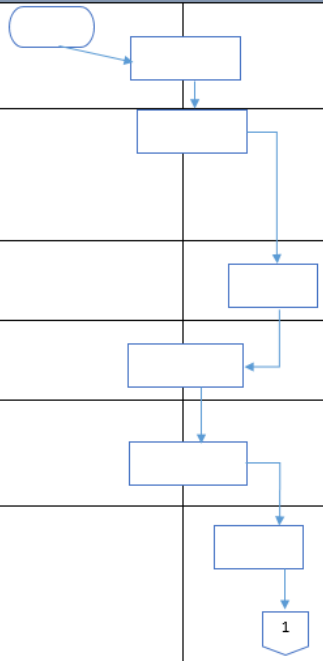
Tipe Backup	Deskripsi
Full Backup	Backup dilakukan untuk seluruh sumber data/file termasuk folder ke media lain dan membutuhkan waktu serta ruang yang besar.
Differential/Incremental Backup	Backup dilakukan untuk file-file yang berubah dari saat backup terakhir dibuat.

Berikut merupakan SOP Back up secara detail beserta pemetaannya terhadap kontrol ISO27002:2013, sub klausul 12.3.1 *information backup*.

SEKOLAH TINGGI ILMU EKONOMI PERBANAS		
	Nomor SOP	PS-04
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	BACKUP DAN RESTORE
	Disahkan oleh	(.....)
DESKRIPSI SOP	**KUALIFIKASI DAN DAFTAR PELAKSANA**	
Prosedur Backup dan Restore Data merupakan prosedur yang bertujuan untuk memastikan backup data yang dilakukans secara berkala telah sesuai dan data yang di backup telah lengkap	**DAFTAR PELAKSANA** - Kasie TIK - Administrator **KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis back up dan restore data - Memiliki kemampuan pemahaman terhadap database, server dan perangkat lain pendukung back up data - Memiliki kemampuan komunikasi yang baik	
KETERKAITAN		
-		
REFERENSI	**PERLENGKAPAN / PERSYARATAN**	
ISO27002:2013 – Sub Klausul 12.3.1 *Information Backup*	- Perangkat media back up dan server - Instruksi Kerja Back up - Instrusk kerja Restore - Formulir Klasifikasi Data (FM-05) - Formulir Log Backup Data (FM-06) - Formulir Restore Data (FM-07)	
PERINGATAN	**PENCATATAN DAN PENDATAAN**	
Jika SOP ini tidak dijalankan, maka back up data tidak berjalan dengan baik sehingga dapat mengakibatkan risiko yang berkaitan dengan ketersediaan (*availability*) data serta terganggunya proses bisnis	- Mencatat pengklasifikasian data padaformulir Klasifikasi Data (FM-06) - Mencatat hasil back up data pada formulir Log Backup Data (FM-07) - Mencatat proses dan hasil restore data pada formulir Restore Data (FM-08	

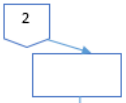
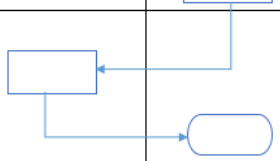
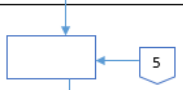
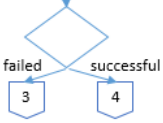
Memastikan bahwa tipe back up dan frekuensi back up telah sesuai dengan kebutuhan bisnis dan juga telah mempertimbangkan keamanan informasi dan tingkat kritikalitas informasi *(The extent (full/differential backuo) and frequency should be reflect the business requirements, the security of the information involved and the criticality of the information*)

	URAIAN PROSEDUR	PELAKSANA			DOKUMEN TERKAIT
		Kasie TIK	Administrator	Sistem	
1.	Proses umum sebelum melakukan back up data				
1.1	Melakukan klasifikasi data dan menentukan tingkat kritikalitas data				
a.1	**Membuat strategi backup** Melakukan klasifikasi terhadap data dan menentukan tingkatan kritikalitas data untuk menentukan tipe backup yang dibutuhkan				FM-06 Formulir Klasifikasi Data
a.2	Melakukan pembaharuan pada formulir Daftar Klasifikasi Data				
a.3	Membuat sebuah strategi untuk melakukan backup data berdasarkan Daftar Klasifikasi Data				
a.4	Menentukan penjadwalan untuk backup data sesuai dengan tingkatan kritikalitas data dan tipe backup telah sesuai				
b.1	**Penentuan Media Backup** Administrator melakukan *checklist* pemeliharaan media back up data setiap awal semester untuk memastikan keamanan media back up				



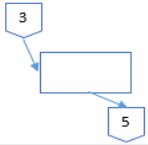
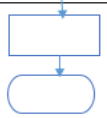
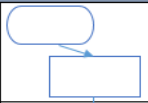
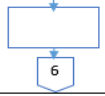
	URAIAN PROSEDUR	PELAKSANA			DOKUMEN TERKAIT
		Kasie TIK	Administrator	Sistem	
2.	Proses back up data secara berkala				
2.1	Menginstruksikan Administrator untuk melakukan back up secara berkala	1			
2.2	Melakukan setting penjadwalan backup dan memastikan penjadwalan backup data sesuai dengan ketentuan penjadwalan backup data				
2.3	Backup data secara otomatis untuk server Sistem informasi (SISFO) pada pukul 12.00 dan 21.00				
2.4	Backup data secara otomatis untuk server File Server pada pukul 19.00				
2.5	Melakukan *monitoring* (pemantauan) secara berkala untuk memastikan bahwa hasil eksekusi backup data telah akurat dan lengkap				
2.6	Mengelola *log* pada sistem *back up* data untuk memastikan keberhasilan data yang ter-*back up* dan data yang tidak berhasil di-*back up*		2		

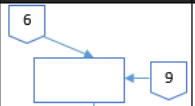
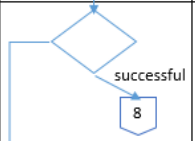
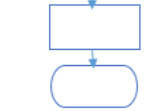
Dalam prosedur operasional harus ada pemantauan hasil eksekusi back up untuk mengetahui kegagalan backup pada penjadwalan back up otomatis *(Operational procedure should monitor the execution of backups and address failures of scheduled back up*)

	URAIAN PROSEDUR	PELAKSANA			DOKUMEN TERKAIT
		Kasie TIK	Administrator	Sistem	
2.7	Membuat laporan pada formulir Log Backup Data				FM-07 Formulir Log Backup Data
2.8	Memastikan bahwa administrator telah mengimplementasikan dan melakukan *monitoring* (pemantauan) secara berkala untuk backup data dengan melakukan validasi terhadap log backup data				FM-07 Formulir Log Backup Data
3.	Proses uji coba back up data secara berkala				
3.1	Melakukan uji back up data secara berkala 3 bulan sekali				
3.2	Melakukan set up persiapan uji coba back up data				
3.3	Melakukan uji coba back up data pada media back up yang telah disiapkan				
3.4	Menganalisis log back up data ***Apakah back up berhasil?***				

Melakukan uji coba secara berkala pada media *back up* untuk memastikan bahwa proses *back up* dapat berjalan dengan baik ketika diperlukan *(Back up media should be regularly tested to ensure that they can be relied upon for emergency use*)

Dalam prosedur operasional harus ada pemantauan hasil eksekusi back up untuk mengetahui kegagalan backup pada penjadwalan back up otomatis *(Operational procedure should monitor the execution of backups and address failures of scheduled back up*)

	URAIAN PROSEDUR	PELAKSANA			DOKUMEN TERKAIT
		Kasie TIK	Administrator	Sistem	
a.1	**Status Failed** Melakukan kembali proses uji coba back up data pada sub 3.2				
b.1	**Status Successful** Melakukan pengecekan kesesuaian data yang berhasil ter-back up				
b.2	Memastikan tidak ada data yang corrupt				
b.3	Membuat laporan pada formulir uji coba log back up data				FM-07 Formulir Log Backup Data
4.	Proses Restore Data				
4.1	Menentukan database yang akan dilakukan restore				
4.2	Menentukan jadwal pelaksanaan restore data				

	URAIAN PROSEDUR	PELAKSANA			DOKUMEN TERKAIT
		Kasie TIK	Administrator	Sistem	
4.3	Melakukan proses restore data				
4.4	Menganalisis hasil restore data **Apakah Restore data berhasil?**				
a4	**Failed** Administrator melakukan kembali proses restore data (kembali ke poin 4.3)				
b4	**Successful** Adminitrator mendokumentasikan pelaksanaan retore data dengan mengisi Formulir Restore Data				FM-8 Formulir Restore Data
4.5	Memvalidasi formulir Restore data				

Gambar 6.4. Standard Operating Procedure Back up dan Restore

6.5.5 Prosedur Proteksi Lingkungan Server

Prosedur proteksi lingkungan server menjelaskan mengenai langkah-langkah yang dapat dilakukan oleh Bagian TIK untuk melakukan pengamanan pada server dan lingkungan sekitar server. Prosedur ini mengacu pada kontrol yang ada di Cobit 5, DSS05.03 *manage endpoint security*. Dalam prosedur proteksi lingkungan server, juga didefinisikan standard umum terhadap pemeliharaan server. Dimana daftar standard umum untuk pemeliharaan server tersebut berguna untuk memudahkan Bagian TIK dalam memastikan pemenuhan proteksi lingkungan server.

1. **Standard Pemeliharaan server**
   Berikut ini merupakan standard pemeliharaan server untuk memastikan keamanan di sekitar server yang meliputi :
   a) Memastikan bahwa lokasi ruang server berada pada lingkungan yang aksesnya terbatas untuk public (*restricted area*), mudah diawasi, aman dari bahaya genangan air/banjir.
   b) Memastikan bahwa untuk menjamin kelayakan sirkulasi udara, tinggi ruang yang tersedia untuk penempatan rak komputer minimal 2,5 (dua koma lima) meter.
   c) Memastikan bahwa setiap kabel jaringan telah diberi label yang sesuai dan jelas dan diatur untuk memudahkan penangan kesalahan.
   d) Memastikan bahwa jaringan kabel data harus dipisahkan dari jaringan kebel listrik dengan jarak minimal 3 (tiga) meter untuk menghindari dampak radiasi (elektromagnet).
   e) Memastikan bahwa dalam ruangan server telah tersedia alarm api dan asap, alat pengukur suhu dan

kelembapan serta perangkat pengawasan video/gambar.

f) Memastikan bahwa pada lokasi ruang server tersedia fasilitas *Uninterruptible Power Supply (UPS)* yang memiliki kapasitas yang cukup untuk memberikan pasokan lisyrik selama minimal 15 (lima belas) menit kepada semua perangkat komputer yang ada dalam ruang server pada saat sumber listrik ke ruang server mengalami gangguan.
g) Memastikan selain perangkat dan fasilitas pengolahan data dan informasi tidak boleh dihubungkan ke perangkat *Uninterruptible Power Supply (UPS).*
h) Memastikan pada lokasi ruang server harus tersedia generator listrik dengan fungsi pengaturan pasokan daya otomatis dengan kapasitas yang cukup untuk keseluruhan perangkat komputer dan fasilitas pendukungnya, seperti *server, router* dan perangkat lainnya yang ada pada ruang server.
i) Memastikan fasilitas *Air Conditioning System* yang ada harus mempunyai kapasitas yang sesuai dengan volume ruang server, termasuk beban panas yang dihasilkan perangkat komputer maupun jaringan, dengan aliran udara yang baik dan tetap dapat beroperasi ketika aliran listrik utama padam. Suhu udara di ruang server diatur dalam batas 20^0 - 25^0 dengan kelembaban relative antara 40 – 45 %
j) Memastikan bahwa fasilitas pemadam api yang tersedia harus mampu memadamkan api dalam waktu kurang dari 2 (dua) menit dan menggunakan gas yang tidak merusak perangkat ataupun membahayakan manusia.

k) Memastikan komputer pada ruang server tidak digunakan sebagai sarana *log-on* oleh pegawai lain tanpa izin khusus dari Kepala Bagian TIK.

l) Memastikan bahwa prosedur akses ruang server telah berjalan dengan baik dengan melakukan peninjauan terhadap *log-book* akses ruang server.

Berikut merupakan SOP Proteksi Lingkungan Server secara detail beserta pemetaannya terhadap kontrol Cobit 5 DSS05.03 *manage endpoint security*.

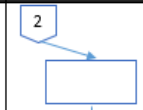
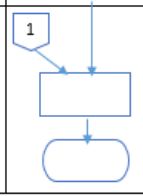
SEKOLAH TINGGI ILMU EKONOMI PERBANAS	**Nomor SOP**	PS-05
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	**PROTEKSI LINGKUNGAN SERVER**
	Disahkan oleh	(.....)
DESKRIPSI SOP	**KUALIFIKASI DAN DAFTAR PELAKSANA**	
Prosedur proteksi lingkungan server merupakan prosedur untuk memastikan bahwa server telah memiliki proteksi secara fisik untuk menghindari timbulnya risiko kerusakan server yang dapat berdampak pada hilangnya data akibat kondisi lingkungan sekiar server yang tidak dikelola dengan baik	**DAFTAR PELAKSANA** - Pegawai Bagian TIK - Administrator **KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis dan konfigurasi server - Memiliki kemampuan teknologi informasi dan komunikasi yang baik - Memiliki kemampuan komunikasi yang baik	
KETERKAITAN		
Kebijakan Keamanan Perangkat dan Komunikasi		
REFERENSI	**PERLENGKAPAN / PERSYARATAN**	
COBIT 5 – Kontrol DSS05.03 *Manage Endpoint Security*	- Formulir Pemeliharaan Fisik Server (FM-08)	
PERINGATAN	**PENCATATAN DAN PENDATAAN**	
Jika SOP ini tidak dijalankan, maka proteksi terhadap fisik server akan berkurang dan tidak sesuai dengan standard sehingga dapat mengakibatkan risiko yang berkaitan dengan hilangnya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) data serta terganggunya proses bisnis	- Mencatat hasil pemenuhan *checklist* keamanan fisik server pada formulir Pemeliharaan Fisik Server (FM-09)	

Melakukan konfigurasi pada sistem operasi dengan tepat dan juga mengelola konfigurasi jaringan dengan tepat *(Configure operating systems in a secure manner. Manage netrowork configuration in a secure manner*)

Menyediakan proteksi fisik pada server dan perangkat lain *(Provide physical protection of endpoint system*)

	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Administrator	Kepala Bagian TIK	Sistem	
1.	Proses pengamanan lingkugan server				
1.1	Melakukan pemeliharaan terhadap server dengan memastikan keamanan di sekitar ruang server secara berkala 3 bulan sekali				
1.2	Mengisi formulir pemeliharaan server yang berisi *checklist* keamanan fisik server sesuai dengan temuan kondisi pada saat itu				FM-08 Pemeliharaan Server
1.3	Melakukan validasi formulir pemeliharaan server untuk memastikan perawatan, pemeliharaan, pemeriksaan secara berkala				
	Apakah terdapat kondisi yang tidak sesuai dengan kebutuhan keamanan dalam pemeliharaan server?		Ya / Tidak → 1		
a.	Memerintahkan untuk melakukan tindakan korektif (*corrective*)		→ 2		

Menyediakan proteksi fisik pada server dan perangkat lain *(Provide physical protection of endpoint system*)

	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Administrator	Kepala Bagian TIK	Sistem	
b.	Melakukan tindakan korektif sesuai dengan instruksi dan memperbaiki kondisi server				
c.	Memperbaharui Formulir Pemeliharaan Server dan melakukan validasi kepada Kepala Bagian TIK				FM-08 Pemeliharaan Server

Gambar 6.5. Standard Operating Procedure Proteksi Lingkungan Server

6.5.6 Prosedur Akses Ruang Server

Prosedur akses ruang server menjelaskan mengenai proses untuk memastikan akses pada area penting khususnya ruang server terkontrol dengan baik dan memastikan bahwa akses terhadap area ruang akses telah terautorisasi. Prosedur ini mengacu pada kontrol pada Cobit 5 DSS05.05 *manage physical access to IT Assets* dan juga kontrol ISO27002:2013 sub klausul 11.1.2 *physical entry controls.*

SEKOLAH TINGGI ILMU EKONOMI PERBANAS		
	Nomor SOP	PS-06
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	AKSES RUANG SERVER
	Disahkan oleh	(.....)

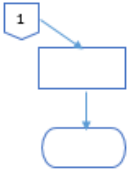
DESKRIPSI SOP	KUALIFIKASI DAN DAFTAR PELAKSANA
Prosedur Akses Ruang Server merupakan prosedur untuk memastikan bahwa akses pada area penting seperti ruang server terkontrol dengan baik dan memastikan seluruh akses terhadap area tersebut telah terautorisasi dan memiliki sebuah *log* aktivitas yang dapat dimonitor dengan baik	**DAFTAR PELAKSANA** - Administrator - Civitas Akademika - Pihak Eksternal **KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis dan konfigurasi server - Memiliki kemampuan teknologi informasi dan komunikasi yang baik - Memiliki kemampuan komunikasi yang baik
KETERKAITAN	
Kebijakan Keamanan Perangkat dan Komunikasi	
REFERENSI	**PERLENGKAPAN / PERSYARATAN**
COBIT 5 – Kontrol DSS05.05 *Manage Physical Access to IT Assets* ISO27002:2013 – Sub Klausul 11.1.2 *Physical Entry Controls*	- Formulir Log Pegawai (FM-9) - Formulir Log Daftar Pengunjung (FM-10)
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan, maka keamanan terhadap server akan berkurang dan tidak sesuai dengan standard sehingga dapat mengakibatkan risiko yang berkaitan dengan hilangnya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) data serta terganggunya proses bisnis	- Mencatat seluruh akses masuk ke ruang server oleh pegawai pada formulir Pemeliharaan Fisik Server (FM-10) - Mencatat seluruh akses masuk ke ruang server oleh pengunjung baik civitas akademika dan pihak eksternal pada formulir Log Daftar Pengunjung (FM-11)

Mengelola permintaan akses dan memberikan akses kedalam ruang server secara formal/resmi *(Manage the requesting and granting access/ formal access request*)

Menantau semua akses masuk dan harus menemani/melakukan supervise kepada semua pengunjung *(Log and monitor all entry, all visitors should be supervised*)

	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Administrator	Civitas akademik	Pihak eksternal	
1.	Proses akses kedalam ruang server				
1.1	Memastikan bahwa ruang server memiliki kunci untuk mengamankan ruang dari akses yang tidak terautorisasi				
1.2	Memastikan bahwa setiap pintu tertutup/terkunci dengan benar setelah masuk/keluar ruang server				
1.3	Mengakses ruang server dan menunjukan identitas serta izin resmi				
1.4	Meminta identitas kepada civitas akademik dan pihak eksternal dan memastikan identitas telah benar dan valid				
1.5	Mengisi *Log book* sebelum masuk ke dalam ruang server				FM-09 Formulir Log Pegawai FM-10 Formulir Log Daftar Pengunjung
1.6	Mendampingi civitas akademika atau pihak eksternal selama berada di ruang server				

Mengelola dan memantau dengan tepat log book yang berisikan akses masuk ruang sever *(A physical log book of all access should be securely maintained and monitored*)

	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Administrator	Civitas akademik	Pihak eksternal	
1.7	Melakukan *review* dan validasi secara berkala minimal 6 (enam) bulan sekali terhadap aktivitas akses ruang server beradasarkan *Log* daftar pengunjung ruang server				FM-10 Formulir Log Daftar Pengunjung

Gambar 6.6. Standard Operating Procedure Akses Ruang Server

6.5.7 Instruksi Kerja

Dalam mendukung pelaksanaan SOP, dibutuhkan beberapa instruksi kerja yaitu instruksi kerja pemindaian sistem informasi, instruksi kerja back up dan instruksi kerja restore.

6.5.7.1 Instruksi Kerja Pemindaian Sistem Informasi

Dalam dokumen SOP Pencegahan Malware, dibutuhkan sebuah instruksi tindakan preventif yaitu instruksi kerja pemindaian sistem informasi. Instruksi kerja pemindaian sistem informasi ini bertujuan untuk membantu kerja pegawai bagain TIK khusunya administrator aplikasi dalam melakukan pemindaian sistem informasi dan mencari celah kelemahan sistem informasi secara berkala. Berikut ini adalah instruksi kerja pemindaian sistem informasi.

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	IN-01	NO. RILIS : 00
		NO. REVISI : 00
	INSTRUKSI KERJA PEMINDAIAN SISTEM INFORMASI	TANGGAL TERBIT :
		HALAMAN :
	INSTRUKSI KERJA	

A. PELAKSANA

Pegawai Bagian TIK (administrator aplikasi)

B. RINCIAN INSTRUKSI KERJA

1. Tahap pemindaian sistem informasi dimulai dengan melakukan *scan* (pemindaian) terhadap kerentanan atau celah dalam website target dengan menggunakan *tools* ***Netsparker***.
   a. Pada kolom target URL masukan alamat website yang akan di *scanning*
   b. Tekan tombol Start Scan
2. Analisis hasil *scanning*
3. Lanjutkan proses dengan melakukan *port scanning* website dengan menggunakan *tools* ***Nmap.***
   a. Aktifkan **Nmap**
   b. Pada *command* inputkan :
      sudo su dilanjutkan dengan **nmap –V –A (alamat website target)**
4. Analisis hasil *scanning*
5. Tahap selanjutnya adalah melakukan *scanning* dengan menggunakna *tools* Accunetix untuk melakukan pemindaian kelemahan (*vulnerability scanning*) website.
   a. Pada kolom Start URL masukan alamat website yang akan di *scanning*
   b. Tekan tombol Start
   c. Analisis hasil pada kolom Scan Results

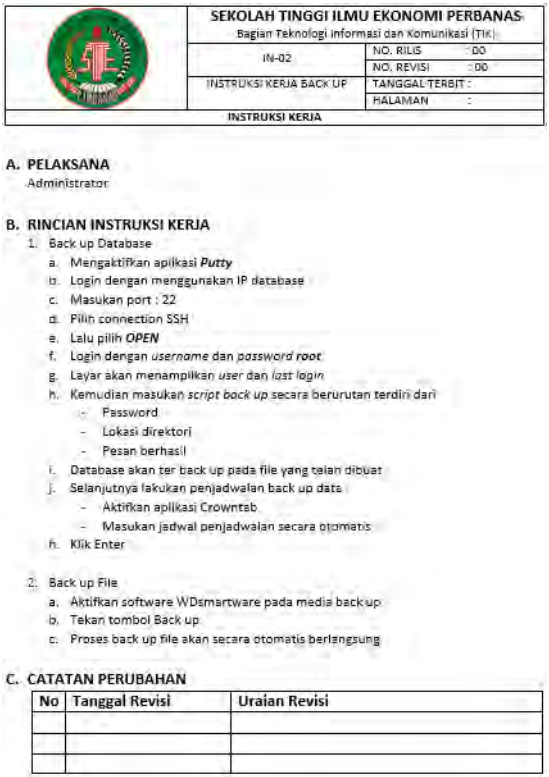
C. CATATAN PERUBAHAN

No	Tanggal Revisi	Uraian Revisi

Gambar 6.7. Instuksi Kerja Pemindaian Sistem Informasi

6.5.7.1 Instruksi Kerja Back up

Dalam dokumen SOP Backup dan Restore, dibutuhkan sebuah instruksi kerja yaitu instruksi kerja back up. Instruksi kerja back up ini bertujuan untuk membantu kerja pegawai bagain TIK baru dalam mempelajari proses back up data maupun back up file serta penjadwalan back up data yang pada umumnya dilakukan secara berkala oleh Bagian TIK. Berikut ini adalah instruksi kerja back up.



	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	IN-02	NO. RILIS : 00 NO. REVISI : 00
	INSTRUKSI KERJA BACK UP	TANGGAL TERBIT : HALAMAN :
INSTRUKSI KERJA		

A. PELAKSANA

Administrator

B. RINCIAN INSTRUKSI KERJA

1. Back up Database
   a. Mengaktifkan aplikasi ***Putty***
   b. Login dengan menggunakan IP database
   c. Masukan port : 22
   d. Pilih connection SSH
   e. Lalu pilih ***OPEN***
   f. Login dengan *username* dan *password root*
   g. Layar akan menampilkan *user* dan *last login*
   h. Kemudian masukan *script back up* secara berurutan terdiri dari
      - Password
      - Lokasi direktori
      - Pesan berhasil
   i. Database akan ter back up pada file yang telah dibuat
   j. Selanjutnya lakukan penjadwalan back up data
      - Aktifkan aplikasi Crowntab
      - Masukan jadwal penjadwalan secara otomatis
   h. Klik Enter

2. Back up File
   a. Aktifkan software WDsmartware pada media back up
   b. Tekan tombol Back up
   c. Proses back up file akan secara otomatis berlangsung

C. CATATAN PERUBAHAN

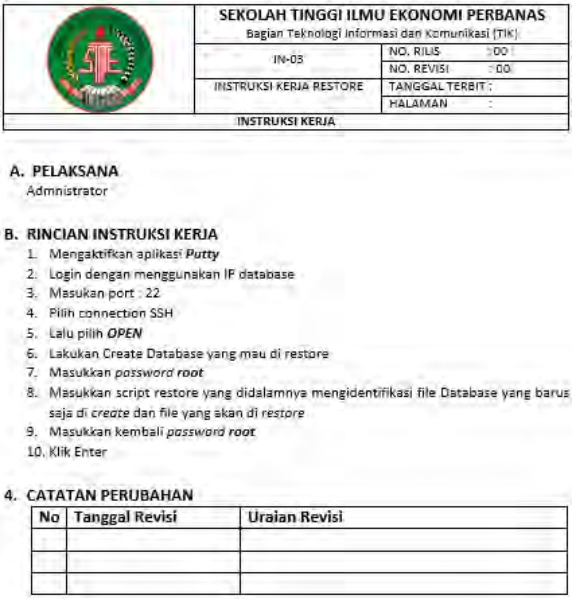
No	Tanggal Revisi	Uraian Revisi

Gambar 6.8. Instruksi Kerja Back up

6.5.7.1 Instruksi Kerja Restore

Dalam dokumen SOP Backup dan Restore, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja restore. Instruksi kerja

restore ini bertujuan untuk membantu kerja pegawai bagain TIK baru dalam mempelajari proses restore data yang pada umumnya dilakukan secara berkala oleh Bagian TIK. Berikut ini adalah instruksi kerja restore.



	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	IN-03	NO. RILIS : 00 NO. REVISI : 00
	INSTRUKSI KERJA RESTORE	TANGGAL TERBIT : HALAMAN :
INSTRUKSI KERJA		

A. PELAKSANA

Administrator

B. RINCIAN INSTRUKSI KERJA

1. Mengaktifkan aplikasi ***Putty***
2. Login dengan menggunakan IP database
3. Masukan port : 22
4. Pilih connection SSH
5. Lalu pilih ***OPEN***
6. Lakukan Create Database yang mau di restore
7. Masukkan *password* ***root***
8. Masukkan script restore yang didalamnya mengidentifikasi file Database yang barus saja di *create* dan file yang akan di *restore*
9. Masukkan kembali *password* ***root***
10. Klik Enter

4. CATATAN PERUBAHAN

No	Tanggal Revisi	Uraian Revisi

Gambar 6.9. Instruksi Kerja Restore

6.5.8 Formulir

Dalam mendukung pelaksanaan SOP, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 8 formulir yang dibutuhkan untuk mendukung pelaksanaan SOP.

6.5.8.1 Formulir Perbaikan Sistem Informasi

Formulir perbaikan sistem informasi adalah usulan formulir yang dapat digunakan oleh Bagian TIK untuk mendokumentasikan setiap penambahan fitur maupun perubahan dan perbaikan yang

dilakukan pada sistem informasi yang dikelola. Formulir perbaikan sistem informasi dapat dilihat pada Lampiran H.

6.5.8.2 Permintaan Pergantian Password

Formulir permintaan pergantian password adalah usulan formulir yang dapat digunakan seluruh civitas untuk mengajukan permintaan pergantian password apabila pengguna merasa bahwa terdapat indikasi informasi mengenai password telah diketahui pihak lain. Formuli yang dibuat dibedakan menjadi dua kategori yaitu formulir permintaan pergantian password untuk pegawai (dosen dan pegawai) dan juga untuk mahasiswa. Formulir permintaan pergantian password terlampir pada Lampiran H.

6.5.8.3 Formulir Laporan Gangguan Keamanan Informasi

Formulir laporan gangguan keamanan informasi digunakan untuk mendokumentasikan proses penangan gangguan dalam prosedur pengelolaan gangguan keamanan informasi. Tujuan dari dibuatnya formulir ini adalah untuk memastikan adanya tindakan penanggulangan insiden yang terstandar dan juga terdokumentasi sehingga dapa digunakan sebagai bahan evaluasi bagi Bagian TIK. Gambar 26 merupakan usulan rancangan dari laporan gangguan keamanan informasi. Formulir laporan gangguan keamanan informasi terlampir dalam Lampiran H.

6.5.8.4 Formulir Evaluasi Sistem Informasi

Formulir evaluasi sistem informasi digunakan untuk mendokumentasikan proses pencegahan terhadap bahaya malware dalam prosedur Pencegahan Malware. Formulir ini digunakan oleh pegawai Bagian TIK untuk melakukan pelaporan terhadap kelemahan dalam sistem informasi, dan menentukan tindakan perbaikan dan inisiatif pencegahan yang dapat dilakukan. Formulir evaluasi sistem informasi terlampir dalam Lampiran H.

6.5.8.5 Formulir Klasifikasi Data

Formulir klasifikasi data digunakan untuk menentukan strategi back up yang akan digunakan. Berdasarkan kontrol dalam

ISO27002:2013, penentuan strategi back up data ditentukan sesuai dengan kebutuhan bisnis organisasi dilihat dari kebutuhan keamanan dan tingkat kritikalitas data. Klasifikasi data akan didasarkan pada tingkat sensitivitas data dan tingkat kritikalita data. Formulir klasifikasi data terlampir dalam Lampiran H.

6.5.8.6 Formulir Log Backup Data

Formulir log back up digunakan oleh administrator DBA untuk melakukan pemantauan (*monitoring*) secara berkala pada hasil eksekusi back up data. Tujuan dari formulir log back up data ini adalah untuk memastikan bahwa hasil eksekusi back up data telah akurat dan lengkap dan juga untuk memastikan keberhasilan data yang ter-back up dan data yang tidak berhasil di-back up. Formulir log back up data terlampir dalam Lampiran H.

6.5.8.7 Formulir Restore

Formulir restore digunakan untuk permintaan kebutuhan restore data oleh pihak tertentu/unit kerja tertentu. Formulir restore data dibutuhkan untuk menjaga integritas data dan memastikan bahwa setiap proses restore data terdokumentasi dengan baik dan telah di validasi oleh pegawai bagian TIK yang bertanggung jawab. Formulir restore terlampir dalam Lampiran H.

6.5.8.8 Formulir Pemeliharaan server

Formulir pemeliharaan server digunakan oleh administrator untuk melaksanakan prosedur pemeliharaan terhap server yang dilakukan secara berkala 3 bulan sekali dengan melakukan *checklist* pada pemenuhan keamanan untuk server dan lingkungan sekitar server. Formulir pemeliharaan server terlampir dalam Lampiran H.

6.5.8.9 Formulir Log Pegawai

Formulir log pegawai digunakan oleh administrator untuk memastikan bahwa akses pada area ruang server terkontrol dengan baik untuk memastikan bahwa seluruh akses terhadap

area tesebut telah terautoriasai. Formulir log pegawai terlampir dalam Lampiran H.

6.5.8.10 Formulir Log Daftar Pengunjung

Formulir log daftar pengunjung digunakan oleh administrator untuk memastikan bahwa akses pada area ruang server terkontrol dengan baik untuk memastikan bahwa seluruh akses terhadap area tesebut telah terautoriasai. Formulir log daftar pengunjung ini digunakan untuk mendukung prosedur akses kedalam ruang server. Formulir Log Pegawai terlampir dalam Lampiran H.

6.6 Hasil Pengujian SOP

Pengujian SOP dilakukan dengan verifikasi dan validasi. Verifikasi dilakukan dengan wawancara untuk memastikan kesesuian antara prosedur yang dihasilkan dengan kebutuhan STIE Perbanas. Sementara validasi dilakukan dengan cara mensimulasikan SOP untuk mengetahui ketepatan prosedur ketika diimplementasikan dalam kasus yang nyata.

6.6.1 Hasil Verifikasi

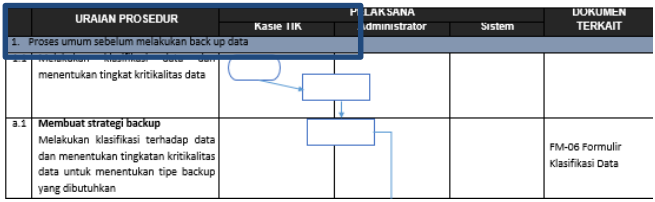
Verifikasi SOP dilakukan dengan cara wawancara pada Kasie Bagian TIK yang hasilnya secara detail akan dilampirkan pada Lampiran G. Dari hasil verifikasi, dibutuhkan beberapa revisi dokumen SOP, yaitu :

1. **Perubahan Pelaksana dalam Prosedur Backup**
   Setelah melakukan veririkasi, Kasie Bagian TIK melakukan koreksi pada pelaksana prosedur Backup bahwa dalam prosedur tersebut yang telibat adalah Kasie TIK dan administrator secara langsung. Sehingga, perubahan yang dilakukan dapat dilihat pada gambar berikut.

- Sebelum Perubahan

Gambar 6.10. Pelaksana sebelum perubahan

- Setelah Perubahan

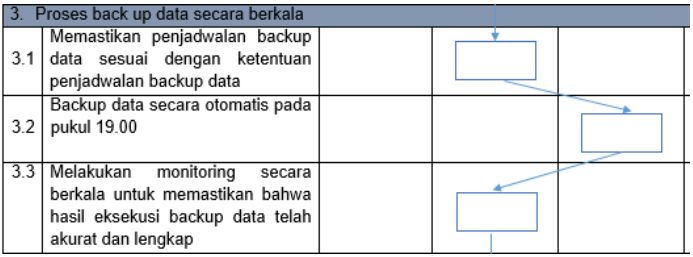


Gambar 6.11. Pelaksana setelah perubahan

2. Perubahan Penjadwalan Back Up Data

Setelah melakukan verifikasi, Kasie Bagian TIK memberikan informasi mengenai waktu penjadwalan back up yang lebih sesuai dengan kondisi kekinian yang ada pada STIE Perbanas. Sehingga, perubahan yang dilakukan dapat dilihat pada gambar berikut.

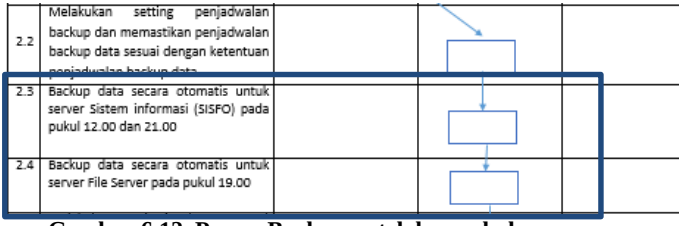
- Sebelum Perubahan



3.	Proses back up data secara berkala
3.1	Memastikan penjadwalan backup data sesuai dengan ketentuan penjadwalan backup data
3.2	Backup data secara otomatis pada pukul 19.00
3.3	Melakukan monitoring secara berkala untuk memastikan bahwa hasil eksekusi backup data telah akurat dan lengkap

Gambar 6.12. Proses Back up sebelum perubahan

- Setelah Perubahan



2.2	Melakukan setting penjadwalan backup dan memastikan penjadwalan backup data sesuai dengan ketentuan penjadwalan backup data
2.3	Backup data secara otomatis untuk server Sistem informasi (SISFO) pada pukul 12.00 dan 21.00
2.4	Backup data secara otomatis untuk server File Server pada pukul 19.00

Gambar 6.12. Proses Back up setelah perubahan

3. Penambahan Prosedur Uji Coba Backup Data

Berdasarkan hasil verifikasi kepada Kasie TIK STIE Perbanas, diketahui bahwa dalam proses back up data sering kali status yang muncul dalam *log back up* sistem tidak sesuai dengan kondisi data yang berhasil di *back up*. Dengan kata lain, terjadi *file corrupt* ketika data berusaha di *restore*. Sehingga, dalam SOP Back Up ditambahkan proses untuk melakukan uji coba back up data secara berkala. Penambahan proses tersebut bertujuan untuk memastikan ketepatan proses *back up* yang berlangsung setiap harinya. Gambar 23 adalah penambahan proses uji coba back up data pada prosedur Back Up.

3.	Proses uji coba back up data secara berkala				
3.1	Melakukan uji back up data secara berkala 3 bulan sekali				
3.2	Melakukan set up persiapan uji coba back up data				
3.3	Melakukan uji coba back up data pada media back up yang telah disiapkan				
3.4	Menganalisis log back up data ***Apakah back up berhasil?***		failed 3 successful 4		

a.1	**Status Failed** Melakukan kembali proses uji coba back up data pada sub 3.2		3 5		
b.1	**Status Successful** Melakukan pengecekan kesesuaian data yang berhasil ter-back up		4		
b.2	Memastikan tidak ada data yang corrupt				
b.3	Membuat laporan pada formulir uji coba log back up data				FM-07 Formulir Log Backup Data

Gambar 6.14. Penambahan proses uji coba back up

6.6.2 Hasil Validasi

Validasi SOP dilakukan dengan mensimulasikan beberapa aktivitas operasional yang benar-benar terjadi. Validasi yang dilakukan tidak mencakup semua perosedur karena keterbatasan sumber daya pendukung dan kondisi dalam Bagian TIK STIE Perbanas. Berikut adalah pemetaan antara masing-masing prosedur dan skenario simulasinya yang dijelaskan dalam Tabel 6.10.

Tabel 6. 12. Skenarioisasi Simulasi SOP

No	SOP	Skenario	Tanggal	Keterangan
1	SOP Manajemen Password	Kasie TIK meminta programmer untuk menambahkan fitur *strong password* pada sistem informasi kepegawaian dan salah satu mahasiswa yaitu Bagus Prasojo melakukan permiintaan pergantian *password*	4 Januari 2016	Dilakukan dengan baik
2	SOP Pengelolaan dan Pencegahan Malware	Mengkaji log sistem pada anti virus yang digunakan oleh STIE	4 Januari 2016	Dilakukan secara terbatas yaitu hanya sebatas mengkaji *log* sistem pada E-scan, tidak

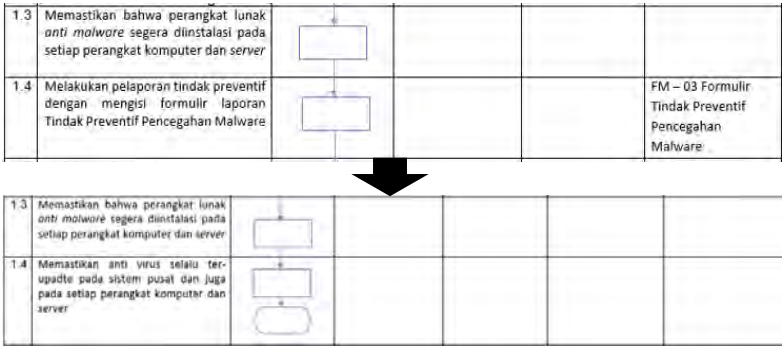
		Perbanas yaitu E-Scan		sampai melakukan simulasi gangguan malware dan simulasi penanganan gangguan malware dikarenakan keterbatasan media untuk melakukan uji coba
3	SOP Pengelolaan Gangguan Sistem Informasi	Mengkaji hasil pemindaian sistem informasi Kepegawaian yang telah dilakukan oleh pegawai bagian TIK dengan menggunakn *tools* Accunetix	4 Januari 2016	Dilakukan secara terbatas yaitu hanya sebatas mengkaji hasil pemindaian yang dilakukan oleh pegawai bagian TIK, tidak sampai proses kajian evaluasi sistem dikarenakan keterbatas waktu
4	SOP Bacup	Pegawai Bagian TIK melakukan uji coba back up dan restore data mahasiswa	4 Januari 2016	Dilakukan dengan baik
5	SOP Proteksi Ruang Server	Pegawai Bagian TIK melakukan pengecekan proteksi server pada ruang server	4 Januari 2016	Dilakukan dengan baik
6	SOP Akses Ruang	Mahasiswa ITS	4 Januari	Dilakukan dengan baik

	Server	mengakses ruang server dengan tujuan penelitian	2016	

Berdasarkan hasil dari pross validasi yang telah dilakukan dan terdokumentasi secara detail pada Lampiran G, maka dibutuhkan beberapa revisi pada dokumen SOP Keamanan Data yaitu sebagai berikut :

1. **Perubahan Aktivtas pada SOP Pengelolahan dan Pencegahan Malware**

   Sebelum perubahan, SOP Pengelolahan dan Pencegahan Malware memiliki formulir Tindak Preventif Pencegahan Malware yang nantinya akan berisikan *checklist* tindakan yang telah dilakukan untuk pencegahan malware. Namun setelah melakukan validasi dengan Pegawai Bagian TIK, proses pencegehan malware telah dilakukan secara otomatis pada sistem dan telah dapat dikontrol melalui log sistem, seperti pada anti virus E-Scan setiap harinya *update* sistem dilakukan terpusat dan Pegawai Bagian TIK yang bertanggung jawab dapat langsung memastikan *update* anti virus pada log sistem E-Scan. Sehingga formulir Tindak Preventif Pencegahan Malware dihapuskan karena tidak sesuai dengan kebutuhan dan kondisi pada STIE Perbanas. Berikut perubahan aktivitas pada SOP Pencegahan Malware.



Gambar 6.13. Perubahan Aktivitas pada SOP Pengelolaan dan Pencegahan Malware

Berdasarkan hasil perubahan aktivitas tersebut, maka dibutuhkan perubahan pada formulir pendukung SOP Pengelolaan dan Pencegahan Malware. Berikut ini adalah formulir Tindak Preventif Pencegahan Malware, dimana formulir tersebut tidak dibutuhkan dikarenakan tindak preventif dalam pencegahan malware telah terdokumentasi dalam sistem dengan baik.

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-03	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR TINDAK PREVENTIF PENCEGAHAN MALWARE	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Laporan Tindak Preventif Pencegahan Malware
Bulan ..... s.d .....Tahun .....

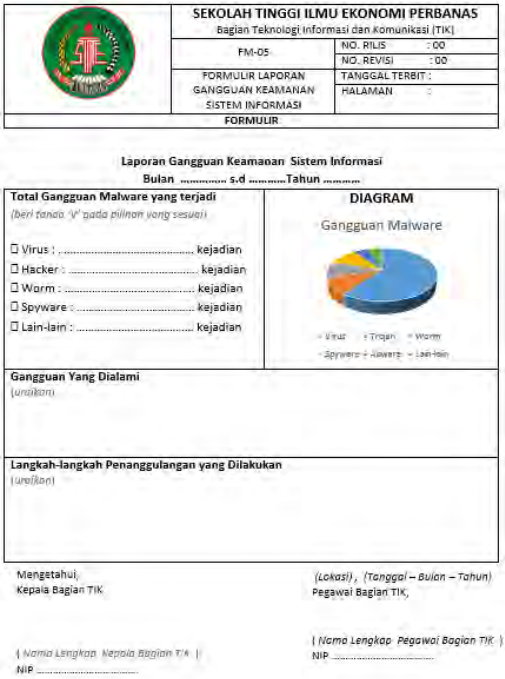
Tindakan Preventif yang berhasil dilakukan *(beri tanda 'V' pada pilihan yang sesuai)*	Keterangan : *(diisi keterangan pendukung tindakan preventif pencegahan malware yang dilakukan)*
☐ Upgrade dan patch sistem operasi dan aplikasi **Perangkat Lunak Anti Malware** ☐ *Updated* Anti virus ☐ Anti *Spyware* ☐ *Spam Filtering* ☐ *Web Content filtering* **Instalasi Perangkat Lunak Anti Malware** ☐ Pada perangkat Komputer ☐ Pada Server	
	(Lokasi) , (Tanggal – Bulan – Tahun) Pegawai Bagian TIK, *(Nama Lengkap Pegawai Bagian TIK)* NIP .....

Gambar 6.14. Formulir Tindak Preventif Pencegahan Malware

2. Perubahan formulir pada SOP Pengelolahan Gangguan Sistem Informasi

Sebelum perubahan, SOP Pengelolahan Gangguan Sistem Informasi memiliki formulir Pengelolaan Gangguan Sistem Informasi. Dimana formulir berfungsi sebagai pelaporan untuk mengetahui gangguan/insiden terkait

keamanan data yang terjadi selama kurun waktu tiga bulan. Formulir tersebut bertujuan untuk menjadi evaluasi bagi Bagian TIK terkait keefektifan tindak preventif yang telah dilakukan, dimana seharusnya efektifitas dan ketepatan tindak preventif dapat dilihat dari berkurangnya gangguan/insiden yang terjadi atau berulang. Berikut ini adalah formulir Pengelolaan Gangguan Sistem Informasi sebelum dilakukan perubahan.



	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-05	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LAPORAN GANGGUAN KEAMANAN SISTEM INFORMASI	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

Laporan Gangguan Keamanan Sistem Informasi
Bulan ..... s.d .....Tahun .....

Total Gangguan Malware yang terjadi
(beri tanda 'V' pada pilihan yang sesuai)

- ☐ Virus : ..... kejadian
- ☐ Hacker : ..... kejadian
- ☐ Worm : ..... kejadian
- ☐ Spyware : ..... kejadian
- ☐ Lain-lain : ..... Kejadian

DIAGRAM

Gangguan Malware

Gangguan Yang Dialami
(uraikan)

Langkah-langkah Penanggulangan yang Dilakukan
(uraikan)

Mengetahui,
Kepala Bagian TIK

(Nama Lengkap Kepala Bagian TIK)
NIP .....

(Lokasi), (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)
NIP .....

Gambar 6.17. Formulir Pengelolaan Gangguan Sistem Informasi

Setelah dilakukan pengujian terhadap SOP Pengelolaan Gangguan Sistem Informasi, ditemukan kekurangan dalam formulir. Ketika Pegawai Bagian TIK melakukan pengisian jumlah kejadi dari setiap gangguan, tidak terdapat *log* terjadinya gangguan dan

beberapa gangguan seperti gangguan akibat kesalahan manusia (*human error*) tidak dapat tercakup dalam pelaporan gangguan system informasi. Sehingga penulis mengusulkan perubahan dalam formulir tersebut dengan menambahkan table log untuk gangguan keamanan informasi secara umum. Berikut ini adalah formulir laporan gangguan keamanan informasi setelah dilakukan perubahan.

SEKOLAH TINGGI ILMU EKONOMI PERBANAS

Bagian Teknologi Informasi dan Komunikasi (TIK)

	FM-04	NO. REVISI 00
	FORMULIR LAPORAN GANGGUAN KEAMANAN INFORMASI	TANGGAL TERBIT
		HALAMAN

FORMULIR

Gangguan Keamanan Sistem Informasi

Bulan ..... Tahun .....

No	Tanggal	Gangguan Kemanan Yang Terjadi	Tindakan Penyelesaian	Tanggal Penyelesaian		Status Gangguan	Staf yang Menangani
				Mulai	Selesai		
1	(1)	(2)	(3)	(4)	(5)		
(dst)							

Gambar 6.18. Perubahan Formulir Gangguan Keamanan Sistem informasi

Tabel diatas berguna untuk mendokumentasikan seluruh gangguan keamanan informasi dan tidak terbatas hanya pada gangguan pada sistem informasi. Sehingga pada formulir laporan gangguan keamanan informasi juga ditambahkan beberapa kategori yang meimiliki tingkat kemungkinan terjadi yang tinggi yaitu *netcard* (pemutusan jaringan wifi) dan *human error*. Berikut ini adalah perubahan pada formulir laporan gangguan keamanan informasi.

Laporan Gangguan Keamanan Informasi
Bulan ..... s.d .....Tahun .....

Total Gangguan Keamanan Informasi yang terjadi *(beri tanda 'V' pada pilihan yang sesuai)*

☐ Virus	.....	Kejadian
☐ Netcard	.....	Kejadian
☐ Hacker	.....	Kejadian
☐ human Error	.....	Kejadian
☐ Lain-lain	.....	Kejadian

DIAGRAM

Gangguan Malware

Virus, Trojan, Worm, Spyware, Adware, Lain-lain

Gangguan Yang Dialami
(uraikan per poin)

Langkah-langkah Penanggulangan yang Dilakukan
(uraikan per poin)

Mengetahui,
Kasie TIK

(Nama Lengkap Kepala Bagian TIK)
NIP .....

(Lokasi), (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)
NIP .....

Gambar 6.19. Perubahan Formulir Gangguan Keamanan Informasi

Halaman ini sengaja dikosongkan

BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

7.1 Kesimpulan

Kesimpulan yang dibuat adalah jawaban dari perumusan masalah yang telah didefinisikan sebelumnya dan berdasarkan hasil penelitian yang telah dilakukan. Kesimpulan yang didapat dari tahap analisis hingga perancangan dan validasi dokumen produk adalah :

1. **Analisis risiko kemanan data STIE Perbanas berdasarkan tahap penilaian risiko pada kerangka kerja ISO 27002:2013**

   Analisis risiko dilakukan dengan menggunakan metode FMEA dan menganalisis ancaman serta kerentanan dari aset informasi yaitu perangkat lunak (*software*), perangkat keras (*hardware*), data, jaringan dan sumber daya manusia (*people*). Berdasarkan hasil evaluasi penilaian risiko, dapat diketahui bahwa STIE Perbanas memiliki beberapa kemungkinan risiko yang tinggi yang dapat timbul terkait keamanan data yaitu risiko manipulasi data dengan nilai RPN 200, risiko pencurian data dengan nilai RPN 140, risiko kehilangan data dengan nilai RPN 160 dan risiko data yang tidak valid dengan nilai RPN 108. Risiko tersebut muncul dikarenakan oleh berbagai penyebab seperti serangan *hacker, virus, human error* dan kurangnya kontrol keamanan fisik. Dari hasil evaluasi risiko tersebut, selanjutnya dilakukan analisis kebutuhan mitigasi risiko yang berupa sebuah pengimplementasian kontrol kebijakan, praktek dan prosedur. Berikut merupakan hasil analisis risiko terkait keamanan data berdasarkan prioritas nilai RPN tertinggi.

Tabel 7. 1. Hasil Priotitas Risiko Tertinggi terkait Kemanan Data

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Level Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Nilai RPN
Data	Data demografi mahasiswa, Data akademik dan Data file server	R13	Very High	Manipulasi data	Username dan password diketahui oleh pengguna lain	200
		R13	High	Manipulasi data	Terdapat hacker yang memanipulasi data	160
		R12	High	Pencurian data	Terdapat hacker yang mencuri data	140
		R15	Medium	Data Hilang	Server rusak	96
Hardware	Server	R5	Medium	Data Hilang	Virus	112
		R5	Medium	Data Hilang	Kesalahan DBA	84
		R4	Medium	Pencurian data	Ruang server kurang diberi pengamanan	100
		R4	Medium	Pencurian data	Kesalahan konfigurasi server	100
Sumber Daya Manusia	Pegawai TI	R20	Medium	Data yang ada tidak valid	Kesalahan dalam input data	108

2. **Hasil pembuatan *Standard Operating Procedure* (SOP) Keamanan Data berdasarkan hasil analisis Risiko dan mengacu pada kerangka kerja Cobit 5 dan ISO 27002:2013**

   Berdasarkan hasil analisis risiko dan rekomendasi mitigasi risiko, didapatkan usulan pembuatan 6 prosedur yaitu 1) SOP Manajemen Password 2) SOP Pengelolaan dan Pencegahan Malware 3) SOP Pengelolaan Gangguan Sistem Informasi 4) SOP Back up dan Restore 5) SOP Proteksi Lingkungan Sever 6) SOP Akses Ruang Server.

   Selain 6 prosedur tersebut, dihasilkan juga beberapa instrument pendukung dokumen SOP berupa instruksi dan formulir untuk melengkapi dokumen SOP tersebut. Instrument yang dihasilkan adalah 3 instruksi kerja yaitu 1) Instruksi Kerja Pemindaian Sistem Informasi 2) Instruksi Kerja Backup dan 3) Instruksi Kerja Restore, sedangkan formulir yang dihasilkan yaitu 10 formulir yang terdiri dari 1) Formulir Perbaikan Sistem Informasi 2) Formulir Permintaan Pergantian Password 3) Formulir Evaluasi Sistem informasi 4) Formulir Laporan Gangguan Keamanan Informasi 5) Formulir Klasifikasi Data 6) Formulir Log Backup Data 7) Formulir Restore Data 8) Formulir Pemeliharaan server 9) Formulir Log Pegawai 10) Formulir Log Daftar Pengunjung. Keseluruhan isi dokumen SOP dibukukan secara terpisah dari buku tugas akhir ini dan menjadi sebuah dokumen produk berjudul **Standard Operating Procedure (SOP) Keamanan Data STIE Perbanas**.

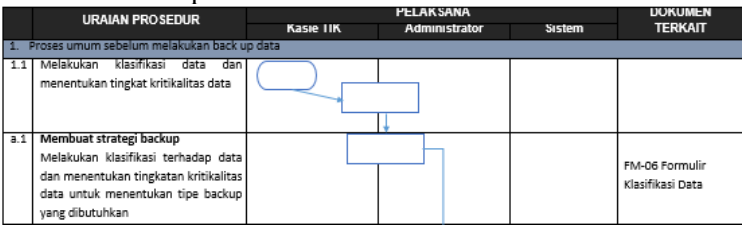
3. **Hasil Pengujian dokumen SOP**

   Pengujian dokumen SOP dilakukan dengan melakukan verifikasi dan simulasi untuk memvalidasi ketepatan dokumen. Hasil dari kedua pengujian SOP tersebut menunjukan bahwa ada beberapa bagian dari dokumen

yang perlu diperbaiki dan disesuaikan dengan kondisi STIE perbanas.

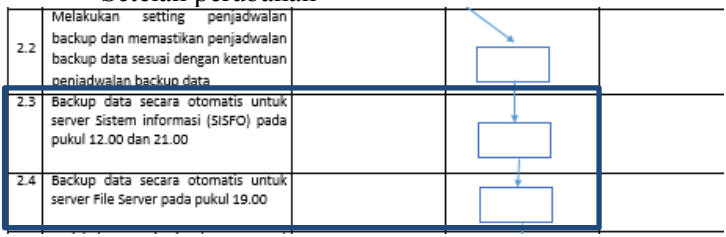
Verifikasi tersebut menghasilkan beberapa perubahan dokumen yang antara lain :

1. **Perubahan Pelaksana dalam Prosedur Backup**
   Peubahan pelaksana dalam prosedur Backup yaitu melibatkan pihak Kasie TIK dan administrator aplikasi/programmer.
   - Setelah perubahan



Gambar 7.1. Pelaksana prosedur Back up setelah perubahan

2. **Perubahan Penjadwalan Back Up Data**
   Perubahan waktu penjadwalan back up yang lebih sesuai dengan kondisi kekinian yang ada pada STIE Perbanas.
   - Setelah perubahan



Gambar 7.2. Proses Back up setelah perubahan

Dan pada proses pengujian validasi terdapat perubahan dokumen yang antara lain :

3. Perubahan formulir pada SOP Pengelolahan Gangguan Sistem Informasi

SOP Pengelolahan Gangguan Sistem Informasi memiliki formulir Pengelolaan Gangguan Sistem Informasi. Namun, ketika Pegawai Bagian TIK melakukan pengisian jumlah kejadi dari setiap gangguan, tidak terdapat *log* terjadinya gangguan dan beberapa gangguan seperti gangguan akibat kesalahan manusia (*human error*) tidak dapat tercakup dalam pelaporan gangguan system informasi. Sehingga penulis mengusulkan perubahan dalam formulir tersebut dengan menambahkan table log untuk gangguan keamanan informasi secara umum. Berikut ini adalah formulir laporan gangguan keamanan informasi setelah dilakukan perubahan.

SEKOLAH TINGGI ILMU EKONOMI PERBANAS
Bagian Teknologi informasi dan komunikasi (TIK)

FM-04	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR LAPORAN GANGGUAN KEAMANAN INFORMASI	TANGGAL TERBIT	:
	HALAMAN	
FORMULIR		

Gangguan Keamanan Sistem Informasi
Bulan ..... Tahun .....

No	Tanggal	Gangguan Kemanan Yang terjadi	Tindakan Penyelesaian	Tanggal Penyelesaian		Status Gangguan	Staf yang Menangani
				Mulai	Selesai		
1	(1)	(2)	(3)	(4)	(5)		
(dst)							

Gambar 7.3. Formulir Laporan Gangguan Keamanan Informasi setelah perubahhan

Gambar 7.4. Formulir Laporan Gangguan Keamanan Informasi setelah perubahhan

Pada dasarnya pengelolaan untuk keamanan data pada STIE Perbanas telah dilakukan, namun pelaksanaanya hanya bersifat umum seperti melakukan perbaikan pada celah kelemahan. Kurangnya pendokumentasian proses yang terjadi mengakibatkan perbaikan yang dilakukan tidak dapat ditinjau lebih lanjut sehingga efektifitas dari tindak preventif dan korektif yang dilakukan tidak dapat dievaluasi dengan baik. Dengan dibuatnya dokumen SOP

Keamanan Data ini diharapkan beberapa risiko yang dapat mengakibatkan hilangnya kerahasiaan (*confidential*), keutuhan (*integrity*) dan ketersediaan (*availability*) data dapat diminimalisir kemungkinan terjadinya.

7.2 Saran

Saran yang dapat peneliti sampaikan terkait dengan pengerjaan tugas akhir ini meliputi dua hal, yaitu saran untuk pihak manajemen STIE Perbanas dan saran untuk penelitian selanjutnya.

Saran yang dapat diberikan untuk pihak manajemen STIE Perbanas adalah :

1. Penulis menyarankan agar dokumen SOP yang telah diuji bisa benar-benar diterapkan dengan baik. Hal pertama yang dapat dilakukan oleh pihak STIE Perbanas adalah melakukan rencana penerapan dan melakukan sosialisasi pada seluruh pihak yang terkait pada seluruh pelaksanan SOP.
2. Usulan instruksi kerja pemindaian sistem informasi dapat diimplememtasikan dengan baik oleh pegawai bagian TIK khususnya administrator aplikasi untuk menemukan celah dan kelemahan sistem informasi secara berkala sehingga dapat meminimalisir serangan *hacker* dan hilangnya kerahasiaan, integritas dan ketersediaan data.
3. Usulan formulir log book pegawai dan pengunjung untuk akses ruang server dapat diimplementasikan dengan baik untuk mengelola limitasi hak akses masuk pada ruang server.
4. Usulan formulir pemeliharaan server juga dapat diimplementasikan dengan baik untuk secara berkala memastikan proteksi langsung pada server sehingga risiko kehilangan data akibat kurangnya kontrol keamanan dalam server dapat diminimalisir.

Saran yang dapat penulis berikan untuk penelitian selanjutnya adalah :

1. Penelitian ini sebatas pembuatan dokumen SOP hingga proses pengujian tanpa memantau pengimplementasian SOP tersebut dan pengaruhnya bagi proses bisnis organisasi. Untuk penelitian selanjutnya, dapat dilakukan pengujian dan evaluasi keefektifan dokumen SOP ini terhadap peningkatan keamanan data pada STIE Perbanas.
2. Penelitian ini hanya mengacu pada beberapa kontrol dalam kerangka kerja Cobit 5 dan ISO27002:2013 dan tidak secara keseluruhan memenuhi salah satu domain atau klausul pada kerangka kerja tesebut, karena pada dasarnya penelitian ini didasarkan pada hasil penilaian risiko untuk melakukan mitigasi pada risiko dengan tingkat prioritas tertinggi. Sehingga dalam penelitian selanjutnya dianjurkan untuk melengkapi objektif pada salah satu domain atau klausul pada kerangka kerja sehingga kontrol dalam penyusunan SOP lebih menyeluruh dan patuh.

LAMPIRAN A
HASIL WAWANCARA DENGAN PEMBANTU KETUA BIDANG AKADEMIK STIE PERBANAS

Berikut ini adalah lampiran dokumen dari penelitian ini.

I. Informasi Interview -1

- Nama Narasumber : Dr. Drs. Emanuel Kritijadi, MM
- Jabatan : Pembantu ketua Bidang Akademik
- Jenis Kelamin : L
- Tanggan dan Waktu : 4 Nopember 2015

A. Informasi Narasumber

1. Apakah peran dan tanggung jawab anda sebagai Pembantu Ketua Bidang Akademik?
   Mengelola pelaksanaan rencana strategis bidang pendidikan dan pengajaran serta menyusun dan mengusulkan kepada ketua STIE Perbanas mengenai sistem dan peraturan/ketentuan bidang akademik, pengembangan metode dan evaluasi pengajaran, sistem penjaminan kualitas pendidikan, pembinaan dan pengembangan jurusan dan program diploma, pengelolaan data untuk kepentingan akreditasi dan laporan bidang akademik.

2. Apa sajakah aktivitas utama dalam proses bisnis Perbanas?
   Secara keseluruhan aktvitas utama terdiri dari proses utama yaitu penerimaan mahasiswa → kegiatan harmoni → FRS → Perkuliahan → UTS → UAS → (*magang untuk D3*) →Tugas Akhir → Yudisium → Wisuda

B. Pertanyaan mengenai Keamanan Data

Tabel A. 1. Hasil wawancara terkait keamanan data

Pertanyaan Identifikasi	Jawaban Narasumber
1. Menurut anda, apa sajakah data yang kritikal dan sensitive dalam operasional di STIE Perbanas?	Yang paling kritikal ada dua yaitu data demografi dan data akademik. Data demografi adalah data data seperti data mahasiswa termasuk data seperti nama, alamat, riwayat pendidikan, presetasi dan lainnya sedangkan data akademik yaitu data nilai perkuliahan, IPK dan lainnya
2. Siapa saja yang memiliki hak akses terhadap data kritikal dan sensitive yang disebutkan diatas?	Mahasiswa memiliki akses terhadap masing masing data demografinya namun hanya pada batas dapat melihat dan tidak dapat melakukan perubahan terhadap data tersebut. Hal itu dikarenakan sesuai dengan kebijakan bahwa mahsiswa dibatasi atas perubahan data agar data yang di inputkan sejak mahasiswa diterima hingga kelulusan tetap sama, dan apabila mahasiswa akan melakukan perubahan maka harus melalui prosedur terlebih dahulu. Sedangkan

Pertanyaan Identifikasi	Jawaban Narasumber
	untuk data akademik seperti nilai setiap dosen akan menginputkan nilai pada batas waktu yang ditentukan dan jika lewat dari batas waktu tersebut maka dosen dapat melakukan perubahan dengan melalui prosedur terlebih dahulu dan atas sepengatahun bidang akademik. Mahasiswa dapat melihat nilainya melalui sistem informasi akademik mahasiswa dengan terlebih dahulu melakukan login dengan username dan password.
3. Apa saja praktek pengamanan data yang telah dilakukan oleh STIE Perbanas terhadap data kritikal dan sensitive yang disebutkan diatas?	Seperti penggunaan username dan password untuk setiap akses pada sistem informasi akademik, kemudian adanya batasan bahwa mahasiswa tidak dapat melakukan perubahan data sendiri namun harus terlebih dahulu lewat admin dan prosedur yang ada.
4. Apa saja ancaman yang pernah terjadi terhadap data kritikal dan sensitif yang disebutkan diatas?	Sebelum ada kebijakan mahasiswa tidak dapat melakukan perubahan data ada beberapa permasahalan seperti data mahasiswa dengan data kelulusan tidak sesuai namun kini telah ada kebijakannya. Selain itu, permasalahan yang lainnya terkadang nilai yang diinputkan dapat berubah namun kasusnya tidak banyak, hanya saja hal tersebut mengganggu, karena tentunya kepercayaan akan data nilai yang lainnya akan diragukan, apakah nilai yang lain telah benar seperti itu.

C. Pengelolaan Aset (Asset Management)

1. Apakah STIE Perbanas telah memilki prosedur pengelolaan data?
Untuk saat ini, prosedur yang dimiliki belum spesifik mengenai pengelolaan datanya

Aspek Kerahasiaan (*confidentiality*)

Tabel A. 2. Hasil wawancara terkait aset pada aspek kerahasiaan (confidentiality)

Pertanyaan Identifikasi	Jawaban Narasumber
1. Apakah STIE Perbanas telah memiliki prosedur pengelolaan hak akses?	Sudah ada dengan masing masing harus login terlebih dahulu namun belum terdokumentasi
2. Bagaimana cara STIE Perbanas mengelola prosedur hak akses tersebut?	Sebenarnya belum ada prosedur khusus untuk pengelolaan hak aksesnya sendiri
3. Adakah perbedaan hak akses bagi setiap pemilik hak akses?	Sudah ada, dengan permintaan login ke setiap sistem informasi akademik
4. Bagaimana cara pengelolaan perbedaan	Pada login tersebut ada batasan batasan seperti jika mahasiswa hanya dapat melihat data tidak bisa mengubah data, sedangkan

Pertanyaan Identifikasi	Jawaban Narasumber
hak akses tersebut?	dosesn dengan login dapat menginputkan data namun hanya pada batas waktu yang ditentukan, dan apabila melewati batas waktu input datanya harus sepengetahuan bidang akademik dengan pengajuan permintaan dan lewat prosedur terlebih dahulu seperti itu

Aspek Keutuhan (*integrity*)

Tabel A. 3. Hasil wawancara terkait aset pada aspek keutuhan (integrity)

Pertanyaan Identifikasi	Jawaban Narasumber
1. Apakah STIE Perbanas telah memiliki prosedur bagi setiap pemilik hak akses dalam melakukan modifikasi atau pembaharuan data?	Belum ada prosedur khusus mengenai modifikasi atau pembaharuan data, hanya saja ada sebuah prosedur yaitu audit trail yang tujuannya untuk melakukan pelacakan data apabila ada ketidaksesuaian data antara proses di sisfor (sistem informasi akademik dan lainnya) dengan proses manual
2. Seperti apa kontrol akses untuk modifikasi data yang sudah berjalan selama ini?	Hal ini mungkin langsung dapat ditanyakan pada bagian TIK
3. Apa saja cara yang telah ditempuh dalam mengelola	Dengan pembatasan pembatasan seperti tadi, sehingga dosen hanya dapat menginputkan nilai pada waktu antara setelah

Pertanyaan Identifikasi	Jawaban Narasumber
proses modifikasi ataupun pembaharuan data? (seperti : selama proses input data ada kontrol akses yang membatasi, selama pemrosesan data bagaimana?)	UTS yaitu batas waktunya 3 minggu dan setelah UAS batas waktunya 2 minggu dan jika akan melakukan perubahan nilai harus melalui pengajuan langsung ke bagian akademik
4. Kebutuhan keamanan seperti apa saja yang telah diimplementasikan untuk memastikan modifikasi dan pembaharuan data tetap dapat terjaga akurasi dan kebenarannya?	Yang paling penting bagi bidang akademik yaitu mengenai batasan atau limitasi untuk modifikasi datanya agar data tetap konsisten sehingga tidak muncul masalah ketidaksesuaian data

Aspek Ketersediaan (*availability*)

Tabel A. 4. Hasil wawancara terkait aset pada aspek ketersediaan (availability)

Pertanyaan Identifikasi	Jawaban Narasumber
1. Apakah STIE Perbanas telah memiliki prosedur dalam pencegahan (*preventing*)	Sebenarnya belum ada prosedur khusus yang terdokumentasi mengenai bagaimana sebaiknya pengelolaan pada software maupun hardware seperti server seperti itut, namun pada

Pertanyaan Identifikasi	Jawaban Narasumber
terhadap kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	ruangan server sendiri kondisinya sudah ada penataan kabel, sudah ada detektor asap dan hal hal lain yang pada umumnya ada untuk pengamanan
2. Langkah pencegahan (*preventing*) seperti apa yang sudah dilakukan untuk menjaga ketersediaan data setiap saat?	Selain menjaga lokasi server, sudah dilakukan sebenarnya proses seperti *backup* data dan proses *restore* data yang dilakukan secara berkala namun untuk teknisnya bagian TIK yang lebih mengetahui
3. Apakah STIE Perbanas telah memiliki prosedur dalam pemulihan (*recovery*) terhadap kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	Untuk *recovery* sendiri sudah ada proses *restore* seperti saat terjadi kebakaran beberapa minggu yang lalu, sebenarnya data akademik berhasil di restore dalam waktu kurang lebih 3 hari namun ada pula kehilangan data khususnya pada data diktat ajar dosen karena tidak berhasil *restore* pada data yang ada di e-learning
4. Langkah pemulihan (*recovery*) seperti apa yang sudah dilakukan untuk menjaga ketersediaan data setiap saat?	Khusus untuk server sudah ada penangkal petir, kemudian peletakan lokasi server sudah mengikuti pengamanan pada umumnya dengan adanya pemantauan suhu ruangan, detektor dan lainnya dan sarana gedung sudah mulai diperbaiki

D. Identifikasi Ancaman serta kebutuhan Keamanan

Tabel A. 5. Hasil wawancara terkait ancaman dan kebutuhan keamanan

Pertanyaan Identifikasi	Jawaban Narasumber
1. Seberapa sering masing masing ancaman (yang disebutkan sebelumnya) tersebut terjadi?	Untuk nilai akademik yang berubah sebenarnya setiap semester terjadi hanya kasusnya tidak banyak, namun hal tersebut sangat mengganggu karena mengakibatkan nilai lainnya tidak dapat dipastikan kebenarannya sehingga perlu dilakukan pengecekan dan memakan waktu
2. Apakah dampak dari masing masing ancaman (yang disebutkan sebelumnya) tersebut terhadap berjalannya proses bisnis?	Dampaknya mungkin tidak secara langsung mengganggu proses bisnis hanya saja seperti permaslaahan perubahan nilai akademik tersebut akan mengakibatkan data lain menjadi tidak dapat dipercaya namun secara keseluruhan tidak pernah ada dampak sampai kehilangan data
3. Apakah telah ada prosedur keamanan yang diterapkan untuk mengatasi dampak ancaman (yang disebutkan	Secara dokumentasi belum ada namun sebenarnya sudah dilakukan praktek pengamanannya seperti tadi batasan perubahan nilai oleh dosen, batasan mahasiswa tidak dapat merubah data kemudian ada proses backup dan proses restore

Pertanyaan Identifikasi	Jawaban Narasumber
sebelumnya) tersebut? Seperti apa?	namun
4. Kebutuhan keamanan seperti apa yang dibutuhkan berdasarkan masing masing ancaman (yang disebutkan sebelumnya)?	Mungkin jika kebutuhan keamanan secara teknis bagian TIK yang akan lebih memahami namun dari sudut pandang saya mungkin dibutuhkan standard untuk keamanannya dan kini memang Perbanas sedang mengembangkan blue print TIK untuk memastikan pengelolaan TIK nya

Halaman ini sengaja dikosongkan

LAMPIRAN B
HASIL WAWANCARA DENGAN KASIE TIK STIE PERBANAS

II. Informasi Interview -2

- Nama Narasumber : Hariadi Yutanto, S.Kom, M.Kom
- Jabatan : Kasie TIK (Manajemen Jaringan dan Technical Support)
- Jenis Kelamin : L
- Tanggan dan Waktu : 22 Oktober 2015

A. Informasi Narasumber

1. Apakah peran dan tanggung jawab anda sebagai Kasie TIK?
   Mengelola perangkat keras, perangkat lunak, dan jaringan secara terintegrasi, sebagai *system administrator*, melakukan instalasi perangkat keras komputer dan jaringan di seluruh unti kerja, sebagai *network administrator*, mengelola database server, mengendalikan dan mengkoordinasikan tugas *technical support* terhadap *hardware* dan perangkal lunak *operating system*
2. Apa sajakah aktivitas utama dalam bagian TIK di Perbanas?
   Mengelola layanan TI untuk mahasiswa dan staf yang terdiri dari Simas (sistem informasi akademik mahasiswa) dan sistem informasi staf, e-learning yang berisi materi perkuliahan, e-mail, hostpot dan login file server, dan selain itu mengelola seluruh aset TIK (hardware,

software, jaringan). Dan layanan TI yang khusus diberikan untuk mahasiswa adalah email, hostpot dan file server.

3. Bagaimana proses umum penerapan TI pada Bagian TIK di STIE Perbanas?
   Proses yang berjalan diawali dengan pendaftaran mahasiswa baru dengan menggunakan sistem SPMB online. Kemudian data mahasiswa tersebut akan disimpan di bagian kemahasiswaan. Lalu, terdapat sistem SIMAS yang terdiri sistem informasi akademik, kemahasiswaa, keuangan, kepegawaian, kesekretariatan dan lainnya. Dimana dengan simas kemahasiswaan mahasiswa dan dosen dapat melakukan proses KRS, memasukan nilai (untuk dosen) dan melihat nilai (untuk mahasiswa), dan berbagai aktivitas akademik lainnya. Kemudian, dalam sistem e learning mahasiswa dapat mengambil materi perkuliahan dan memudahkan dosen untuk proses mengajar. Selain itu, terdapat juga sistem perpustakaan untuk dapat mengakses penelitian dan tugas akhir mahasiswa.

B. Pertanyaan mengenai Keamanan Data

Tabel B. 1. Hasil wawancara terkait keamanan data

Pertanyaan Identifikasi	Jawaban Narasumber
1. Menurut anda, apa sajakah data yang kritikal dan sensitive dalam	Seluruh data yang ada di Sistem informasi seperti Simas dan sistem informasi staf serta seluruh data yang ada pada file server karena data ini untuk masing masing unit kerja dan data yang ada

Pertanyaan Identifikasi	Jawaban Narasumber
operasional di STIE Perbanas?	di elearning karena isinya tentang materi ajar dosen.
2. Siapa saja yang memiliki hak akses terhadap data kritikal dan sensitive yang disebutkan diatas?	Setiap civitas memiliki hak akses terhadap data tersebut, namun dibatasi dari sistem loginnya. Sehingga data yang dapat diakses disesuaikan dengan *role* nya masing masing.
3. Dimana saja data kritikal dan sensitive yang disebutkan diatas disimpan?	Untuk server krittis yaitu server untuk SIMAS, kepegawaian dan perpustakaan disimpan dalam ruangan satu ruangan server sendiri. Dan untuk database nya menggunakan postgree. Dan servernya vmware.
4. Apa saja praktek pengamanan data yang telah dilakukan oleh STIE Perbanas terhadap data kritikal dan sensitive yang disebutkan diatas?	Usaha yang telah dilakukan oleh organisasi untuk pengamanan antara lain memasang firewall untuk keamanan sistem.. Khusus untuk akses langsung pada database yaitu untuk melakukan mengakses langsung dan modifikasi database hanya dapat dilakukan oleh satu orang administrator. Lalu, juga telah dilakukan back up data penting setiap harinya di waktu tertentu. Dan juga organisasi telah berusaha melakukan sosialisasi keamanan kepada mahasiswa.
5. Apa saja ancaman yang pernah terjadi terhadap data kritikal dan sensitif	Kerusakan pada server dan juga hardware dapat menjadi ancaman terhadap hilangnya data. Selain itu, pernah terjadi kasus mahasiswa mencoba mengambil soal melalui sebuah aplikasi,

Pertanyaan Identifikasi	Jawaban Narasumber
yang disebutkan diatas?	kasus tersebut terjadi satu kali. Kemudian ancaman lain yang tidak luput seperti virus, adanya *breach* tentu saja, adanya data *saved password* yang dicuri.
6. Apa saja kebutuhan pengamanan untuk masing masing data kritikal dan sensitive yang disebutkan diatas?	Tentu saja memasang firewall dan antivirus untuk keamanan sistem. Juga diperlukan penerapan beberapa peraturan untuk menjaga keamanan dari aset TI. Selain itu, juga sudah dibuatkan sebuah *file directory*. Dan Karena pada umumnya selain permasalahan pada sistem, hardware maupun software, terkadang kurangnya *awareness* dari individu masing masing juga menjadi permasalahan dalam keamanan informasi.

C. Pengelolaan Aset (Asset Management)

1. Apakah STIE Perbanas telah memilki prosedur pengelolaan data?

Untuk saat ini, prosedur yang dimiliki belum spesifik mengenai pengelolaan datanya.

Aspek Kerahasiaan (*confidentiality*)

Tabel B. 2. Hasil wawancara terkait aset pada aspek kerahasiaan (*confidentiality*)

Pertanyaan Identifikasi	Jawaban Narasumber
1. Apakah STIE Perbanas telah memiliki prosedur pengelolaan hak akses?	Sebenernya telah ada prosedurnya, namun tidak terdokumentasikan. Prosedur yang sudah berjalan yaitu pada sistem login dimana terdapat sistem login untuk civitas pada

Pertanyaan Identifikasi	Jawaban Narasumber
	wifi, file server dan seluruh sistem informasi yang disebutkan tadi.
2. Bagaimana cara STIE Perbanas mengelola prosedur hak akses tersebut?	Pengelolaannya lewat login, yaitu pada 1 file server yang digunakan untuk banyak unit kerja, maka aksesnya dibedakan dan dilakukan juga berulang kali *update roles* dikarenakan proses perputaran pegawai dalam unit kerja terus berubah setiap beberapa waktu, dan hal ini berlum terdapat prosedurnya.
3. Adakah perbedaan hak akses bagi setiap pemilik hak akses?	Iya sudah ada, sistem login sudah berjalan dan dalam blue print TIK yang akan dikembangkan akan dilakukan diimplementasikan SSO (*Singel Sign On*) namun masih berusaha ditinjau oleh manajemen atas.
4. Bagaimana cara pengelolaan perbedaan hak akses tersebut?	Pertama adanya portal login lewat WPA/WP, kemudian mahasiswa tida dapat akses lokal atau mengakses jaringan dosen, mahasiswa hanya akses langsung ke internet, kemudian file server mahasiswa dan dosen berbeda dari loginnya dan akses wifi juga melalui login serta melakukan terus menerus *update roles* untuk akses pengguna.

Aspek Keutuhan (*integrity*)

Tabel B. 3. Hasil wawancara terkait aset pada aspek keutuhan (*integrity*)

Pertanyaan Identifikasi	Jawaban Narasumber
1. Apakah STIE Perbanas telah memiliki prosedur bagi setiap pemilik hak akses dalam melakukan modifikasi atau pembaharuan data?	Sudah ada, namun tidak dalam bentuk prosedur tertulis. Hanya sebuah peraturan.
2. Seperti apa kontrol akses untuk modifikasi data yang sudah berjalan selama ini?	Kontrol sejauh ini melalui sistem loginnya. Dan hanya satu administrator yang dapat login kedalam database.
3. Apa saja cara yang telah ditempuh dalam mengelola proses modifikasi ataupun pembaharuan data?	Dalam sistem login tersebut. apabila mahasiswa maka tidak dapat melakukan perubahan apapun hanya melihat data, jika dosen dapat menambah data dan mengubah data. Dan juga hanya terdapat satu administrator yang dapat mengakses langsung pada database dan melakukan modifikasi data
4. Kebutuhan keamanan seperti apa saja yang telah diimplementasikan untuk memastikan modifikasi dan pembaharuan data tetap	Sebenernya kebutuhannya limitasi modifikasi data. Selain itu kebutuhan untuk sosialisasi keamanan informasi kepada mahasiswa, karena hal yang menggangu adalah mahasiswa seringkali menyebarkan password mereka ke teman terdekat saat proses KRS, sehingga menyebabkan banyaknya komplain

Pertanyaan Identifikasi	Jawaban Narasumber
dapat terjaga akurasi dan kebenarannya?	saat KRS dimana data mereka dirubah oleh teman atau bahkan dihapus selurunya, dan hal ini sulit dilacak secara sistem.

Aspek Ketersediaan (*availability*)

Tabel B. 4. Hasil wawancara terkait aset pada aspek ketersediaan (availability)

Pertanyaan Identifikasi	Jawaban Narasumber
1. Apakah STIE Perbanas telah memiliki prosedur dalam pencegahan (*preventing*) terhadap kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	Ada beberapa prosedur yang telah ada namun ada yang telah dijalankan dan ada juga yang belum. Contoh SOP yang telah dijalankan adalah mengenai SLA, jaringan LAN, Maintenance, jaringan Internet dan pembuatan Email. Salah satu SOP yang belum dijalankan adalah SOP mengenai pengelolaan komplain. Selain itu SOP mengenai penanganan bencana belum ada.
2. Langkah pencegahan (*preventing*) seperti apa yang sudah dilakukan untuk menjaga ketersediaan data setiap saat?	Organisasi melakukan backup pada database setiap hari, biasanya pada malam hari. Selain itu juga dilakukan backup server dan NAS (Network-Attached Storage). Penataan kabel sudah ada. Masing – masing kabel sudah ditata sendiri-sendiri dan masing masing kabel telah memiliki label untuk mempermudah pengaturan.

Pertanyaan Identifikasi	Jawaban Narasumber
3. Apakah STIE Perbanas telah memiliki prosedur dalam pemulihan (*recovery*) terhadap kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	Prosedur dalam bentuk SOP mungkin tidak tapi sebenarnya sudah dilakukan back up data setiap malam. Dan untuk recovery juga belum ada namun saat kemaren terjadi kebakaran recovery data dan restore data berhasil dilakukan hanya saja ada beberapa data yang tidak dapat terselematkan yaitu data e learning, untuk data simas sendiri berhasil diselamatkan seluruhnya.
4. Berapa kali organisasi melakukan *maintenance* terhadap aset teknologi informasi yang mendukung fungsional bisnis kritis organisasi?	Pada awal semester (6 bulan sekali) organisasi melakukan maintenance keseluruhan untuk setiap kelas dan lab yang kemudian akan menghasilkan laporan. Apabila ada kerusakan maka akan diserahkan kebagian Umum yang kemudian bertugas memanggil orang untuk memperbaiki atau mengganti aset. Selain itu maintenance untuk lab juga dilakukan sebelum aktivitas UAS dan UTS dan juga nantinya akan menghasilkan laporan.

D. Identifikasi Ancaman serta kebutuhan Keamanan

Tabel B. 5. Hasil wawancara terkait ancaman dan kebutuhan keamanan

Pertanyaan Identifikasi	Jawaban Narasumber
1. Seberapa sering masing masing ancaman (yang disebutkan sebelumnya) tersebut terjadi?	Untuk data KRS yang dirubah dan dihapus karena menyebarkan password hampir terjadi setiap KRS berlangsung hanya saja kasusnya tidak banyak. Selain itu ancaman lainnya terjadi namun dengan kasus yang tidak banyak.
2. Apakah dampak dari masing masing ancaman (yang disebutkan sebelumnya) tersebut terhadap berjalannya proses bisnis?	Dampak dari ancaman KRS sebenarnya mengakibatkan proses KRS terganggu namun tidak besar dampaknya. Namun dampak yang paling terasa adalah kebakaran kemaren, mungkin karena tidak adanya prosedur yang benar sehingga terjadi kebakaran tersebut.
3. Apakah telah ada prosedur keamanan yang diterapkan untuk mengatasi dampak ancaman (yang disebutkan sebelumnya) tersebut? Seperti apa?	Organisasi belum menerapkan standard keamanan tertentu hanya ada beberapa prosedur yang dibuat mengenai pengelolaan SI/TI.
4. Kebutuhan keamanan seperti apa yang dibutuhkan	Organisasi telah memasang firewall dan antivirus untuk keamanan sistem. Selain itu untuk keamanan Wifi juga telah

Pertanyaan Identifikasi	Jawaban Narasumber
berdasarkan masing masing ancaman (yang disebutkan sebelumnya)?	dipasang *anti-netcut*. Organisasi juga telah menerapkan beberapa peraturan untuk menjaga keamanan dari aset TI. Selain itu organisasi juga berencana akan membuat DRP untuk keamanan saat terjadi bencana. Selain itu, karena kelemahan teknis yang dimiliki oleh organisasi antara lain adalah firewall yang digunakan hanya microtix, belum ada mirroring untuk database selain itu mahasiswa juga belum bisa reset password sendiri harus manual melalui admin TI, maka akan dibutuhkan sistem SSO tadi.

LAMPIRAN C
HASIL PENILAIAN RISIKO (*RISK REGISTER*)

Tabel C. 1. Hasil Penilaian Risiko

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
Hardware	Kerusakan pada Server	Proses bisnis terhambat	8	Seluruh sistem seperti SIMAS, kepegawaian dan perpustakaan berada pada 1 fisik server sehingga apabila server mengalami kerusakan dampaknya akan menghambat proses bisnis hingga penurunan citra organisasi. Selain itu, secara finansial kerusakan server membutuhkan biaya pengadaan yang tinggi	Gempa bumi	3	Kemungkinan terjadi kecil	Letak lokasi ruang server di lantai 2	5	Kontrol yang dilakukan sudah mampu mengamankan aset server namun keefektifannya masih rata-rata	**120**	High	Bagian Umum
					Badai dan Petir	5	Kemungkinan terjadi setiap tahunnya	Terdapat penangkal petir	2	Kontrol yang dilakukan sudah mampu mengamankan aset server dari risiko kerusakan	**80**	Medium	Bagian Umum
					Banjir	5	Kemungkinan terjadi setiap tahunnya	Letak lokasi ruang server di lantai 2	2	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko kerusakan akibat banjir	**80**	Medium	Bagian Umum
		Penurunan citra organisasi			Kebakaran	2	Terjadi tahun lalu namun kecil sekali kemungkinannya	Terdapat smoke detector dan *fire extinguisher*	3	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko kerusakan akibat kebakaran berulang	**48**	Low	Bagian Umum

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
		Organisasi mengalami kerugian secara finansial			Kebocoran dan Kerusakan pada Bangunan	5	Kemungkinan terjadi setiap tahunnya	Terdapat maintenance yang dilakukan 6 bulan sekali	5	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance dilakukan berkala setiap 3 bulan	**200**	Very High	Bagian Umum
	Server berhenti	Proses bisnis terhambat	7	Terhambatnya proses bisnis akibat server berhenti bekerja dapat mengakibatkan ketidakpuasan dari seluruh civitas karena seluruh sistem yang digunakan berada pada satu server fisik	Kerusakan pada Genset dan UPS	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah memiliki UPS dan Genset	Lokasi genset dan UPS terdapat pada lokasi aman dan terdapat maintenance yang dilakukan 6 bulan sekali	2	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko dengan adanya UPS dan Genset	**56**	Medium	Bagian TIK
					Listrik Mati	7	Kemungkinan terjadinya tinggi	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko dengan adanya UPS dan Genset	**98**	Medium	Bagian Umum
	Kinerja server menurun	Berkurangnya kepercayaan civitas akademika	3	Kinerja server menurun dapat mengakibatkan berkurangnya kepercayaan dari civitas karena seluruh	RAM mengalami kelebihan memori	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena	Maintenance dilakukan 6 bulan sekali	4	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance	**48**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				sistem berada pada satu sistem namun menurunnya kinerja server hanya berdampak kecil pada berjalannya keseluruhan proses bisnis			telah dilakukan maintenance berkala setiap 6 bulan			dilakukan berkala setiap 3 bulan			
		Menurunnya prouktivitas			Kinerja Procesor menurun akibat terlalu banyak kapasitas data	3	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah dilakukan maintenance berkala setiap 6 bulan	Maintenance dilakukan 6 bulan sekali	4	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance dilakukan berkala setiap 3 bulan	**36**	Low	Bagian TIK
					Tempat penyimpanan (*Harddisk)* penuh	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah dilakukan maintenance berkala setiap 6 bulan	Maintenance dilakukan 6 bulan sekali	4	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance dilakukan berkala setiap 3 bulan	**48**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Pencurian data	Penurunan citra organisasi	5	Pencurian data dapat mengakibatkan tersebarnya data dan bocornya data penting akademik dan hal ini dapat mengakibatkan penurunan citra organisasi namun pencurian data tidak mengakibatkan hilangnya data dan dampak yang diakibatkan cukup tinggi	Ruang Server kurang diberi pengamanan	5	Kemungkinan terjadinya setiap tahunnya karena belum memiliki standard prosedur pengamanan ruang server	Ruang server dikunci dan tidak semua dapat masuk ke dalam ruangan	4	Kontrol yang dilakukan sudah cukup namun belum ada log book mengenai siapa saja yang masuk kedalam ruang server	**100**	Medium	Bagian TIK
		Penyalahgunaan data			Kesalahan Konfigurasi Server	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah dilakukan maintenance berkala setiap 6 bulan	Terdapat pelatihan terhadap staf bagian TIK	5	Kontrol yang dilakukan sudah sesuai namun sosialisasi yang dilakukan kurang memberikan pengaruh terhadap awareness civitas atas keamanan data	**100**	Medium	Bagian TIK
	Data Hilang	Proses bisnis terhambat	7	Data hilang dapat menghambat berjalannya proses bisnis ketika data mengenai kemahasiswaan dan akademik dibutuhkan sehingga dampaknya	Kesalahan DBA	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena DBA telah terlatih	Melakukan pelatihan pada DBA	3	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko *human eror* pada DBA	**84**	Medium	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				cukup tinggi	Virus	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena dilakukan maintenance dan pengecekan lisensi oleh bagian TIK	Memasang antivirus E-scan	4	Kontrol yang dilakukan sudah cukup baik dan bagian TIK telah melakukan pengecekan setiap 6 bulan sekali	**112**	Medium	Bagian TIK
	Kerusakan pada PC	Menurunnya produktivitas	4	Kerusakan PC dapat menghambat aktivitas dalam proses bisnis yang didukung oleh TI dan hali ini mengakibatkan menurunnya kinerja dan terhambatnya proses bisnis serta mengakibatkan kerugian secara finansial bagi organisasi namun dampak yang diakibatkan tidak begitu tinggi karena proses utama perkuliahan tetap dapat berjalan	Gempa Bumi	3	Kemungkinan terjadi kecil	Letak lokasi ruang kerja di lantai 2	5	Kontrol yang dilakukan sudah mampu mengamankan PC namun keefektifannya masih rata-rata	**60**	Low	Bagian Umum
		Organisasi mengalami kerugian secara finansial			Badai dan Petir	5	Kemungkinan terjadi setiap tahunnya	Terdapat penangkal petir	2	Kontrol yang dilakukan sudah mampu mengamankan PC dari risiko kerusakan	**40**	Low	Bagian Umum
					Banjir	5	Kemungkinan terjadi setiap tahunnya	Letak lokasi ruang server di lantai 2	2	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko kerusakan PC akibat banjir	**40**	Low	Bagian Umum

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
		Proses bisnis terhambat			Kebakaran	2	Terjadi tahun lalu namun kecil sekali kemungkinan nya	Terdapat smoke detector dan *fire extinguisher*	3	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko kerusakan PC akibat kebakaran berulang	**24**	Low	Bagian Umum
					Kebocoran dan Kerusakan pada Bangunan	5	Kemungkinan terjadi setiap tahunnya	Terdapat maintenance yang dilakukan 6 bulan sekali	4	Kontrol yang dilakuka cukup baik namun secara best practice seharusnya maintenance dilakukan 3 bulan sekali	**80**	Medium	Bagian Umum
					Keyboard, mouse atau monitor mengalami kerusakan karena pemakaian berlebih	3	Kemungkinan terjadinya kecil	Terdapat maintenance yang dilakukan 6 bulan sekali	2	Kontrol yang dilakukan sudah cukup baik dan bagian TIK telah melakukan pengecekan prasarana secara berkala	**24**	Low	Bagian TIK
	PC tidak dapat menyala	Menurunnya produktivitas	3	Dampak yang diakibatkan tidak terlalu tinggi karena hanya menghambat aktivitas yang membutuhkan dukungan TI namun secara keseluruhan	Kerusakan pada Genset dan UPS	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Terdapat maintenance yang dilakukan 6 bulan sekali	4	Kontrol yang dilakukan cukup baik namun secara best practice seharusnya maintenance dilakukan 3 bulan sekali	**48**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				proses perkuliahan tetap dapat berjalan dengan baik	Listrik Mati	7	Kemungkinnan terjadinya sangat tinggi	Sudah terdapat genset saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**42**	Low	
	PC terkena virus	Menurunnya produktivitas	3	Dampak yang diakibatkan tidak terlalu tinggi karena hanya menghambat aktivitas yang membutuhkan dukungan TI namun secara keseluruhan proses perkuliahan tetap dapat berjalan dengan baik	antivirus tidak update	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Terdapat antivirus e-scan	5	Kontrol yang dilakukan cukup yaitu dengan menggunakan antivirus E-Scan	**60**	Low	Bagian TIK
Software	Aplikasi tidak dapat diakses	Proses bisnis terhambat	5	Proses bisnis akan terhambat akibat aplikasi tersebut menjadi pendukung dalam proses perkuliahan seperti e-learning dimana seluruh materi ajar dosen berada pada sistem tersebut	Listrik Mati	7	Kemungkinnan terjadinya sangat tinggi	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**70**	Low	Bagian Umum
		Menurunnya produktivitas			Server Down	5	Kemungkinan terjadi setiap tahun	Adanya perawatan maintenance pada server 6 bulan sekali	3	Kontrol yang dilakukan sudah cukup baik untuk menanggulangi permasalahan server	**75**	Low	Bagian TIK
	Aplikasi diakses oleh pihak yang tidak berwenang	Tersebarluasnya data orgnisasi	9	Dengan diaksesnya aplikasi oleh pihak yang tidak berwenang dapat mengakibatkan bocornya data	Kesalahan dalam pemberian hak akses	3	Kemungkinan terjadinya kecil	Adanya peraturan dalam pembatasan hak akses	4	Kontrol yang dilakukan sudah cukup baik namun masih kurang mampu faktor eksternal yang	**108**	Medium	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				akademik dan kemahasiswaan serta data lain yang sifatnya *confidential* sehingga dapat yang diakibatkan sangat tinggi						berusaha masuk kedalam sistem			
Data	Data tidak dapat diakses	Menurunnya produktivitas	5	Data tidak dapat diakses mengakibatkan penurunan kinerja dan terhambatnya proses bisnis hanya pada aktivitas yang membutuhkan dukungan TI sehingga dampak yang dihasilkan tidak menyeluruh dan tinggi	Listrik Mati	7	Kemungkinan terjadinya tinggi	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**70**	Low	Bagian TIK
		Proses bisnis terhambat			Server Down	5	Kemungkinan terjadi setiap tahun namun kecil	Adanya perawatan maintenance pada server 6 bulan sekali	3	Kontrol yang dilakukan sudah cukup baik untuk menanggulangi permasalahan server	**75**	Low	Bagian TIK
		Berkurangnya kepercayaan civitas akademika											Bagian TIK
	Pencurian data	Berkurangnya kepercayaan civitas akademika	7	Pencurian data dapat mengakibatkan tersebarnya data dan bocornya data penting akademik dan hal ini dapat mengakibatkan berkurangnya kepercayaan civitas dan dampak yang diakibatkan cukup tinggi	Terdapat hacker yang mencuri data	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Adanya firewall dan pengamanan jaringan	5	Kontrol yang dilakuan sudah cukup untuk mengamankan data dari hacker	**140**	High	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Manipulasi data	Komplain dari civitas akademika	8	Manipulasi data akademik dan mahasiswa dapat mengakibatkan komplain dan berkurangnya kepercayaan civitas terhadap pengamanan yang sudah dilakukan oleh organisasi sehingga hal ini berdampak cukup tinggi karena beberapa data bersifat *confidential*	Username dan password diketahui oleh pengguna lain	5	Kemungkinan terjadi setiap tahunnya	Diadakan sosialisasi kepada civitas akademika	5	Kontrol yang dilakukan sudah cukup untuk meningkatkan awareness civitas terhadap data *confidential*	**200**	Very High	Pengguna SISFO
		Berkurangnya kepercayaan civitas akademika			Terdapat hacker yang memanipulasi data	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Adanya firewall dan sosialisasi dari Bagian TIK ke civitas	5	Kontrol yang dilakuan sudah cukup untuk mengamankan data dari hacker	**160**	High	Bagian TIK
	Backup data gagal	Informasi yang ditampilkan tidak terbaru/terkini	4	Backup data gagal tidak berdampak cukup besar terhadap proses bisnis karena telah ada kontrol notifikasi dari sistem apabila back up data mengalami kegagalan, sehingga pihak TIK telah dapat mengatasi dampaknya dengan cepat	Kapasitas media penyimpanan overload	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Maintenance oleh DBA	3	Kontrol yang dilakukan sudah cukup baik dengan maintenance yang dilakukan sehingga kapasitas penyimpanan selalu terkontrol	**48**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Data hilang	Komplain dari civitas akademika	8	Data hilang dapat menghambat berjalannya proses bisnis ketika data mengenai kemahasiswaan dan akademik dibutuhkan sehingga dampaknya cukup tinggi	Server Rusak	3	Kemungkinan terjadinya kecil	Melakukan maintenance yang dilakukan 6 bulan sekali serta backup data setiap harinya	4	Kontrol yang dilakukan sudah cukup naik namun berdasarkan *best practice* seharusnya dilakukan selama 3 bulan sekali	**96**	Medium	Bagian TIK
		Proses bisnis terhambat			Virus/Bug	5	Kemungkinan terjadi setiap tahunnya	Adanya antvirus e-scan	4	Kontrol yang dilakukan sudah cukup baik dan sesuai untuk menanggulangi virus	**160**	High	Bagian TIK
Jaringan	Kurangnya kontrol pengamanan kabel	Proses bisnis terhambat	5	Kabel merupakan komponen yang penting untuk memastikan hubungan antar perangkat keras sehingga dampak yang diakibatkan cukup tinggi	Kabel rusak	5	Kemungkinan terjadi setiap tahunnya karena adanya hewan pengerat	Sudah ada pelabelan dan pengaturan kabel	2	Kontrol yang dilakukan saat ini sudah sangat baik untuk memastikan kabel terkelola dengan baik	**50**	Low	Bagian TIK
	Internet Mati	Produktivitas menurun	5	Internet mati dapat mengakibatkan terhambatnya aktivitas yang membutuhkan dukungan TI dan cukup berdampak pada keseluruhan aktivitas dalam proses bisnis	Listrik Mati	7	Kemungkinan terjadinya tinggi	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**70**	Low	Bagian Umum
					Wifi rusak	3	Kemungkinan terjadinya kecil karena adanya kontrol yang	Melakukan maintenance yang dilakukan 6 bulan sekali	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi kerusakan wifi	**30**		Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
							telah dilakukan						
					Genset mati	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Melakukan maintenance yang dilakukan 6 bulan sekali	4	Kontrol yang dilakukan cukup baik namun secara best practice seharusnya maintenance dilakukan 3 bulan sekali	**80**	Medium	Bagian TIK
					Kabel Rusak	5	Kemungkinan terjadi setiap tahunnya karena adanya hewan pengerat	Sudah ada pelabelan dan pengaturan kabel	2	Kontrol yang dilakukan saat ini sudah sangat baik untuk memastikan kabel terkelola dengan baik	**50**	Low	Bagian TIK
	Akses internet lambat	Komplain dari civitas akademika	5	Akses internet lambat dapat mengakibatkan banyaknya komplain dan menurunnya produktivitas karena pada umumnya banyak aktivitas yang didukung oleh TI sehingga dampak yang dihasilkan cukup tinggi	Kesalahan Konfigurasi	5	Kemungkinan terjadi setiap tahunnya	Melakukan maintenance 6 bulan sekali	4	Kontrol yang dilakukan cukup baik namun secara best practice seharusnya maintenance dilakukan 3 bulan sekali	**100**	Medium	Bagian TIK
		Produktivitas menurun			Ada yang melakukan netcut	7	Kemungkinan terjadinya tinggi	Memasang anti netcut	2	Kontrol yang dilakukan saat ini sudah sangat baik untuk memastikan tidak ada lagi yang dapat melakukan netcut	**70**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
Sumber Daya Manusia	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Tersebarluasnya data organisasi mengakibatkan hilangnya kerahasiaan dari data dan hal ini sangat berdampak besar karena dapat mengakibatkan pula hilangnya kepercayaan civitas	Penurunan Kompetensi Karyawan Pegawai Non-TI	3	Kemungkinan terjadinya kecil karena adanya kebijakan dan etika kerja untuk pegawai	Adanya pelatihan untuk Pegawai Non-TI	4	Kontrol yang dilakukan cukup baik untuk mengatasi adanya penyalahgunaan data dalam internal organisasi	**60**	Low	Pengguna SISFO
					Adanya praktik KKN di perusahaan	2	Kemungkinan terjadinya sangat kecil karena adanya kebijakan dan etika kerja untuk pegawai	Adanya kebijakan dan prosedur serta sosialisasi dari Bagian TIK ke civitas	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelanggaran etika kerja oleh pegawai	**30**	Low	Pengguna SISFO
	Data yang ada tidak valid	Penurunan citra organisasi Komplain dari civitas akademika	5	Data yang ada tidak valid memiliki nilai cukup tinggi karena dampak yang dihasilkan adalah pada pemrosesan dan output data sehingga hasil yang ditampilkan akan berbeda dan hal ini mengakibatkan ketidakpuasan civitas hingga penurunan citra organisasi	Kesalahan dalam input data	5	Kemungkinan terjadi setiap tahunnya seperti kesalahan mengetik atau memasukan data pada sistem seperti sistem kepegawaian dan keuangan	Adanya pelatihan untuk karyawan	3	Kontrol yang dilakukan sudah baik untuk mengatasi kesalahan berulang dilakukan oleh pegawai	**75**	Low	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Pelanggaran regulasi hak akses	Berkurangnya kepercayaan civitas akademika	3	Pelanggaran regulasi hanya mungkin terjadi pada internal organisasi dimana pada umumnya terjadi di lingkungan pegawai	Penyalahgunaan akses regulasi	3	Kemungkinan terjadinya kecil karena namun regulasi terjadi hampir setiap 2 tahun dan pelanggaran akses mungkin terjadi baik yang diketahui maupun tidak	Adanya kebijakan dan prosedur regulasi	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya penyalahgunaan akses oleh pegawai	**27**	Low	Bagian TIK
	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Tersebarluasnya data organisasi mengakibatkan hilangnya kerahasiaan dari data dan hal ini sangat berdampak besar karena dapat mengakibatkan pula hilangnya kepercayaan civitas	Penurunan Kompetensi Pegawai TI	3	Kemungkinan terjadinya kecil	Adanya pelatihan untuk Pegawai TI	4	Kontrol yang dilakukan cukup baik untuk mengatasi adanya penyalahgunaan data dalam internal organisasi	**60**	Low	Pengguna SISFO
					Adanya praktik KKN di perusahaan	3	Kemungkinan terjadinya kecil karena telah ada kebijakan dan aturan etika kerja pegawai	Adanya kebijakan dan prosedur serta sosialisasi dari Bagian TIK ke civitas	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelanggaran etika kerja oleh pegawai	**45**	Low	Pengguna SISFO
	Data yang ada tidak valid	Komplain dari civitas akademika	6	Data yang ada pada database dan dikelola oleh pegawai TI	Kesalahan dalam input data	6	Kemungkinan terjadinya cukup tinggi	Adanya pelatihan untuk	3	Kontrol yang dilakukan sudah baik untuk	**108**	Medium	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				apabila tidak valid memiliki nilai cukup tinggi karena dampak yang dihasilkan adalah mengakibatkan menurunya kepercayaan civitas hingga mengakibatkan menurunnya kepuasan dari civitas dan dapat mengakibatkan pula menurunnya reputasi			karena pegawai TI selalu berhubungan dengan sistem	karyawan		mengatasi kesalahan berulang dilakukan oleh pegawai			
	Pelanggaran regulasi	Penurunan citra organisasi	3	Pelanggaran regulasi hanya mungkin terjadi pada internal organisasi dimana pada umumnya terjadi di lingkungan pegawai	penyelahgunaan akses regulasi	4	Kemungkinan terjadinya rendah karena regulasi terjadi hanya setia 2 tahun sekali	Adanya kebijakan dan prosedur regulasi	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya penyalahgunaan akses oleh pegawai	**36**	low	Pengguna SISFO
	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Tersebarluasnya data organisasi mengakibatkan hilangnya kerahasiaan dari data dan hal ini sangat	Penurunan Kompetensi Dosen	3	Kemungkinan terjadinya kecil	Adanya kebijakan dan etika kerja	4	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelanggaran etika kerja oleh pegawai	**60**	Low	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				berdampak besar karena dapat mengakibatkan pula hilangnya kepercayaan civitas	Adanya praktik KKN di perusahaan	2	Kemungkinan terjadinya sangat kecil	Adanya kebijakan dan etika kerja	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelangaran etika kerja	**30**	Low	Pengguna SISFO
	Data yang ada tidak valid	Komplain dari civitas akademika	5	Data yang ada tidak valid memiliki nilai cukup tinggi karena dampak yang dihasilkan adalah pada pemrosesan dan output data sehingga hasil yang ditampilkan akan berbeda dan hal ini mengakibatkan ketidakpuasan civitas hingga penurunan citra organisasi	Kesalahan dalam input data nilai	5	Kemungkinan terjadinya setiap tahun walau kasusnya tidak banyal	Adanya pelatihan untuk dosen	3	Kontrol yang dilakukan sudah baik untuk mengatasi kesalahan berulang dilakukan oleh pegawai	**75**	Low	Pengguna SISFO
	Sharing Password Mahasiswa/i	Komplain dari civitas akademika	7	Penyebaran password oleh mahasiswa memiliki dampak	Manipulasi data	6	Terjadi hampir disetiap FRS	Sosialisasi kepada mahasiswa/i	5	Kontrol yang dilakukan kurang dapat mengatasi	**210**	Very High	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
		Penurunan citra organisasi		yang besar dikarenakan data yang ada dalam masing masing akun mahasiswa bersifat rahasia dan selain itu sistem *change password* belum dimiliki dalam sistem kemahasiswaannya dan hanya admin yang dapat mengubah passoword			semester baru walau dengan kasus yang tidak banyak			kurangnya awareness mengenai pentingnya menjaga kerahasiaan data			

LAMPIRAN D
JUSTIFIKASI PEMETAAN RISIKO DENGAN KONTROL COBIT 5

Tabel D. 1. Justifikasi pemetaan risiko dan kebutuha kontrol pada kerangka kerja Cobit 5

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Kontrol Cobit 5	Justifikasi
Data	Data demografi mahasiswa, Data akademik dan Data file server	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	DSS05.04 Manage user identity and logical access	Kontrol yang memastikan seluruh pengguna memiliki hak akses yang sesuai dengan kebutuhan bisnis dan telah terkoordinasi dengan unit bisnis yang mengelola pemberian hak akses. Kontrol ini dibutuhkan untuk memastikan bahwa tidak ada manipuasli data yang diakarenakan adanya pihak yang tidak berwenang mengakses sistem dengan menggunakan *password* dan *username* pengguna lain.

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Kontrol Cobit 5	Justifikasi
		13	Manipulasi data	Terdapat hacker yang memanipulasi data	DSS05.01 Protect Against Malware	Kontrol dalam mengimplementasi dan mengelola aksi pencegahan, pendeteksian dan pembenaran terhadap proteksi sistem informasi dalam organisasi terhadap *malware*. Kontrol ini berguna untuk memastikan bahwa sistem telah memiliki pengamanan yang baik sehingga dapat mengatasi teknik *hacker* dalam mencoa masuk kedalam sistem dan memanipulasi data.
		15	Data Hilang	Virus/bug	DSS05.01 Protect Against Malware	Kontrol dalam mengimplementasi dan mengelola aksi pencegahan, pendeteksian dan pembenaran terhadap proteksi sistem informasi dalam organisasi terhadap *malware*. Kontrol ini bergun sebagai tindak preventif dalam memastikan sistem

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Kontrol Cobit 5	Justifikasi
						informasi telah memiliki pengamanan sistem yang baik sehingga dapat terhindari dari ancaman *malware.*
		12	Pencurian data	Terdapat hacker yang mencuri data	DSS05.01 Protect Against Malware	Kontrol dalam mengimplementasi dan mengelola aksi pencegahan, pendeteksian dan pembenaran terhadap proteksi sistem informasi dalam organisasi terhadap *malware*. Kontrol ini bergun sebagai tindak preventif dalam memastikan sistem informasi telah memiliki pengamanan sistem yang baik sehingga dapat terhindari dari ancaman *malware.*

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Kontrol Cobit 5	Justifikasi
Data	Data demografi mahasiswa, Data akademik dan Data file server	15	Data Hilang	Server rusak	DSS05.03 Manage Endpoint Security	Kontrol dalam memastikan keamanan terhadap endpoint system yaitu laptop, server dan perangkat jaringan sesuai dengan kebutuhan keamanan untuk melakukan proses, penyimpanan dan transmisi data. Kontrol ini bertujuan untuk memastikan seluruh perangkat endpoint telah memiliki pengelolaan keamaan dengan baik sehingga dapat mengurangi adanya risiko kerusakan pada perangkat.
Hardware	Server	5	Data Hilang	Virus	DSS05.01 Protect Against Malware	Kontrol dalam mengimplementasi dan mengelola aksi pencegahan, pendeteksian dan pembenaran terhadap proteksi sistem informasi dalam organisasi terhadap *malware*. Kontrol ini bergun sebagai tindak

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Kontrol Cobit 5	Justifikasi
						preventif dalam memastikan sistem informasi telah memiliki pengamanan sistem yang baik sehingga dapat terhindari dari ancaman *malware.*
Hardware	Server	5	Data Hilang	Kesalahan DBA	DSS05.03 Manage Endpoint Security	Kontrol dalam memastikan keamanan terhadap endpoint system yaitu laptop, server dan perangkat jaringan sesuai dengan kebutuhan keamanan untuk melakukan proses, penyimpanan dan transmisi data. Kontrol ini bertujuan untuk memastikan seluruh perangkat endpoint telah memiliki pengelolaan keamaan dengan baik sehingga dapat mengurangi adanya risiko kerusakan pada perangkat.

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Kontrol Cobit 5	Justifikasi
Hardware	Server	4	Pencurian data	Ruang server kurang diberi pengamanan	DSS05.05 Manage physical access to IT assets	Kontrol dalam membatasi akses pada area penting dalam organisasi. Kontrol ini memastikan seluruh akses terhadap area penting terautorisasi, memiliki sebuah *log* dan termonitor dengan baik.
Hardware	Server	4	Pencurian data	Kesalahan konfigurasi server	DSS05.03 Manage Endpoint Security	Kontrol dalam memastikan keamanan terhadap *endpoint system* yaitu laptop, server dan perangkat jaringan sesuai dengan kebutuhan keamanan untuk melakukan proses, penyimpanan dan transmisi data. Kontrol ini bertujuan untuk memastikan seluruh perangkat endpoint telah memiliki pengelolaan keamaan dengan baik sehingga dapat mengurangi adanya risiko kerusakan pada perangkat.

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan	Kontrol Cobit 5	Justifikasi
Sumber Daya Manusia	Pegawai TI	20	Data yang ada tidak valid	Kesalahan dalam input data	DSS06.02 Control The Processsing of Information	Kontrol untuk memastikan pegeksekusian dari operasional proses bisnis khususnya dalam pemrosesan informasi telah benar, lengkap, akurat, tepat waktu dan aman.

Halaman ini sengaja dikosongkan

LAMPIRAN E
JUSTIFIKASI PEMATAAN RISIKO DENGAN KONTROL ISO27002:2013

Tabel E. 1. Justifikasi pemetaan kebutuhan kontrol pada kerangka kerja ISO27002:2013

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
Data	Data demografi mahasiswa, Data akademik dan Data file server	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	9.3.1 Use of Secrets Authentication Information	Kontrol dalam penggunaan informasi rahasian sebagai pengamanan autentikasi pengguna. Kontrol ini bertujuan untuk memastikan bahwa terdapat proteksi dalam penggunaan *password* pengguna.
					9.4.3 Password Management System	Kontrol dalam melakukan pengelolaan *password* dan memastikan kualitas dari setiap *password*. Sehingga kontrol ini berguna untuk memastikan bahwa penggunaan *password* oleh setiap pengguna telah sesuai dengan

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
						standard keamanan.
		13	Manipulasi data	Terdapat hacker yang memanipulasi data	16.1 Management of information security incidents and improvements	Kontrol dalam memastikan organisasi memiliki pendekatan yang konsistem dan efektif dalam mengatasi adanya *events* dalam keamanan informasi dan celah kerentanan.
		15	Data Hilang	Virus/bug	12.2.1 Control Against Malware	Kontrol untuk mengimplementasikan deteksi, pencegahan dan pemulihan terhadap malware. Kontrol ini berguna untuk memastikan bahwa terdapat kontrol preventif dalam mengatasi ancaman virus yang dapat mengakibatkan hilangnya

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
						data.
					12.3.1 Information Backup	Kontrol untuk melakukan *backup* data penting secara berkala. Kontrol ini bertujuan untuk memastikan proses backup dan juga termasuk didalamnya restore menghasilkan data yang lengkap dan akurat. Sehingga kontrol ini penting untuk menjaga ketersediaan data dan integritas data.
		12	Pencurian data	Terdapat hacker yang mencuri data	10.1.1 Policy on the Use of Crypthographic Control	Kontrol dalam mengembangkan dan mengimplementasikan sistem kriptografi dalam memberikan tambahan proteksi terhadap informasi. kontrol ini merupakan

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
						kontrol yang berguna dalam menjaga kerahasiaan data dengan kalasifikasi tinggi tetap terjaga *confidentiality* nya dengan menggunakna teknik kriptografi.
					10.1.2 Key Management	Kontrol dalam penggunaan kriptografi. Kontrol ini berguna sebagai standard dalam penentuan kunci kriptografi yang digunakan dalam melakukan enkripsi data pentinga/rahasia.
					7.2.3 Disciplinary Process	Kontrol dalam menindisiplinkan pegawai yang melakukan pelanggaran keamanan informasi. kontrol ini berguna untuk memastikan setiap pengguna sistem baik internal tidak melakukan tindakan mencari

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
						celah kelemahan sistem untuk mengakses data yang bersifat *confidential.*
		15	Data Hilang	Server rusak	12.3.1 Information Backup	Kontrol untuk melakukan *backup* data penting secara berkala. Kontrol ini bertujuan untuk memastikan proses backup dan juga termasuk didalamnya restore menghasilkan data yang lengkap dan akurat. Sehingga kontrol ini penting untuk menjaga ketersediaan data dan integritas data.
Hardware	Server	5	Data Hilang	Virus	12.2.1 Control Against Malware	Kontrol untuk mengimplementasikan deteksi, pencegahan dan pemulihan terhadap *malware.* Kontrol ini berguna untuk memastikan bahwa

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
						terdapat kontrol preventif dalam mengatasi ancaman virus yang dapat mengakibatkan hilangnya data.
Hardware	Server	5	Data Hilang	Kesalahan DBA	12.4.3 Administrator & Operator Logs	Kontrol untuk memastikan aktivitas sistem administrator dan sistem operasi selalu tercatat dalam sebuah *log* dan selalu terkendali. Sehingga apabila adanya kesalahan yang diakibatkan *human error* maka dapat dilakukan audit trail untuk melacak kesalahan yang terjadi.
Hardware	Server	4	Pencurian data	Ruang server kurang diberi pengamanan	11.1.2 Physical Entry Controls	Kontrol untuk memastikan hanya pegawai yang memiliki autorisasi yang dapat mengakses area penting. Kontrol ini penting untuk menghindari adanya akses

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
						pada ruang server oleh pihak yang tidak berwenang.
Hardware	Server	4	Pencurian data	Kesalahan konfigurasi server	12.4.3 Administrator & Operator Logs	Kontrol untuk memastikan aktivitas sistem administrator dan sistem operasi selalu tercatat dalam sebuah *log* dan selalu terkendali. Kontrol ini berfungsi untuk memastikan keamanan server dari adanya kelalaian administrator sehingga diperlukan log untuk dapat melacak kesalahan yang terjadi.
Sumber Daya Manusia	Pegawai TI	20	Data yang ada tidak valid	Kesalahan dalam input data	14.1.2 Securing Application Services on Public Networks	Kontrol untuk memastikan layanan aplikasi dalam jaringan umum terproteksi dari aktivitas pelanggaran kemanan informasi seperti modifikasi.

Halaman ini sengaja dikosongkan

LAMPIRAN F
REKOMENDASI MITIGASI RISIKO

Tabel F. 1. Rekomendasi Mitigasi Risiko berdsarkan pemetaan kontrol pada kerangka kerja Cobit 5 dan ISO27002:2013

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013		
Data	Data demografi mahasiswa, Data akademik dan Data file server	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	DSS05. 04 Manage User Identity and Logical Access	Untuk memastikan seluruh pengguna memiliki hak akses yang sesuai dan telah terkoordinasi dengan unit bisnis yang mengelola pemberian hak akses.	• Mengelola hak akses pengguna sesuai dengan fungsional bisnisnya dalam proses bisnis • Mengidentifikasikan secara unik setiap aktifitas pemrosesan data yang dilakukan oleh setiap peran dalam masing masing fungsional bisnis • Mengautentikasi pengguna yang melakukan perubahan • Memastikan autoritas pengguna • Melakukan pembagian dan pengelolaan hak akses akun pengguna • Melakukan pengelolaan secara	• Adanya autentikasi untuk login pengguna SISFO • Adanya perbedaan hak akses untuk masing masing *role* dalam SISFO • Adanya prosedur yang telah berjalan untuk melakukan pergantian *password* mahasiswa	• Bagian TIK yang khusus memiliki hak dalam melihat dan mengubah akses pengguna harus secara berkala meninjau ulang dan mengalokasikan hak akses ketika ada staf/pegawai yang pindah unit fungsional • Bagian TIK harus mengelola log sistem dengan baik secara berkala • Seluruh perubahan hak akses (penambahan, modifikasi dan penghapusan) harus tercatat dalam sistem dengan baik • Bagian TIK harus mengelola dan mengimplementasikan prosedur audit trail yang telah ditetapkan

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013		
							berkala untuk meninjau ketapatan hak akses setiap pengguna • Mengelola audit trail		untuk melacak akses pada informasi yang rahasia/sensitif
					9.3.1 Use Of Secrets Authentication Information	Untuk pengelolaan penggunaan informasi rahasian sebagai pengamanan autentikasi pengguna	• Memastikan setiap pengguna menjaga kerahasiaan autentikasi informasi • Menghindari penyimpanan password pada lokasi yang bersifat umum (kertas, perangkat lunak, handphone) • Memastikan adanya proteksi terhadap password apabila password digunakan sebagai informasi autentikasi • Apabila password digunakan sebagai autentikasi tidak digunakan untuk kebutuhan bisnis dan kebutuhan non-binis • Apabila password digunakan sebagai	• Adanya autentikasi untuk login pengguna SISFO • Adanya batasan dalam SISFO bahwa perubahan, penambahan dan penghapusan akun dan password pengguna hanya dapat dilakukan oleh database administrator • Telah dilakukan sosialisasi kepada mahasiswa dan	Bagian TIK membuat aturan / kebijakan penggunaan autentikasi pada akun pengguna yang mencakup : • Pengguna tidak diperbolehkan melakukan *share* informasi autenttikasi • Pengguna tidak diperbolehkan menyimpan informasi autentikasi pada tempat yang dapat dilihat oleh pengguna lain (kertas, *mobile device*) • Ketika password digunakan sebagai informasi autentikasi, maka pengguna harus membuat password yang berkualitas • Aturan perubahan informasi autentikasi

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
							autentikasi maka password harus memenuhi standard kualitas *strong password*	dosen untuk praktik keamanan TI	apabila terindikasi kemungkinan bocornya informasi autentikasi
					9.4.3 Password Management System	Untuk pengelolaan *password* dan memastikan kualitas *password*	• Memastikan pemilihan password yang berkualitas • Memastikan sistem tidak menampilkan password dalam kolom password ketika pengguna mengintputkannya • Memastikan pengguna mengganti password default pada awal log in • Menyimpan data password didatabase berbeda dari sistem aplikasi data • Menyimpan dan mentransmisikan password dalam cara yang aman (enskripsi) • Menghimbau untuk melakukan	• Adanya batasan dalam SISFO bahwa perubahan, penambahan dan penghapusan akun dan password pengguna hanya dapat dilakukan oleh database administrator • *Password* yang digunakan telah sesuai dengan *strong password*	• SISFO Perbanas membuat aturan penggunaan password yang benar unuk setiap pengguna yang mencakup : - Pengguna diharuskan melakukan request perubahan password apabila informasi password diketahui pengguna lain / bocor - Pengguna tidak boleh melakukan *share login* - Menggunakan aturan *strong password* untuk pengguna seluruh SISFO - Melakukan reset maupun pergantian password pengguna secara berkala sesuai dengan kebijakan yang ada

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
							pergantian password secara berkala sesuai dengan kebutuhan • Mengelola data password dan memastikan tidak ada penggunaan kembali password lama		• Membuat sebuah ***prosedur mengenai manajemen password yang mencakup proses pengelolaan pergantian password***
					16.1 Management of information security incidents and improvements	Untuk memastikan konsistensi dan efektifitas dari pendekatan pengelolaan gangguan keamanan informasi	• Pengelolaan pelaporan kejadian/*events* keamanan informasi • Pengklasifikasin kejadian/*events* keamanan informasi • Pengelolaan pelaporan kelemahan sistem keamanan • Penilaian dan pengambilan keputusan terhadap gangguan/*events* keamanan sistem informasi • Pengelolaan respon pada gangguan keamanan informasi	• Pembuatan dan pelaksanaan beberapa SOP mengenai SI/TI oleh Bagian TIK • Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI	• Bagian TIK harus membangun sebuah prosedur dalam penangan serangan *hacker* yang termasuk didalamnya: - Penetuan klasifikasi gangguan - Pelaporan gangguan - Pengelolaan dan pelaporan kelemaham sistem informasi - Pengelolaan respon terhadap gangguan keamanan untuk selanjutnya dijadikan *knowledge management*

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013		
		12	Pencurian data	Terdapat hacker yang mencuri data	10.1.1 Policy on the Use of Cryptographic Controls	Untuk mengembangkan dan mengimplementasikan sistem kriptografi dalam memberikan tambahan proteksi terhadap informasi	• Menentukan informasi bisnis penting yang perlu diproteksi dengan sistem kriptografi harus berdasarkan persetujuan manajemen tertinggi • Menggunakan pendekatan *key management* dalam memproteksi metode kunci kriptografi dan pemulihan enkripsi informasi apabila terjadi kehilanagan atau kerusakan kunci kriptografi • Menggunakan enkripsi pada informasi sensitive pada saat penyimpanan maupun transmisi data	• Melakukan klasifikasi data yang akan di back up secara berkala berdasarkan tingkat kepentingan data • Adanya *update patch* dan *firewall* secara berkala	• Bagian TIK harus mengklasifikasikan informasi berdasarkan tingkat kepentingan informasi dari sudut pandang bisnis sebelum menentukan penggunaan enkripsi • Bagian TIK perlu mengaplikasikan enrkipsi berdasaran pada hasil penilaiain risiko • Bagian TIK perlu menentukan standard kunci enkripsi yang akan digunakan sesuai dengan kebutuhan bisnis • Pengaplikasian enkripsi pada data yang bersifat rahasia dilakukan selama proses penyimpanan maupun proses transmisi data
					7.2.3 Disciplinary Process	Untuk menindisiplinkan pegawai yang	• Proses formal pendisiplinan yang dilakukan harus tepat bagi pegawai yang	• Telah dilakukan sosialisasi kepada	• Perlu adanya sebuah peninjauan gangguan sistem informasi setelah terjadinya serangan

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
						melakukan pelanggaran keamanan informasi	melakukan pelanggaran terhadap keamanan informasi • Proses formal juga harus mencakup menimbang faktor penyebabnya dan dampak terhadap bisnis • Proses formal juga harus menimbang pelaku pelanggaran apakah dari internal dan eksterl organisasi dan faktor lainnya	mahasiswa dan dosen untuk praktik keamanan TI	oleh hacker • Dalam melakukan tindak lanjut untuk pencurian data yang dilakukan oleh hacker dari internal STIE Perbanas, perlu adanya sebuah peraturan formal untuk mengatur pelanggaran terhadap keamanan informasi yang dilakukan oleh pihak internal
		15	Data Hilang	Server rusak	DSS05.03 Management Endpoint Security	Untuk memastikan keamanan terhadap endpoint system (server) sesuai dengan kebutuhan keamanan dalam melakukan proses,	• Konfigurasi sistem operasi dengan proteksi yang tepat • Menggunakan mekanisme *lock* pada device endpoint • Melakukan enkripsi pada informasi sesuai dengan klasifikasi data • Mengelola akses pada device endpoint • Mengelola	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk perangkat TI pada setiap kelas dan lab • Pada ruang server telah dipasang smoke detector untuk	• Bagian TIK harus melakukan pengelolaan dan perawatan terhadap infrastruktur seperti server dan infrasturktur jaringan seperti hub, switch dan kabel secara berkala selama 3 bulan sekali • ***Membuat prosedur mengenai proteksi server*** • Mekukan *checklist*

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013		
						penyimpanan dan transmisi data	konfigurasi jaringan dengan proteksi yang tepat • Menyediakan proteksi fisik bagi device endpoint	memberikan peringatan apabila terhadi kebakaran • Telah ada fire extinguisher untuk memadamkan api saat terjadi kebakaran • Ada penguncian pada ruang server dan kunci selalu dipegang oleh Bagian TIK	keamanan server setiap hari • Membuat sebuah ***log aktivitas untuk kegiatan yang berhubungan dengan akses server secara langsung***
					12.3.1 Information Backup	Untuk melakukan *backup* data penting secara berkala	• Membuat kebijakan backup data yang mencakup kebutuhan retensi dan proteksi • Memastikan adanya fasilitas backup (server backup) • Back up yang dilakukan secara berkala harus sesuai dengan kebutuhan bisnis	• Telah dilakukan back up server dan NAS setiap hari secara berkala dan terjadwal • Data hanya dapat dimasukkan, diganti dan dihapus oleh database	• Bagian TIK secara berkala mengontrol bahwa salinan data selama proses backup telah lengkap • ***Membuat prosedur mengenai backup data dan termasuk didalamnya restore data dan pengujian back up data*** • Memastikan lokasi

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013		
							• Lokasi media backup harus berada pada lokasi tersendiri • Media untuk backup harus secara berkala diuji dan ditinjau kesesuaian waktu restore yang diperlukan • Memonitor eksekusi dari backup dan meninjau kegagalan penjadwalan backup untuk memastikan kelengkapan dari backup data	administrator saja	server selalau terkontrol dengan baik dengan memonitor prosedur perawatan dan pengelolaan server berjalan dengan baik

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
Hardware	Server	5	Data Hilang	Virus	DSS05.01 Protect Against Malware	Untuk memastikan implementasi dan pengelolaan aksi pencegahan, pendeteksian dan pembenarani terhadap malware	• Mengkomunikasikan dan menjalankan prosedur pencegahan • Menginstal dan mengaktifkan software/tools untuk memproteksi terhadap malware • Secara berkala meninjau dan mengevaluasi ancaman • Memfilter *traffic* data dan informasi yang masuk • Melakukan pencerdasan secara berkala mengenai malware dengan memanfaatkan email dan internet sebagai penyebaran informasi	• Adanya antivirus (e-scan) dan telah di update terus menerus setiap hari • Pada lab tidak dapat dipasang USB • Pada lab tidak dapat di install aplikasi dari luar • Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI	Bagian TIK secara berkala memastikan firewall telah mampu melindungi sistem dari serangan malware • Membuat ***prosedur mengenai pengelolaan serangan malware*** • Membatasi akses langsung pada server • Membuat peraturan bagi pengguna maupun administrator untuk tidak boleh menghubungkan device lain (seperti usb) pada server
					12.2.1 Control Aagainst Malware	untuk implementasikan aksi deteksi, pencegahan dan pemulihan	• Membuat peraturan yang melarang penggunaan software yang tidak terautorisasi • Melakukan tinjauan	• Adanya antivirus (e-scan) dan telah di update terus menerus setiap hari	• Bagian TIK seharusnya membentuk kontrol khusus untuk memantau dan mengelola *traffic* jaringan melalui aplikasi yang sudah

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
						terhadap *malware*	berkala pada software dan sistem data konten • Pemulihan serangan malware • Menginstal dan memperbaharui software pendeteksi malware • Melakukan scnning pada komputer dan media lainnya • Mendefinisikan prosedur dan tanggung jawab dalam memproteksi malware • Melakukan pelaporan dan pemulihan serangan malware	• Pada lab tidak dapat dipasang USB • Pada lab tidak dapat di install aplikasi dari luar • Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI	dimiliki, untuk menjaga kerahasiaan dan integritas data yang melewati jaringan *public* atau nirkabel serta untuk melindungi sistem SISFO serta untuk memastikan ketersediaan layanan jaringan dan komputer yang terhubung
			Data Hilang	Kesalahan DBA	DSS05.03 Management Endpoint Security	Untuk memastikan keamanan terhadap endpoint system (server) sesuai dengan	• Konfigurasi sistem operasi dengan proteksi yang tepat • Menggunakan mekanisme *lock* pada device endpoint • Mengelola akses	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk perangkat TI pada setiap	• Membuat prosedur mengenai proteksi lingkungan server • Membuat ***prosedur mengenai akses langsung pada server*** • Membuat sebuah ***log***

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
						kebutuhan keamanan dalam melakukan proses, penyimpanan dan transmisi data	pada device endpoint • Menyediakan proteksi fisik bagi device endpoint	kelas dan lab	***aktivitas untuk kegiatan yang berhubungan dengan akses server secara langsung***
					12.4.3 Administrator and Operator Logs	Untuk memastikan aktivitas sistem administrator dan sistem operasi selalu tercatat dalam sebuah *log* dan selalu terkendali	• Memproteksi dan meninjau *log* administrator untuk mengelola akuntabilitas dari hak akses	• Memiliki prosedur mutu terkait pelacakan log sistem yaitu audit trail	• Bagian TIK harusnya menambahkan pengendalian rekaman yaitu log aktivitas dalam sistem SISFO untuk memudahkan pelacakan apabila terjadi kesalahan • Log pada sistem SISFO seharusnya mencakup log aktivitas untuk user maupun administrator

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
		4	Pencurian data	Ruang server kurang diberi pengamanan	DSS05.05 Manage Physical Access to IT Assets	Untuk membatasi akses pada area penting dan memastikan seluruh akses terhadap area penting terautorisasi, memiliki sebuah *log* dan termonitor dengan baik	• Mengelola permintaan dan memberikan akses pada fasilitas terkomputerisasi • Memastikan permintaan akses dilakukan secara formal berdasarkan prosedur yang ada dan diketahui oleh pihak TI • Memastikan pemberian akses didasarkan pada fungsi kerja dan tanggung jawab • Memiliki log untuk memonitor seluruh akses pada lokasi penting • Meregistrasikan seluruh pengunjung apabila akan memasuki lokasi penting	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk perangkat TI pada setiap kelas dan lab • Ada penguncian pada ruang server dan kunci selalu dipegang oleh Bagian TIK	• Membuat prosedur mengenai akses pada ruang server • Membuat sebuah *log* yang berisikan aktivitas dan kepentingan selama melakukan akses langsung pada server
					11.1.2 Physical Entry	Untuk memastikan hanya pegawai	• Waktu dan tanggal masuk pengunjung harus tercatat	• Dilakukan maintenance rutin setiap 6	• Bagian TIK selalu megontrol dan melakukan supervisi

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013		
					Controls	yang memiliki autorisasi yang dapat mengakses area penting	• Pengunjung harus disupervisi selama berada dalam lokasi penting kecuali telah memiliki persetujuan akses • *Log book* untuk memasuki lokasi penting harus selalu ditinjau dan dikelola	bulan sekali (diawal semester) untuk perangkat TI pada setiap kelas dan lab • Ada penguncian pada ruang server dan kunci selalu dipegang oleh Bagian TIK	untuk kegiatan yang berhubungan dengan akses langsung pada server • Membuat prosedur mengenai akses pada ruang server • Membuat sebuah *log* yang berisikan aktivitas dan kepentingan selama melakukan akses langsung pada server
			Pencurian data	Kesalahan konfigurasi server	DSS05.03 Management Endpoint Security	Untuk memastikan keamanan terhadap endpoint system (server) sesuai dengan kebutuhan keamanan dalam melakukan proses, penyimpanan dan transmisi data	• Konfigurasi sistem operasi dengan proteksi yang tepat • Menggunakan mekanisme *lock* pada device endpoint • Melakukan enkripsi pada informasi sesuai dengan klasifikasi data • Mengelola akses pada device endpoint • Mengelola konfigurasi jaringan	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk perangkat TI pada setiap kelas dan lab • Ada penguncian pada ruang server dan kunci selalu dipegang oleh Bagian TIK	• Bagian TIK harus melakukan pengelolaan dan perawatan terhadap infrastruktur seperti server dan infrasturktur jaringan seperti hub, switch dan kabel secara berkala selama 3 bulan sekali • Bagian TIK seharusnya membuat sebuah intruksi kerja yang jelas mengenai konfigurasi server • Membuat sebuah log

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
							dengan proteksi yang tepat • Menyediakan proteksi fisik bagi device endpoint		aktivitas untuk kegiatan yang berhubungan dengan akses server secara langsung
Sumber Daya Manusia	Pegawai TI	20	Data yang ada tidak valid	Kesalahan dalam input data	DSS06.02 Control the Processing of Information	Untuk memastikan pegeksekusian dari operasional proses bisnis khususnya dalam pemrosesan informasi telah benar, lengkap, akurat, tepat waktu dan aman	• Melakukan autentikasi sebelum pengguna melakukan input data untuk memastikan autorisasi • Mengelola integritas dan validitas data selama proses penginputan data berlangsung • Memvalidasi inputan dan edit data • Mengelola output data dan menampilkan output data hanya pada pengguna yang memiliki autorisasi	• Membedakan role dan hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fugsinya	• Sistem SISFO selalu meminta login pada pengguna setelah *user section* berlangsung selama lebih dari 20 menit • Membuat prosedur mengenai respon kesalahan validasi data
					14.1.2	Untuk	• Menentukan	• Membedakan	• Bagian TIK

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan Cobit 5 dan ISO27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol Cobit 5 dan ISO27002:2013**		
					Securing Application Services on Public Networks	memastikan layanan aplikasi dalam jaringan umum terproteksi dari aktivitas pelanggaran kemanan informasi seperti modifikasi	limitasi kolom untuk input data yang spesifik • Memastikan karakter pada kolom sesuai dengan input data yang diharapkan • Memastikan adanya log aktivitas untuk setiap input data yang dilakukan oleh pengguna • Sistem aplikasi harus mampu menampilkan kembali informasi yang diinputkan oleh pengguna untuk memastikan akurasi dan kelengkapan data	role dan hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fugsinya • Memiliki prosedur mutu terkait pelacakan log sistem yaitu audit trail	seharusnya meninjau SISFO untuk memastikan telah ada limitasi pada kolom inputan data dengan spesifik dan memastikan bahwa kareakter sesuai dengan inputan data yang diharapkan • Sistem SISFO memiliki log untuk setiap inputan data yang dilakukan pengguna untuk memastikan prosedur audit trail yang telah dimiliki oleh Bagian TIK dapat berjalan dengan baik

Halaman ini sengaja dikosongkan

LAMPIRAN G
HASIL VERIFIKASI DAN VALIDASI SOP

Hasil verifikasi SOP

Tabel dibawah ini berisikan penjelasan dari hasil verifikasi dokumen produk SOP Keamanan Data STIE Perbanas yang dilakukan dengan Kasie TIK STIE Perbanas. Verifikasi dokumen produk SOP dilakukan dengan teknik wawancara secara langsung.

Tanggal Wawancara : 14 Desember 2015
Nama Narasuber : Hariadi Yutanto, S.Kom, M.Kom
Peran Narasumber : Kasie TIK STIE Perbanas

Tabel G. 1. Hasil wawancara terkait verifikasi prosedur dalam Dokumen SOP Keamanan Data

Pertanyaan	Jawaban
Menurut Bapak apakah kebijakan yang di rekomendasikan telah sesuai dengan kondisi pada STIE Perbanas? Atau adakah kebijakan yang kurang sesuai dan perlu diubah?	Karena secara spesifik belum ada kebijakan khusus mengenai Teknologi Informasi dan Komunikasi di STIE Perbanas ini, sehingga kebijakan yang direkomendasikan untuk dokumen SOP ini dapat diterima. Dan juga karena Bagian TIK juga sedang mengembangkan draft kebijakan untuk Blue Print TI, sehingga menurut saya beberapa kebijakan yang direkomendasikan ini dapat diterima dan diajukan untuk diimplementasikan.
Menurut Bapak apakah ada istilah yang kurang tepat yang digunakan dalam dokumen SOP ini?	Secara keseluruhan sudah tepat.
Apakah menurut Bapak ada aktivitas dalam SOP yang perlu	Ada beberapa koreksi untuk prosedur di Back up, khususnya

diperbaiki atau ditambahkan?	untuk penjadwalan Back up. Jadi di Perbanas ini Back up berkala secara otomatis pada server SISFO dilakukan dua kali yaitu pada pulul 12.00 dan 21.00 sedangkan untuk Back up file server pada pukul 19.00.
	Selain itu, untuk prosedur Back up ini menurut saya yang lebih kritis sehingga perlu di spesifikan juga bagaimana prosedur dari uji back up. Karena ada beberapa kasus yang pernah terjadi yaitu data saat di *restore* tidak sesuai dengan data back up walaupun status pada log sistem menunjukan *success* sehingga perlu adanya uji coba berkala pada proses back up.
	Dan juga pada prosedur permintaan pergantian password, mungkin bisa di spesifikan lagi karena untuk permintaan pergantian password mahasiswa dan dosen/pegawai alurnya berbeda. Beberapa dosen/pegawai apabila akan mengganti password dapat langsung meghubungi beberapa pegawai Bagian TIK melalui via telpon atau email dan lainnya.
Terakait dengan formulir dalam mendukung setiap prosedur yang dihasilkan apakah ada koreksi?	Secara keseluruhan sudah lengkap dan cukup, mungkin lebih lanjut kesesuiannya bisa dilihat pada saat simulasi prosedurnya saja dengan pegawai bagian TIK lain yang terkait dengan prosedur tersebut
Terkait dengan instruksi kerja	Untuk *scanning* sebenarnya biasa

untuk pencegahan malware rekomendasi penggunaan *tools* nya apakah sudah sesuai?	dilakukan dengan *tools* Nicto. Namun rekomendasi ini bisa diterima.

Hasil Validasi Pengujian SOP

Berikut ini adalah lampiran yang berisi hasil skenario pengujian SOP beserta formulir-formulir yang diisi saat pengujian prosedur berlangsung.

1. Pengujian SOP Manajemen Password

Tanggal Pengujian : 4 Januari 2016
Pelaksana : Yusuf Effendi, Pegawai Bagian TIK
Bagus Prasojo, Mahasiswa STIE Perbanas

Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 2. Hasil pengujian SOP Manajemen Passowrd

No	Aktivitas	Keterangan
Proses Pengelolaan Password		
1	Mempersiapkan prosedur perubahan *password* lama dan melakukan *setup* pada seluruh sistem.	Proses persiapan termasuk *coding* penambagan fitur pada sistem informasi kepegawaian uji coba (bajool.perbanas.ac.id) telah dilakukan
2	Menyediakan *password default* sementara yang telah sesuai dengan standar *strong password* untuk masing masing pengguna sistem	Password default untuk pegawai telah disiapkan, namun hanya sebatas untuk pegawai bagian TIK sebagai uji coba
3	Mensosialisasikan penambahan fitur baru kepada seluruh civitas akademika melalui website resmi	Tidak dilakukan, karena prosedur yang dilakukan hanya sebatas uji coba
4	Mengirimkan *email* yang berisikan	Email pegawai

	password default sementara untuk seluruh pengguna sistem dan informasi mengenai ketentuan penggunaan kualitas standard *strong password*	didapatkan dari database pegawai dan email pemberitahuan pergantian fitur dalam sistem informasi berhasil dikirimkan, namun sebatas hanya pada salah satu pegawai TIK
5	Salah satu pegawai Bagian TIK lain sebagai pengguna sistem informasi kepegawaian mencoba melakukan *log in*.	Pegawai bagain TIK lain berhasil mengakses email dan melakukan log in pada sistem kepegawaian uji coba
6	Sistem menampilkan notifikasi untuk meminta civitas akademika melakukan pergantian *password default* dengan *password* baru yang sesuai dengan ketentuan kualitas standard *strong password*	Sistem berhasil menapilkan permintaan pergantian password
7	Mengelola data penggunaan password lama dan memastikan tidak ada penggunaan kembali *password default*	Tidak dilakukan
Proses Permintaan Pergantian Password		
1	Pengguna sistem melakukan permintaan pergantian *password (*dalam simulasi ini pengguna adalah pegawai bagian TIK*)*	Bagus Prasojo salah satu mahasiswa STIE Perbanas datang ke bagian TIK dengan membawa surat persetujuan permintaan pergantian password
2	Mahasiswa selanjutnya mengisi formulir permintaan pergantian password dengan menyertakan alasan permintaan pergantian *password*	Mahasiswa mengisi formulir permintaan pergantian password
3	Pegawai Bagian TIK melakukan validasi pada formulir permintaan	Pegawai Bagian TIK melakukan validasi

	pergantian password	formulir permintaan pergantian password
4	Pegawai Bagian TIK kemudian mengirimkan *email* yang berisikan *link* untuk menginputkan *password* baru kepada pengguna sistem yang melakukan permintaan pergantian *password*	Pegawai Bagian TIK kemudian mengirimkan email untuk mahasiswa berdasarkan kolom email yang ada pada formulir
5	Pengguna Sistem kemudian mengakses *link* dan menginputkan *password* baru	Berhasil dilakukan oleh mahasiswa
6	Sistem selanjutnya melakukan verifikasi dan validasi inputan *password* baru	Sistem berhasil memverifikas password baru dan password ter-*record* dalam database mahasiswa

2. Pengujian SOP Pengelolaan dan Pencegahan Malware

Tanggal Pengujian : 4 januari 2016
Pelaksana : Yusuf Efendi, Pegawai Bagian TIK
Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 3. Hasil pengujian SOP Pengelolaan dan Pengcegahan Malware

No	Aktivitas	Keterangan
Proses Pencegahan Malware		
1	Menyediakan perangkat/fasilitas anti malware : anti virus, anti spyware, spam filerting dan web contenct filtering	Telah disediakan oleh Bagian TIK
2	Memastikan bahwa perangkat lunak *anti malware* segera diinstalasi pada setiap perangkat komputer dan *server*	Telah dilakuan oleh Bagian TIK melalui sistem terpusat
3	Melakukan pelaporan tindak preventif dengan mengisi formulir laporan Tindak Preventif Pencegahan Malware	Formulir ini dihilangkan karena tidak sesuai dengan kondisi yang ada, formulir ini

		kemudian diganti dan digabungkan dengan formulir laporan gangguan sistem informasi menjadi ***formulir laporan gangguan keamanan informasi***
Proses Penangan Gangguan Malware *Proses ini dilakukan dilakuakn terbatas*		
1	Sistem menampilkan beberapa indikasi umum terjadinya gangguan malware,	Proses ini tidak disimulasikan karena keterbatasan media untuk uji coba *malware*
2	Pegawai Bagian TIK melakukan pelaporan insiden/gangguan keamanan informasi dalam formulir Laporan Gangguan Keamanan Informasi	Proses ini dilakukan terbatas dan hanya berdasarkan pada log sistem E-Scan
3	Mengkomunikasikan insiden/gangguan dengan administrator baik sistem, jaringan maupun aplikasi terkait untuk menentukan rencana penanggulangan insiden/gangguan	Proses ini tidak dilakukan karena tidak melakukan uji coba *malware*
4	Menyediakan sarana penangan malware	Bagian TIK telah memiliki sarana atau software dalam penangan malware
5	Apabila gangguan telah berhasil diatasi, Pegawai Bagian TIK kemudian melaporkan status penyelesaian insiden/gangguan a) Melaporkan status penyelesaian insiden/gangguan keamanan sistem informasi kepada pihak terkait.	Tidak dilakukan karena uji coba malware tidak dilakukan dan terbatas pada analisis log sistem pada anti virus E-Scan

	b) Melakukan pembaharuan pelaporan pada formulir Laporan Gangguan Kemanan Informasi	

3. Pengujian SOP Pengelolaan Gangguan Sistem Informasi

Tanggal Pengujian : 4 Januari 2016
Pelaksana : Yusuf Effendi, Pegawai Bagian TIK
Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 4. Hasil pengujian SOP Pengelolaan Gangguan Sistem Informasi

No	Aktivitas	Keterangan
Proses Penanganan Gangguan Serangan Hacker		
1	Sistem menampilkan beberapa indikasi umum terjadinya gangguan serangan hacker	Dilakukan terbatas pada kajian pada hasil pengujian scanning sistem informasi kepegawian (online-staff.perbanas.ac.id)
2	Melakukan pelaporan insiden/gangguan keamanan informasi dalam formulir Laporan Gangguan Keamanan Informasi	Dilakukan dengan baik pada formulir yang tersedia
3	Mengkomunikasikan insiden/gangguan dengan administrator baik sistem, jaringan maupun aplikasi terkait untuk menentukan rencana penanggulangan insiden/gangguan	Tidak dilakukan karena tidak melakukan pengujian/simulasi serangan *hacker*
4	Melakukan analisis keamaan sistem informasi dengan melakukan pemindaian/*scanning* secara berkala terhadap perangkat pengolah informasi untuk menemukan kelemahan sistem sesuai dengan instruksi kerja pemindaian perangkat pengolah informasi.	Tidak dilakukan karena tidak melakukan pengujian/simulasi serangan *hacker*

5	Mencatat hasil analisis gangguan sistem informasi yang berupa laporan yang berupa : a) Analisis dan penyusunan tindakan perbaikan (*corrective*) lanjutan yang perlu diterapkan untuk menghindari terulangnya kejadian serupa b) Penerapan inisiatif tindakan pencegahan (*preventive*) terhadap area yang memiliki potensi rentan terhadap gangguan/insiden sejenis	Tidak dilakukan karena tidak melakukan pengujian/simulasi serangan *hacker*
6	Melakukan peloporan status penyelesaian insiden/gangguan keamanan informasi	Tidak dilakukan karena tidak melakukan pengujian/simulasi serangan *hacker*
7	Melakukan pembaharuan pelaporan pada formulir Laporan Gangguan Kemanan Sistem Informasi	Dilakukan terbatas berdasarkan hasil scanning sistem informasi kepegawian (online-staff.perbanas.ac.id)

4. Pengujian SOP Back up dan Restore

Tanggal Pengujian : 4 Januari 2016
Pelaksana :Yusuf Effendi, Pegawai Bagian TIK
Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 5. Hasil pengujian SOP Back up dan Restore

No	Aktivitas	Keterangan
Proses Back up data secara berkala		
1	Melakukan setting penjadwalan backup dan memastikan penjadwalan	Dilakukan dengan baik melalui aplikasi

	backup data sesuai dengan ketentuan penjadwalan backup data : - Backup data secara otomatis untuk server Sistem informasi (SISFO) pada pukul 12.00 dan 21.00 - Backup data secara otomatis untuk server File Server pada pukul 19.00	crowntab
2	Mengelola *log* pada sistem *back up* data untuk memastikan keberhasilan data yang ter-*back up* dan data yang tidak berhasil di-*back up*	Dilakukan dengan baik dengan melihat hasil back up pada direktori yang telah ditentukan
3	Membuat laporan pada formulir Log Backup Data	Dilakukan dengan baik pada formulir log back up data
Proses Restore data		
1	Menentukan database yang akan dilakukan restore	Dilakukan dengan baik yaitu pada database mahasiswa pada media back up dbase sisfo
2	Menentukan jadwal pelaksanaan restore data	Dilakukan dengan baik pada aplikasi crowntab
3	Melakukan proses restore data	Proses dalam sistem berjalan dengan baik
4	Menganalisis hasil restore data **Successful** Adminitrator mendokumentasikan pelaksanaan retore data dengan mengisi Formulir Restore Data **Failed** Administrator melakukan kembali proses restore data (kembali ke poin 3)	Hasil restore data ***successful***, sehingga lanjut pada poin 5
4a	Mendokumentasikan pelaksanaan retore data dengan mengisi Formulir	Dilakukan dengan baik pada formulir

	Restore Data	restore data
4b	Melakukan kembali proses restore data (kembali ke poin 3)	Tidak perlu dilakukan
Proses Uji Coba Back up Data secara berkala		
1	Melakukan uji back up data	Uji coba back up dilakukan dengan baik dengan menggunakan aplikasi ***Putty*** dan data yang di backup adalah database mahasiswa pada media back up dbase sisfo
2	Melakukan set up persiapan uji coba back up data	Dilakukan dengan baik pada aplikasi ***Putty*** dan penjadwalan back up pada aplikasi ***crowntab*** sesuai dengan Intruksi kerja Back up dan Inturksi kerja Restore
3	Melakukan uji coba back up data pada media back up yang telah disiapkan	Dilakukan pada media back up dbase sisfo
4	Administrator menganalisis log back up data **Status Failed** -Administrator melakukan kembali proses uji coba back up data pada poin 2 **Status Successful** -Administrator melakukan pengecekan kesesuaian data yang berhasil ter-back up -Administrator memastikan tidak ada data yang corrupt	Status ***successful*** sehingga melanjutkan pada poin 5

a1	Melakukan kembali proses uji coba back up data pada poin 2	Tidak perlu dilakukan
b1	Melakukan pengecekan kesesuaian data yang berhasil ter-back up	Dilakukan dengan baik
b2	Membuat laporan pada formulir log back up data	Dilakukan dengan baik pada formulir log back up data

5. Pengujian Proteksi Lingkungan Server

Tanggal Pengujian : 4 Januari 2016
Pelaksana : Rizky Andriawan, Pegawai Bagian TIK
Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 6. Hasil pengujian SOP Proteksi Lingkungan Server

No	Aktivitas	Keterangan
Proses Pengamanan Lingkungan Server		
1	Melakukan pemeliharaan terhadap server dengan memastikan keamanan di sekitar ruang server	Dilakukan dengan baik
2	Mengecek proteksi server pada ruang server	Dilakukan dengan baik
3	Mengisi formulir pemeliharaan server yang berisi *checklist* keamanan server sesuai dengan temuan kondisi pada saat itu.	Dilakukan dengan baik pada formulir pemeliharaan server
	Kasie TIK selalu melakukan validasi formulir pemeliharaan server	Tidak dilakukan dalam uji coba
a	Apabila terdapat kondisi yang tidak sesuai, maka Kasie TIK memerintahkan untuk melakukan tindakan korektif (*corrective*)	Tidak dilakukan dalam uji coba
b	Memperbaharui Formulir Pemeliharaan Server dan melakukan validasi kepada Kasie TIK	Tidak dilakukan dalam uji coba

6. Pengujian Akses Ruang Server

Tanggal Pengujian : 4 Januari 2016
Pelaksana : Rizky Andriawan, Pegawai Bagian TIK
Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 7. Hasil pengujian SOP Akses Ruang Server

No	Aktivitas	Keterangan
Proses Akses ke dalam ruang server		
1	Memastikan bahwa ruang server memiliki kunci untuk mengamankan ruang dari akses yang tidak terautorisasi	Dilakukan dengan baik
2	Memastikan bahwa setiap pintu tertutup/terkunci dengan benar setelah masuk/keluar ruang server.	Dilakukan dengan baik
3	Civitas akademik dan pihak eksternal yang akan mengakses ruang server harus menunjukan identitas dan telah memiliki izin langsung dari administrator	Dilakukan dengan baik, pihak eksternal yang masuk kedalam ruang server adalah mahasiswa ITS yang telah memiliki ijin untuk melakukan penelitian di STIE Perbanas dan harus meninggalkan KTM pada Pegawai Bagian TIK yang bertanggung jawab
4	Meminta identitas kepada civitas akademik dan pihak eksternal dan memastikan identitas telah benar dan valid	Dilakukan dengan baik
5	Civitas akademika dan pihak eksternal kemudian harus mengisi *Log book* sebelum masuk ke dalam ruang server	Dilakukan dengan baik sebelum memasuki ruang

		server pada formulir log akses ruang server pengunjung
6	Administrator harus selalu mendampingi civitas akademika atau pihak eksternal selama berada di ruang server	Dilakukan dengan baik
7	Melakukan *review* dan validasi secara berkala minimal 6 (enam) bulan sekali terhadap aktivitas akses ruang server beradasarkan *Log* daftar pengunjung ruang server	Tidak dilakukan dalam uji coba

Hasil Pengujian Formulir

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-01	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PERBAIKAN SISTEM INFORMASI	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

Laporan Perbaikan Sistem Informasi
Tanggal ..4.. **Bulan** Januari **Tahun** ..2016..

Tanggal	4-1-2015	Pukul	08.00
Nama	Hariadi Tutanto		
Unit Kerja	ICT		
Menu & Submenu yang diperbaiki	Reset Password staff		
Uraian Perbaikan	Mohon diberikan fasilitas strong Password untuk reset Password Dosen dan karyawan		
REALISASI KERJA			
Analisis/Tinjuan (*disii oleh TIK*)	Masih belum ada fasilitas strong Password di aplikasi staff		
Perbaikan (*disii oleh TIK*)	menambah fasilitas strong password di aplikasi staff		
Tanggal Mulai	4-1-2015	Pukul	08.30
Tanggal Selesai	4-1-2015	Pukul	12.00

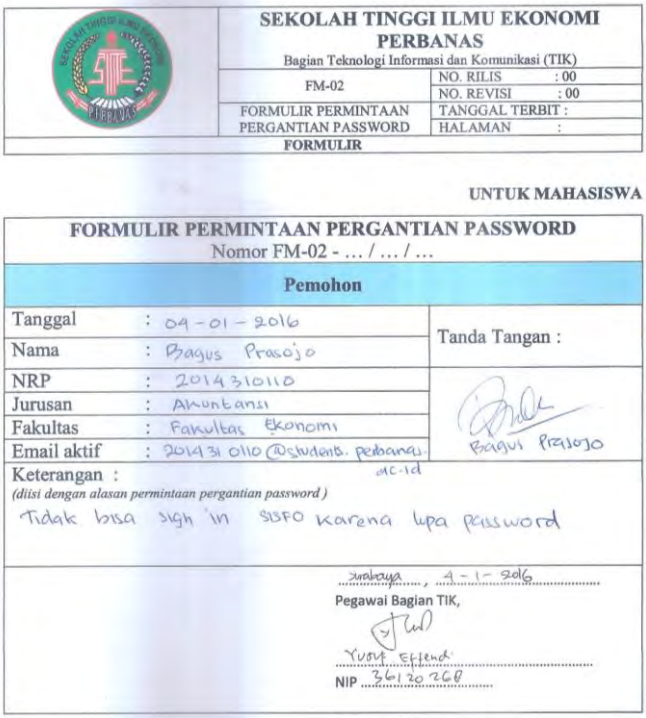
Mengetahui,
Kepala Bagian TIK

.....
NIP .....

Surabaya, 4-01-2016
Pegawai Bagian TIK,

Yusuf Effendi
NIP 36120268

Gambar G.1. Pengujian Formulir Perbaikan Sistem Informasi



SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)		
FM-02	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR PERMINTAAN PERGANTIAN PASSWORD	TANGGAL TERBIT	:
	HALAMAN	:
FORMULIR		

UNTUK MAHASISWA

FORMULIR PERMINTAAN PERGANTIAN PASSWORD
Nomor FM-02 - ... / ... / ...

Pemohon

Tanggal	: 04-01-2016	Tanda Tangan :
Nama	: Bagus Prasojo	
NRP	: 2014310110	
Jurusan	: Akuntansi	
Fakultas	: Fakultas Ekonomi	
Email aktif	: 2014310110@students.perbanas.ac.id	Bagus Prasojo

Keterangan :
(diisi dengan alasan permintaan pergantian password)
Tidak bisa sign in SISFO karena lupa password

Surabaya, 4-1-2016
Pegawai Bagian TIK,

Yusuf Effendi
NIP 36120268

Gambar G.2. Hasil Pengujian Formulir Perminataan Pergantian Password oleh Mahasiswa

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-08	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR RESTORE DATA	TANGGAL TERBIT : HALAMAN :
FORMULIR		

FORMULIR RESTORE DATA	
Tanggal Backup	*Tanggal melakukan backup data* 4-1-2016
Nama Staf	*Nama pegawai yang melakukan restore data* Yuclf. Effendi
Sumber Data	*Keterangan terkait sumber data backup* Perbanas-040116-230001 backup
Data yang di back up	*Keterangan terkait data yang di backup* Perbanas-skripsi-its
Tipe Back up	☑ **Full Backup** ☐ **Partial/Incremental Backup**
Media Back up	*Media yang digunakan untuk penyimpanan data backup* Obase sicfo
Recovery point of objective	*Keterangan bagian data yang akan di restore setelah pemulihan layanan teknologi informasi*
Catatan : Untuk uji Coba	
	(Lokasi), (Tanggal – Bulan – Tahun) Pegawai Bagian TIK, Yuclf Effendi (*Nama Lengkap Pegawai Bagian TIK*) NIP 361202268

Gambar G.3. Hasil Pengujian Formulir Restore Data

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-07	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LOG BACKUP DATA	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Log Backup Sheet
Bulan ..Januari... **Tahun** ..2016.....

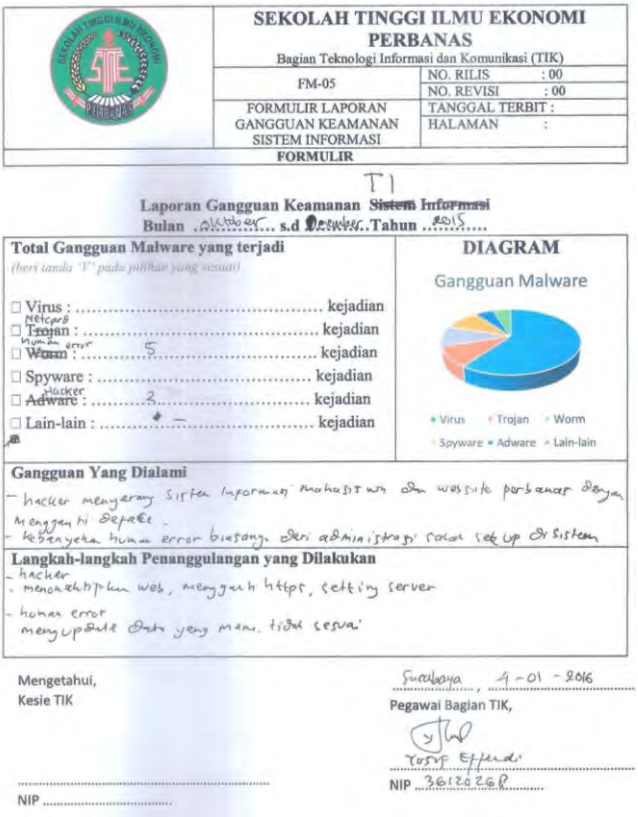
Tanggal	Waktu	Metode Backup	Jumlah Media	Nama Media Backup	Isi Media Backup	Status Backup	Keterangan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
04-1-2015	13:56	Full Database	1	server dbase SISFO	database mahasiswa	sukses	

Keterangan Pengisian :
(1) Diisi dengan tanggal backup
(2) Diisi dengan waktu backup berhasil dilakukan (*backup completed*)
(3) Diisi dengan metode backup yang dilakukan
(4) Diisi dengan jumlah media backup
(5) Diisi dengan nama media backup
(6) Diisi dengan keterangan data/file dalam media backup
(7) Diisi dengan status backup
(8) Diisi dengan keterangan dari status backup (data yang berhasil/data yang tidak di-*backup*, error yang terjadi, dll)

Surabaya, 4-01-2016
Pegawai Bagian TIK,

Yusuf Effendi
NIP 3C120268

Gambar G.4. Hasil Pengujian Formulir Log Backup Sheet



SEKOLAH TINGGI ILMU EKONOMI PERBANAS
Bagian Teknologi Informasi dan Komunikasi (TIK)

FM-05	NO. RILIS : 00 NO. REVISI : 00
FORMULIR LAPORAN GANGGUAN KEAMANAN SISTEM INFORMASI	TANGGAL TERBIT : HALAMAN :

FORMULIR

T1

Laporan Gangguan Keamanan ~~Sistem Informasi~~
Bulan ..Oktober.. s.d Desember..Tahun ..2015....

Total Gangguan Malware yang terjadi
(beri tanda 'V' pada jawaban yang sesuai)

- ☐ Virus : ..... kejadian
- ☐ Trojan : ..... kejadian (Netcard)
- ☐ Worm : 5 kejadian (human error)
- ☐ Spyware : ..... kejadian
- ☐ ~~Adware~~ : 3 kejadian (hacker)
- ☐ Lain-lain : — kejadian

DIAGRAM

Gangguan Malware

Virus Trojan Worm Spyware Adware Lain-lain

Gangguan Yang Dialami

- hacker menyerang sistem informasi mahasiswa dan website perbanas dengan menggunakan depe€e.
- kebanyakan human error biasanya dari administrator server set up dr sistem

Langkah-langkah Penanggulangan yang Dilakukan

- hacker
  - menonaktifkan web, menggunakan https, setting server
- human error
  menyupdate data yang mana tidak sesuai

Mengetahui,
Kesie TIK

.....
NIP .....

Surabaya, 4-01-2016
Pegawai Bagian TIK,

Yosep Effendi
NIP 36120268

Gambar G.5. Hasil Pengujian Formulir Laporan Gangguan Keamanan Informasi

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-11	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LOG DAFTAR PENGUNJUNG	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

Log Akses Pengunjung dalam Ruang Server
Tanggal .....09..... Bulan ...01.....
Tahun ..2016....

No	Tanggal	Waktu		Nama Lengkap	Instansi/Organisasi	Tujuan Kedatangan	Perijinan Akses	Keterangan	Tanda Tangan
		Masuk	Kelaur						
	(1)	(2)	(3)	(4)	(5)	(6)	☐	(7)	(8)
1.	09/01/2016	09.00	09.05	Sabrina L. Putri	ITS	Uji Coba SOP	☑		
2	09/01/2016	09.00	09.05	Aulia N F	ITS	Uji Coba SOP	☑		
							☐		

Keterangan Pengisian :
(1) Diisi dengan tanggal akses
(2) Diisi dengan waktu masuk pengunjung dalam ruang server
(3) Diisi dengan waktu keluar pengunjung dalam ruang server
(4) Diisi dengan nama lengkap pengunjung, sesuai dengan kartu identitas (KTP/KTM,dll)
(5) Diisi dengan Instansi/Organisasi yang mewakangi pengunjung
(6) Diisi dengan keterangan tujuan atau keperluan kedatangan pengunjung
(7) Diisi dengan keterangan perijinan akses pengunjung (surat perijinan resmi, dll)

Surabaya, 9 - 1 - 2016
Pegawai Bagian TIK,
Rusky Andriawan
NIP 36140597

Gambar G.6. Hasil Pengujian Formulir Log Akses Pengunjung dalam Ruang Server

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-09	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PEMELIHARAAN FISIK SERVER	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

Laporan Pemeliharaan Fisik Server
Bulan ~~November~~ Oktober **s.d** ~~Juni~~ Desember **Tahun** 2017

Checklist Pemeliharaan Fisik Server

Kondisi Ruang Server
- ☑ Berada pada lingkungan yang aksesnya terbatas oleh publik
- ☑ Berada pada lingkungan yang aman dari bahaya genangan air/banjir
- ☑ Tinggi ruang untuk penempatan rak minimal 2,5 meter
- ☑ Suhu udara dalam ruangan berada dalam batas 20^0-25^0
- ☑ kelembaban relative dalam ruangan antara 40 – 45 %
- ☑ Kabel jaringan telah diberi label yang sesuai dan jelas
- ☑ Jaringan kabel data terpisah dari jaringan kabel listrik dengan jarak minimal 3 (tiga) meter

Fasilitas Pendukung dalam Ruang Server
- ☑ Tersedia Alarm api dan asap
- ☑ Tersedia Alat Pengukur Suhu dan Kelembapan
- ☑ Tersedia *Uninterruptible Power Supply (UPS)*
- ☑ Tersedia Generator Listrik
- ☑ Tersedia *Air Conditioning System*
- ☑ Tersedia *Log book* untuk Akses Ruang Server

Keterangan Tambahan :

Surabaya, 4-1-2018
Pegawai Bagian TIK,

Rusty Andriawan
NIP 36140397

Gambar G.7. Hasil Pengujian Formulir Pemeliharaan server

Konfirmasi hasil Verifikasi dan Validasi oleh Pihak STIE Perbanas

Berikut ini adalah lampiran verifikasi dan validasi pihak STIE Perbanas terkait proses analisis risiko, proses perancangan SOP dan isi dokumen akhir SOP Keamanan Data STIE Perbanas.

Verifikasi dan validasi ini dilakukan kepada Kasie TIK STIE Perbanas untuk memastikan hasil analisis risiko yang termasuk didalamnya penilaian risiko, evaluasi risiko dan mempriortitaskan risiko telah sesuai dengan kondisi STIE Perbanas.

SURAT KONFIRMASI
Kesesuaian Hasil Analisis Risiko TI untuk STIE Perbanas Surabaya

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Aulia Nur Fatimah
NRP : 5212100058
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis risiko TI untuk STIE Perbanas kepada Kasie Teknologi Informasi dan Komunikasi (TIK) TIK STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis risko TI untuk STIE Perbanas yang dibuat secara khusus, sesuai dengan kebutuhan STIE Perbanas.

Atas perhatian dan kesediaan Bapak/Ibu Pimpinan, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI Surabaya, 6 November 2015	
Mengetahui, Kasie Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas	Peneliti
Hariadi Yutanto, S.Kom, M.Kom	Aulia Nur Fatimah

Gambar G.8. Verifikasi dan validasi kesesuaian analisis risiko oleh Kasie TIK STIE Perbanas

Verifikasi dan validasi ini dilakukan kepada Kasie TIK STIE Perbanas untuk memastikan perancangan SOP Keamanan Data yang akan disusun oleh peneliti sesuai dengan kebutuhan STIE Perbanas.

SURAT KONFIRMASI
Kesesuaian Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Aulia Nur Fatimah
NRP : 5212100058
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian prosedur dalam Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas kepada Kasie Teknologi Informasi dan Komunikasi (TIK) TIK STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi prosedur yang dibuat secara khusus dalam Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas, sesuai dengan kebutuhan STIE Perbanas.

Atas perhatian dan kesediaan Bapak/Ibu Pimpinan, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI Surabaya, 14 Desember 2015	
Mengetahui, Kasie Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas	Peneliti
Hariadi Yutanto, S.Kom, M.Kom	Aulia Nur Fatimah

Gambar G.9. Verifikasi dan validasi kesesuaian prosedur dalam dokumen SOP Keamanan Data oleh Kasie TIK STIE Perbanas

Verifikasi dan validasi ini dilakukan kepada Pegawai Bagian TIK STIE Perbanas terkait pengujian SOP (validasi skenarioisasi) dilakukan dengan baik.

SURAT KONFIRMASI

Kesesuaian Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Aulia Nur Fatimah
NRP : 5212100058
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian prosedur dalam Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas kepada Pegawai Fungsional Bagian Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil pengujian prosedur yang dibuat secara khusus dalam Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas, telah sesuai dengan kebutuhan STIE Perbanas.

Atas perhatian dan kesediaan Bapak/Ibu, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI Surabaya, 4 Januari 2016	
Mengetahui, Staf Fungsional Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas	Peneliti
Ruky Andriawan	Aulia Nur Fatimah

Gambar G.10. Verifikasi dan validasi Pengujian SOP oleh Pegawai Bagian TIK

SURAT KONFIRMASI

Kesesuaian Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Aulia Nur Fatimah
NRP : 5212100058
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian prosedur dalam Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas kepada Pegawai Fungsional Bagian Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil pengujian prosedur yang dibuat secara khusus dalam Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas, telah sesuai dengan kebutuhan STIE Perbanas.

Atas perhatian dan kesediaan Bapak/Ibu, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI Surabaya, 4 Januari 2016	
Mengetahui, Staf Fungsional Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas	Peneliti
Yusuf Effendi	Aulia Nur Fatimah

Gambar G.11. Verifikasi dan validasi Pengujian SOP oleh Pegawai Bagian TIK

Verifikasi dan validasi ini dilakukan kepada Pembantu Ketua 1 Bidang Akademik STIE Perbanas untuk memastikan kesesuaian Dokumen produk *Standard Operating Procedure* (SOP) Keamanan Data telah sesuai dengan kondisi STIE Perbanas.

SURAT KONFIRMASI
Kesesuaian Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Aulia Nur Fatimah
NRP : 5212100058
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas kepada Pembantu Ketua 1 Bidang Akademik STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi isi Dokumen *Standard Operating Procedure* (SOP) Keamanan Data untuk STIE Perbanas yang dibuat secara khusus, sesuai dengan kebutuhan STIE Perbanas.

Atas perhatian dan kesediaan Bapak/Ibu Pimpinan, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI Surabaya, 14 Desember 2015	
Mengetahui, Pembantu Ketua 1 Bidang Akademik STIE Perbanas	Peneliti
Dr. Drs. Emanuel Kristanto, MM	Aulia Nur Fatimah

Gambar G.12. Verifikasi dan Validasi Dokumen Produk SOP Keamanan Data oleh Pembantu Ketua 1 Bidang Akademik STIE Perbanas

Halaman ini sengaja dikosongkan

LAMPIRAN H
LAMPIRAN FORMULIR

Berikut ini adalah lampiran formulir yang dihasilkan dalam penelitian.

Formulir Perbaikan Sistem Informasi

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-01	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PERBAIKAN SISTEM INFORMASI	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

Laporan Perbaikan Sistem Informasi

Tanggal ..... Bulan .....Tahun .....

Tanggal		Pukul	
Nama			
Unit Kerja			
Menu & Submenu yang diperbaiki			
Uraian Perbaikan			
REALISASI KERJA			
Analisis/Tinjuan *(disii oleh TIK)*			
Perbaikan *(disii oleh TIK)*			
Tanggal Mulai		Pukul	
Tanggal Selesai		Pukul	

Mengetahui,
Kepala Bagian TIK

(Nama Lengkap Kepala Bagian TIK)
NIP .....

(Lokasi), (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)
NIP .....

Formulir Permintaan Pergantian Password Pegawai

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-02	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PERMINTAAN PERGANTIAN PASSWORD	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

UNTUK PEGAWAI

FORMULIR PERMINTAAN PERGANTIAN PASSWORD Nomor FM-02 - ... / ... / ...	
Pemohon	
Tanggal :	Tanda Tangan :
Nama :	
NIP :	
Jabatan :	
Unit Kerja :	
Email aktif :	
Keterangan *(diisi dengan alasan permintaan pergantian password)*	
(Lokasi), *(Tanggal – Bulan – Tahun)* Pegawai Bagian TIK, (*Nama Lengkap Pegawai Bagian TIK*) NIP	

Formulir Permintaan Pergantian Passwrod Mahasiswa

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-02	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PERMINTAAN PERGANTIAN PASSWORD	TANGGAL TERBIT : HALAMAN :
FORMULIR		

UNTUK MAHASISWA

FORMULIR PERMINTAAN PERGANTIAN PASSWORD Nomor FM-02 – ... / ... / ...	
Pemohon	
Tanggal :	Tanda Tangan :
Nama :	
NRP :	
Jurusan :	
Fakultas :	
Email aktif :	
Keterangan *(diisi dengan alasan permintaan pergantian password)*	
(Lokasi), (Tanggal – Bulan – Tahun) Pegawai Bagian TIK, *(Nama Lengkap Pegawai Bagian TIK)* NIP	

Formulir Evaluasi Sistem Informasi

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-04	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR EVALUASI SISTEM INFORMASI	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Laporan Pemantauan dan Evaluasi Sistem Informasi
Bulan ..... s.d .....Tahun .....

No	Objek/Data/Sistem yang dipanatau	Kelemahan Yang Ditemukan	Tindakan Perbaikan (*Corrective*)	Tindakan Pencegahan (*Preventive*)	Tanggal Pemantauan	
					Mulai	Selesai
1	*(1)*	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*
(dst)						

(Lokasi) , (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(*Nama Lengkap Pegawai Bagian TIK*)
NIP .....

Keterangan Pengisian :
(1) Diisi dengan nama perangkat lunak atau data yang dipantau.
(2) Diisi dengan kelemahan data atau sistem terhadap gangguan malware
(3) Diisi dengan tindakan perbaikan yang telah diimplementasikan pada objek/data/sistem yang dipantau.
(4) Diisi dengan tindakan pencegahan secara teknis maupun manajemen yang telah diimplementasikan

Formulir Log Back up Data

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-07	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LOG BACKUP DATA	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Log Backup Sheet

Bulan ..... Tahun .....

Tanggal	Waktu	Metode Backup	Jumlah Media	Nama Media Backup	Isi Media Backup	Status Backup	Keterangan
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*	*(8)*

Keterangan Pengisian :

(5) Diisi dengan tanggal backup
(6) Diisi dengan waktu backup berhasil dilakukan (backup error/down)
(7) Diisi dengan metode backup yang dilakukan
(8) Diisi dengan jumlah media backup
(9) Diisi dengan nama media backup
(10) Diisi dengan keterangan isi data/file dalam media backup
(11) Diisi dengan status backup
(12) Diisi dengan keterangan dari status backup (data yang berhasil/data yang tidak dibackup, error yang terjadi, dll)

(Lokasi) , (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)
NIP .....

Formulir Log Pegawai

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-09	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LOG PEGAWAI	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Log Akses Pegawai dalam Ruang Server
Tanggal ..... Bulan .....
Tahun .....

Tanggal	Waktu		Nama Lengkap	Unit Kerja	Tujuan Kedatangan	Perijinan Akses	Keterangan	Tanda Tangan
	Masuk	Kelaur						
(1)	(2)	(3)	(4)	(5)	(6)	☐	(7)	(8)
						☐		
						☐		
						☐		

Keterangan Pengisian :
(1) Diisi dengan tanggal akses
(2) Diisi dengan waktu masuk pegawai dalam ruang server
(3) Diisi dengan waktu keluar pegawai dalam ruang server
(4) Diisi dengan nama lengkap pegawai sesuai dengan kartu identitas (KTP/KTM dll)
(5) Diisi dengan Unit kerja yang menaungi pegawai
(6) Diisi dengan keterangan tujuan atau kepentingan kedatangan pegawai
(7) Diisi dengan keterangan perijinan akses pegawai (surat perijinan resmi dll)
(8) Diisi dengan tanda tangan pegawai

(Lokasi) , (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)
NIP .....

Formulir Log Pengunjung

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-10	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LOG DAFTAR PENGUNJUNG	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Log Akses Pengunjung dalam Ruang Server
Tanggal ..... Bulan .....
Tahun .....

No	Tanggal	Waktu		Nama Lengkap	Instansi/Organisasi	Tujuan Kedatangan	Perijinan Akses	Keterangan	Tanda Tangan
		Masuk	Kelaur						
	(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	☐	*(7)*	*(8)*
							☐		
							☐		
							☐		

Keterangan Pengisian :
(9) Diisi dengan tanggal akses
(10) Diisi dengan waktu masuk pengunjung dalam ruang server
(11) Diisi dengan waktu keluar pengunjung dalam ruang server
(12) Diisi dengan nama lengkap pengunjung sesuai dengan kartu identitas (KTP/KTM dll)
(13) Diisi dengan Instansi/Organisasi yang mewakili pengunjung
(14) Diisi dengan keterangan tujuan atau keperluan kedatangan pengunjung
(15) Diisi dengan keterangan perijinan akses pengunjung (untuk perijinan/resmi, dll)
(16) Diisi dengan tanda tangan pengunjung

(Lokasi), (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)
NIP .....

Formulir Laporan Gangguan Keamanan Informasi

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-04	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LAPORAN GANGGUAN KEAMANAN INFORMASI	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

Gangguan Keamanan Sistem Informasi
Bulan ..... Tahun .....

No	Tanggal	Gangguan Kemanan Yang terjadi	Tindakan Penyelesaian	Tanggal Penyelesaian		Status Gangguan	Staf yang Menangani
				Mulai	Selesai		
1	*(1)*	*(2)*	*(3)*	*(5)*	*(6)*		
(dst)							

Laporan Gangguan Keamanan Informasi
Bulan ..... s.d .....Tahun .....

Total Gangguan Keamanan Informasi yang terjadi *(beri tanda 'v' pada pilihan yang sesuai)*			**DIAGRAM**
☐ Virus	.....	Kejadian	
☐ Netcard	.....	Kejadian	
☐ Hacker	.....	Kejadian	
☐ human Error	.....	Kejadian	
☐ Lain-lain	.....	Kejadian	

Gangguan Yang Dialami
(uraikan per poin)

Langkah-langkah Penanggulangan yang Dilakukan
(uraikan per poin)

Mengetahui,
Kasie TIK

(Nama Lengkap Kepala Bagian TIK)
NIP .....

(Lokasi), (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)
NIP .....

Formulir Klasifikasi Data

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-06	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR KLASIFIKASI DATA	TANGGAL TERBIT : HALAMAN :
FORMULIR		

FORMULIR DAFTAR KLASIFIKASI DATA

Periode ..... Tahun .....

KLASIFIKASI DATA ATAU INFORMASI MENURUT TINGKAT SENSITIVITAS

Klasifikasi Data	Keterangan
Sangat Rahasia (*Strictly Confidential*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian bagi STIE Perbanas
Rahasia (*Confidential*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan atau menurunkan citra dan reputasi STIE Perbanas
Terbatas (*Internal Use Only*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak sah atau tidak berhak akan mengganggu kelancaran kegiatan tetapi tidak akan mengganggu citra dan reputasi STIE Perbanas
Umum (*Public*)	Data yang secara sengaja disediakan untuk dapat diketahui umum dan tidak akan menggangu privasi atau keamanan organsiasi apabila jatuh ke tangan yang tidak berhak

KLASIFIKASI DATA ATAU INFORMASI MENURUT TINGKAT SENSITIVITAS

Tingkatan Kritikalitas Data	RPO	MTD	Penanganan		
			Full Backup	Differential/ Incremental Backup	Lokasi Penyimpanan
Tinggi	Maksimal 24 jam	Maksimal 24 jam	1 x Seminggu	Maksimal 24 jam	*Off Site* dan *On Site*
Sedang	Maksimal 1 minggu	Maksimal 1 minggu	1 x Sebulan	Maksimal 1 Minggu	*Off Site*
Rendah	> 1 Minggu	> 1 Minggu	Minimal 1 x 3 Bulan	> 1 Minggu	*Off Site*

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-04	NO. REVISI : 00
		NO. REVISI : 00
	FORMULIR KLASIFIKASI DATA	TANGGAL TERBIT
		HALAMAN
FORMULIR		

FORMULIR DAFTAR KLASIFIKASI DATA

Periode ..... Tahun .....

DAFTAR KLASIFIKASI DATA ATAU INFORMASI

No	Jenis Data	Klasifikasi	Kritikalitas
1.	Data Demografi		
	3.5 Data Mahasiswa	*Rahasia*	*Tinggi*
	3.6 Data Dosen	*Rahasia*	*Tinggi*
2.	(Klasifikasi Kelompok Data)		
	a. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	b. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	c. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	d. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	e. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	f. *(data)*	*(klasifikasi)*	*(kritikalitas)*
2.	(Klasifikasi Kelompok Data)		
	a. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	b. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	c. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	d. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	e. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	f. *(data)*	*(klasifikasi)*	*(kritikalitas)*
3.	(Klasifikasi Kelompok Data)		
	a. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	b. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	c. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	d. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	e. *(data)*	*(klasifikasi)*	*(kritikalitas)*
	f. *(data)*	*(klasifikasi)*	*(kritikalitas)*

(Lokasi), (Tanggal) – Bulan – Tahun)
Mengetahui,
Ketua STIE Perbanas

(Nama Lengkap Ketua STIE Perbanas)
NIP:.....

Formulir Restore Data

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-07	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR RESTORE DATA	TANGGAL TERBIT : HALAMAN
FORMULIR		

FORMULIR RESTORE DATA	
Tanggal Backup	*Tanggal melakukan backup data*
Nama Staf	*Nama pegawai yang melakukan restore data*
Sumber Data	*Keterangan terkait sumber data backup*
Data yang di back up	*Keterangan terkait data yang di backup*
Tipe Back up	☐ **Full Backup** ☐ **Partial/Incremental Backup**
Media Back up	*Media yang digunakan untuk penyimpanan data backup*
Recovery point of objective	*Keterangan bagian data yang akan di restore setelah penuilihan layanan teknologi informasi*
Catatan :	
	(Lokasi), (Tanggal – Bulan – Tahun) Pegawai Bagian TI*, *(Nama Lengkap Pegawai Bagian TIK)* NIP .....

Formulir Pemeliharaan server

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-08	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PEMELIHARAAN FISIK SERVER	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

Laporan Pemeliharaan Fisik Server

Bulan ..... s.d .....Tahun .....

Checklist Pemeliharaan Fisik Server

Kondisi Ruang Server

- ☐ Berada pada lingkungan yang aksesnya terbatas oleh publik
- ☐ Berada pada lingkungan yang aman dari bahaya genangan air/banjir
- ☐ Tinggi ruang untuk penempatan rak minimal 2,5 meter
- ☐ Suhu udara dalam ruangan berada dalam batas 20° - 25°
- ☐ kelembaban relative dalam ruangan antara 40 – 45 %
- ☐ Kabel jaringan telah diberi label yang sesuai dan jelas
- ☐ Jaringan kabel data terpisah dari jaringan kabel listrik dengan jarak minimal 3 (tiga) meter

Fasilitas Pendukung dalam Ruang Server

- ☐ Tersedia Alarm api dan asap
- ☐ Tersedia Alat Pengukur Suhu dan Kelembapan
- ☐ Tersedia *Uninterruptible Power Supply (UPS)*
- ☐ Tersedia Generator Listrik
- ☐ Tersedia *Air Conditioning System*
- ☐ Tersedia *Log book* untuk Akses Ruang Server

Keterangan Tambahan :

(Lokasi), (Tanggal – Bulan – Tahun)

Pegawai Bagian TIK,

(Nama Lengkap Pegawai Bagian TIK)

NIP .....

DAFTAR PUSTAKA

[1] ISO/IEC27001. (2013). *Information Technology - Security Techniques - Information Security Management System - Requirements.* Switzerland: ISO/IEC 2013.

[2] R Stup. (2002). Standard Operating Procedures: Managing The Human Variables. *National Mastitis Council Regional Meeting Proceedings*.

[3] Utomo, M., Noor Ali, A. H., & Affandi, I. (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik ITS Vol. 1 No 1*, A288 - A293 .

[4] Bertino, E., & Ferrari, E. (t.thn.). *Data Security.* Milano: Universit`a degli Studi di Milano.

[5] Stephen, F., & Solms, R. V. (2005). Real Time Information Integrity, System Integrity, Data Integrity adn Continous Assurance. *Computer & Security* , 604-613.

[6] ISO/IEC. (2005). *ISO/IEC 27002 Information Technology - Security Technique - Code of Practice for Information Security Management.* Switzerland: ISO/IEC.

[7] ITGI. (2007). *Cobit 4.1* . USA: IT Governance Institute.

[8] ITGI, & OGC. (2008). *Aligning Cobit 4.1, ITIL V3 and Cobit 27002 for Business Benefit, A Management Briefing from ITGI and OGC.* United States of America: ITGI, ISACA, OGC, TSO.

[9] Woodroof, J., & Searcy, D. (2001). *Continous Audit : Model Development and Implementation Within a Debt Covenant Compliance Domain.* Dipetik September 22, 2015, dari http://raw.rutgers.edu/: http://raw.rutgers.edu/continuousauditing/

[10] ISO 31000:2009, *Risk Management – Principles and Guidelines*

[11] George, W., & Hunter, R. (2007). *IT Risk : Turning Business Threats into Competitive Advantage.* Boston: Harvard Business School Press.

[12] Djohanputro, B. (2008). Manajemen Risiko Korporat. *Pendidikan dan Pembinaan Manajemen*.

[13] ISRMC. (2009). *Information Security Handbook*. Dipetik 10 14, 2015, dari ISHandbook bsewall: ishandbook.bsewall.com

[14] Violino, B. (2010, May 3). *CSO Security and Risk*. Retrieved 2014, from CSO: m.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience

[15] Panda, P. (2005). The OCTAVE Approach to Information Security Risk Assessment. *ISACA Journal Vol 4* .

[16] Christopher J. Alberts, S. B. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework.* Canada: Software Engineering Institure.

[17] Setiawan, A. (2008). EVALUASI PENERAPAN TEKNOLOGI INFORMASI DI PERGURUAN TINGGI SWASTA YOGYAKARTA DENGAN MENGGUNAKAN MODEL COBIT FRAMEWORK. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI 2008)*, A15 - A20.

[18] Ross, J., & Weill, P. (2004). *IT Governance, How Top Performers Manage IT Decision Rights for Superior Results.* Boston: Harvard Business School Press.

[19] Akyar, I. (2012). *Standard Operating Procedures (What Are They Good For)*. Turkey.

[20] KPRS. (2013). *Pedoman Pembuatan Standar Operating Procedures (SOPs)*. Jakarta: Pusat da Informasi.

[21] Suminar, B. (t.thn.). *Kriteria SOP Yang Baik.* Jakarta: Sistem Penjamin Mutu Internal Untuk Perguruan Tinggi.

[22] USEP. (2007). *Guidence for Preparing Standrd Operating Procedures (SOP).* Washington: Office of Environmental Information.

BIODATA PENULIS

Penulis bernama lengkap Aulia Nur Fatimah, biasa dipanggi Aulia. Penulis dilahirkan di Makassar pada hari Rabu Tanggal 11 Mei 1994 dan merupakan anak kedua dari tiga bersaudara. Penulis telah menempuh pendidikan formal di SDN Perak Barat II Perak Surabaya, tamat SMP di SMPN 1 Surabaya, tamat SMA di SMAN 15 Surabaya, dan kemudian masuk perguruan tinggi negeri ITS Surabaya pada jurusan Sistem Informasi (SI), Fakultas Teknologi Informasi pada tahun 2012. Adapun pengalaman yang didapatkan penulis selama di ITS, yakni berkecimpung di organsiasi kemahasiswaan di jurusan SI selama dua tahun kepengurusan. Penulis pernah menjalani kerja praktik di Perusahaan Telekomunikasi yaitu PT. Telkom Indonesia Divre V Surabaya pada Divisi IS Operational Support selama kurang lebih 1,5 bulan pada tahun 2015. Pengalaman yang didapatkan penulis selama bekerja praktik yaitu membangun sebuah aplikasi ICE Suramadu untuk pelaporan *event* Indihome di daerah Suramadu.

Pada pengerjaan Tugas Akhir di Jurusan Sistem Informasi ITS, penulis mengambil bidang minat Manajemen Sistem Informasi dengan topik Manajemen Risiko TI, Tata Kelola TI dan Keamanan Aset Informasi , yakni mengenai pembuatan dokumen Standard Operating Procedure (SOP) Kemanan Data yang mengacu pada kontrol kerangka kerja Cobit 5 dan ISO27002:2013 pada STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas di Surabaya. Untuk menghubungi penulis, dapat melalui email : aulialili58@gmail.com