TUGAS AKHIR - KS 141501

PENILAIAN DAN MITIGASI RISIKO KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 MENGGUNAKAN METODE PMBOK (STUDI KASUS : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

ASSESSMENT AND MITIGATION OF SECURITY RISK OF INFORMATION SYSTEM BASED ON ISO / IEC 27001: 2013 STANDARD USING PMBOK METHOD (CASE STUDY : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

Alif Satria Perdana
NRP 0521 14 4000 0034

Dosen Pembimbing 1:
Hanim Maria Astuti, S.Kom., M.Sc.

Dosen Pembimbing 2:
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

TUGAS AKHIR – KS 141501

PENILAIAN DAN MITIGASI RISIKO KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 MENGGUNAKAN METODE PMBOK (STUDI KASUS : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

Alif Satria Perdana
NRP 0521 14 4000 0034

Dosen Pembimbing 1:
Hanim Maria Astuti, S.Kom., M.Sc.

Dosen Pembimbing 2:
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

FINAL PROJECT – KS 141501

ASSESSMENT AND MITIGATION OF SECURITY RISK OF INFORMATION SYSTEM BASED ON ISO / IEC 27001: 2013 STANDARD USING PMBOK METHOD (STUDY CASE : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

Alif Satria Perdana
NRP 0521 14 4000 0034

Supervisor 1 :
Hanim Maria Astuti, S.Kom., M.Sc.

Supervisor 2 :
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom.

DEPARTMENT OF INFORMATION SYSTEMS
Faculty of Information Technology and Communication
Institute of Technology Sepuluh Nopember
Surabaya 2018

LEMBAR PENGESAHAN

PENILAIAN DAN MITIGASI RISIKO KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 MENGGUNAKAN METODE PMBOK (STUDI KASUS : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

TUGAS AKHIR
Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember

Oleh:
Alif Satria Perdana
0521 14 4000 0034

Surabaya, Juli 2018

KEPALA
DEPARTEMEN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

PENILAIAN DAN MITIGASI RISIKO KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 MENGGUNAKAN METODE PMBOK (STUDI KASUS : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

TUGAS AKHIR

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

Oleh :

Alif Satria Perdana
0521 14 4000 0034

Disetujui Tim Penguji : Tanggal Ujian : 03 Juli 2018
Periode Wisuda : September 2018

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

Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom. **(Pembimbing 2)**

Sholiq, S.T., M.Kom., M.SA **(Penguji 1)**

Ir. Achmad Holil Noor Ali, M.Kom. **(Penguji 2)**

PENILAIAN DAN MITIGASI RISIKO KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 MENGGUNAKAN METODE PMBOK (STUDI KASUS : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

Nama Mahasiswa : Alif Satria Perdana
NRP : 0521 14 4000 0034
Departemen : Sistem Informasi FTIK-ITS
Dosen Pembimbing 1: Hanim Maria Astuti, S.Kom., M.Sc.
Dosen Pembimbing 2: Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom.

ABSTRAK

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember (ITS) Surabaya merupakan direktorat yang memiliki fungsi menangani seluruh kegiatan teknologi informasi dan sistem informasi yang ada di ITS. Risiko yang biasa terjadi pada organisai dalam bidang TI adalah risiko keamanan informasi, seperti pencurian data, layanan tidak bisa diakses, dsb. Penanganan risiko keamanan sistem informasi di DPTSI ITS belum diterapkan dengan baik sehingga dapat mengakibatkan terganggunya proses bisnis yang berjalan.

Dalam memenuhi kebutuhan keamanan aset informasi diperlukan adanya standar dalam bentuk kontrol keamanan sistem informasi untuk meminimalkan risiko serta meningkatkan keamanan sistem informasi. Standar yang digunakan dalam penelitian ini adalah standar ISO/IEC 27001:2013 sebagai kerangka kerja dalam identifikasi risiko keamanan sistem informasi dan penilaian risiko keamanan sistem informasi dibuat berdasarkan hasil wawancara dan justifikasi dari DPTSI ITS. Standar ISO/IEC 27002:2013 digunakan sebagai standar kontrol dari hasil penilaian risiko keamanan sistem informasi.

Hasil yang diharapkan dalam penelitian ini adalah dokumen kontrol yang sesuai dengan kebutuhan keamanan sistem informasi DPTSI ITS dengan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013.
Kata kunci: Manajemen Risiko, ISO/IEC 27001:2013, ISO/IEC 27002:2013

ASSESSMENT AND MITIGATION OF SECURITY RISK OF INFORMATION SYSTEM BASED ON ISO / IEC 27001: 2013 STANDARD USING PMBOK METHOD (CASE STUDY: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)

Name	**: Alif Satria Perdana**
NRP	**: 0521 14 4000 0034**
Department	**: Sistem Informasi FTIK-ITS**
Supervisor 1	**: Hanim Maria Astuti, S.Kom., M.Sc.**
Supervisor 2	**: Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom.**

ABSTRACT

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya is a directorate that has a function to handle all activity of information technology and information systems. Handling of information security in DPTSI ITS has not been properly implemented so, it can lead to disrupting the business process.

To fulfilling security need of information assets required a standard in form of information security controls to minimize risks and improve the information systems security. Standard that used in this study is ISO/IEC 27001:2013 standard as a framework for identifying and assessing the risk of information system security based on interviews and justification of DPTSI ITS. ISO/IEC 27002:2013 used as a control standard from the information system security assessment result.

The expected result in this research is controlled document fit the information security requirements of DPTSI ITS based on standard ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

Keywords : Risk Management, ISO/IEC 27001:2013, ISO/IEC 27002:2013

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Bismillahirohmanirrohim

Puji Syukur peneliti panjatkan pada Allah SWT yang telah memberikan rahmat dan ridho-Nya kepada penulis, sehingga dapat menyelesaikan buku tugas akhir dengan judul :

"**PENILAIAN DAN MITIGASI RISIKO KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 MENGGUNAKAN METODE PMBOK (STUDI KASUS : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)**"

Sebagai syarat untuk memperoleh gelar Sarjana Komputer di Departemen Sistem Informasi – Institut Teknologi Sepuluh Nopember Surabaya

Pada kesempatan ini, saya ingin menyampaikan banyak terima kasih kepada semua pihak yang telah memberikan dukungan, bimbingan, arahan, bantuan dan semangat dalam menyelesaikan tugas akhir ini, terima kasih ini saya sampaikan kepada:

1. Kedua orang tua penulis yang selalu memberikan doa dan dukungan baik secara moral dan materi untuk menyelesaikan tugas akhir ini
2. Ibu Hanim Maria Astuti, S.Kom., M.Sc dan Bapak Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom. Selaku dosen pembimbing yang telah meluangkan waktu dan tidak pernah bosan dalam membimbing penulis dalam menyelesaikan tugas akhir ini.
3. Bapak Cahya Purnama Dani, A.Md., Bapak Radityo Prasetianto Wibowo, S.Kom., M.Kom. dan Ibu Anny Yuniarti, S.Kom., M. Comp. SC yang telah bersedia meluangkan waktunya untuk menjadi narasumber dalam penelitian ini.

4. Bapak Prof. Ir. Arif Djunaidy, M.SC., Ph.D. selaku dosen wali yang selalu memberikan arahan kepada penulis selama menjadi perkuliahan hingga pengerjaan Tugas Akhir.
5. Teman-teman yang ada di Lab MSI dan Teman "Seperguruan Bu Hanim", serta teman-teman Osiris yang telah berjuang bersama dari maba hingga akhir membantu dan selalu bertanya *progress* untuk menyelesaikan penelitian ini.
6. Teman-teman Begundal (Akmal, Alfan, Arif, Ayik, Bintang, Dhimas, Egas, Fikry, Gradi, Guntur, Hendro, dan Ilham) yang telah memberikan semangat dalam menyelesaikan penelitian ini.
7. Teman-teman Lab ADDI yang bersedia menampung ketika lab MSI tutup atau sedang ramai.
8. Pak Hermono sebagai laboran MSI yang membantu penulis dalam pengurusan administrasi penyelesaian Tugas Akhir ini.
9. Serta pihak lain yang telah memberikan dukungan dan berkontribusi demi kelancaran penyelesaian tugas akhir ini.

Penyusunan tugas akhir ini masih sangat jauh dari kata sempurna, untuk itu peneliti menerima kritik dan saran yang membangun untuk perbaikan di masa yang akan datang. Penelitian ini diharapkan dapat menjadi salah satu acuan untuk penelitian serupa dan bermanfaat bagi pembaca.

Surabaya, Juli 2018

Penulis

DAFTAR ISI

Halaman ini sengaja dikosongkan

DAFTAR TABEL

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

1.1 Latar Belakang

Organisasi dari segala jenis dan ukuran akan menghadapi ketidakpastian baik secara internal maupun eksternal, dimana efek ketidakpastian pada organisasi ini disebut “risiko”. Setiap aktivitas di organisasi mempunyai risiko tersendiri. Organisasi mengelola risiko dengan melakukan identifikasi, analisis, evaluasi dan penerapan kontrol atau kendali risiko sesuai dengan kebutuhan organisasi. Manajemen risiko dapat diterapkan pada banyak tingkatan area, waktu, fungsi, proyek, dan aktivitas tertentu [1].

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember (ITS) Surabaya adalah organisasi yang bertugas untuk menyediakan dan mengelola layanan teknologi informasi ITS termasuk di dalamnya mendukung aktivitas akedemik, penelitian, dan pengabdian masyarakat, serta manajerial di ITS untuk mencapai visi misinya. DPTSI ITS menggunakan teknologi informasi (TI) dalam menunjang proses bisnis sendiri ataupun menunjang proses bisnis ITS. Dimana salah satu fungsi DPTSI ITS adalah pelaksanaan penjaminan keamanan sistem informasi [2]. Pada DPTSI ITS sendiri telah dilakukan penilaian lima area Indeks KAMI dimana penggunaan sistem elektroniknya masuk didalam kategori tinggi dan hasil akhirnya DPTSI ITS masuk ke dalam kategori masih sangat kurang [3].

Keamanan informasi memiliki peran vital dalam organisasi. Manajemen sebagai aspek yang mengelola organisasi bertujuan untuk dukungan optimal pada tujuan bisnis. Sistem Manajemen Keamanan Informasi (SMKI) dirancang sesuai dengan standar internasional memberikan dasar untuk implementasi strategi keamanan informasi yang efisien, dan efektif [4]. Pendekatan dari keamanan informasi yang dapat dilakukan bergantung pada situasi yang dihadapi seperti jenis organisasi, model bisnis, ataupun tujuan keamanan informasi setiap organisasi.

DPTSI ITS sebagai organisasi yang terus dikembangkan dan memiliki aktivitas beragam, yang mengakibatkan munculnya ancaman, kerentanan, dan risiko keamanan informasi yang semakin kompleks [5]. Kerangka kerja dan standar yang relevan terkait dengan penelitian ini, yaitu ISO/IEC 27001:2013 berfungsi sebagai acuan kebutuhan penetapan, penerapan, pemeliharaan, dan peningkatan sistem manajemen keamanan informasi [6]. Sedangkan ISO/IEC 27002:2013 berfungsi sebagai acuan dalam memilih kontrol pada proses penerapan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001 [7]. Kontrol yang diterapkan dapat disesuaikan dengan kebutuhan organisasi berdasarkan hasil analisa risiko keamanan sistem informasi yang telah dilakukan.

ISO/IEC 27001:2013 merupakan standar internasional yang menyediakan persyaratan untuk penetapan, penerapan, pemeliharaan, dan peningkatan sistem manajemen keamanan informasi [6]. Sistem manajemen keamanan informasi mengamankan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi dengan menerapkan proses manajemen risiko. Standar ini dapat digunakan oleh internal dan eksternal untuk menilai kemampuan organisasi dalam memenuhi kebutuhan keamanan informasinya [6].

ISO/IEC 27002:2013 merupakan standar internasional yang dirancang bagi organisasi sebagai acuan dalam memilih kontrol pada proses penerapan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001 [7]. Informasi yang berhubungan dengan proses, sistem, jaringan, dan individu yang terlibat dalam operasional adalah aset penting bagi organisasi. Dimana aset tersebut membutuhkan perlindungan dari berbagai macam ancaman baik dari internal ataupun eksternal organisasi. Perubahan proses bisnis atau sistem pada organisasi dapat menciptakan risiko baru pada keamanan informasi. Keamanan informasi yang efektif dapat mengurangi risiko dengan melakukan perlindungan aset organisasi terhadap ancaman dan

kerentanan, kemudian mengurangi dampak risiko terhadap aset organisasi [7].

Demikian, salah satu bentuk dalam optimalisasi keamanan sistem informasi di DPTSI ITS adalah dengan melakukan manajemen risiko keamanan sistem informasi dengan standar ISO/IEC 27001 untuk memastikan risiko keamanan sistem informasi tidak mengganggu proses bisnis yang ada di DPTSI ITS.

1.2 Rumusan Masalah

Berdasarkan uraian dari latar belakang di atas, rumusan masalah yang menjadi fokus utama dan akan diselesaikan dalam tugas akhir ini antara lain :

1. Apa saja risiko keamanan sistem informasi DPTSI ITS?
2. Bagaimana rekomendasi kontrol keamanan sistem informasi DPTSI ITS?

1.3 Batasan Masalah

Berdasarkan permasalahan yang telah dijabarkan di atas, batasan masalah dalam tugas akhir ini adalah sebagai berikut :

1. Ruang lingkup penelitian ini berfokus pada keamanan sistem informasi yang ada di SubDit Pengembangan Sistem Informasi DPTSI ITS Surabaya, SubDit Infrastruktur dan Keamanan Teknologi Informasi, dan SubDit Layanan Teknologi dan Sistem Informasi
2. Analisis dan penilaian risiko keamanan sistem informasi dilakukan dengan menggunakan metode penilaian yang dibuat berdasarkan PMBOK dan disesuaikan dengan wawancara dari pihak DPTSI ITS.
3. Tindakan manajemen risiko keamanan sistem informasi yang dilakukan dalam penelitian ini hanya sampai pada penilaian dan pemberian kontrol risiko keamanan sistem informasi sesuai dengan ISO/IEC 27002:2013
4. Penilaian risiko fokus pada risiko yang berdampak negatif bagi organisasi.

1.4 Tujuan

Berdasarkan hasil perumusan masalah dan batasan masalah di atas, maka tujuan yang ingin dicapai dari tugas akir ini adalah :

1. Mengidentifikasi risiko keamanan sistem informasi yang terdapat pada DPTSI ITS.
2. Memberikan rekomendasi kepada pihak DPTSI ITS terkait kontrol keamanan sistem informasi berdasarkan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013.

1.5 Manfaat

Manfaat yang dapat diperoleh dari pengerjaan tugas akhir ini adalah sebagai berikut :

1. Bagi dunia akademis, tugas akhir ini diharapkan dapat memberikan kontribusi dalam manajemen risiko sistem keamaan informasi pada DPTSI ITS berdasarkan ISO/IEC 27001:2013 dan ISO/IEC 27002:2013.
2. Bagi instansi terkait, hasil penilaian dan rekomendasi kontrol yang diusulkan diharapkan dapat dijadikan sebagai pedoman pengelolaan risiko keamanan sistem informasi pada DPTSI ITS sesuai dengan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013.

1.6 Relevansi

Tugas akhir ini mengenai Penilaian dan Mitigasi Risiko Keamanan Sistem Informasi. Tugas akhir tersebut berkaitan dengan mata kuliah Manajemen Risiko Teknologi Informasi, Tata Kelola TI, dan Keamanan Aset Informasi.

BAB II
TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai penelitian sebelumnya dan dasar teori yang menjadi acuan atau landasan dalam pengerjaan tugas akhir ini. Dasar teori memberikan gambaran secara umum dari tugas ini.

2.1 Penelitian Sebelumnya

Penelitian ini, menggunakan beberapa penelitian terdahulu yang akan digunakan sebagai pedoman dan referensi dalam melaksanakan proses-proses dalam penelitian, seperti pada yang terdapat pada Tabel 2.1. Informasi yang disampaikan berisi tentang penelitian sebelumnya, hasil penelitian, dan hubungan penelitian yang akan dilakukan terhadap penelitian sebelumnya dalam rangka tugas akhir ini.

Tabel 2.1 Penelitian Sebelumnya

Penelitian 1	
Judul Penelitian	Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Berdasarkan standar ISO 27001:2005 dan ISO 27002:2013 menggunakan metode FMEA (Studi Kasus ISNET) [8]
Nama Peneliti, Tahun Penelitian	Krisna Harinda Dewantara, 2016
Metodologi	• Penelitian dilakukan di ISNET ITS dengan menggunakan metode FMEA untuk melakukan penilaian risiko. • Standar yang menjadi acuan adalah standar ISO 27001:2005 dan ISO 27002:2013

	• Peneliti menggunakan metode FMEA untuk penilaian risiko
Relevansi Penelitian	Menggunakan standar ISO 27001 dan 27002, Dapat menjadi acuan risiko yang mungkin terjadi di DPTSI ITS
Penelitian 2	
Judul Penelitian	Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 pada *Helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember [9]
Nama Peneliti, Tahun Penelitian	Chitra Utami Putri, 2017
Metodologi	• Penelitian dilakukan di DPTSI ITS • Penilaian risiko berdasarkan metode penilaian COBIT 5 *for Risk* • Penelitian menggunakan domain COBIT 5 APO12 *Manage Risk*
Relevansi Penelitian	Penelitian dilakukan di DPTSI ITS, Risiko yang ditemukan dapat menjadi acuan dalam penggalian risiko yang akan dilakukan dalam penelitian ini yaitu menggunakan standar

	ISO 27001:2013 dan ISO 27002:2013
Penelitian 3	
Judul Penelitian	Pembuatan Dokumen SOP (Standar Operasional Prosedur) Keamanan Aset Informasi yang Mengacu pada Kontrol Kerangka Kerja ISO 27002:2013 (Studi Kasus: CV Cempaka Tulungagung) [10]
Nama Peneliti, Tahun Penelitian	Dheni Indra Rachmawan, 2017
Metodologi	• Penelitian dilakukan di CV Cempaka Tulungagung dengan menggunakan kerangka kerja ISO 27002:2013 • Penilaian risiko menggunakan metode FMEA
Relevansi Penelitian	Penelitin menggunakan ISO 27002:2013, kontrol risiko dan risiko yang didapatkan dapat menjadi acuan dalam pembuatan kontrol di DPTSI ITS

Analisis kesenjangan dari ketiga penelitian sebelumnya yang menjadi acuan untuk penelitian ini dapat dilihat pada Tabel 2.2.

Tabel 2.2 Analisis Gap Penelitian Sebelumnya

Penelitian 1	Penelitian 2	Penelitian 3
• Penelitian dilakukan di ISNET ITS risiko.	• Penelitian dilakukan di DPTSI ITS	• Penelitian dilakukan di CV Cempaka Tulungagung

Penelitian 1	Penelitian 2	Penelitian 3
• Standar yang menjadi acuan adalah standar ISO 27001:2005 dan ISO 27002:2013 • Peneliti menggunakan metode FMEA untuk penilaian risiko	• Penilaian risiko berdasarkan metode penilaian COBIT 5 *for Risk* • Penelitian menggunakan domain COBIT 5 APO12 *Manage Risk*	dengan menggunakan kerangka kerja ISO 27002:2013 • Penilaian risiko menggunakan metode FMEA
Pendukung : Standar yang digunakan sama yaitu ISO 27001 dan ISO 27002	Pendukung : Tempat studi kasus yang digunakan sama	Pendukung : Standar yang digunakan sama yaitu ISO 27002

PENELITIAN YANG DIUSULKAN : PENILAIAN DAN MITIGASI RISIKO KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 MENGGUNAKAN METODE PMBOK (STUDI KASUS : DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS)
• Penilaian dan mitigasi risiko keamanan informasi • Menggunakan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 • Menggunakan metode penilaian PMBOK • Penilaian dilakukan oleh peneliti dengan cara wawancara, observasi dan studi dokumen

- Penilaian dilakukan pada tiga Subdit yang ada di Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS

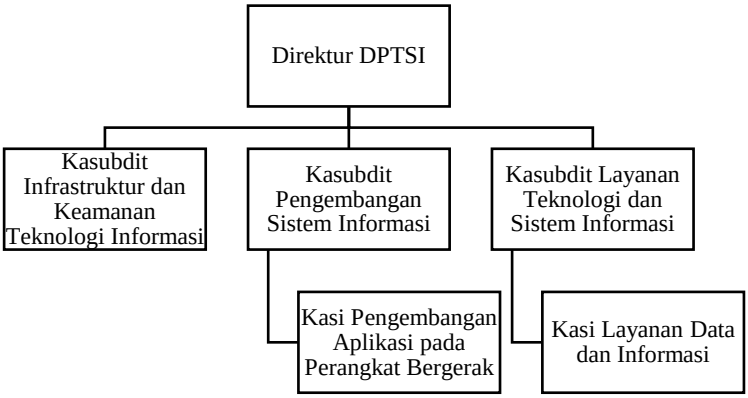
2.2 Dasar Teori

Bagian ini akan membahas teori dan bahan penelitian lain yang menjadi dasar informasi untuk mengerjakan tugas akhir ini.

2.2.1 Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI)

DPTSI ITS awalnya adalah sebuah unit yakni UPT Pusat Komputer yang dibentuk pada tahun 1982. Lembaga ini memiliki beberapa fungsi dalam menjalankan tugasnya yang dijabarkan sebagai berikut [2] :

1. Penyusunan rencana, program, dan anggaran lembaga.
2. Pelaksanaan penelitian dan pengembangan teknologi dan sistem informasi.
3. Pelaksanaan penjaminan keamanan sistem informasi
4. Pelaksanaan peningkatan kemampuan dan kompetensi tenaga pendidikan di bidang teknologi dan sistem informasi.
5. Pengelolaan sistem informasi berbasis web.
6. Pelaksanaan pemberian layanan jasa dibidang teknologi dan sistem informasi.
7. Pelaksanaan koordinasi dan kerjasama antar institusi berbasis teknologi dan sistem informasi.
8. Pelaksanaan monitoring dan evaluasi pengembangan teknologi dan sistem informasi.
9. Pelaksanaan urusan administrasi Lembaga.



Gambar 2.1 Struktur Organisasi DPTSI ITS [11]

Menurut peraturan Rektor Institut Teknologi Sepuluh Nopember Nomor 10 Tahun 2016, DPTSI terdiri atas tiga subdirektorat dan dibantu oleh dua seksi. Adapun tugas dan fungsi serta proses bisnis dari setiap subdirektorat dan seksi adalah sebagai berikut.

1. Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, dan pelaporan untuk pengembangan dan pengkajian infrastruktur dan keamanan teknologi informasi. Dalam melaksanakan tugasnya Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi menyelenggarakan fungsi:
   a. penyiapan bahan perumusan kebijakan dan standar mutu pengembangan infrastruktur dan keamanan teknologi informasi;
   b. pelaksanaan pengembangan infrastruktur dan keamanan teknologi informasi;
   c. pelaksanaan pengawasan dan pemantauan pengembangan infrastruktur dan keamanan teknologi informasi;
   d. pelaksanaan pemeliharaan infrastruktur dan keamanan teknologi informasi; dan

e. pelaksanaan evaluasi dan pelaporan infrastruktur dan keamanan teknologi informasi.

2. Subdirektorat Pengembangan Sistem Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan pengembangan sistem informasi. Dalam melaksanakan tugasnya Subdirektorat Pengembangan Sistem Informasi menyelenggarakan fungsi:
   a. penyiapan bahan perumusan kebijakan dan standar mutu pengembangan sistem informasi;
   b. pelaksanaan pengembangan sistem informasi;
   c. pelaksanaan pengawasan dan pemantauan pengembangan sistem informasi;
   d. pelaksanaan pemeliharaan data dan sistem informasi; dan
   e. pelaksanaan evaluasi dan pelaporan pengembangan sistem informasi.
3. Seksi Pengembangan Aplikasi pada Perangkat Bergerak mempunyai tugas melakukan penyusunan bahan perumusan kebijakan, pelaksanaan pengembangan, pengawasan dan pengendalian, pemeliharaan, serta pemantauan, evaluasi, dan pelaporan untuk pengembangan aplikasi pada perangkat bergerak.
4. Subdirektorat Layanan Teknologi dan Sistem Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, operasional layanan, pengawasan dan pemantauan, evaluasi, dan pelaporan untuk layanan teknologi dan sistem informasi. Dalam melaksanakan tugasnya Subdirektorat Layanan Teknologi dan Sistem Informasi menyelenggarakan fungsi:
   a. penyiapan bahan perumusan kebijakan dan standar mutu layanan teknologi dan sistem informasi;
   b. pelaksanaan operasional layanan teknologi dan sistem informasi;

c. pelaksanaan pengawasan dan pemantauan layanan teknologi dan sistem informasi; dan
d. pelaksanaan evaluasi dan pelaporan layanan teknologi dan sistem informasi.

5. Seksi Layanan Data dan Informasi mempunyai tugas melakukan penyusunan bahan perumusan kebijakan, penyiapan dan pengorganisasian data, pengawasan dan pengendalian, serta pemantauan, evaluasi, dan pelaporan untuk layanan data dan informasi.

2.2.2 RACI

Pendefinisian dan penetapan sebuah peran dan tanggung jawab menjadi sangat penting untuk keberhasilan sebuah program dalam organisasi [12]. Tanpa peran dan tanggung jawab yang jelas dapat mengakibatkan konflik ataupun kesalahan komunikasi pada internal organisasi. Cara yang dapat digunakan oleh pemimpin dalam mendefinisikan dan memperjelas peran dan tanggung jawab adalah dengan menggunakan matriks RACI.

1. *Responsible* (R)
   Orang yang bertanggung jawab untuk melaksanakan tugas atau aktivitas yang telah didefinisikan.
2. *Accountable* (A)
   Orang yang bertanggung jawab dalam pengambilan keputusan sebuah tugas atau aktivitas.
3. *Consulted* (C)
   Orang yang berperan dalam konsultasi sebelum sebuah keputusan atau tindakan dilakukan.
4. *Informed* (I)
   Orang yang perlu diberikan informasi setelah keputusan atau tindakan dilakukan.

Tabel 2.3 Contoh Tabel RACI [12]

	Peran A	Peran B	Peran C	Peran D
Aktivitas 1	R	A	C	I
Aktivitas 2	A	R	I	
Aktivitas 3	C	C		A
Aktivitas 4	I	R	R	A

2.2.3 Aset

Beberapa definisi aset antara lain sebagai berikut :

1. Sesuatu yang memiliki nilai tukar; modal; kekayaan [13].
2. Sumber daya organisasi yang dilindungi. Dimana aset dapat berupa bentuk logis seperti situs web atau informasi yang dikontrol atau dimiliki oleh organisasi; atau aset berbentuk fisik seperti sistem komputer atau objek nyata lainnya [14].
3. Semua yang bernilai pada organisasi, termasuk di dalamnya informasi yang mendukung misi organisasi [15].

Berdasarkan beberapa definisi aset di atas, maka dapat disimpulkan aset adalah semua sumber daya yang memiliki nilai bagi perusahaan atau organisasi.

2.2.4 Aset Informasi

Aset informasi merupakan sebuah informasi yang dapat dipahami, dibagi, dilindungi, dan dimanfaatkan dengan efektif serta memiliki nilai, risiko, konten dan siklus hidup yang dapat dikenali dan dikelola [16]. Definisi lain dari aset informasi adalah informasi yang bernilai bagi organisasi, dan sistem yang menyimpan, mengolah, dan mengirim informasi [17]. Aset informasi Berikut adalah daftar dan nilai aset informasi pada umumnya yang diuraikan pada Tabel 2.5.

Tabel 2.4 Keterangan Nilai Aset

Keterangan	Nilai Aset
Sangat rendah	1
Rendah	2
Sedang	3

Keterangan	Nilai Aset
Kritis	4
Sangat kritis	5

Tabel 2.5 Contoh Aset Informasi [18]

No.	Kelas Aset	Tingkat Aset	Aset	Nilai Aset
1	Berwujud	Infrastruktur fisik	Pusat data	5
2	Berwujud	Infrastruktur fisik	Server	3
3	Berwujud	Infrastruktur fisik	Komputer *desktop*	1
4	Berwujud	Infrastruktur fisik	Komputer mobile	3
5	Berwujud	Infrastruktur fisik	*PDAs*	1
6	Berwujud	Infrastruktur fisik	Telepon seluler	1
7	Berwujud	Infrastruktur fisik	Aplikasi perangkat lunak server	1
8	Berwujud	Infrastruktur fisik	Aplikasi perangkat lunak pengguna akhir	1
9	Berwujud	Infrastruktur fisik	Alat pengembangan	3
10	Berwujud	Infrastruktur fisik	*Routers*	3
11	Berwujud	Infrastruktur fisik	*Switch* jaringan	3

No.	Kelas Aset	Tingkat Aset	Aset	Nilai Aset
12	Berwujud	Infrastruktur fisik	Mesin fax	1
13	Berwujud	Infrastruktur fisik	PBXs	3
14	Berwujud	Infrastruktur fisik	*Removable media* (kaset, disket, USB, dll)	1
15	Berwujud	Infrastruktur fisik	Pasokan listrik	3
16	Berwujud	Infrastruktur fisik	Pasokan listrik yang tidak pernah putus	3
17	Berwujud	Infrastruktur fisik	Sistem pemadam api	3
18	Berwujud	Infrastruktur fisik	Sistem pendingin udara	3
19	Berwujud	Infrastruktur fisik	Sistem penyaringan udara	1
20	Berwujud	Infrastruktur fisik	Sistem kontrol lingkungan lainnya	3
21	Berwujud	Data intranet	*Source code*	5
22	Berwujud	Data intranet	Data sumber daya manusia	5
23	Berwujud	Data intranet	Data keuangan	5
24	Berwujud	Data intranet	Data pemasaran	5
25	Berwujud	Data intranet	*Passwords* karyawan	5

No.	Kelas Aset	Tingkat Aset	Aset	Nilai Aset
26	Berwujud	Data intranet	Kunci kriptografi pribadi karyawan	5
27	Berwujud	Data intranet	Kunci kriptografi sistem komputer	5
28	Berwujud	Data intranet	Kartu pintar	5
29	Berwujud	Data intranet	Hak milik intelektual	5
30	Berwujud	Data intranet	Data untuk kebutuhan peraturan *(GLBA, HIPAA*, etc*)*	5
31	Berwujud	Data intranet	Nomor jaminan sosial karyawan	5
32	Berwujud	Data intranet	Nomor SIM karyawan	5
33	Berwujud	Data intranet	Rencana strategis	3
34	Berwujud	Data intranet	Laporan kredit konsumen	5
35	Berwujud	Data intranet	Laporan medis karyawan	5
36	Berwujud	Data intranet	Pengenal biometrik karyawan	5
37	Berwujud	Data intranet	Data kontak bisnis karyawan	1
38	Berwujud	Data intranet	Data kontak pribadi karyawan	3
39	Berwujud	Data intranet	Data pembelian pesanan	5

No.	Kelas Aset	Tingkat Aset	Aset	Nilai Aset
40	Berwujud	Data intranet	Desain infrastruktur jaringan	3
41	Berwujud	Data intranet	Situs web internal	3
42	Berwujud	Data intranet	Data etnografis karyawan	3
43	Berwujud	Data extranet	Data kontrak mitra	5
44	Berwujud	Data extranet	Data keuangan mitra	5
45	Berwujud	Data extranet	Data kontrak mitra	3
46	Berwujud	Data extranet	Aplikasi kolaborasi mitra	3
47	Berwujud	Data extranet	Kunci kriptografi mitra	5
48	Berwujud	Data extranet	Laporan kredit mitra	3
49	Berwujud	Data extranet	Data pembelian pesanan mitra	3
50	Berwujud	Data extranet	Data kontrak pemasok	5
51	Berwujud	Data extranet	Data keuangan pemasok	5
52	Berwujud	Data extranet	Data kontrak pemasok	3
53	Berwujud	Data extranet	Aplikasi kolaborasi pemasok	3

No.	Kelas Aset	Tingkat Aset	Aset	Nilai Aset
54	Berwujud	Data extranet	Kunci kriptografi pemasok	5
55	Berwujud	Data extranet	Laporan kredit pemasok	3
56	Berwujud	Data extranet	Data pembelian pesanan pemasok	3
57	Berwujud	Data extranet	Situs web penjualan	5
58	Berwujud	Data extranet	Data situs web pemasaran	3
59	Berwujud	Data extranet	Data kartu kredit konsumen	5
60	Berwujud	Data extranet	Data kontak konsumen	3
61	Berwujud	Data extranet	Kunci kriptografi umum	1
62	Berwujud	Data extranet	Siaran pers	1
63	Berwujud	Data extranet	Laporan resmi	1
64	Berwujud	Data extranet	Dokumentasi produk	1
65	Berwujud	Data extranet	Materi pelatihan	3
66	Tidak Berwujud	Reputasi		5
67	Tidak Berwujud	Niat baik		3
68	Tidak Berwujud	Moral karyawan		3

No.	Kelas Aset	Tingkat Aset	Aset	Nilai Aset
69	Tidak Berwujud	Produktifitas karyawan		3
70	Layanan TI	Pesan	*E-mail*/penjadwalan	3
71	Layanan TI	Pesan	Pesan singkat	1
72	Layanan TI	Pesan	*Microsoft outlook Web Access (OWA)*	1
73	Layanan TI	Infrastruktur inti	Layanan direktori aktif	3
74	Layanan TI	Infrastruktur inti	*Domain Name System (DNS)*	3
75	Layanan TI	Infrastruktur inti	*Dynamic host configuration protocol (DHCP)*	3
76	Layanan TI	Infrastruktur inti	Alat manajemen perusahaan	3
77	Layanan TI	Infrastruktur inti	Pembagian file	3
78	Layanan TI	Infrastruktur inti	Penyimpanan	3
79	Layanan TI	Infrastruktur inti	*Dial-up remote access*	3
80	Layanan TI	Infrastruktur inti	Jaringan telepon	3
81	Layanan TI	Infrastruktur inti	Akses *virtual private networking (VPN)*	3

No.	Kelas Aset	Tingkat Aset	Aset	Nilai Aset
82	Layanan TI	Infrastruktur inti	*Microsoft Windows Internet Naming Service (WINS)*	1
83	Layanan TI	Infrastruktur inti	Layanan kolaborasi *(*contoh *microsoft sharepoitnt)*	

2.2.5 Risiko

Risiko adalah probabilitas kejadian yang tidak diinginkan [17]. Sedangkan menurut Knight terdapat dua definisi dari sebuah ketidakpastian (*uncertainty*) yang telah diterima secara umum, yaitu risiko mengacu pada hasil yang dapat dipastikan sedangkan ketidakpastian mengacu pada hasil yang tidak dapat dipastikan [19]. Risiko sendiri terdiri atas tiga faktor yaitu [20]:

1. **Aset (*asset*)**
   Aset terbagi atas dua jenis yaitu *tangible* berupa aset yang berbentuk yang memiliki nilai finansial seperti uang, gedung, *hardware*, *software*, pegawai [21]. Sedangkan aset *intangible* dapat berupa *data*, catatan, dokumen baik itu berbentuk *hardcopy* ataupun *softcopy* [21].
2. **Ancaman (*threat*)**
   Ancaman merupakan keadaan atau kejadian yang memiliki kemungkinan atau potensi hilangnya atau kerusakan pada aset [22].
3. **Kerentanan (*vulnerability*)**
   Kerentanan merupakan kelemahan dari sebuah aset atau desain infrastruktur, implementasi, aktivitas operasional yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab [22].

2.2.6 Sistem Informasi

Sistem informasi merupakan seluruh perangkat lunak, perangkat keras, data, sumber daya manusia, prosedur, dan jaringan dalam pemanfaatan sumber daya informasi pada organisasi [17].

1. Perangkat lunak
   Perangkat lunak ialah program aplikasi yang memberikan instruksi ke perangkat keras untuk melakukan suatu fungsi tertentu sesuai dengan kegunaan perangkat lunak ataupun perangkat keras terkait
2. Perangkat keras
   Perangkat fisik yang mendukung implementasi SI/TI seperti Laptop, PC.
3. Data
   Fakta yang yang dikumpulkan oleh organisasi, baik dalam bentuk mentah atau dalam bentuk yang sudah diolah.
4. Sumber daya manusia
   Pihak yang bertanggung jawab dalam pengoperasian SI/TI, seperti administrator, perancang sistem, pengguna sistem
5. Prosedur
   Kumpulan langkah atau tahapan yang harus diikuti oleh *stakeholder* organisasi dalam organisasi dalam melakukan suatu tindakan atau tugas.
6. Jaringan
   Merupakan penghubung antar perangkat yang memungkinkan perangkat untuk saling berkomunikasi satu sama lain sehingga perangkat dapat bekerja secara bersamaan untuk tujuan tertentu.

Dalam menentukan keberhasilannya sebuah sistem informasi dibagi berdasarkan empat dimensi [23]:

1. Kepuasan dukungan tugas
   Tingkat kepuasan seberapa baik sebuah sistem dalam memenuhi/membantu mencapai suatu tugas atau tanggung jawab.
2. Kepuasan dukungan keputusan

Tingkat kepuasan kemampuan sistem informasi dalam memberikan informasi untuk mendukung keputusan yang akan dibuat dalam proses bisnis.

3. Kepuasan antarmuka
   Tingkat kepuasan dari segi presentasi, format, kemudahan dalam penggunaan, dan efisiensi sistem informasi.
4. Kepuasan kerja
   Tingkat kepuasan mengenai keselarasan antara sistem informasi dengan dunia kerja sosioteknikal pengguna yang melibatkan perasaan, kebutuhan fisik, dan kondisi psikologis dari pengguna.

Kegagalan sistem informasi adalah sistem informasi tidak memenuhi harapan pengguna atau ketidakmampuan kinerja yang baik atau sistem yang berfungsi. Kegagalan sistem informasi dapat dilihat dari lima perspektif, yaitu Sosial dan Organisasi, Manajemen Proyek, Sistem Perushaan, Negara Pengembang, dan Resistensi Pengguna [24].

Tabel 2.6 Perspektif Kegagalan Sistem Informasi

Perspektif	Kategori	Faktor
Sosial dan organisasi	Kegagalan ekspektasi [25]	• Koresponden • Proses • Interaksi
	Kegagalan Keputusan [26]	• Keputusan
Manajemen Proyek	Proses [27]	• Estimasi yang buruk dan/atau penjadwalam yang buruk • Manajemen risiko yang kurang baik • Perencanaan yang kurang baik • *Quality assurance* yang pendek atau singkat

Perspektif	Kategori	Faktor
		• Pendefenisian kebutuhan yang buruk • Kegagalan kontraktor • Kontrol manajemen yang kurang baik • *Front end* yang membuang-buang waktu • *Code* yang buruk • Perencanaan yang dibawah tekanan • Desain yang tidak memadai • Sumber daya yang tidak memadai • Perencanaan yang ditunda
	Orang [27]	• Manajemen *stakeholder* yang tidak efektif • Personil yang lemah dan/atau masalah pada tim • Proyek sponsorship yang tidak memadai • Permasalahan politik • Kekurangan sumber daya • Ekspektasi yang tidak realistis • Motivasi yang buruk • Berangan-angan • Gesekan antara *developers* dan konsumen • Heroik

Perspektif	Kategori	Faktor
		• Penambahan orang pada akhir proyek • *Premature or overly frequent convergence* • Lingkungan kerja yang tidak baik • Masalah pegawai yang tidak terkontrol
	Produk [27]	• Cakupan yang buruk • *Research-oriented development* • Persyaratan yang terlalu tinggi/mahal • Negosiasi yang tarik ulur • Developer yang mahal
	Teknologi [27]	• *Silver-bullet syndrome* • Kurangnya kontrol pada *code* • Penghematan yang berlebihan terhadap *tools* atau metode • Peralihan *tool* di tengah proyek
Sistem perusahaan	Organisasi perusahaan yang tidak cocok [28]	• Fungsionalitas • Data • Kegunaan • Peran • Kontrol • Budaya organisasi
Negara Pengembang	*Archetypes* [29] [30]	• Kesenjangan konteks negara • Hard-soft gaps • Kesenjangan sektor publik dan swasta

Perspektif	Kategori	Faktor
Resistensi pengguna	Masalah individu [31]	• Ketidakpastian • Masukan • Kontrol / daya • Kemunduran diri
	Masalah Sistem [31]	• Masalah teknis • Kompleksitas
	Masalah organisasi [31]	• Fasilitas • Lingkungan • Komunitas • Pelatihan
	Masalah proses [31]	• Perubahan keterampilan kerja • Beban kerja • ketidakcocokan

2.2.7 Risiko Sistem Informasi

Risiko sistem adalah risiko yang berkaitan dengan sistem informasi. Risiko sistem informasi dapat berupa ancaman terhadap aset sistem informasi seperti kegagalan pada perangkat lunak, perangkat keras, kesalahan manusia, *spam*, *virus*, *malicious attacks*, termasuk juga bencana alam. Berikut adalah contoh ancaman yang dapat berdampak pada bisnis organisasi yang diuraikan pada Tabel 2.7.

Tabel 2.7 Contoh Ancaman Sistem Informasi [18]

No.	Level ancaman	Contoh ancaman
1	Bencana	Kebakaran
2	Bencana	Banjir
3	Bencana	Gempa bumi
4	Bencana	Badai
5	Bencana	Serangan teroris
6	Bencana	Kerusuhan
7	Bencana	Tanah longsor
8	Bencana	Salju longsor

No.	Level ancaman	Contoh ancaman
9	Bencana	Kecelakaan industri
10	Kesalahan mekanik	Mati listrik
11	Kesalahan mekanik	Kegagalan perangkat keras
12	Kesalahan mekanik	Jaringan mati
13	Kesalahan mekanik	Kesalahan kontrol lingkungan
14	Kesalahan mekanik	Kecelakaan konstruksi
15	Non-orang jahat	Kurangnya informasi pegawai
16	Non-orang jahat	Kurangnya informasi pengguna
17	Orang jahat	*Hacker, cracker*
18	Orang jahat	*Computer criminal*
19	Orang jahat	Spionase industri
20	Orang jahat	Spionase pemerintah
21	Orang jahat	*Social engineering*
22	Orang jahat	Pagawai yang tidak puas
23	Orang jahat	Bekas pagawai yang tidak puas
24	Orang jahat	Teroris
25	Orang jahat	Pagawai lalai
26	Orang jahat	Pagawai yang tidak jujur
27	Orang jahat	*Code mobile* berbahaya

Dalam risiko terdapat juga kerentanan yang dapat memberikan dampak pada organisasi, berikut adalah contoh kerentanan yang biasa ditemui pada organisasi diuraikan pada Tabel 2.8.

Tabel 2.8 Contoh Kerentanan Sistem Informasi [18]

No.	Kelas kerentanan	Kerentanan	Contoh (opsional)
1	Fisik	Pintu yang tidak terkunci	
2	Fisik	Fasilitas komputer yang tidak dijaga	
3	Fisik	Sistem pemadaman api tidak memadai	
4	Fisik	Desain gedung yang buruk	
5	Fisik	Konstruksi gedung yang buruk	
6	Fisik	Konstruksi menggunakan material yang mudah terbakar	
7	Fisik	*Finishing* menggunakan material yang mudah terbakar	
8	Fisik	Jendela yang tidak terkunci	
9	Fisik	Dinding yang rentan terhadap serangan fisik (rapuh)	
10	Fisik	Dinding ruangan tidak tertutup rapat	
11	Alam	Fasilitas berada di tempat yang salah	

No.	Kelas kerentanan	Kerentanan	Contoh (opsional)
12	Alam	Fasilitas berada di zona banjir	
13	Alam	Fasilitas berada di zona longsor	
14	Perangkat keras	Terdapat *patch* yang hilang	
15	Perangkat keras	*Firmware* yang telah usang	
16	Perangkat keras	Kesalahan konfigurasi sistem	
17	Perangkat keras	Sistem tidak terlindungi secara fisik	
18	Perangkat keras	Protokol manajemen terbuka untuk umum	
19	Perangkat lunak	Antivirus yang kadaluarsa (tidak *update*)	
20	Perangkat lunak	*Patch* yang tidak lengkap atau hilang	
21	Perangkat lunak	Aplikasi yang ditulis dengan buruk	*Cross site scripting*
22	Perangkat lunak	Aplikasi yang ditulis dengan buruk	SQL *injection*
23	Perangkat lunak	Aplikasi yang ditulis dengan buruk	Kelemahan pada *code*

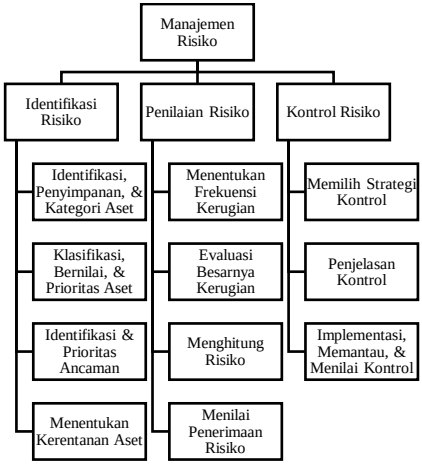
No.	Kelas kerentanan	Kerentanan	Contoh (opsional)
			seperti *buffer overflows*
24	Perangkat lunak	Kesengajaan membuat kelemahan	*Vendor backdoors* untuk manajemen atau *system recovery*
25	Perangkat lunak	Kesengajaan membuat kelemahan	*Spyware* seperti *keyloggers*
26	Perangkat lunak	Kesengajaan membuat kelemahan	*Trojan horses*
27	Perangkat lunak	Kesengajaan membuat kelemahan	
28	Perangkat lunak	Kesalahan konfigurasi	Sistem tidak diamankan
29	Perangkat lunak	Kesalahan konfigurasi	Sistem tidak diaudit
30	Perangkat lunak	Kesalahan konfigurasi	Sistem tidak dipantau
31	Media	Gangguan listrik	
32	Komunikasi	Protokol jaringan yang tidak terenkripsi	
33	Komunikasi	Koneksi terhubungan ke banyak jaringan	

No.	Kelas kerentanan	Kerentanan	Contoh (opsional)
34	Komunikasi	Mengizinkan protokol yang tidak perlu	
35	Komunikasi	Tidak ada penyaringan antara segmen jaringan	
36	Manusia	Prosedur didefinisikan dengan buruk	Respon yang tidak memadai
37	Manusia	Prosedur didefinisikan dengan buruk	Penyediaan secara manual
38	Manusia	Prosedur didefinisikan dengan buruk	*Disaster recovery plans* yang tidak memadai
39	Manusia	Prosedur didefinisikan dengan buruk	Melakukan *testing* pada sistem produksi
40	Manusia	Prosedur didefinisikan dengan buruk	Pelanggaran yang tidak dilaporkan
41	Manusia	Prosedur didefinisikan dengan buruk	Kontrol perubahan yang buruk
42	Manusia	Pencurian *credentials*	

2.2.7.1 Manajemen Risiko

Manajemen risiko merupakan proses identifikasi, penilaian, dan pengambilan langkah untuk mengurangi risiko ke tingkat yang dapat diterima oleh organisasi [17]. Ancaman atau risiko disini dapat berasal dari internal dan eksternal sehingga dalam penanganannya diperlukan strategi untuk mengatasi atau meminimalisir risiko yang mungkin terjadi [32]. Manajemen risiko memiliki tiga komponen, yaitu [17]:

1. *Risk Identification* (identifikasi risiko)
   Dokumentasi risiko terhadap aset informasi yang dimiliki oleh organisasi
2. *Risk Assessment* (penilaian risiko)
   Menentukan dampak risiko aset informasi terhadap organisasi
3. *Risk Control* (pengendalian risiko)
   Penerapan pengendalian untuk mengurangi risiko aset informasi ke tingkat yang dapat diterima oleh organisasi.



Gambar 2.2 Komponen Manajemen Risiko [17]

2.2.8 Manajemen Risiko Sistem Informasi

Manajemen risiko sistem informasi adalah proses organisasi melakukan tindakan meminimalkan risiko keamanan sistem informasi yang dianggap dapat mengurangi kemungkinan

terjadinya risiko atau mengurangi dampak dari risiko yang terjadi [33].

2.2.9 Kontrol

Beberapa definisi kontrol antara lain sebagai berikut:

1. Aktivitas yang dilakukan untuk mengurangi risiko aset informasi terhadap serangan ancaman [34].
2. Sebuah mekanisme keamanan, kebijakan, atau prosedur yang dianggap dapat melawan serangan, mengurangi risiko, menyelesaikan kerentanan, dan meningkatkan keamanan dalam sebuah organisasi [17].
3. Setiap proses, kebijakan prosedur, panduan, praktik, atau struktur organisasi, yang dapat bersifat administratif, teknis, manajemen, atau hukum yang memodifikasi risiko keamanan informasi [35].

2.2.10 Kerangka Kerja Manajemen Risiko

Tingkat keberhasilan suatu menajemen risiko pada organisasi bergantung pada efektivitas kerangka manajemen dalam menyediakan panduan yang akan diimplementasikan pada organisasi. Kerangka kerja akan membantu manajemen untuk mengelola risiko dengan efektif.

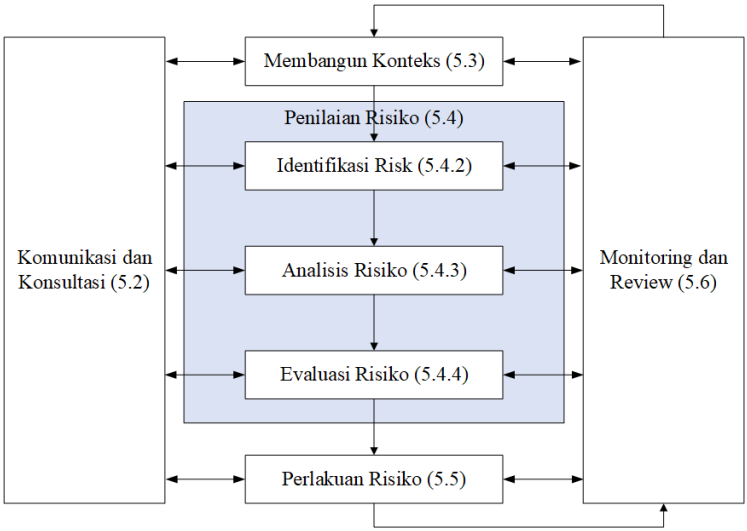
Agar manajemen risiko dapat berjalan dengan baik, maka dibutuhkan kerangka kerja yang sudah tersertfikasi dan telah diakui secara global dimana mempunyai metode atau panduan yang dapat dijadikan pedoman dalam pembuatan pengelolaan risiko yang ada pada organisasi.

2.2.10.1 ISO 31000

ISO 31000:2009, *Risk management – Principle and guidelines*, beriskan tentang prinsip, *framework*, dan proses manajemen risiko. Standar ISO 31000 dapat digunakan untuk segala organisasi tanpa memperhatikan ukuran, aktivitas, dan sektor organisasi [36].

Penggunaan ISO 31000 dapat membantu organisasi dalam meningkatkan pencapaian tujuan dari organisasi, memperbaiki

identifikasi peluang, dan ancaman, sehingga pengalokasian dan penggunaan sumber daya dapat menjadi lebih efektif dalam penanganan risiko pada organisasi [36]. ISO 31000 tidak dapat digunakan sebagai standar dalam proses sertifikasi, sehingga belum ada organisasi yang tersertifikasi ISO 31000. Standar ini dapat digunakan untuk audit atau manajemen risiko dengan membandingkat praktik manajemen risiko dengan organisasi lain (*benchmarking*) [1].



Gambar 2.3 Proses Manajemen Risiko ISO 31000 [1]

2.2.11 Kriteria Penilaian

Kriteria penilaian merupakan kriteria untuk membantu dalam mengidentifikasi peristiwa yang berdampak bagi organisasi. Termasuk didalamnya potensi dampak kerusakan yang terjadi, jumlah waktu pemulihan, dan kerugian finansial bagi. Dimana kriteria harus mencerminkan nilai, tujuan, dan sumber daya organisasi.

Tabel 2.9 Kerangka Penilaian [37]

Nilai	Skala	Probabilitas	Dampak		
			Waktu	Biaya	Kualitas
5	Sangat tinggi	>75%	> 6 bulan	>500 juta	Berdampak besar pada seluruh organsasi
4	Tinggi	51-75%	3-6 bulan	101-500 juta	Berdampak pada seluruh fungsi organisasi
3	Sedang	31-50%	1-3 bulan	51-100 juta	Berdampak pada fungsional utama organisasi
2	Rendah	11-30%	1-4 minggu	6-50 juta	Berdampak kecil pada seluruh fungsi organiasasi
1	Sangat rendah	1-10%	1 minggu	0-5 juta	Berdampak kecil pada fungsi sekunder organisasi

Melalui penilaian risiko berdasarkan probabilitas dan dampak risiko, maka didapatkan prioritas berdasarkan matriks risiko yang dibagi kedalam tiga wilayah warna. Berikut adalah gambaran matriks risiko yang ditampilkan pada Tabel 2.10.

Tabel 2.10 Matriks Risiko [35]

Pr						
	5	Sedang	Sedang	Tinggi	Tinggi	Tinggi
	4	Sedang	Sedang	Sedang	Tinggi	Tinggi

	3	Rendah	Sedang	Sedang	Sedang	Tinggi
	2	Rendah	Rendah	Sedang	Sedang	Sedang
	1	Rendah	Rendah	Rendah	Sedang	Sedang
		1	2	3	4	5
		Dampak				

2.2.12 Keamanan Informasi

Keamanan informasi merupakan perlindungan kerahasiaan, integritas dan ketersediaan aset informasi, baik selama proses penyimpanan, pengelolaan ataupun pada saat pengiriman dengan menerapkan kebijakan, edukasi, pelatihan, dan kesadaran terhadap teknologi [17]. Semakin banyak informasi yang disimpan, dikelola dan dibagikan oleh perusahaan maka semakin besar pula risiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan [38].

Keamaan Informasi bertanggung jawab untuk melindungi aset informasi terlepas bagaimana format informasi, perjalanan, pemrosesan atau bagaimana penyimpanan informasi terkait. Dalam keamanan informasi terdapat tiga komponen utama yaitu segitiga CIA yang dijabarkan sebagai berikut [17]:

2.2.13 Sistem Manajemen Keamanan Informasi (SMKI)

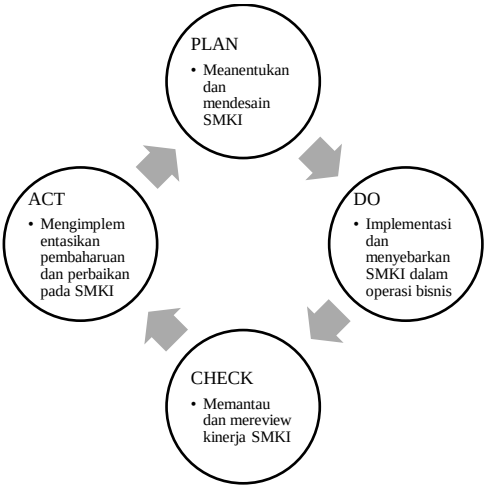
Sistem Manajemen Keamanan Informasi (SMKI) atau yang biasa dikenal dengan *Information Security Management System* (ISMS) adalah semua kebijakan yang berkaitan dengan pengawasan dan manajemen keamanan informasi untuk mencapai tujuan organisasi [39]. Penerapan sistem manajemen keamanan informasi pada organisasi harus memiliki pedoman untuk manajemen organisasi. Pedoman tersebut telah dinyatakan oleh Direktorat Sistem Informasi, kedepannya dapat dilakukan penyesuaian dalam pengelolaan keamanan informasi mengingat pesatnya perkembangan teknologi informasi. Berikut adalah pedoman yang disebutkan [40]:

1. Manajemen umum
2. Kebijakan
3. Manajemen risiko

4. Arsitektur dan desain keamanan
5. Isu pengguna
6. Manajemen sistem dan jaringan
7. Otentikasi dan otorisasi
8. Pengawasan dan audit
9. Keamanan fisik
10. Rencana keberlanjutan dan pemulihan bencana

Standar yang direkomendasikan dalam penerapan SMKI adalah ISO/IEC 27001 yang menjadi prasyarat untuk standar 2700x *family* [41]. Hal ini didukung juga oleh Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 4 tahun 2016 pasal 7 ayat 1 dan 2.

Dalam panduan SMKI termasuk di dalamnya mengenai pengelolaan orang, proses, dan sistem TI dalam manajemen risiko. SMKI dikembangkan dengan pendekatan model *plan, do, check, act (PDCA)* [41].



Gambar 2.4 Proses Model SMKI [41]

2.2.14 ISO/IEC 27001:2013

International Organization for Standardization (ISO), dan *International Electrotechnical Commision* (IEC) adalah badan

yang menetapkan standar internasional yang terdiri dari perwakilan dari badan standarisasi setiap negara [6]. Salah satu standar yang diekeluarkan adalah ISO/IEC 27001 yang merupakan standar yang menetapkan kebutuhan dalam membangun, menerapkan, mempertahankan, dan peningkatan berkelanjutan sebuah sistem manajemen keamanan informasi (SMKI) dalam organisasi yang mencakup penilaian dan perlakuan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi [42]. ISO/IEC 27001 terdiri atas 7 klausal kontrol dalam 35 kategori keamanan informasi [6].

2.2.14.1 *Context of the organization*

1. *Understanding the organization and its context*
   Organisasi harus menentukan masalah internal dan eksternal yang sesuai dengan tujuan dan sesuai dengan hasil yang diharapkan dari sistem manajemen keamanan informasi.
2. *Understanding the needs and expectations of interested parties*
   Organisasi harus menentukan :
   a. Pihak yang berkepentingan yang relevan dengan sistem manajemen keamanan informasi; dan
   b. Kebutuhan dari pihak yang berkepentingan yang relevan dengan keamanan informasi.
3. *Determining the scope of information security management system*
   Organisasi menentukan ruang lingkup dengan menentukan batas dan penerapan dari sistem manajemen keamanan informasi. Menentukan ruang ruang lingkup, dengan mempertimbangkan :
   a. Masalah internal dan eksternal berdasarkan *context of organization*;
   b. Kebutuhan berdasarkan *Understanding the needs and expectations of interested parties*; dan
   c. Ketergantungan dan antarmuka antara aktivitas yang dilakukan oleh organisasi dan organisasi lain.
4. *Information security management sytem*

Organisasi harus menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi sesuai dengan kebutuhan standar internasional ini.

2.2.14.2 *Leadership*

1. *Leadership and commitment*
   Top management harus menunjukkan kepemimpinan dan komitmen mengenai sistem manajemen keamanan informasi dengan :
   a. Memastikan kebijakan dan tujuan keamanan informasi yang ditetapkan sesuai dengan arahan strategis organisasi;
   b. Memastikan integrasi kebutuhan sistem manajemen keamanan informasi sesuai dengan proses organisasi;
   c. Memastikan ketersediaan sumber daya sistem manajemen keamanan informasi;
   d. Mengkomunikasikan pentingnya manajemen keamanan informasi yang efektif yang sesuai dengan kebutuhan sistem manajemen keamanan informasi;
   e. Memastikan sistem manajemen keamanan informasi mendapatkan hasil yang diharapkan;
   f. Mengarahkan dan mendukung orang yang berkontribusi terhadap efektivitas sistem manajemen keamanan informasi;
   g. Mendorong untuk peningkatan yang berkelanjutan; dan
   h. Mendukung manajemen lain untuk menunjukkan kepemimpinan seusai dengan bidangnya.
2. *Policy*
   Top management harus menentukan kebijakan keamanan informasi :
   a. Sesuai dengan tujuan organisasi;
   b. Termasuk tujuan keamanan informasi (*Information security objectives and planning to achieve them*) atau menyediakan kerangka kerja untuk menetapkan tujuan keamanan informasi;
   c. Termsasuk komitmen untuk memenuhi kebutuhan terkait dengan keamanan informasi; dan

d. Termasuk komitmen untuk peningkatan yang berkelanjutan sistem manajemen keamanan informasi.

Kebijakan keamanan informasi harus :

e. Tersedia sebagai dokumentasi informasi;
f. Dikomunikasikan dengan organisasi; dan
g. Tersedia bagi pihak yang berkepentingan; sewajarnya.

3. *Organizatioanl roles, responsibilities and authorities*

Top management harus menetapkan tanggung jawab dan wewenang untuk peran dalam keamanan infomasi;

a. Memastikan sistem manajemen keamanan informasi sesuai dengan kebutuhan standar internasional; dan
b. Melaporkan kinerja sistem manajemen keamanan informasi ke *top management*.

2.2.14.3 *Planning*

1. *Action to address risk and opportunities*
   Ketika merencanakan sistem manajemen keamanan informasi, organisasi harus mempertimbangkan masalah berdasarkan *Understanding the organization and its context* dan *Understanding the needs and expectations of interested parties* serta menentukan risiko dan peluang yang perlu ditangani :
   a. *Information security risk assesment*
      Organisasi mennentukan dan menerapkan penilaian risiko keamanan :
      i. Menetapkan dan menjaga kriteria risiko keamanan informasi:
         - Kriteria penerimaan risiko; dan
         - Kriteria dalam penilaian risiko keamanan informasi;
      ii. Memastikan bahwa penilaian keamanan informasi kembali menghasilkan hasil yang konsisten, valid dan dan dapat dibandingkan.
      iii. Identifikasi risiko keamanan informasi:

- Menerapakan proses penilaian risiko keamanan informasi untuk mengidentidikasi dampak terhadap confidentiality, integrity, dan availability di ruang lingkup sistem manajemen keamanan informasi; dan
- Identifikasi pemilik risiko;

iv. Analisis risiko keamanan informasi :
- Menilai potensi akibat yang dihasilkan jika risiko teridentifikasi;
- Menilai kemungkinan terjadinya dari risiko yang teridentifikasi; dan
- Menentukan tingkatan risiko;

v. Evaluasi risiko keamanan informasi:
- Membandingkan hasil analisis risiko dengan kriteria risiko; dan
- Prioritisasi risiko yang telah dianalisis untuk penanganan risiko.

b. *Information security risk treatment*

Organisasi harus menetapkan dan menerapkan sebuah proeses penanganan risiko keamanan informasi untuk :

i. Memilih opsi penanganan risiko keamanan informasi yang sesuai dengan hasil penilaian;
ii. Menentukan semua kontrol yang dibutuhkan dalam implementasi penanganan risiko keamanan informasi yang dipilih;
iii. Membandingkan kontrol yang ditentukan dengan lampiran A dan verifikasi tidak ada kontrol yang dihilangkan;
iv. Membuat pernyataan penerapan yang berisi kontrol yang diperlukan dan justifikasi untuk inklusi, apakah kontrol diimplementasikan atau tidak, dan justifikasi untuk pengecualian pada lampiran A;
v. Merumuskan rencana penanganan risiko keamanan informasi; dan
vi. Memperoleh persetujuan pemilik risiko terhadap rencanan penanganan risiko keamanan informasi dan penerimaan sisa risiko keamanan informasi.

2. *Information security objectives and planning to achieve them*

   Organisasi menetapkan tujuan keamanan informasi pada fungsi dan tingkatan yang relevan :

   a. Konsisten dengan kebijakan keamanan informasi*;*
   b. Terukur
   c. Mempertimbangkan kebutuhan keamanan informasi yang berlaku, dan hasil penilaian risiko dan penanganan risiko;
   d. Dikomunikasikan;
   e. Diperbarui sesuai dengan kebutuhan;

   Dalam merencanakan bagaimana mencapai tujuan keamanan informasi, organisasi harus menentukan:

   f. Apa yang harus diselesaikan;
   g. Sumber daya yang dibutuhkan;
   h. Siapa yang bertanggung jawab;
   i. Kapan selesai; dan
   j. Bagaimana hasil akan dievaluasi.

2.2.14.4 *Support*

1. *Resources*

   Organisasi harus menentukan dan menyediakan sumber daya yang dibutuhkan untuk pembentukan, implementasi, dan pemeliharaan dan peningkatan berkelanjutan sistem manajemen keamanan informasi.

2. *Competence*

   Organisasi harus :

   a. Menentukan kompetensi orang yang diperlukan untuk bekerja dengan kendali keamanan informasi;
   b. Memastikan orang tersebut berkompeten berdasarkan pendidikan, pelatihan, atau pengalaman;
   c. Jika memungkinkan, mengambil tindakan untuk memperoleh kompetensi yang diperlukan, dan mengevaluasi efektivitas tindakan yang diambil; dan
   d. Menyimpan dokumentasi informasi yang diperlukan sebagai bukti kompetensi.

3. *Awareness*

Orang yang bekerja di bawah kontrol organiasasi harus sadar terhadap:

a. Kebijakan keamanan informasi;
b. Kontribusi mereka terhadap efektivitas sistem manajemen keamanan informasi, termasuk keuntungan dari peningkatan kinerja keamaan informasi; dan
c. Implikasi yang tidak sesuai dengan kebutuhan sistem manajemen keamanan informasi.

4. *Communication*

Organisasi harus menentukan kebutuhan komunikasi internal dan eksternal yang untuk sistem manajemen keamanan informasi termasuk:

a. Apa yang dikomunikasikan;
b. Kapan dikomunikasikan;
c. Dengan siapa dikomunikasikan;
d. Siapa yang harus berkomunikasi; dan
e. Dimana proses komunikasi harus dilakukan.

5. *Documented information*

Sistem manajemen keamanan informasi organisasi harus termasuk dokumen informasi yang dibutuhkan dalam standar ini, dan dokumen informasi yang ditentukan oleh organisasi untuk keperluan efektivitas sistem manajemen keamanan informasi.

a. Membuat dan memperbarui

   Dalam membuat dan memperbarui dokumen informasi organisasi harus mamastikan kesesuaian:

   i. Identifikasi dan deskripsi (seperti judul, tanggal, penulis, atau nomor referensi);
   ii. Format (seperti bahasa, versi perangkat lunak)
   iii. Ulasan dan persetujuan untuk kesesuaian dan kecukupan.

b. Kontrol informasi dokumen

   Dokumen informasi yang diperlukan dalam sistem manajemen keamanan informasi dan standar internasional ini harus dikontrol untuk memastikan:

   i. Tersedia dan sesuai untuk digunakan, dimana, dan kapanpun dibutuhkan; dan

ii. Terlindungi (kehilangan dari kerahasiaan, penggunaan yang tidak perlu, atau kehilangan integritas).

Untuk kontrol dokumen informasi organisasi harus manangani aktivitas berikut;

iii. Distribusi, akses, pengambilan, dan penggunaan;
iv. Penyimpanan, dan pemeliharaan;
v. Kontrol perubahan (seperti kontrol versi); dan
vi. Retensi dan disposisi.

2.2.14.5 *Operation*

1. *Operational planning and control*
   Organisasi harus merencanakan, menerapkan, dan mengendalikan proses kebutuhan keamanan informasi sesuai dengan kebutuhan yang telah ditentukan sebelumnya.
2. *Information security risk assessment*
   Organisasi melakukan penilaian keamanan informasi pada waktu yang interval yang telah direncanakan.
3. *Information security risk treatment*
   Organisasi menerapkan rencana penanganan risiko keamaanan informasi.

2.2.14.6 *Performance evaluation*

1. *Monitoring, measurement, analysis, and evaluation*
   Organisasi harus mengevaluasi kinerja keamanan informasi dan efektivitas dari sistem manajemen keamanan informasi. Organisasi harus menentukan :
   a. Apa yang harus dipantau dan diukur, termasuk proses keamanan informasi dan kontrol;
   b. Metode untuk pemantauan, pengukuran, analisis, dan evaluasi;
   c. Kapan pemantauan dan pengukuran harus dilakukan;
   d. Siapa yang harus memantau dan mengukur;
   e. Kapan hasil pemantauan dan pengukuran harus dianalisis dan evaluasi; dan
   f. Siapa yang harus menganalisis dan mengevaluasi hasil.

2. *Internal audit*
   Organisasi harus melakukan audit internal pada interval yang direncanakan untuk mendapatkan informasi mengenai sistem manajemen keamanan informasi
   a. Menyesuaikan dengan:
      i. Kebutuhan organisasi untuk sistem manajemen keamanan informasi; dan
      ii. Kebutuhan standar internasioanal.
   b. Efektivitas implementasi dan perawatan;
   c. Merencanakan, menetapkan, melaksanakan, dan memelihara program audit, termasuk frekuensi, metode, tanggung jawab, kebutuhan perencanaan, dan pelaporan.
   d. Mendefinisikan kriteria audit dan ruang lingkup setiap audit;
   e. Memilih auditor dan mengadakan audit untuk memastikan tujuan dan kenetralan proses audit;
   f. Memastikan hasil audit dilaporkan relevan dengan manajemen; dan
   g. Menyimpan dokumen informasi sebagai bukti program audit dan hasil audit.
3. *Management review*
   Top management harus meninjau sistem manajemen keamanan informasi untuk memastikan kesesuaian, kecukupan, dan efektivitas dari perencanaan yang telah dilakukan. Pihak manajemen harus memberikan ulasan dengan pertimbangan :
   a. Status tindakan dari ulasan manajemen sebelumnya;
   b. Perubahan masalah internal dan eksternal yang relevan dengan sistem manajemen keaman informasi;
   c. *Feedback* kinerja keamanan infomrasi, termasuk:
      i. Ketidaksesuain dan tindakan korektif;
      ii. Hasil pemantuan dan pengukuran;
      iii. Hasil audit; dan
      iv. Pemenuhan tujuan keamanan informasi.
   d. *Feedback* dari pihak yang berkepentingan;

e. Hasil penilaian dan status rencana penanganan risiko; dan
f. Peluang untuk peningkatan yang berkelanjutan.

2.2.14.7 *Improvement*

1. *Nonconformity and corrective action*
   Jika terjadi ketidaksesuaian, organisasi harus melakukan tindakan yang sesuai dengan kebutuhan yang diperlukan.
   a. Reaksi terhadap ketidaksesuain
   b. Evaluasi yang dibutuhkan untuk menghilangkan penyebab ketidaksesuain agar tidak terulang atau terjadi di tempat lain;
   c. Menerapkan tindakan yang dibutuhkan;
   d. Meninjau efektivitas tindakan korektif yang diambil;
   e. Membuat perubahan sistem manajemen keamanan informasi, jika diperlukan.
   f. Sifat ketidaksesuaian dan semua tindakan diambil; dan
   g. Hasil tindakan korektif.
2. *Continual improvement*
   Organisasi harus terus memperbaiki kesesuaian, kecukupan, dan efektivitas sistem manajemen keamanan informasi.

2.2.15 ISO/IEC 27002:2013

Standar ISO/IEC 27002:2013 merupakan penanaman ulang dari ISO/IEC 17799:2005. Dimana standar ini digunakan sebagai titik awal penyusunan dan pengembangan Sistem Manajemen Keamanan Informasi (SMKI). Pada standar ini terdapat panduan dalam perencanaan dan implementasi suatu program untuk melindungi aset informasi [43]. Berikut adalah beberapa penerapan SMKI pada standar ini [43]:

- Semua kegiatan harus sesuai dengan tujuan dan proses pengamanan informasi yang didefinisikan dengan jelas dan didokumentasikan dalam suatu kebijakan dan prosedur.
- Standar ini memberikan kontrol pengamanan, yang dapat digunakan oleh organisasi untuk diimplementasikan berdasarkan kebutuhan spesifik bisnis organisasi.

- Semua pengukuran pengamanan yang digunakan dalam *Information Security Management System* (ISMS) harus diimplementasikan sebagai hasil dari analisis risiko untuk mengeliminasi atau untuk mengurangi level risiko hingga level yang dapat diterima.
- Suatu proses harus dapat memastikan adanya verifikasi secara berkelanjutan terhadap semua elemen sistem pengamanan melalui audit dan *review.*
- Suatu proses harus dapat memastikan peningkatan berkelanjutan dari semua elemen informasi dan sistem manajemen pengamanan.

ISO/IEC 27002:2013 merupakan panduan standar keamanan informasi organisasi dan praktik manajemen keamanan informasi yang termasuk di dalamnya pemilihan, implementasi, dan manajemen kontrol dengan pertimbangan risiko keamanan informasi di lingkungan organisasi yang dirancang untuk digunakan oleh organisasi. ISO/IEC 27002 terdiri atas 14 klausal kontrol keamanan dalam 35 kategori keamanan utama dan 114 kendali [8]:

1. *Information security policies*
   a. *Management direction for information security*
      Memberikan arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan kebutuhan dan peraturan bisnis.
2. *Organization of information security*
   a. *Internal organization*
      Menetapkan kerangka kerja manajemen untuk menginisiasi dan mengendalikan implementasi dan operasional keamanan informasi organisasi.
   b. *Mobile devices and teleworking*
      Memastikan keamanan telekomunikasi dan penggunaan perangkat *mobile*.
3. *Human resource security*
   a. *Prior to employment*
      Memastikan karyawan dan kontraktor mengerti mengenai tanggung jawab dan sesuai dengan perannya.

b. *During employment*
   Memastikan karyawan dan kontraktor mengetahui dan memenuhi tanggung jawab keamanan informasi.
c. *Termination and change of employment*
   Melindungi kepentingan organisasi sebagai bagian dari proses perubahan atau mengakhiri pekerjaan.

4. *Asset management*
   a. *Responsibility for assets*
      Mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang sesuai.
   b. *Information classification*
      Memastikan informasi mendapatkan tingkatan perlindungan yang sesuai berdasarkan tingkat kepentingannya di organisasi.
   c. *Media handling*
      Mencegah akses, modifikasi, menghapus, atau menghancurkan informasi yang tersimpan secara tidak sah.
5. *Access control*
   a. *Business requirements of access control*
      Membatasi akses dan fasilitas pengolahan informasi.
   b. *User access management*
      Memastikan akses bagi pengguna yang berwenang dan mencegah akses yang tidak sah ke dalam sistem dan layanan.
   c. *User responsibilities*
      Membuat pengguna bertanggung jawab untuk melindungi informasi autentikasi meraka.
   d. *System and application access control*
      Mencegah akses yang tidak sah ke dalam sistem dan aplikasi.
6. *Cryptography*
   a. *Cryptograhic controls*

Memastikan penggunaan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keaslian dan/atau integritas informasi.

7. *Physical and enviromental security*
   a. *Secure areas*
      Mencegah akses fisik, merusak, dan menganggu secara tidak sah terhadap informasi dan fasilitas pengolahan informasi organisasi.
   b. *Equipment*
      Mencegah kerugian, kerusakan, pencurian, atau kompromi terhadap aset dan gangguan operasional organisasi.
8. *Operations security*
   a. *Operational procedures and responsibilities*
      Memastikan operasional fasilitas pengolahan informasi berjalan dengan benar dan aman.
   b. *Protection from malware*
      Memastikan informasi dan fasilitas pengolahan informasi terlindungi dari *malware.*
   c. *Backup*
      Melindungi dari kehilangan data.
   d. *Logging and monitoring*
      Mencatat kejadian dan menghasilkan bukti
   e. *Control of operational software*
      Memastikan integritas sistem operasional
   f. *Technical vulnerability management*
      Mencegah ekploitasi kerentanan teknis.
   g. *Information systems audit controls*
      Meminimalkan dampak audit terhadap sistem operasional

9. *Communications security*
   a. *Network security management*
      Memastikan perlindungan informasi pada jaringan dan mendukung fasilitas pengolahan informasi.

b. *Information transfer*
   Menjaga keamanan informasi yang ditransfer dari internal maupun eksternal organisasi.

10. *System acquisition, development and maintenance*
    a. *Security requirements of information systems*
       Memastikan keamanan informasi sebagai bagian yang tidak terpisahkan dari seluruh siklus hidup sistem informasi. Termasuk dalam kebutuhan sistem informasi dalam penyediaan layanan melalui jaringan publik.
    b. *Security in development and support processes*
       Memastikan desain dan implementasi keamanan informasi dalam siklus pengembangan sistem informasi.
    c. *Test data*
       Memastikan keamanan data yang digunakan dalam pengujian.
11. *Supplier relationships*
    a. *Information security in supplier relationship*
       Memastikan perlindungan aset organisasi yang dapat diakses oleh pemasok.
    b. *Supplier service delivery management*
       Menjaga tingkat keamanan informasi dan pelayanan dengan pemasok sesuai dengan kesepakatan.
12. *Information security incident management*
    a. *Management of information security incidents and improvements*
       Memastikan pendekatan yang konsisten efektif terhadap manajemen insiden keamanan informasi, termasuk komunikasi mengenai kejadian dan kelemahan keamanan.

13. *Information security aspect of business continuity management*
    a. *Information ssecurity continuity*
       Kontinuitas keamanan informasi harus ditanamkan dalam kontinuitas sistem manajemen bisnis organisasi.

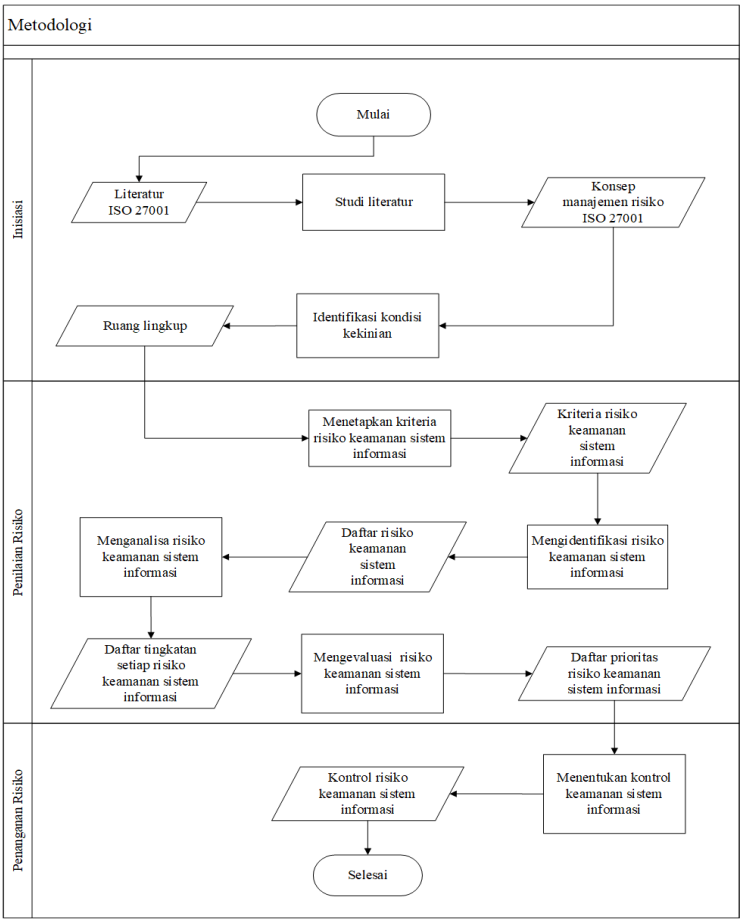
b. *Redundancies*
   Memastikan ketersediaan fasilitas pengolahan informasi.

14. Compliance

a. *Compliance with legal and contractual requirements*
   Menghindari pelanggaran hukum, undang-undang, atau kontrak terkait dengan keamanan informasi dan kebutuhan keamanan.
b. *Information security reviews*
   Memastikan implementasi dan operasional keamanan informasi sesuai dengan kebijakan dan prosedur organisasi.

BAB III
METODOLOGI PENELITIAN

Pada begian ini akan dijelaskan mengenai metodologi dalam pengerjaan Tugas Akhir, sehingga langkah-langkah pengerjaan menjadi sistematis dan terorganisir. Berikut merupakan metodologi pengerjaan tugas akhir berdasarkan kerangka kerja ISO/IEC 27001:2013 yang ditunjukkan pada Gambar 3.1



Gambar 3.1 Metodologi Penelitian

3.1 Studi Literatur

Tahapan ini merupakan tahapan awal dari proses pengerjaan tugas akhir ini. Pada tahap ini akan dilakukan studi literatur dengan mengumpulkan referensi dari penelitian sebelumnya, buku, jurnal, atau dokumen terkait. Tahap ini akan dilakukan kajian tentang konsep dan metode yang akan digunakan dalam penyelesaian masalah yang dijabarkan pada tugas akhir ini. Selain itu dilakukan juga pengumpulan data melalui buku Tugas Akhir alumni Departemen Sistem Informasi pada DPTSI ITS terkait risiko keamanan sistem informasi. Serta dilakukan pembuatan *interview protocol* dalam tugas akhir ini.

3.2 Identifikasi Kondisi Kekinian

Pada tahap ini akan dilakukan penggalian isu internal dan eksternal serta penggalian kebutuhan dan harapan keamanan sistem informasi dari pihak yang berkepentingan yang ada di DPTSI sebagai penunjang dalam tugas akhir.

Tahap ini didukung dengan studi literatur yang dilakukan sebelumnya. Pada tahapan dilakukan juga pembuatan tabel RACI model untuk memetakan narasumber penunjang dalam proses pembuatan kriteria dan identifikasi risiko keamanan sistem informasi.

Tabel 3.1 Identifikasi Kondisi Kekinian

Input	Proses	Output
• *Interview protocol* kebutuhan dan harapan • *Interview protocol* isu internal dan eksternal	• Penggalian isu internal dan eksternal • Penggalian harapan pihak yang berkepentingan • Studi dokumen terkait sistem informasi di DPTSI	• Ruang lingkup penelitian

3.3 Menetapkan Kriteria Risiko Keamanan Sistem Informasi

Pada tahapan ini dilakukan penetapan kriteria risiko yang akan dijadikan dasar dalam penilaian risiko keamanan sistem informasi seperti justifikasi dampak dan kemungkinan terjadinya risiko keamanan sistem informasi berdasarkan organisasi dan masukan dari orang yang terlibat langsung dalam aktivitas yang ada pada RACI model.

Tabel 3.2 Menetapkan Kriteria Risiko Keamanan Sistem Informasi

Input	Proses	Output
• Ruang lingkup penelitian	• Wawancara • Studi dokumen	Kriteria risiko keamanan sistem informasi: • Kriteria dampak risiko

3.4 Mengidentifikasi Risiko Keamanan Sistem Informasi

Pada tahapan ini dilakukan proses identifikasi risiko keamanan sistem informasi yang berdampak terhadap *confidentiatlity*, *integrity* dan *availability* serta pemilik risiko pada DPTSI ITS. Identifikasi dilakukan untuk menentukan potensi kerusakan, dan mendapatkan wawasan terhadap bagaimana, dimana, dan kenapa kerusakan bisa terjadi. Selain itu dilakukan juga identifikasi terhadap aset, proses bisnis, ancaman, kontrol yang telah ada, kerentanan, dan konsekuensi terhadap komponen sistem informasi.

Tabel 3.3 Mengidentifikasi Risiko Keamanan Informasi

Input	Proses	Output
Kriteria risiko keamanan sistem informasi:	• Wawancara • Studi dokumen • Observasi	Daftar risiko keamanan sistem informasi: • Daftar aset • Daftar ancaman

Input	Proses	Output
• Kriteria dampak risiko		• Daftar kontrol • Daftar kerentanan

3.5 Menganalisa Risiko Keamanan Sistem Informasi

Pada tahapan ini dilakukan penilaian potensi akibat yang dihasilkan, dan dampak risiko keamanan sistem informasi terhadap aset dan proses bisnis organisasi.

Tabel 3.4 Menganalisa Risiko Keamanan Sistem Informasi

Input	Proses	Output
Daftar risiko keamanan sistem informasi: • Daftar aset • Daftar ancaman • Daftar kontrol • Daftar kerentanan	Analisis risiko keamanan sistem informasi	Daftar penilaian risiko sistem informasi: • Daftar risiko • Daftar penilaian risiko

3.6 Mengevaluasi Risiko Keamanan Sistem Informasi

Pada tahapan ini dilakukan membandingkan hasil analisis risiko dengan kriteria yang telah dibuat sebelumnya dan prioritas risiko untuk proses menentukan kontrol keamanan sistem informasi yang akan dilakukan pada tahap selanjutnya.

Tabel 3.5 Mengevaluasi Risiko Keamanan Sistem Informasi

Input	Proses	Output
• Daftar risiko • Daftar penilaian risiko	Evaluasi risiko keamanan sistem informasi	• Daftar tingkatan atau prioritas risiko

3.7 Menentukan Kontrol Keamanan Sistem Informasi

Pada tahapan ini dilakukan pemilihan kontrol sebagai aksi penanganan risiko keamanan informasi berdasarkan prioritas

risiko yang telah dilakukan sebelumnya. Kontrol keamanan informasi yang digunakan berdasarkan ISO/IEC 27002:2013. Dalam proses penentuan kontrol, setiap risiko akan dipetakan berdasarkan kontrol yang relevan dan sesuai dengan kebutuhan risiko.

Tabel 3.6 Menentukan Kontrol Keamanan Sistem Informasi

Input	Proses	Output
• Daftar tingkatan atau prioritas risiko	• Menentukan kontrol keamanan sistem informasi	• Daftar kontrol setiap risiko keamanan sistem informasi

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Pada bagian ini dijelaskan mengenai perancangan pengerjaan tugas akhir. Dimana perancangan yang dibuat termasuk perancangan studi kasus dan perancangan terkait hal-hal yang akan dilakukan untuk mengerjakan tugas akhir ini.

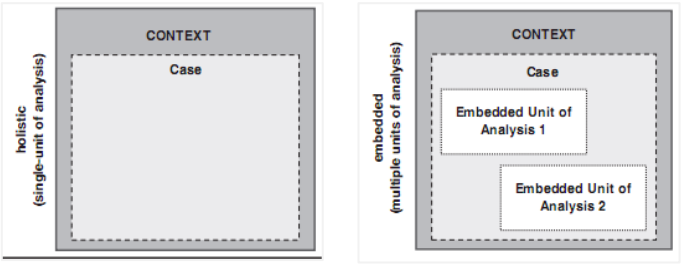
4.1 Perancangan Studi Kasus

Pada bagian perancangan studi kasus ini dijelaskan mengenai tujuan dari studi kasus yang diangkat dan *unit of analysis* yang diangkat.

4.1.1 Tujuan Studi Kasus

Penelitian pada tugas akhir ini bertujuan untuk mengidentifikasi risiko berdasarkan identifikasi risiko keamanan sistem informasi pada DPTSI ITS menggunakan kerangka kerja ISO/IEC 27001:2013. Untuk mencapai tujuan dalam penelitian tugas akhir ini menggunakan metode wawancara, studi dokumen dan observasi dalam proses penggalian data.

Studi kasus dibagi menjadi dua, yaitu *single-case design* dan *multiple-case design*. Perancangan studi kasus yang digunakan pada tugas akhir ini adalah *single-case design*, dimana perancangan *single-case design* dibagi menjadi dua tipe, yaitu *single unit of analysis* dan *multiple unis of analysis*. Yang ditunjukkan pada Gambar 4.1.



Gambar 4.1 Tipe Studi Kasus Single-Case Design

Penggunaan *single unit of analysis* menghasilkan pemahaman yang lebih dalam dalam subjek yang dianalisis sedangkan, *multiple unit of analysis* menghasilkan bukti yang lebih kuat dengan membandingkan persamaan dan perbedaan antara setiap subjek [44].

Tugas akhir ini menggunakan satu studi kasus dengan *single unit of analysis*. *Unit of analysis* dalam tugas akhir ini adalah melakukan analisis terhadap risiko keamaanan sistem informasi yang terjadi pada DPTSI ITS.

4.1.2 *Unit of Analysis*

Unit of analysis yang digunakan pada tugas akhir ini adalah identifikasi dan penilaian risiko keamanan sistem informasi pada unit yang ada di DPTSI ITS.

4.2 Data yang Diperlukan

Pada bagian ini dijelaskan mengenai data yang diperlukan untuk menunjang penelitian tugas akhir ini. Dalam penelitian dibutuhkan data yang akan digunakan dalam mendukung tahapan penggalian data dan informasi terkait studi kasus peneilitan tugas akhir ini. Berikut adalah tujuan dalam proses penggalian data dalam penelitian ini antara lain sebagai berikut:

Tabel 4.1 Perancangan Metode Tujuan Penggalian Data

Tujuan	Metode
Mengetahui gambaran Tata Kelola Keamanan Informasi, seperti tupoksi, peran dan tanggung jawab dalam pengelolaan keamanan sistem informasi dari pimpinan unit kerja hingga ke operasional.	Wawancara, Studi Dokumen
Mengetahui daftar aset sistem informasi yang ada di Direktorat Pengembangan Teknologi Sistem Informasi	Wawancara, Observasi, Studi Dokumen

Tujuan	Metode
Mengetahui daftar kontrol keamanan sistem informasi yang sudah diterapkan atau masih dalam tahap perancangan, seperti kebijakan, peratutan, dan strategi.	Wawancara, Observasi, Studi Dokumen
Mengetahui daftar kejadian terkait keamanan sistem informasi yang pernah terjadi di DPTSI, seperti server down, pengguna tidak dapat melakukan akses, dll.	Wawancara, Studi Dokumen

4.3 Persiapan Pengumpulan Data

Pada persiapan pengumpulan data yang akan dilakukan termasuk metode yang akan digunakan, narasumber, data yang dibutuhkan, dan uraian rancangan pertanyaan yang akan dalam pengumpulan data. Penggalian informasi pada DPTSI ITS akan dilakukan dengan studi dokumen, wawancara pada narasumber terkait.

Studi dokumen dilakukan pada dokumen terkait informasi keamanan sistem informasi yang dapat diperoleh dari staff dan unit yang ada pada DPTSI ITS. Sedangkan narasumber wawancara adalah orang yang bersangkutan pada proses bisnis tertentu terkait dengan risiko keamanan sistem informasi.

4.4 Pengumpulan Data

Pada bagian ini dejelaskan tentang metode pengumpulan data. Pengumpulan data dalam peneltian ini metode pengumpulan data yang digunakan ialah wawancara, observasi, dan studi dokumen setiap unit yang ada di DPTSI ITS. Berikut merupakan pemetaan metode dalam penggalian data yang ditampilkan pada.

4.4.1 Wawancara

Wawancara dilakukan untuk mengumpulkan informasi langsung kepada narasumber. Teknik wawancara yang digunakan ialah teknik wawancara semi terstruktur.

Wawancara yang dilakukan bertujuan untuk memahami proses bisnis yang ada di DPTSI ITS. Dimana narasumber yang berperan atau terlibat langsung dalam keamanan sistem informasi yang akan terlebih dahulu menggunakan model RACI.

4.4.1.1 Tujuan Wawancara

Tujuan wawancara pada penelitian ini untuk mendapatkan informasi yang tepat dari narasumber yang terpercaya. Berikut tujuan wawancara ditampilkan pada Tabel 4.2.

Tabel 4.2 Tujuan Wawancara

Narasumber	Tujuan Wawancara
KaSubDit Pengembangan Sistem Informasi	• Mengetahui gambaran Tata Kelola Keamanan Informasi, seperti tupoksi, peran dan tanggung jawab dalam pengelolaan keamanan sistem informasi dari pimpinan unit kerja hingga ke operasional. • Mengetahui daftar aset sistem informasi yang ada di Direktorat Pengembangan Teknologi Sistem Informasi SubDit Pengembangan Sistem Informasi ITS Surabaya. • Mengetahui daftar kontrol keamanan sistem informasi yang sudah diterapkan atau masih dalam tahap perancangan, seperti kebijakan, peratutan, dan strategi. • Mengetahui daftar kejadian terkait keamanan sistem informasi yang pernah terjadi di DPTSI, seperti server down,

Narasumber	Tujuan Wawancara
	pengguna tidak dapat melakukan akses, dll.
Staf Pemeliharaan Jaringan dan Perangkat Keras	• Mengetahui daftar aset sistem informasi yang ada di Direktorat Pengembangan Teknologi Sistem Informasi SubDirektorat Infastruktur dan Keamanan Teknologi Informasi ITS Surabaya. • Mengetahui daftar kontrol keamanan sistem informasi yang sudah diterapkan atau masih dalam tahap perancangan, seperti kebijakan, peratutan, dan strategi. • Mengetahui daftar kejadian terkait keamanan sistem informasi yang pernah terjadi di DPTSI, seperti server down, pengguna tidak dapat melakukan akses, dll.
Kasi Layanan Data dan Informasi	• Mengetahui daftar aset sistem informasi yang ada di Direktorat Pengembangan Teknologi Sistem Informasi SubDirektorat Layanan Teknologi dan Sistem Informasi ITS Surabaya. • Mengetahui daftar kontrol keamanan sistem informasi yang sudah diterapkan atau masih dalam tahap perancangan, seperti kebijakan, peratutan, dan strategi. • Mengetahui daftar kejadian terkait keamanan sistem

Narasumber	Tujuan Wawancara
	informasi yang pernah terjadi di DPTSI, seperti server down, pengguna tidak dapat melakukan akses, dll.

4.4.1.2 Perancangan *Interview Protocol*

Perancangan *interview protocol* adalah perancangan daftar pertanyaan yang akan digunakan agar proses wawancara menjadi terarah. Dimana *interview protocol* akan digunakan untuk menggali kondisi kekinian organisasi terkait risiko keamanan sistem informasi yang kerap muncul pada DPTSI ITS. Perancangan awal *interview protocol* yaitu menambahkan informasi terkait pelaksanan *interview* dan narasumber, sebelum melakukan perancangan daftar pertanyaan dalam *interview protocol*. Berikut konten pelaksanaan wawancara dan narasumber yang ditampilkan pada Tabel 4.3.

Tabel 4.3 Perancangan Narasumber Wawancara

Interview Protocol	
Tujuan	*Mengetahui tugas pokok dan fungsi dari Direktorat Pengembangan Teknologi Sistem Informasi ITS Surabaya.*
Tanggal	*12 April 2018*
Tempat	*DPTSI*
Narasumber	*Dr. Eng. Febriliyan Samopa, S.Kom., M.Kom.*
Jabatan	*Direktur DPTSI*

Instrumen wawancara pada *interview protocol* dibuat oleh penulis dan akan dibacakan kepada responden atau ditampilkan ketika melakukan wawancara. *Interviewer* akan mencatat dan

merekap respon dari responden pada *interview protocol* yang ditampilkan pada Tabel 4.4.

Tabel 4.4 Perancangan *Interview Protocol*

Daftar Pertanyaan		
No.	**Pertanyaan**	**Jawaban**
1	Bagaimana proses bisnis di DPTSI ITS?	
2		

Penentuan narasumber dilakukan untuk memudahkan proses ketika melakukan pengumpulan data. Dalam penentuan narasumber harus memperhatikan kapasitas dan kewenangan narasumber serta informasi yang diberikan valid, dan pertanyaan yang telah dirumuskan relevan dengan narasumber terkait. Berikut narasumber dalam penelitian yang ditampilkan pada Tabel 4.5.

Tabel 4.5 Narasumber Penelitian

Nama Narasumber	Jabatan
Anny Yuniarti, S.Kom., M.Comp.Sc.	KaSubDit Pengembangan Sistem Informasi
Cahya Purnama Dani, A.Md.	Staff Pemeliharaan Jaringan dan Perangkat Keras
Radityo Prasetianto Wibowo, S.Kom., M.Kom.	Kasi Layanan Data dan Informasi

Setelah melakukan wawancara kepada narasumber yang ada di DPTSI ITS. Selanjutnya akan ditentukan narasumber yang akan diwawancara terkait keamanan sistem informasi yang ada selanjutnya dengan pemodelan RACI untuk mengetahui setiap orang yang bertanggung jawab pada setiap sistem informasi yang dikembangkan oleh DPTSI.

Tabel 4.6 Perancangan Penanggung Jawab Sistem Informasi

Sistem Informasi	Nama A	Nama B	Nama C
Siakad	✔		✔

4.4.2 Observasi

Metode ini dilakukan dengan melakukan pengamatan langsung oleh penulis pada DPTSI ITS. Observasi yang dilakukan bertujuan untuk mendapatkan informasi tambahan yang dapat dijadikan penunjang dalam penelitian tugas akhir ini. Hasil yang diharapkan dari observasi ini adalah dokumentasi berupa foto dari penerapan keamanan sistem informasi yang ada di DPTSI ITS.

4.4.3 Studi Dokumen

Studi dokumen merupakan metode yang digunakan untuk mendukung informasi yang telah dan yang belum didapatkan yang berkaitan dengan hasil wawancara ataupun observasi. Informasi yang didapatkan terkait kondisi kekinian DPTSI ITS seperti struktur organisasi, tupoksi, *log* aktivitas, dan kebijakan terkait dengan keamanan sistem informasi baik dalam bentuk dokumen fisik ataupun digital. Studi dokumen yang dilakukan juga dapat dijadikan sebagai bukti dari wawancara dan observasi yang telah dilakukan.

4.4.4 Penilaian Risiko

Dalam melakukan analisa data akan dilakukan analisa dan penilaian risiko, dengan menggunakan pendekatan ISO/IEC 27001:2013, dan ISO/IEC 27002:2013. Dimana pendekatan proses penilaian risiko yaitu dengan menetapkan dan mengelola kriteria, mengidentifikasi risiko, menganalisa risiko, dan mengevaluasi risiko.

4.4.4.1 Identifikasi Risiko

Dalam melakukan identifikasi risiko berdasarkan metode pada ISO/IEC 27005:2011 dengan melakukan identifikasi terhadap aset, ancaman, kontrol yang telah ada, kerentanan, dan konsekuensi yang ada. Luaran dari proses identifikasi risiko

adalah daftar risiko. Daftar risiko ini nantinya akan dijadikan masukan pada proses analisa risiko.

4.4.4.1.1 Identifikasi Aset

Pada proses ini dilakukan identifikasi aset yang ada berdasarkan kategori aset, untuk mengetahui aset apa saja yang ada terkait dengan keamanan sistem informasi. Berikut perancangan identifikasi aset yang ditampilkan pada Tabel 4.7.

Tabel 4.7 Identifikasi Aset

No.	Kategori Aset	Aset
1	Perangkat Keras	Server

4.4.4.1.2 Identifikasi Ancaman

Pada proses ini dilakukan identifikasi ancaman pada setiap aset yang bertujuan untuk mengetahui setiap ancama terhadap setiap aset. Berikut perancangan identifikasi ancaman terhadap aset yang ditampilkan pada Tabel 4.8.

Tabel 4.8 Identifikasi Ancaman

No.	Aset	Ancaman
1	Server	Server down

4.4.4.1.3 Identifikasi Kontrol

Pada proses ini dilakukan identifikasi terhadap kontrol yang telah ada atau dalam perencanaan pada setiap aset yang ada pada organisasi. Berikut perancangan terhadap identifikasi kontrol pada aset yang ditampilkan pada Tabel 4.9.

Tabel 4.9 Identifikasi Kontrol

No.	Aset	Kontrol
1	Server	Ruangan dilengkapi CCTV

4.4.4.1.4 Identifikasi Kerentanan

Pada proses ini dilakukan identifikasi kerentanan terhadap setiap aset organisasi. Berikut perancangan terhadap identfikasi kerentanan yang ditampilkan pada Tabel 4.10.

Tabel 4.10 Identifikasi Kerentanan

No.	Aset	Kerentanan
1	Server	Ruangan tidak dikunci

4.4.4.1.5 Risk Register

Pada proses ini dilakukan pemetaan terhadap seluruh ancaman, kerentanan yang dapat memberikan dampak buruk terhadap organisasi. Berikut contoh *risk register* yang ditampilkan pada Tabel 4.11.

Tabel 4.11 *Risk Register*

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
Perangkat keras	Server	Kesalahan konfigurasi	Kurangnya pengawasan ketika maintenance	HR-01	Kerusakan Perangkat Keras	Proses bisnis tergangu terkait dengan penggunaan server

4.4.4.2 Analisis Risiko

Dalam analisa risiko dilakukan proses penilaian risiko yang terjadi berdasarkan probabilitas dan dampak dari sebuah risiko, dimana dampak yang diakibatkan dapat dibagi menjadi tiga yaitu berdasarkan waktu, finansial, dan kualitas.

Tabel 4.12 Analisis Risiko

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
Perangkat	Server	HR-01	5	Dapat mengakibatkan	2	Server telah ditangani	Sedang

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
Keras				server tidak bisa melayani proses bisnis ITS		oleh pihak yang berkompeten	

4.4.4.2.1 Penentuan Nilai Probabilitas

Pengukuran nilai probabilitas dilihat tingkat frekuensi atau tingkat kemungkinan terjadinya sebuah risiko yang dapat mengakibatkan kegagalan. Pada Tabel 4.13 ditampilkan penjelasan dari nilai probabilitas.

Tabel 4.13 Kriteria Nilai Probabilitas

Nilai	Skala	Probabilitas
5	Sangat tinggi	>75%
4	Tinggi	51-75%
3	Sedang	31-50%
2	Rendah	11-30%
1	Sangat rendah	1-10%

4.4.4.2.2 Penentuan Nilai Dampak

Pengukuran nilai dampak dilihat berdasarkan seberapa besar intensitas suatu risiko atau gangguan yang mempengaruhi organisasi. Dimana dampak dibagi menjadi tiga yaitu waktu, finansial, dan kualitas. Berikut merupakan penjelasan dari nilai dampak yang ditampilkan pada Tabel 4.14.

Tabel 4.14 Kriteria Nilai Dampak

Nilai	Skala	Dampak
5	Sangat tinggi	Berdampak besar terhadap tujuan ITS
4	Tinggi	Berdampak sedang terhadap tujuan ITS
3	Sedang	Berdampak besar terhadap tujuan DPTSI / berdampak kecil terhadap tujuan ITS
2	Rendah	Berdampak sedang terhadap tujuan DPTSI
1	Sangat rendah	Berdampak kecil terhadap tujuan DPTSI

4.5 Evaluasi Risiko

Evaluasi risiko merupakan tahap prioritas risiko keamanan sistem informasi dengan melibatkan organisasi terkait. Sehingga risiko yang diprioritaskan sesuai dengan kebutuhan dari organisasi.

Tabel 4.15 Matrik Risiko

Probabilitas						
	5	Sedang	Sedang	Tinggi	Tinggi	Tinggi
	4	Sedang	Sedang	Sedang	Tinggi	Tinggi
	3	Rendah	Sedang	Sedang	Sedang	Tinggi
	2	Rendah	Rendah	Sedang	Sedang	Sedang
	1	Rendah	Rendah	Rendah	Sedang	Sedang
		1	2	3	4	5
		Dampak				

4.6 Perancangan Mitigasi Risiko dan Kontrol ISO/IEC 27002:2013

Perancangan pemetaan risiko dan kontrol dilakukan untuk menentukan tujuan kontrol ISO/IEC 27002:2013 yang dibutuhkan dalam meminimalkan risiko keamanan sistem informasi. Berikut pemetaan risiko keamanan sistem informasi dengan kontrol ISO/IEC 27002:2013 yang ditampilkan pada Tabel 4.17.

Tabel 4.16 Keterangan Implementasi

Nilai Implementasi	Keterangan
1	Tidak dapat diimplementasikan
2	Diimplementasikan sebagian / dimodifikasi
3	Dapat diimplementasikan

Tabel 4.17 Perancangan Pemetaan Risiko dan Kontrol ISO/IEC 27002:2013

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002	Justifikasi ISO/IEC 27002	Mitigasi	Bentuk mitigasi	Nilai Implementasi
Server	HR-01	Kerusakan perangkat	Kesalahan konfigurasi	Sedang	11.2.4 Equipment	Kontrol tentang	Treat	Konfigurasi server	2

Halaman ini sengaja dikosongkan

BAB V
IMPLEMENTASI

Pada bab ini dijelaskan tentang implementasi setiap tahapan dan 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 ini bertujuan untuk mengidentifikasi dan menganalisa risiko yang berkaitan dengan keamanan sistem informasi yang ada di DPTSI ITS. Dalam pelaksanaan pengumpulan data dilakukan dengan wawancara, observasi, dan studi dokumen terkait keamanan sistem informasi DPTSI ITS. Hasil dari wawancara, observasi, dan studi dokumen yang dilakukan dapat dilihat di lampiran A.

5.1.1 Identifikasi Aset Sistem Informasi

Penentuan aset sistem informasi ini dilakukan dengan wawancara, studi dokumen, dan observasi. Dimana aset yang diidentifikasi merupakan aset yang digunakan atau aset penunjang proses bisnis di DPTSI ITS.

Tabel 5.1 Identifikasi Aset

No	Kategori Aset	Aset
1	Perangkat Keras	Server
2		Komputer Desktop/Laptop
3		AC Presisi
4		AC Konvensional
5		Genset
6		*Firewall*
7		CCTV
8	Perangkat Lunak	Integra
9		Siakad

No	Kategori Aset	Aset
10		SIM Verifikasi
11		SMITS
12		SIM Beasiswa
13		SIM Ormawa
14		SIP Maba
15		SIM Keuangan
16		e-Aset (Developing)
17		SIM Mondits (Monitoring Pendapatan ITS)
18		SIM AMU (Aset Manajemen Unit)
19		SIM Kepegawaian
20		e-Kepangkatan (Developing)
21		SIM Kinerja
22		e-Perkantoran
23		SIM Penelitian
24		Silacak (Developing)
25		SIP Monev
26		API
27	Data	Database
28	Jaringan	Kabel *fiber optic*/Kabel UTP
29		*Router*
30		*Access Point*
31		*Switch*
32	Manusia	Pegawai

5.1.2 Identifikasi Ancaman

Ancaman merupakan kejadian yang mungkin terjadi dan pernah terjadi pada aset yang dapat mengakibatkan terganggunya proses bisnis. Identifikasi ancaman dilakukan dengan menggabungkan informasi yang didapatkan ketika wawancara, observasi dan studi literatur.

Tabel 5.2 Identifikasi Ancaman Aset

No.	Aset	Ancaman
1	Server	Kesalahan konfigurasi
2		AC diruangan server mati
3		Memory server penuh
4		Overload
5		Server terserang virus/malware
6		Pasokan listrik terputus
7		Debu/korosi
8		Serangan *cybercrime*
9		Bencana (Gempa bumi, kebakaran)
10	Komputer Desktop/Laptop	Terkena virus/malware
11		Pencurian/hilang
12		Perawatan yang kurang baik
13	AC Presisi	Hilangnya pasokan listrik
14		Perawatan yang tidak dilakukan dengan benar
15		Debu dan kotoran
16	AC Konvensional	Hilangnya pasokan listrik
17		Perawatan yang tidak dilakukan dengan benar
18		Debu dan kotoran
19	Genset	Perawatan yang tidak dilakukan dengan benar
20	*Firewall*	Kesalahan konfigurasi
21	CCTV	CCTV Mati
22		Kualitas gambar yang kurang baik
23		Perawatan yang tidak dilakukan dengan benar
24	Sistem Informasi	Database error
25		Server mati

No.	Aset	Ancaman
26		Space memory kurang/penuh
27		Listrik mati
28		Sistem informasi lambat
29		Cyber crime
30		Hak akses pegawai yang mutasi/pensiun belum diganti/dihapus
31		storage penuh (belum fleksibel/cloud)
32		ketergantungan antar Subdit
33		penyalahgunaan wewenang pegawai/units
34	Database	Data *corruption*
35		Kesalahan konfigurasi
36		Data *loss*
37		Cyber crime
38	Kabel *fiber optic* / Kabel UTP	Putus/rusak
39	*Router*	Hilangnya pasokan listrik
40		Kesalahan konfigurasi
41	*Access Point*	Hilangnya pasokan listrik
42		Debu dan kotoran
43		Kesalahan konfigurasi
44	*Switch*	Hilangnya pasokan listrik
45		Debu dan kotoran
46		Kesalahan konfigurasi
47	Pegawai	penyalahgunaan wewenang
48		Pegawai yang lalai

5.1.3 Identifikasi Kontrol

Kontrol merupakan kebijakan, aktivitas, atau mekanisme pengamanan keamanan sistem informasi untuk melindungi aset dari serangan atau bahaya. Kontrol akan diidentifikasi berdasarkan wawancara, studi dokumen, dan observasi yang dilakukan oleh penulis.

Tabel 5.3 Identifikasi Kontrol Organisasi

No.	Aset	Kontrol Organisasi
1	Server	Terdapat CCTV pada pintu masuk
2		Terpasang sensor sidik jari
3		Dikunci
4		Dilengkapi dengan AC Presisi yang berjalan 24 jam 7 hari
5		Backup pasokan listrik menggunakan genset
6	Komputer Desktop/Laptop	Dilengkapi Antivirus
7		Login credential/ menggunakan password
8	AC Presisi	Terdapat sensor suhu secara *realtime*, jika suhu naik akan memberikan notifikasi kepada pegawai
9		Dilakukan perawatan teratur 2-3 bulan sekali oleh pihak ketiga
10		Kinerja AC dilakukan secara bergantian (terdapat 2 AC)
11	AC Konvensional	Hanya dilakukan perawatan teratur 2-3 bulan oleh pihak ketiga
12	Genset	Dipegang oleh bagian Sarana dan Prasarana ITS
13	*Firewall*	Update software secara teratur
14	CCTV	Terpasang di pintu masuk

No.	Aset	Kontrol Organisasi
15		penghapusan otomatis ketika kapasitas memori penuh untuk rekaman 3 hari paling lama
16		Menggunakan teknologi *motion detection*
17	Sistem Informasi	Menggunakan SSO untuk sistem informasi
18		Dilakukan backup database secara rutin
19		Dilakukan backup aplikasi secara rutis
20	Database	Dilakukan backup secara rutin
21		Disimpan pada server
22	Kabel *fiber optic* /*Kabel UTP*	Tidak ada kontrol khusus
23	*Router*	Diletakkan di ruangan khusus
24		Ruangan dilengkapi dengan AC
25	*Access Point*	Di kerangkeng untuk *Access point* yang berada diluar DPTSI
26	*Switch*	Disimpan pada rak khusus
27		Disimpan pada ruangan yang memiliki AC
28	Pegawai	Peraturan organisasi

5.1.4 Identifikasi Kerentanan

Kerentanan adalah kelemahan dari sebuah aset atau desain infrastruktur, implementasi, aktivitas operasional yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Kerentanan akan diidentifikasi berdasarkan aset yang telah diidentifikasi sebelumnya, serta berdasarkan wawancara, studi dokumen, dan observasi yang dilakukan oleh penulis.

Tabel 5.4 Identifikasi Kerentanan

No.	Aset	Kerentaan
1	Server	Suhu ruangan tidak stabil
2		Memory overload
3		Pegawai lupa mengecek pulsa pada alat notifikasi server
4		Pemberitahuan suhu server tidak terkirim
5	Komputer Desktop/Laptop	User tidak menggunakan password pada perangkat
6		User tidak memperbarui antivirus di perangkat
7	AC Presisi	Perawatan yang dilakukan kurang baik oleh pihak ketiga
8	AC Konvensional	Perawatan yang dilakukan kurang baik oleh pihak ketiga
9	Genset	Perawatan dipegang oleh Sarpras ITS
10	*Firewall*	Update yang tidak teratur
11	CCTV	Jumlah CCTV yang masih kurang
12		Penempatan CCTV kurang tepat
13	Sistem Informasi	Kesalahan konfigurasi database
14		penyalahgunaan wewenang pada unit
15		kapasitas memory masih terbatas
16		storage penuh (belum fleksibel/cloud)
17		Masih bergantung pada server lantai 6 perpus
18		Ketergantungan pada 1 orang / orang tertentu
19		Tidak bisa diakses
20		Memory penuh
21		Hacking

No.	Aset	Kerentaan
22		*update role user* tidak valid
23		Admin bisa menambah role admin lagi
24		tidak ada log user
25	Database	Ketergantungan antar Subdit
26	Kabel *fiber optic* /Kabel UTP	Kurangnya pengecekan yang teratur
27	*Router*	Kurangnya pengawasan untuk perangkat yang diluar DPTSI
28	*Access Point*	Kurangnya pengawasan untuk perangkat yang diluar DPTSI
29	*Switch*	Kurangnya pengawasan untuk perangkat yang diluar DPTSI
30	Pegawai	Pegawai lalai
31		Terbatasnya sumber daya

BAB VI
HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil dan pembahasan yang telah didapatkan dalam penelitian ini untuk menjawab rumusan masalah.

6.1 Identifikasi Risiko

Pembahasan hasil identifikasi risiko dibuat berdasarkan ancaman, kontrol dan kontrol yang telah diidentifikasi sebelumnya berdasarkan aset yang ada di DPTSI ITS.

Pada Tabel 6.1 dibuat tabel risiko berdasarkan ancaman, kerentanan dan dampak berdasarkan hasil wawancara dengan narasumber dari pihak DPTSI ITS dan analisis yang dilakukan dalam penelitian ini.

Tabel 6.1 Identifikasi Dampak Risiko

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
Perangkat Keras	Server	Kesalahan konfigurasi	Kurangnya pengawasan ketika *maintenance*	HR-01	Kerusakan Perangkat Keras	Proses bisnis terganggu terkait dengan penggunaan server
		AC diruangan server mati	Monitoring AC yang kurang baik	HR-02		

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Memory server penuh	Monitoring kapasitas memory tidak dilakukan dengan baik	HR-03		
		Overload Akses	Kapasitas memory tidak sanggup melayani akses yang banyak sekaligus	HR-04	Sistem informasi/server tidak bisa diakses	
		Server terserang virus/malware	Tidak dilakukan update antivirus secara berkala	HR-05	Kerusakan perangkat keras	
				HR-06	Sistem informasi/server tidak bisa diakses	

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Pasokan listrik terputus	Tidak ada backup daya/genset tidak berfungsi	HR-07	Kerusakan perangkat keras	
				HR-08	Sistem informasi/server tidak bisa diakses	
		Debu/korosi	Maintenance hardware yang tidak teratur	HR-09	Kerusakan Perangkat Keras	

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Serangan *cybercrime*	Terdapat celah keamanan yang luput dari pengawasan	HR-10	Sistem informasi/server tidak bisa diakses	
				HR-11	Kerusakan perangkat keras	
		Bencana (Gempa bumi, kebakaran)	DRP belum disiapkan dengan baik	HR-12	Kerusakan perangkat keras	
	Komputer Desktop/Laptop	Terkena virus/malware	Update antivirus yang tidak berkala	HR-13	Kerusakan perangkat keras	Proses bisnis yang bergantung pada penggunaan Komputer
		Pencurian/hilang	Ruangan yang tidak terkuci	HR-14		

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Perawatan yang kurang baik	Tidak dilakukan maintenance dengan baik terhadap perangkat	HR-15		*desktop*/laptop terganggu
	AC Presisi	Hilangnya pasokan listrik	Tidak ada backup daya/genset tidak berfungsi	HR-16	Server *overheat*	Sistem informasi tidak berjalan dengan baik/ tidak bisa diakses

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Debu dan kotoran	Tidak dilakukan maintenance dengan baik terhadap perangkat	HR-17	Kerusakan Perangkat Keras	sistem down
	AC Konvensional	Hilangnya pasokan listrik	Tidak ada backup daya/genset tidak berfungsi	HR-18	Server *overheat*	Server *overheat*
		Debu dan kotoran	Tidak dilakukan maintenance dengan baik terhadap perangkat	HR-19	Kerusakan perangkat keras	Kerusakan pada perangkat

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
	Genset	Genset tidak berfungsi	Perawatan yang tidak dilakukan dengan benar	HR-20	Server/sistem informasi down/ Proses bisnis terganggu	Proses bisnis tidak dapat berjalan ketika terjadi pemadaman PLN
	Firewall	Kesalahan konfigurasi	Maintenance perangkat yang kurang baik	HR-21	Pembobolan sistem oleh pihak yang tidak bertanggung jawab	Proses bisnis tidak dapat berjalan dengan baik

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
			Tidak dilakukan update firewall secara berkala	HR-22	Server terserang virus/malware	pencurian/pengubahan informasi yang ada pada server
	CCTV	CCTV Mati	Maintenance perangkat yang kurang baik	HR-23	Aktivitias tidak dapat terpantau	Terjadi pembobolan
		Kualitas gambar yang kurang baik		HR-24	Aktivitias tidak dapat terpantau dengan baik	
		Perawatan yang tidak dilakukan dengan benar		HR-25	Kerusakan perangkat keras	
Perangkat Lunak	Sistem Informasi	Database error	Kesalahan konfigurasi/input pada *database*	SR-01	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Terganggunya proses bisnis unit

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Server mati	Tidak ada *backup* daya/genset tidak berfungsi dengan baik	SR-02		
		storage/memory penuh	Kurangnya monitoring terhadap *space memory* yang tersedia	SR-03		

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Cyber crime	Terdapat celah keamanan yang luput dari pengawasan	SR-04	Pembobolan sistem oleh pihak yang tidak bertanggung jawab	Pencurian/pengubahan informasi yang ada pada sistem informasi
		Hak akses pegawai yang mutasi/pensiun belum diganti/dihapus	Kurangnya pengawasan terhadap hak akses yang ada pada sistem	SR-05	Orang dapat mengakses data/informasi yang bukan haknya/ Penyalahgunaan wewenang	Data/informasi pada sistem menjadi tidak benar/invalid

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
Data	Database	Data *corruption*	Tidak dilakukan backup	DR-01	Data penting rusak/tidak dapat diakses	Proses bisnis menjadi terganggu
		Kesalahan konfigurasi		DR-02		
		Data *loss*		DR-03		
		Cyber crime		DR-04	Data penting diubah/dicuri	Data penting organisasi disalahgunakan

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
Jaringan	Kabel *fiber optic* / UTP	Putus/rusak	Tidak ada maintenance secara berakala	NR-01	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Proses bisnis terganggu
	Router	Hilangnya pasokan listrik	Kurangnya pengawasan terhadap perangkat	NR-02	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Jaringan down
		Kesalahan konfigurasi		NR-03		
	Access Point	Hilangnya pasokan listrik	Kurangnya pengawasan	NR-04	Sistem informasi tidak bisa diakses/tidak	Jaringan down

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
		Kesalahan konfigurasi	terhadap perangkat	NR-05	berjalan dengan baik	
		Debu dan kotoran		NR-06	Kerusakan perangkat keras	
	Switch	Hilangnya pasokan listrik	Kurangnya pengawasan terhadap perangkat	NR-07	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Jaringan down
		Kesalahan konfigurasi		NR-08		
		Debu dan kotoran		NR-09	Kerusakan perangkat keras	

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
Manusia	Pegawai	Penyalahgunaan wewenang	Kurangnya monitoring terhadap aktivitas pegawai	PR-01	Pembobolan sistem oleh pihak yang tidak bertanggung jawab	Informasi organisasi diakses oleh pihak yang tidak bertanggung jawab
		Pegawai yang lalai		PR-02	Kecelakaan kerja	SDM berkurang
				PR-03	*Social engineering*	Informasi organisasi diakses oleh pihak yang

Kategori Aset	Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
				PR-04	Pencurian data	tidak bertanggung jawab

6.2 Penilaian Risiko

Dalam tahap ini dilakukan penilaian terhadap risiko yang telah diidentifikasi, penilaian dikategorikan berdasarkan probabilitas dan dampak terhadap organisasi.

Penilaian tersebut akan digunakan untuk menentukan tingkat sebuah risiko berdasarkan matriks yang menjadi acuan prioritas risiko.

Tabel 6.2 Penilaian Risiko

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
Perangkat Keras	Server	HR-01	5	Kesalahan konfigurasi dapat mengakibatkan server tidak bisa melayani proses bisnis ITS	2	Server telah ditangani oleh pihak yang berkompeten sesuai dengan kompetensinya	Sedang

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
		HR-02	5	Jika terjadi dapat mengakibatkan server overheat sehingga mengganggu server tidak bisa melayani proses bisnis ITS	1	Telah disediakan sensor pada untuk mendeteksi suhu pada server	Sedang
		HR-03	3	Jika terjadi server masih bisa melayani dan hanya berdampak kecil pada ITS	2	Telah dilakukan penambahan kapasitas sesuai dengan permintaan *stakeholder*	Sedang
		HR-04	3	Jika terjadi server masih bisa melayani dan hanya berdampak kecil pada ITS	1	Biasanya hanya terjadi ketika awal semester perkuliahan ketika frs	Rendah
		HR-05	2	Serangan virus atau malware akan menggangu proses bisnis di DPTSI	1	Sangat jarang terjadi, sudah terpasang firewall dan antivirus	Rendah

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
		HR-06	2	Serangan virus atau malware akan menggangu proses bisnis di DPTSI	1	Sangat jarang terjadi, sudah terpasang firewall dan antivirus	Rendah
		HR-07	5	Jika terjadi akan berdampak pada seluruh sistem informasi yang ada di server dan menggangu secara keseluruhan ITS	2	Telah disediakan UPS dan genset	Sedang
		HR-08	5	Jika terjadi akan berdampak pada seluruh sistem informasi yang ada di server dan menggangu secara keseluruhan ITS	2	Telah disediakan UPS dan genset	Sedang
		HR-09	2	Jika terjadi hanya berdampak pada DPTSI	1	Sangat jarang terjadi, karena server telah disimpan pada ruangan khusus	Rendah

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
		HR-10	4	Jika terjadi maka akan mengakibatkan server/sistem informasi tidak dapat diakses/ rusak sehingga akan berdampak pada ITS	1	Telah terpasang anti virus dan *firewall* pada server	Sedang
		HR-11	4	Jika terjadi maka akan mengakibatkan server/sistem informasi tidak dapat diakses/ rusak sehingga akan berdampak pada ITS	1	Telah terpasang anti virus dan *firewall* pada server	Sedang
		HR-12	5	Jika terjadi akan berdampak besar pada seluruh ITS termasuk DPTSI	1	Sangat jarang terjadi	Sedang
	Komputer Desktop/Laptop	HR-13	1	Jika terjadi hanya berdampak kecil pada DPTSI dan tidak berdampak sama sekali ke ITS	2	Pada dekstop atau laptop telah terpasang antiviru	Rendah

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
				dan aset mudah digantikan			
		HR-14	1	Jika terjadi hanya berdampak kecil pada DPTSI dan tidak berdampak sama sekali ke ITS dan aset mudah digantikan	1	Sangat jarang terjadi	Rendah
		HR-15	1	jika terjadi hanya berdampak kecil pada DPTSI dan tidak berdampak sama sekali ke ITS dan aset mudah digantikan	2	Desktop/ laptop diganti ketika sudah usang	Rendah
	AC Presisi	HR-16	5	Jika terjadi akan mengakibatkan server *overheat* sehingga server tidak dapat berjalan dan sistem informasi	1	Sudah disediakan *backup* genset	Sedang

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
				tidak dapat diakses untuk seluruh ITS			
		HR-17	5	Jika terjadi akan mengakibatkan kinerja server overheat sehingga server tidak dapat berjalan dan sistem informasi tidak dapat diakses untuk seluruh ITS	1	Sudah ditempatkan pada tempat yang sesuai dan bersirkulasi baik	Sedang
	AC Konven-sional	HR-18	2	Pendingin utama server menggunakan AC presisi	2	Pendingin jarang dipake	Rendah
		HR-19	2	Pendingin utama server menggunakan AC presisi	2	Pendingin jarang dipake	Rendah
	Genset	HR-20	5	Jika genset tidak dapat bekerja ketika terjadi pemadaman listrik akan mengakibatkan	1	Beban genset terlalu tinggi	Sedang

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
				sistem informasi tidak dapat diakses			
	Firewall	HR-21	3	Jika terjadi dapat mengakibatkan server terserang virus atau *cyber crime*	1	*Maintenance firewall* telah dipegang oleh pihak yang dianggap berkompeten oleh DPTSI	Rendah
		HR-22	3	Jika terjadi dapat mengakibatkan server terserang virus atau cyber crime	1	*Maintenance firewall* telah dipegang oleh pihak yang dianggap berkompeten oleh DPTSI	Rendah
	CCTV	HR-23	2	Jika terjadi aset atau fasilitas DPTSI menjadi tidak terpantau	1	Sangat jarang terjadi	Rendah
		HR-24	2	Jika terjadi aset atau fasilitas DPTSI menjadi tidak terpantau dengan optimal	1	Sangat jarang terjadi	Rendah
		HR-25	2	Jika terjadi aset atau fasilitas DPTSI	1	Sangat jarang terjadi	Rendah

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
				menjadi tidak terpantau			
Sistem Informasi	Sistem Informasi	SR-01	5	Jika terjadi akan berdampak pada seluruh data yang ada didalamnya termasuk data keperluan ITS	1	Sangat jarang terjadi	Sedang
		SR-02	5	Jika terjadi akan maka akan berdampak pada seluruh sistem informasi	2	Telah ada backup daya berupa UPS dan genset	Sedang
		SR-03	4	Jika terjadi mengakibatkan data tidak dapat tersimpan sehingga menganggu proses bisnis baik di lingkungan ITS ataupun DPTSI	1	Jarang dikarenakan, setiap sistem informasi memiliki space masing-masing	Sedang
		SR-04	5	Jika terjadi dapat menganggu proses	1	Server penyimpanan sistem informasi sudah	Sedang

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
				bisnis pada seluruh ITS ataupun DPTSI		dilengkapi anti virus dan firewall	
		SR-05	2	Jika terjadi orang dapat menganggu proses bisnis di DPTSI	3	Mutasi atau pemberhentian karyawan terkadang hak akses belum dicabut atau diubah	Sedang
Data	Database	DR-01	4	Jika terjadi data pada database akan rusak sehingga menggangu proses bisnis ITS ataupun DPTSI	2	Data sudah dibackup sercara berkala	Sedang
		DR-02	4	Jika terjadi dapat mengakibatkan data yang ada didalam database menjadi rusak dan mengganggu proses bisnis ITS	3	Tidak ada konfigurasi khusus untuk database	Sedang
		DR-03	5	Jika terjadi dapat menggangu proses bisnis ITS dan DPTSI	2	Kapasitas server sudah memenuhi kebutuhan	Rendah

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
		DR-04	5	Jika terjadi akan mengakibatkan proses bisnis baik di pihak ITS ataupun DPTSI menjadi terganggu	3	Server telah diamankan dengan anti virus dan firewall	Tinggi
Jaringan	Kabel *fiber optic* / UTP	NR-01	3	Jika terjadi dapat mengakibatkan jaringan atau koneksi terputus sehingga mengakibatkan terganggunya proses bisnis	1	Dilakukan pengecekan secara berkala	Rendah
	Router	NR-02	5	Jika terjadi maka jaringan di ITS akan ternggganggu sehingga sistem informasi tidak dapat diakses atau digunakan	1	Sangat jarang terjadi, router disimpan diruangan khusus dan di backup dengan UPS	Sedang
		NR-03	5	Jika terjadi maka jaringan di ITS akan	1	Konfigurasi dilakukan oleh pihak DPTSI	Sedang

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
				terngganggu sehingga sistem informasi tidak dapat diakses atau digunakan		langsung yang sesuai dengan bidangnya	
	Access Point	NR-04	1	Berdampak sangat kecil pada DPTSI dan tdak mengganggu proses bisni	3	boasa terjadi dikarenakan arus listrik yang tidak stabil atau ketidaksengajaan orang mencabut power dari access point	Rendah
		NR-05	1	Berdampak sangat kecil pada DPTSI dan tdak mengganggu proses bisni	1	Access point tidak perlu konfigurasi khusus	Rendah
		NR-06	1	Berdampak sangat kecil pada DPTSI dan tdak mengganggu proses bisni	2	Biasa terjadi terutama pada access point yang berada diruangan terbuka	Rendah
	Switch	NR-07	3	Jika terjadi akan mengibatkan	1	Sangat jarang terjadi, switch disimpan	Rendah

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
				perangkat tidak terhubung satu sama lain		diruangan khusus dan di backup dengan UPS	
		NR-08	3	Jika terjadi akan mengibatkan perangkat tidak terhubung satu sama lain	1	Switch tidak perlu konfigurasi khusus	Rendah
		NR-09	3	Jika terjadi akan mengakibatkan kerusakan switch dan perangkat lain tidak dapat terhubung satu sama lain	3	Switch disimpan di ruangan tertentu	Sedang
Manusia	Pegawai	PR-01	5	Jika terjadi orang yang tidak bertanggung jawab membobol sistem yang ada di DPTSI sehingga proses bisnis di ITS menjadi terganggu	1	Belum pernah terjadi	Sedang

Kategori Aset	Aset	Risk ID	Nilai Dampak	Justifikasi Dampak	Nilai Probabilitas	Justifikasi Probabilitas	Level
		PR-02	1	Untuk pekerjaan berisiko tinggi atau diluar bidang DPTSI dilkukan oleh pihak ketiga	2	Untuk aktivitas khusus, sudah menggunakan peralatan keamanan sesuai dengan standar	Rendah
		PR-03	1	Tidak akan mengganggu proses bisnis DPTSI	1	Belum pernah terjadi	Rendah
		PR-04	1	Tidak akan mengganggu proses bisnis DPTSI	1	Belum pernah terjadi	Rendah

6.3 Mitigasi Risiko

Setelah melakukan penilaian terharap risiko, selanjutnya akan dilakukan identifikasi atau pemilihan kontrol meminimalkan risiko yang akan dilakukan sesuai dengan jenis risiko dan menggunakan acuan standar ISO/IEC 27002:2013

Tabel 6.3 Mitigasi Risiko

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
Server	HR-01	Kerusakan Perangkat Keras	Kesalahan konfigurasi	Sedang	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	*Treat*	Melakukan pengecekan berulang untuk memastikan konfigurasi server	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2d	Orang	2
					12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosesdur untuk setiap pengguna yang membutuhkan	*Treat*	Membuat prosedur konfigurasi dan pengecekan secara berkala terhadap konfigurasi	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64	Kebijakan	2

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
								yang sudah dilakukan	ayat 2a		
	HR-02		AC diruangan server mati	Sedang	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosesdur untuk setiap pengguna yang membutuhkan	*Treat*	Membuat prosedur monitoring terhadap AC Presisi	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2a	Kebijakan	3
					11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari	*Treat*	Memastikan kesesuaian penanganan AC presisi sesuai dengan	Peraturan Rektor Nomor 10	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung		ketentuan dari pabrik	Tahun 2016 Pasal 64 ayat 2c		
	HR-03		Memory server penuh	Sedang	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	*Treat*	Membuat prosedur monitoring aset	Peraturan Rektor Nomor 10 Tahun 2016 Pasal	Kebijakan	2

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
					12.1.3 *Capacity management*	Kontrol yang memastikan penggunaan dari sumber daya haruslah dipantau, disesuaikan, dan proyeksi untuk kebutuhan kapasitas di masa yang akan datang untuk memastikan kinerja sistem sesuai dengan kebutuhan	*Treat*	Melakukan pengecekan secara rutin untuk memastikan ketersediaan *space* pada server	64 ayat 2c	Kebijakan	2

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
	HR-07	Kerusakan Perangkat Keras	Pasokan listrik terputus	Sedang	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung	*Treat*	Memastikan genset tersedia jika terjadi pemadaman listrik oleh PLN	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2b	Kebijakan	3
	HR-08	Sistem informasi/server tidak bisa diakses	Pasokan listrik terputus	Sedang	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan	*Treat*	Memastikan genset tersedia jika terjadi pemadaman listrik oleh PLN	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						dalam aset pendukung			ayat 2b		
	HR-10	Sistem informasi/server tidak bisa diakses	Serangan *cyber crime*	Sedang	11.1.4 *Protecting against external and environment threat*	Kontrol yang memastikan perlindungan fisik seperti bencana alam, serangan jahat, atau kecelakaan	*Treat*	Melakukan pengecekan/ *update* secara rutin pada server	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2c	Sistem	3
	HR-11	Kerusakan Perangkat Keras	Serangan *cyber crime*	Sedang	11.1.4 *Protecting against external and environment threat*	Kontrol yang memastikan perlindungan fisik seperti bencana alam, serangan jahat,	*Treat*	Melakukan pengecekan/update secara rutin pada server	Peraturan Rektor Nomor 10 Tahun 2016	Sistem	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						atau kecelakaan			Pasal 64 ayat 2c		
	HR-12	Kerusakan Perangkat Keras	Bencana (Gempa bumi, kebakaran)	Sedang	11.1.4 *Protecting against external and environment threat*	Kontrol yang memastikan perlindungan fisik seperti bencana alam, serangan jahat, atau kecelakaan	*Take*	Pembuatan *Disaster Recovery Plan*	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2a	Kebijakan	2
					12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	*Treat*	Pembuatan presedur backup dan restore	Peraturan Rektor Nomor 10 Tahun 2016	Kebijakan	2

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
									Pasal 64 ayat 2a		
					12.3.1 *Information backup*	Kontrol yang memastikan salinan dari cadangan informasi, perangkat lunak, dan gambar sistem harus dilakukan dan diuji secara berkala sesuai dengan kebijakan yang berlaku	*Treat*	Melakukan backup informasi/data secara teratur	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2d	Kebijakan	2

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
Genset	HR-20	Kerusakan Perangkat Keras	Genset tidak mampu bekerja dengan baik	Sedang	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung	*Transfer*	Pengecekan rutin untuk kesiapan genset menyuplai listrik untuk seluruh server serta aset pendukung	Dilakukan oleh pihak di luar DPTSI	Kebijakan	3
					11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan	*Transfer*	Melakukan maintenance secara rutin untuk menjaga kinerja genset tetap optimal	Dilakukan oleh pihak di luar DPTSI	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						dalam proses bisnis					
Sistem Informasi	SR-01	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Data base error	Sedang	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	*Treat*	Melakukan maintenance dan pengecekan secara berkala konfigurasi dari database	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2d	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
					12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	*Treat*	Membuat prosedur konfigurasi dan pengecekan secara berkala terhadap konfigurasi yang sudah dilakukan	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2a	Kebijakan	3
	SR-02		Server mati	Sedang	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan	*Treat*	Melakukan maintenance secara rutin untuk menjaga kinerja genset tetap optimal	Dilakukan oleh pihak di luar DPTSI	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						dalam aset pendukung					
	SR-03		storage/memory penuh (belum fleksibel/cloud)	Sedang	12.1.3 *Capacity management*	Kontrol yang memastikan penggunaan dari sumber daya haruslah dipantau, disesuaikan, dan proyeksi untuk kebutuhan kapasitas di masa yang akan datang untuk memastikan kinerja sistem	*Treat*	Melakukan pengecekan secara rutin untuk memastikan ketersediaan *space* pada server	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2c	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						sesuai dengan kebutuhan					
	SR-04	Pembobolan sistem oleh pihak yang tidak bertanggung jawab	Cyber crime	Sedang	11.1.4 *Protecting against external and environment threat*	Kontrol yang memastikan perlindungan fisik seperti bencana alam, serangan jahat, atau kecelakaan	*Treat*	Melakukan investigasi secara berkala untuk memastikan tidak ada celah keamanan sistem informasi	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2d	Sistem	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
					10.1.1 *Policy on the use of cryptographic controls*	Kontrol yang memastikan penggunaan kriptografi secara tepat dan efektif untuk melindungi data atau informasi yang pada organisasi	*Treat*	Menggunakan kriptografi untuk melindungi data atau informasi yang ada di dalam sistem informasi	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2d	Kebijakan	2
					12.4.1 *Event logging*	Kontrol yang mengatur mengenai log kejadian yang merekam aktivitas penggu-na, kesalahan, dan kejadian terkain keamanan	*Treat*	Pembuatan event log untuk mecatat seluruh kejadian yang terjadi didalam sistem informasi	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2c	Sistem	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						informasi yang harus dibuat dan ditinjau secara berkala					
	SR-05	Orang dapat mengakses data/informasi yang bukan haknya/ Penyalahgunaan wewenang	Hak akses pegawai yang mutasi/pensiun belum diganti/dihapus	Sedang	9.2.6 *Removal or adjusment of access rights*	Kontrol yang memastikan hak akses untuk semua karyawan dan pengguna eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan kerja, kontrak, atau perjanjian	*Treat*	Memastikan hak akses sesuai dengan jabatan dan tanggung jawab setiap untuk setiap pengguna dan penghapusan hak akses untuk pegawai yang sudah tidak bekerja	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 67 ayat 2b	Orang	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						atau disesuaikan dengan perubahan					
					9.2.3 *Management of previlaged access rights*	Kontrol yang memastikan alokasi dan penggunaan hak akses harus dibatasi dan dikontrol/ dikendalikan	*Treat*	Memastikan *role* akses sesuai dengan jabatan dan tanggung jawab setiap untuk setiap pengguna	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 67 ayat 2b	Orang	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
					9.4.1 *Information access restriction*	Kontrol yang memastikan akses terhadap informasi dan fungsi sistem aplikasi harus dibatasi berdasarkan kebijakan kontrol akses	*Treat*	Membatasi setiap hak akses sesuai dengan kebijakan organisasi	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 67 ayat 2b	Sistem	3
Database	DR-01	Data penting rusak/tidak dapat diakses	Data *corruption*	Sedang	12.3.1 *Information backup*	Kontrol yang memastikan salinan dari cadangan informasi, perangkat lunak, dan gambar sistem harus dilakukan dan diuji secara	*Treat*	Melakukan backup database secara teratur	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2d	Sistem	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						berkala sesuai dengan kebijakan yang berlaku					
	DR-02		Kesalahan konfigurasi	Sedang	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	*Treat*	Melakukan pengecekan berkala terhadap database	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2c	Orang	3
					12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap	*Treat*	Membuat prosedur konfigurasi dan pengecekan secara berkala	Peraturan Rektor Nomor 10 Tahun	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						pengguna yang membutuhkan		terhadap konfigurasi yang sudah dilakukan	2016 Pasal 65 ayat 2a		
					12.4.1 *Event logging*	Kontrol yang mengatur mengenai log kejadian yang merekam aktivitas pengguna, kesalahan, dan kejadian terkain keamanan informasi yang harus dibuat dan ditinjau secara berkala	*Treat*	Pembuatan event log untuk mecatat seluruh kejadian yang terjadi didalam database	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2c	Sistem	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
	DR-03		Data loss	Sedang	12.3.1 *Information backup*	Kontrol yang memastikan salinan dari cadangan informasi, perangkat lunak, dan gambar sistem harus dilakukan dan diuji secara berkala sesuai dengan kebijakan yang berlaku	*Treat*	Melakukan pengecekan backup database secara teratur	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2c	Orang	3
	DR-04	Data penting diubah/dicuri	Cyber crime	Tinggi	10.1.1 *Policy on the use of cryptographic controls*	Kontrol yang memastikan penggunaan kriptografi secara tepat dan efektif untuk	*Treat*	Menggunakan kriptografi untuk melindungi data atau informasi yang ada di	Peraturan Rektor Nomor 10 Tahun 2016	Sistem	1

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						melindungi data atau informasi yang pada organisasi		dalam database	Pasal 65 ayat 2d		
Router	NR-02	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Hilangnya pasokan listrik	Sedang	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung	*Treat*	Pengecekan rutin untuk kesiapan *genset* menyuplai listrik untuk seluruh server serta aset pendukung dari server	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2b	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
	NR-03		Kesalahan konfigurasi	Sedang	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	*Treat*	Melakukan maintenance secara rutin untuk menjaga *router* tetap optimal	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2d	Orang	2
					12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	*Treat*	Membuat prosedur konfigurasi dan pengecekan secara berkala terhadap konfigurasi yang sudah dilakukan	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2a	Kebijakan	2

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
Switch	NR-09	Kerusakan Perangkat Keras	Debu dan kotoran	Sedang	11.2.1 *Equipment siting and protection*	Kontrol yang memastikan peralatan atau aset diletakkan dan dilindungi untuk mengurangi risiko dan ancaman dari lingkungan dan kemungkinan akses dari pihak yang tidak sah	*Treat*	Penyimpanan switch terbebas dari debu dan kotoran yang dapat mengganggu kinerja dari aset	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2d	Sistem	3
					11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat	*Treat*	Melakukan maintenance secara rutin untuk menjaga switch genset tetap optimal	Peraturan Rektor Nomor 10 Tahun 2016 Pasal	Orang	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						digunakan dalam proses bisnis			64 ayat 2c		
					12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	*Treat*	Membuat prosedur konfigurasi dan pengecekan secara berkala terhadap konfigurasi yang sudah dilakukan	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 64 ayat 2a	Kebijakan	3
Pegawai	PR-01	Pembobolan sistem oleh pihak yang tidak bertan	Penyalahgunaan wewenang	Sedang	6.1.1 *Information security roles and responsibilities*	Kontrol yang memastikan semua tanggung jawab keamanan informasi harus didefinisikan	*Treat*	Pendefinisian fungsi dan tanggung jawab secara jelas untuk setiap pegawai	Dilakukan oleh pihak diluar DPTSI	Kebijakan	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
		ggung jawab				dan dialokasikan					
					7.1.2 *Term and conditions of employment*	Kontrol yang menngatur mengenai perjanjian mengenai tanggung jawab pegawai, kontraktor, dan organisasi terhadap keamanan informasi	*Treat*	Pembuatan perjanjian tanaggung jawab mengenai keamanan informasi untuk semua pegawai	Dilakukan oleh pihak di luar DPTSI	Orang	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
					7.2.2 *Information security awareness, education, and training*	Kontrol yang mengatur mengenai pendidikan dan pelatihan terhadap karyawan dan kontraktor mengenai keamanan informasi secara rutin sesuai dengan fungsi masing-masing	*Treat*	Melakukan pelatihan dan edukasi keamanan informasi terhadap karyawan secara rutin	Dilakukan oleh pihak di luar DPTSI	Orang	3
					9.2.3 *Management of previlaged access rights*	Kontrol yang memastikan alokasi dan penggunaan hak akses harus dibatasi dan	*Treat*	Memastikan *role* akses sesuai dengan jabatan dan tanggung jawab setiap	Peraturan Rektor Nomor 10 Tahun 2016	Orang	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						dikontrol/dikendalikan		untuk setiap pengguna	Pasal 67 ayat 2b		
					9.2.6 *Removal or adjusment of access rights*	Kontrol yang memastikan hak akses untuk semua karyawan dan pengguna eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan kerja, kontrak, atau perjanjian atau disesuaikan	*Treat*	Memastikan hak akses sesuai dengan jabatan dan tanggung jawab setiap untuk setiap pengguna dan penghapusan hak akses untuk pegawai yang sudah tidak bekerja	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 67 ayat 2b	Orang	3

Aset	Risk ID	Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Mitigasi	Bentuk mitigasi	Dasar Mtigasi	Sasaran Mitigasi	Nilai Implementasi
						dengan perubahan					
					12.4.3 *Administrator and operator logs*	Kontrol yang memastikan aktivitas admin dan operator sistem harus dicatat dan dilindungi dan dilakukan peninjauan secara berkala	*Treat*	Memastikan seluruh aktivitas dari admin dan operator dari sistem informasi tercatat pada log	Peraturan Rektor Nomor 10 Tahun 2016 Pasal 65 ayat 2c	Sistem	3

BAB VII
KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dan saran yang bermanfaat untuk perbaikan atau masukan yang bermanfaat untuk penelitian selanjutnya.

7.1 Kesimpulan

Kesimpulan yang dibuat merupakan jawaban dari perumusan masalah yang didefinisikan sebelumnya yang berdasarkan dari hasil penelitian yang telah dilakukan. Kesimpulan yang didapat adalah:

1. Hasil identifikasi risiko yang telah dilakukan didapatkan 47 risiko yang terdiri atas satu risiko dengan level tinggi, 23 risiko dengan level sedang, dan 23 risiko dengan level rendah.
2. Berdasarkan prioritas risiko yang diambil dari risiko dengan level tinggi dan sedang, diidentifikasi 13 kontrol mitigasi risiko berdasarkan ISO/IEC 27002:2013, yaitu :
   a. *6.1.1 Information security roles and responsibilites*
   b. *7.1.2 Term and conditions of employment*
   c. *7.2.2 Information security awareness, education, and training*
   d. *9.2.3 Management of previlaged access rights*
   e. *10.1.1 Policy on the use of cryptographic controls*
   f. *11.1.4 Protecting against external and environment threat*
   g. *11.2.1 Equipment siting and protection*
   h. *11.2.2 Supporting Utilities*
   i. *11.2.4 Equipment Maintenance*
   j. *12.1.1 Documented operations procedures*
   k. *12.1.3 Capacity management*
   l. *12.3.1 Information backup*
   m. *12.4.1 Event logging*

7.2 Saran

Saran penulis kepada peneliti selanjutnya yang akan melakukan penelitian serupa adalah sebagai berikut:

1. Dalam penelitian ini proses identifikasi aset berdasarkan hasil wawancara, dan observasi oleh peneliti. Proses penilaian mencakup pada seluruh aset yang ditemukan tanpa mengolah terlebih dahulu aset kritis yang dimiliki oleh organisasi, maka dari itu sebaiknya melakukan identifikasi terhadap aset kritis dahulu.
2. Metode penilaian penulis berdasarkan PMBOK yang disesuaikan dengan justifikasi organisasi, diharapkan untuk penelitian selanjutnya menggunakan standar lain.

DAFTAR PUSTAKA

[1] International Organization for Standardization ISO, "Risk management - Principles and guidelines," *ISO 310002009*, vol. 31000, p. 24, 2009.

[2] D. ITS, "Tentang DPTSI," 2017. [Online]. Available: https://dptsi.its.ac.id/. [Accessed: 28-Dec-2017].

[3] F. A. Basyarahil, H. M. Astuti, and C. Hidayanto, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya," vol. 6, no. 1, 2017.

[4] Isaca Germany, "Implementation Guideline A practical guideline for implementing an ISMS," p. 64, 2013.

[5] I. Desy, B. C. Hidayanto, and H. M. Astuti, "Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effects Analysis di Divisi TI PT. Bank XYZ Surabaya," *Semin. Nas. Sist. Inf. Indones.*, no. September, pp. 467–472, 2014.

[6] International Organization for Standardization ISO, "Information technology - Security techniques - Information security management systems - Reuirements," *Iso 270012013*, vol. 2013, 2013.

[7] International Organization for Standardization ISO, "Information technology - Security techniques - Code of practice for information security controls," *Iso 270022013*, vol. 2013, 2013.

[8] K. H. Dewantara, "Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Berdasarkan Standar ISO 27001 : 2005 dan ISO 27002 : 2013 Menggunakan Metode FMEA (Studi Kasus : ISNET)," 2016.

[9] C. U. Putri, "Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 pada Helpdesk Subdirektorat Layanan Teknologi dan Sistem Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember," 2017.

[10] D. I. Rachmawan, *Pembuatan Dokumen SOP (Standar Operasional Prosedur) Keamanan Aset Informasi yang Mengacu pada Kontrol Kerangka Kerja ISO 27002 : 2013 (Studi Kasus: CV CempakaTulungagung)*. 2017.

[11] DPTSI, "Struktur Organisasi DPTSI," 2017. [Online]. Available: https://dptsi.its.ac.id/?page_id=152. [Accessed: 28-Dec-2017].

[12] F. Global, "CLARIFYING ROLES & RESPONSIBILITIES WITH THE RACI," no. September, 2016.

[13] KBBI, "Aset." [Online]. Available: https://kbbi.web.id/aset. [Accessed: 28-Dec-2017].

[14] M. E. Whitman and H. J. Mattord, *Principles of Information Security Third Edition*, Third edit. 2009.

[15] International Organization for Standardization ISO, "Information technology. Security techniques. Management of information and communications technology security. Concepts and models for information and communications technology security management," *ISO/IEC 13335-1:2004*, 2004.

[16] National Archives of UK, "Identifying Information Assets and Business Requirements," *Natl. Arch.*, pp. 1–25, 2011.

[17] M. E. Whitman and H. J. Mattord, "Principles of Information Security Fifth Edition," 2016.

[18] Microsoft, "Strategies for Managing Malware Risks," 2006. [Online]. Available: https://msdn.microsoft.com/en-us/library/cc875818.aspx#EAAA. [Accessed: 16-Jan-2018].

[19] G. T. F. Brooke, "Uncertainty, profit and entrepreneurial action: Frank Knight's contribution reconsidered," *J. Hist. Econ. Thought*, vol. 32, no. 2, pp. 221–235, 2010.

[20] Symantec Corporation, "Assets, Threats and Vulnerabilities: Discovery and Analysis," pp. 1–9, 2012.

[21] N. Evans and J. Price, "Responsibility and

Accountability for Information Asset Management (IAM) in Organisations," vol. 17, no. 1, pp. 113–121, 2014.

[22] L. A. Cox, "Some limitations of 'risk = threat x vulnerability x consequence' for risk analysis of terrorist attacks," *Risk Anal.*, vol. 28, no. 6, pp. 1749–1761, 2008.

[23] Y. J. Kim, E. J. Garrity, and G. L. Sanders, "Success Measures of Information Systems," *Encycl. Inf. Syst.*, vol. 4, no. May, p. 299.1-299.15, 2003.

[24] Y. Dwivedi *et al.*, "Institutional Repository Research on information systems failures and successes : status update and future directions Research on Information Systems Failures and Successes : Status Update and Future Directions," *Inf. Syst. Front.*, vol. 17, no. 1, pp. 143–157, 2015.

[25] R. Hirschheim and M. Newman, "Information systems and user resistance theory and practice. The Computer Journal," pp. 398–408, 1988.

[26] C. Sauer, "Why information systems fail: a case study approach," 1993.

[27] R. R. Nelson, "IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices," *MIS Q. Exec.*, vol. 6, no. 2, pp. 67–78, 2007.

[28] D. M. Strong and O. Volkoff, "Understanding Organization–Enterprise System Fit: A Path To Theorizing The Information Technology Artifact," vol. 34, no. 4, pp. 731–756, 2010.

[29] R. Heeks, "Information systems and developing countries: failure, success, and local improvisations," *Inf. Soc.*, vol. 18, no. 2, pp. 101–112, 2002.

[30] R. Heeks, "Health information systems: Failure, success and improvisation," *Int. J. Med. Inform.*, vol. 75, no. 2, pp. 125–137, 2006.

[31] T. Klaus and J. E. Blanton, "User resistance determinants and the psychological contract in enterprise system implementations," *Eur. J. Inf. Syst.*, vol. 19, no. 6, pp. 625–636, 2010.

[32] "Manajemen Risiko." [Online]. Available: http://searchcompliance.techtarget.com/definition/risk-management. [Accessed: 31-May-2017].
[33] M. Herrera, "Risk Control," 2013. [Online]. Available: https://www.mha-it.com/2013/03/the-four-ts-process/. [Accessed: 31-May-2017].
[34] M. E. Whittman and H. J. Mattord, "Management of Information Security Fourth Edition," p. 545, 2013.
[35] International Organization for Standardization ISO, "Information technology - Security technique - Information security risk management," *ISO 270052011*, vol. 2011, 2011.
[36] International Organization for Standardization, "Risk management — Principles and guidelines," 2009. [Online]. Available: https://www.iso.org/iso-31000-risk-management.html. [Accessed: 13-Feb-2018].
[37] Project Management Institute, *Project Management Body of Knowledge: A Guide to the Project Management Body of Knowledge (6th Edition)*. 2017.
[38] R. Sarno and I. Iffano, "Sistem Manajemen Keamanan Informasi," 2009.
[39] Bundesamt für Sicherheit in der Informationstechnik, "BSI-Standard 100-1: Information Security Management Systems (ISMS)," pp. 1–38, 2008.
[40] D. S. Informasi and D. J. A. Telematika, "Pedoman Praktis Manajemen Keamanan Informasi Untuk Pimpinan Organisasi 10 Rekomendasi Terbaik Manajemen Keamanan Informasi," pp. 1–22, 2007.
[41] E. Humphreys, "Information security management system standards," *Datenschutz und Datensicherheit - DuD*, vol. 35, no. 1, pp. 7–11, 2011.
[42] ISO, "ISO/IEC 27001:2013," 2013. [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed: 30-May-2017].
[43] M. A. Ramadhana, "Pembuatan Perangkat Audit Internal TI Berbasis Resiko Menggunakan ISO / IEC 27002 :2007 Pada Proses Pengelolaan Data Studi Kasus

Digital Library ITS," 2007.

[44] J. Gustafsson, "Single case studies vs. multiple case studies: A comparative study," *Acad. Business, Eng. Sci. Halmstad Univ. Sweden*, p. 15, 2017.

Halaman ini sengaja dikosongkan

BIODATA PENULIS

Penulis bernama lengkap Alif Satria Perdana, biasa dipanggil Satria atau Alif. Lahir di Ujung Pandang, 18 Mei 1996 merupakan anak tunggal. Penulis telah menempuh pendidikan formal di SD Inpres Batua 1 Makassar, SMPN 8 Makassar, dan SMAN 17 Makassar. Kemudian diterima di Perguruan Tinggi Negeri ITS Surabaya pada tahun 2014 Departemen Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi. Selama menjadi mahasiswa, penulis aktif dalam kepengurusan Badan Eksekutif Mahasiswa Fakultas Teknologi Informasi dan Komunikasi pada tahun 2015-2017. Penulis pernah melakukan Kerja Praktik pada kantor pusat PT. Semen Tonasa, Biringere, Pangkep. Pengerjaan Tugas Akhir ini penulis memilih laboratorium Manajemen Sistem Informasi (MSI) sebagai tempat bernaung dalam menyelesaikan Tugas Akhir ini. Penulis dapat dihubungi melalui email alifsperdana@gmail.com.

Halaman ini sengaja dikosongkan

LAMPIRAN A

INTERVIEW PROTOCOL

Lampiran ini berisikan pertanyaan *interview protocol* yang dilakukan di DPTSI ITS.

Informasi Pelaksanaan Wawancara	
Tujuan	Mengetahui gambaran Tata Kelola Keamanan Informasi, seperti tupoksi, peran dan tanggung jawab dalam pengelolaan keamanan sistem informasi dari pimpinan unit kerja hingga ke operasional.
Tanggal	
Waktu	
Tempat	
Narasumber	
Jabatan	

No	**Pertanyaan**	**Jawaban**
1	Bagaimana struktur organisasi SubDit Pengembangan Sistem Informasi ITS Surabaya?	
2	Siapa saja *stakeholder* dari SubDit Pengembangan Sistem Informasi ITS Surabaya?	
3	Bagaimana proses bisnis di KaSubDit Pengembangan Sistem Informasi ITS Surabaya?	
4	Bagaimana bentuk pemanfaatan sistem informasi dalam menjalankan proses bisnis sehari-hari?	

A-2

No	Pertanyaan	Jawaban
5	Apa saja aktivitas pada KaSubDit Pengembangan Sistem Informasi ITS Surabaya?	
6	Siapa saja penanggung jawab untuk setiap aktivitas yang ada di KaSubDit Pengembangan Sistem Informasi ITS Surabaya? (Petakan dalam tabel RACI)	
7	Bagaimana prosedur pelaporan jika terjadi insiden atau risiko terkait dengan sistem informasi?	
8	Bagaimana bentuk alokasi anggaran keamanan sistem informasi di KaSubDit Pengembangan Sistem Informasi ITS Surabaya?	

No	Aplikasi	Anny Yuniarti S.Kom., M.Comp.SC	Rizky Januar Akbar, S.Kom., M.Eng	Akhmad Budi K.	Dinar Sekti, S.Kom	Umar Hasan, S.Kom	Rahmad Santoso	Yudhha Nugraha, S.Kom	Ali Mansur	Yoga Ari Tofan	Rangga Dias Novitra	M. Ziqqi Alfiam	Fitria Rizky Aprilina	M. Riduwan
1														
2														
3														
4														
5														
6														
7														

Informasi Pelaksanaan Wawancara	
Tujuan	1. Mengetahui daftar aset sistem informasi yang ada di Direktorat Pengembangan Teknologi Sistem Informasi KaSubDit Pengembangan Sistem Informasi ITS Surabaya. 2. Mengetahui daftar kontrol keamanan sistem informasi yang sudah diterapkan atau masih dalam tahap perancangan, seperti kebijakan, dan peratutan 3. Mengetahui daftar kejadian terkait keamanan sistem informasi yang pernah terjadi di DPTSI, seperti server *down*, pengguna tidak dapat melakukan akses, dll.
Tanggal	
Waktu	
Tempat	
Narasumber	
Jabatan	

No	Pertanyaan	Jawaban
1	Aset sistem informasi (*hardware*, *software*, *data*, *network*, *people*, *procedure*) apa saja yang ada di DPTSI ITS?	Cek tabel *checklist* aset
2	Apa saja insiden yang biasa terjadi pada aset tersebut? Dan bagaimana bentuk penanganan setiap insiden yang terjadi?	Cek tabel *checklist* insiden

No	Pertanyaan	Jawaban
3	Bagaiamana bentuk kontrol pada setiap aset yang ada di DPTSI ITS?	*crosscheck* berdasarkan *checklist* aset
4	Apa saja kerentanan yang pernah terjadi di DPTSI?	Cek tabel *checklist* kerentanan
5	Apakah bentuk penanganan insiden yang telah dilakukan sekarang telah cukup atau masih terdapat kekurangan?	
6	Apakah dalam pengelolaan insiden atau risiko telah berdasarkan standar tertentu?	
7	Bagaimana suatu insiden atau risiko dapat dideteksi ?	
9	Apakah terdapat klasifikasi atau kategori untuk setiap risiko yang terjadi?	
9	Bagaimana suatu risiko dicatat?	
10	Apakah catatan tersebut disimpan dalam direktori khusus?	
11	Detail informasi apa saja yang dicatat dalam data insiden terkait sistem informasi?	
12	Apakah terdapat prioritas khusus dalam penyelesaian insiden terkait risiko sistem informasi yang terjadi?	
13	Apakah terdapat prosedur khusus yang dilakukan dalam meminimalkan risiko?	
14	Bagaimana bentuk penanganan jika terjadi risiko yang belum pernah terjadi	

No	Pertanyaan	Jawaban
	sebelumnya? Terutama jika memerlukan penanganan khusus?	
15	Ketika risiko terjadi, apakah akan dilakukan proses investigasi untuk mengetahui sumber risiko?	
16	Apakah dilakukan proses investigasi secara rutin?	
17	Bagaimana pengambilan atau pembuatan solusi pemulihan insiden terkait keamanan sistem informasi ditentutkan?	
18	Apakah solusi yang dibuat dilakukan *testing* atau diuji coba terlebih dahulu?	
19	Apakah terdapat SOP khusus dalam melakukan penyelesaian suatu insiden ?	
20	Berapa lama waktu yang dibutuhkan dalam menyelesaiakan suatu insiden?	
21	Apakah pernah dilakukan identifikasi risiko terkait keamanan sistem informasi sebelumnya?	
22	Bagaimana DPTSI melakukan monitoring terhadap kejadian atau insiden terkait keamanan sistem informasi?	

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
1	Perangkat keras	Server		
2		Komputer *desktop* / Laptop		
3		Telepon seluler		
4		Mesin fax		
5		*Removable media* (kaset, disket, USB, dll)		
6		Sistem pemadam api		
7		Sistem pendingin udara		
8	Perangkat lunak	*Source code*		
9		*Software* berlisensi		
10		Sistem informasi		

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
11	Data	Data sumber daya manusia		
12		Data keuangan		
13		Data karyawan		
14		Data mitra		
15		Dokumentasi aset		
16	Jaringan	*Dial-up remote access*		
17		Jaringan telepon / Kabel Jaringan		
18		*Routers*		
19		*Switch* jaringan		
20		Akses *virtual private networking (VPN)*		
21		Layanan kolaborasi *(*contoh *microsoft sharepoitnt)*		

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
22		*Domain Name System (DNS)*		
23		*Dynamic host configuration protocol (DHCP)*		
24		*Access point*		
26	Manusia	Pegawai		

No.	Ancaman	Checklist
Bencana		
1	Kebakaran	
2	Banjir	
3	Gempa bumi	
4	Badai	
5	Serangan teroris	
6	Kerusuhan	
7	Tanah longsor	
8	Salju longsor	
9	Kecelakaan industri	
Kesalahan Mekanik		
10	Mati listrik	
11	Kesalahan kontrol lingkungan	
12	Kecelakaan konstruksi	
Non-orang jahat		
13	Kurangnya informasi pegawai	
14	Kurangnya informasi pengguna	
Orang jahat		
15	*Hacker, cracker*	
16	*Computer criminal*	
17	Spionase industri	
18	Spionase pemerintah	
19	*Social engineering*	
20	Pegawai yang tidak puas	
21	Bekas pegawai yang tidak puas	
22	Teroris	
23	Pegawai lalai	
24	Pegawai yang tidak jujur	
25	*Code mobile* berbahaya	
Perangkat keras		
26	Kerusakan	
27	Pencurian	
28	Kesalahan konfigurasi	

No.	Ancaman	Checklist
Perangkat lunak		
29	*Bug* pada perangkat lunak	
30	Serangan virus	
31	Kesalahan konfigurasi	
32	Kesalahan *input* data	
33	Pembobolan sistem	
Jaringan		
34	Gangguan pada *router*	
35	Kerusakan kabel jaringan	
36	Hilang/pencurian perangkat jaringan	
37	Gangguan koneksi internet	

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
1	Fisik	Pintu yang tidak terkunci		
2	Fisik	Fasilitas komputer yang tidak dijaga		
3	Fisik	Sistem pemadaman api tidak memadai		
4	Fisik	Desain gedung yang buruk		
5	Fisik	Konstruksi gedung yang buruk		
6	Fisik	Konstruksi menggunakan material yang mudah terbakar		
7	Fisik	*Finishing* menggunakan material yang mudah terbakar		
8	Fisik	Jendela yang tidak terkunci		

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
9	Fisik	Dinding yang rentan terhadap serangan fisik (rapuh)		
10	Fisik	Dinding ruangan tidak tertutup rapat		
11	Alam	Fasilitas berada di tempat yang salah		
12	Alam	Fasilitas berada di zona banjir		
13	Alam	Fasilitas berada di zona longsor		
14	Perangkat keras	Terdapat *patch* yang hilang		
15	Perangkat keras	*Firmware* yang telah usang		
16	Perangkat keras	Kesalahan konfigurasi sistem		
17	Perangkat keras	Sistem tidak terlindungi secara fisik		

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
18	Perangkat keras	Protokol manajemen terbuka untuk umum		
19	Perangkat lunak	Antivirus yang kadaluarsa (tidak *update*)		
20	Perangkat lunak	*Patch* yang tidak lengkap atau hilang		
21	Perangkat lunak	Aplikasi yang ditulis dengan buruk	*Cross site scripting*	
22	Perangkat lunak	Aplikasi yang ditulis dengan buruk	SQL *injection*	
23	Perangkat lunak	Aplikasi yang ditulis dengan buruk	Kelemahan pada *code* seperti *buffer overflows*	
24	Perangkat lunak	Kesengajaan membuat kelemahan	*Vendor backdoors* untuk manajemen atau *system recovery*	

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
25	Perangkat lunak	Kesengajaan membuat kelemahan	*Spyware* seperti *keyloggers*	
26	Perangkat lunak	Kesengajaan membuat kelemahan	*Trojan horses*	
27	Perangkat lunak	Kesengajaan membuat kelemahan		
28	Perangkat lunak	Kesalahan konfigurasi	Sistem tidak diamankan	
29	Perangkat lunak	Kesalahan konfigurasi	Sistem tidak diaudit	
30	Perangkat lunak	Kesalahan konfigurasi	Sistem tidak dipantau	
31	Media	Gangguan listrik		
32	Jaringan	Protokol jaringan yang tidak terenkripsi		
33	Jaringan	Koneksi terhubungan ke banyak jaringan		

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
34	Jaringan	Mengizinkan protokol yang tidak perlu		
35	Jaringan	Tidak ada penyaringan antara segmen jaringan		
36	Manusia	Prosedur didefinisikan dengan buruk	Respon yang tidak memadai	
37	Manusia	Prosedur didefinisikan dengan buruk	Penyediaan secara manual	
38	Manusia	Prosedur didefinisikan dengan buruk	*Disaster recovery plans* yang tidak memadai	
39	Manusia	Prosedur didefinisikan dengan buruk	Melakukan *testing* pada sistem produksi	
40	Manusia	Prosedur didefinisikan dengan buruk	Kontrol perubahan yang buruk	

LAMPIRAN B

HASIL *INTERVIEW PROTOCOL*

Informasi Pelaksanaan Wawancara	
Tujuan	Mengetahui gambaran Tata Kelola Keamanan Informasi, seperti tupoksi, peran dan tanggung jawab dalam pengelolaan keamanan sistem informasi dari pimpinan unit kerja hingga ke operasional.
Tanggal	23 Mei 2018
Waktu	10.00 – 11.00 WIB
Tempat	Informatika ITS
Narasumber	Anny Yuniarti, S.Kom., M.Comp.Sc.
Jabatan	KaSubDit Pengembangan Sistem Informasi DPTSI ITS

No	Pertanyaan	Jawaban
1	Bagaimana struktur organisasi SubDit Pengembangan Sistem Informasi ITS Surabaya?	Subdit Pengembangan Sistem Informasi terdapat 13 orang yang terdiri atas 1 Kepala, 1 Kasi, 9 pegawai permanen, dan 3 pegawai tidak tetap
2	Siapa saja *stakeholder* dari SubDit Pengembangan Sistem Informasi ITS Surabaya?	*Stakeholder* dari SubDit Pengembangan Sistem Informasi terdiri dari atas: • Atasan langsung, direktur DPTSI, Wakil Rektor 3 • Unit diluar DPTSI, dibawah rektorat
3	Bagaimana proses bisnis di KaSubDit Pengembangan	Pengembangan Sistem Informasi *Maintain* aplikasi

B-2

No	Pertanyaan	Jawaban
	Sistem Informasi ITS Surabaya?	Penanganan masalah terhadap aplikasi
4	Bagaimana bentuk pemanfaatan sistem informasi dalam menjalankan proses bisnis sehari-hari?	Sebagai *tools* pengembangan aplikasi dan alur komunikasi (WA, email, telepon)
5	Apa saja aktivitas pada KaSubDit Pengembangan Sistem Informasi ITS Surabaya?	Penanganan komplain dari unit Pengembangan sistem informasi sesuai dengan permintaan
6	Siapa saja penanggung jawab untuk setiap aktivitas yang ada di KaSubDit Pengembangan Sistem Informasi ITS Surabaya? (Petakan dalam tabel RACI)	Pembagian tanggung jawab dibagi berdasarkan sistem informasi yang ada
7	Bagaimana prosedur pelaporan jika terjadi insiden atau risiko terkait dengan sistem informasi?	Umumnya pelaporan dilakukan ke bagian layanan terlebih dahulu, kemudian diteruskan ke SubDit Pengembangan Sistem Informasi, tetapi biasa juga terjadi langsung menghubungin pihak SubDit Pengembangan Sistem Informasi tanpa melalui SubDit Layanan
8	Bagaimana bentuk alokasi anggaran keamanan sistem informasi di KaSubDit	Untuk alokasi angggaran sudah ditentukan terlebih dahulu tetapi jika terdapat permintaan lain tetap dikerjakan tanpa proses penganggaran

No	Pertanyaan	Jawaban
	Pengembangan Sistem Informasi ITS Surabaya?	

No	Aplikasi	Anny Yuniarti S.Kom., M.Comp.SC	Rizky Januar Akbar, S.Kom., M.Eng	Akhmad Budi K.	Dinar Sekti, S.Kom	Umar Hasan, S.Kom	Rahmad Santoso	Yudhha Nugraha, S.Kom	Ali Mansur	Yoga Ari Tofan	Rangga Dias Novitra	M. Ziqqi Alfiam	Fitria Rizky Aprilina	M. Riduwan
1	Integra			✔										
2	Siakad			✔										
3	SIM Verifikasi			✔		✔								
4	SMITS			✔							✔			
5	SIM Beasiswa							✔	✔					
6	SIM Ormawa							✔	✔					
7	SIP Maba					✔	✔							

No	Aplikasi	Anny Yuniarti S.Kom., M.Comp.SC	Rizky Januar Akbar, S.Kom., M.Eng	Akhmad Budi K.	Dinar Sekti, S.Kom	Umar Hasan, S.Kom	Rahmad Santoso	Yudhha Nugraha, S.Kom	Ali Mansur	Yoga Ari Tofan	Rangga Dias Novitra	M. Ziqqi Alfiam	Fitria Rizky Aprilina	M. Riduwan
8	SIM Keuangan								✔					
9	e-Aset (Developing)					✔								
10	SIM Mondits (Monitoring Pendapatan ITS)													✔
11	SIM AMU (Aset										✔	✔		

No	Aplikasi	Anny Yuniarti S.Kom., M.Comp.SC	Rizky Januar Akbar, S.Kom., M.Eng	Akhmad Budi K.	Dinar Sekti, S.Kom	Umar Hasan, S.Kom	Rahmad Santoso	Yudhha Nugraha, S.Kom	Ali Mansur	Yoga Ari Tofan	Rangga Dias Novitra	M. Ziqqi Alfiam	Fitria Rizky Aprilina	M. Riduwan
	Manajemen Unit)													
12	SIM Kepegawaian						✔			✔		✔		
13	e-Kepangkatan (Developing)						✔					✔		
14	SIM Kinerja						✔					✔		

No	Aplikasi	Anny Yuniarti S.Kom., M.Comp.SC	Rizky Januar Akbar, S.Kom., M.Eng	Akhmad Budi K.	Dinar Sekti, S.Kom	Umar Hasan, S.Kom	Rahmad Santoso	Yudhha Nugraha, S.Kom	Ali Mansur	Yoga Ari Tofan	Rangga Dias Novitra	M. Ziqqi Alfiam	Fitria Rizky Aprilina	M. Riduwan
15	e-Perkantoran								✔				✔	
16	SIM Penelitian									✔	✔			✔
17	Silacak (Developing)													✔
18	SIP Monev					✔		✔						
19	API												✔	

Informasi Pelaksanaan Wawancara	
Tujuan	1. Mengetahui daftar aset sistem informasi yang ada di Direktorat Pengembangan Teknologi Sistem Informasi KaSubDit Pengembangan Sistem Informasi ITS Surabaya. 2. Mengetahui daftar kontrol keamanan sistem informasi yang sudah diterapkan atau masih dalam tahap perancangan, seperti kebijakan, dan peratutan 3. Mengetahui daftar kejadian terkait keamanan sistem informasi yang pernah terjadi di DPTSI, seperti server down, pengguna tidak dapat melakukan akses, dll.
Tanggal	23 Mei 2018
Waktu	11.30 – 12.00 WIB
Tempat	DPTSI ITS
Narasumber	Cahya Purnama Dani, A.Md. Faishal Halim Saputra, S.ST
Jabatan	Staff Pemeliharaan Jaringan dan Perangkat Keras

No	Pertanyaan	Jawaban
1	Aset sistem informasi (*hardware, software, data, network, people, procedure*) apa saja yang ada di DPTSI ITS?	*Cek tabel checklist aset*
2	Apa saja insiden yang biasa terjadi pada aset tersebut?	*Cek tabel checklist insiden*

No	Pertanyaan	Jawaban
	Dan bagaimana bentuk penanganan setiap insiden yang terjadi?	
3	Bagaiamana bentuk kontrol pada setiap aset yang ada di DPTSI ITS?	*Crosscheck berdasarkan checklist aset*
4	Apa saja kerentanan yang pernah terjadi di DPTSI?	*Cek tabel checklist kerentanan*
5	Apakah bentuk penanganan insiden yang telah dilakukan sekarang telah cukup atau masih terdapat kekurangan?	Masih kurang, terkadang masih terdapat insiden yang belum siap untuk ditangani, dan masih sering terjadi
6	Apakah dalam pengelolaan insiden atau risiko telah berdasarkan standar tertentu?	Untuk saat ini belum ada standar tertentu yang digunakan sebagai acuan pengelolaan insiden
7	Bagaimana suatu insiden atau risiko dapat dideteksi ?	Masih berdasarkan laporan dari user/unit
9	Apakah terdapat klasifikasi atau kategori untuk setiap risiko yang terjadi?	Klasifikasi masih berdasarkan sistem informasi yang ada
9	Bagaimana suatu risiko dicatat?	Untuk saat ini pencatatan masih berdasarkan catatan grup yang ada di WA, email, ataupun dari SubDit Layanan

No	Pertanyaan	Jawaban
10	Apakah catatan tersebut disimpan dalam direktori khusus?	Tidak disimpan dalam direktori khusus
11	Detail informasi apa saja yang dicatat dalam data insiden terkait sistem informasi?	User (siapa yang melapor), dan masalah yang terjadi, dan dari unit mana
12	Apakah terdapat prioritas khusus dalam penyelesaian insiden terkait risiko sistem informasi yang terjadi?	Untuk saat ini prioritas masih berdasarkan kebutuhan, jika menyangkut banyak orang maka akan diprioritaskan
13	Apakah terdapat prosedur khusus yang dilakukan dalam meminimalkan risiko?	Untuk saat ini tidak ada prosedur khusus
14	Bagaimana bentuk penanganan jika terjadi risiko yang belum pernah terjadi sebelumnya? Terutama jika memerlukan penanganan khusus?	Untuk penangan risiko khusus atau berdampak besar dan belum pernah terjadi sebelumnya dilakukan rapat atau diskusi bersama seluruh SubDit, untuk sama-sama mencari solusi dari sebuah insiden.
15	Ketika risiko terjadi, apakah akan dilakukan proses investigasi untuk mengetahui sumber risiko?	Ya dilakukan untuk mengetahui sumber sumber masalah dan untuk menemukan solusi untuk risiko terkait.

No	Pertanyaan	Jawaban
16	Apakah dilakukan proses investigasi secara rutin?	Untuk investigasi tidak dilakukan secara rutin, hanya dilakukan monitoring dari sistem.
17	Bagaimana pengambilan atau pembuatan solusi pemulihan insiden terkait keamanan sistem informasi ditentutkan?	Untuk pengambilan keputusan atau solusi biasanya ditentukan dari jenis masalah atau insiden terlebih dahulu, jika masalah terkait dengan jaringan atau perangkat keras atau jaringan diserahkan kepada kami (SubDit IKTI) dan terkait masalah dengan sistem informasi diserahkan pada SubDit Pengembangan Sistem Inforamasi. Tetapi terkadang penanganan insidennya dilakukan secara bersama-sama.
18	Apakah solusi yang dibuat dilakukan *testing* atau diuji coba terlebih dahulu?	Ya dilakukan uji coba dulu, biasanya semacam server atau router kalau sudah diselesaikan di uji dengan mencoba ping, jika sudah respon maka dianggap selesai.
19	Apakah terdapat SOP khusus dalam melakukan penyelesaian suatu insiden ?	Umumnya keluhan dilaporkan ke bagian layanan terlebih dahulu, kemudian bagian layanan akan meneruskan ke bagian terkait sesuai dengan masalah yang dialami
20	Berapa lama waktu yang dibutuhkan dalam menyelesaiakan suatu insiden?	Tergantung dari tingkat masalah untuk masalah minor bisa diselesaikan kurang dari sehari

No	Pertanyaan	Jawaban
21	Apakah pernah dilakukan identifikasi risiko terkait keamanan sistem informasi sebelumnya?	Untuk saat ini tidak pernah, biasanya hanya berdasarkan laporan saja. Jika terjadi laporan baru akan ditindaklanjuti
22	Bagaimana DPTSI melakukan monitoring terhadap kejadian atau insiden terkait keamanan sistem informasi?	Untuk monitoring sendiri hanya menggunakan sistem informasi yang ada, seperti untuk monitoring jaringan, atau server ada sistemnya sendiri untuk monitoring.

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
1	Perangkat keras	Server	✔	Terdapat CCTV pada pintu masuk
				Terpasang sensor sidik jari
				Dikunci
				Dilengkapi dengan AC Presisi yang berjalan 24 jam 7 hari
				Backup pasokan listrik menggunakan genset
2		Komputer *desktop* / Laptop	✔	Dilengkapi Antivirus
				Login credential/ menggunakan password
3		Telepon seluler		
4		Mesin fax		
5		*Removable media* (kaset, disket, USB, dll)	✔	Berdasarkan user
6		Sistem pemadam api	✔	Tidak ada kontrol khusus

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
7		Sistem pendingin udara	✔	Terdapat sensor suhu secara *realtime*, jika suhu naik akan memberikan notifikasi kepada pegawai
				Dilakukan perawatan teratur 2-3 bulan sekali oleh pihak ketiga
				Kinerja AC dilakukan secara bergantian (terdapat 2 AC)
8		Gesnset	✔	Dipegang oleh bagian Sarana dan Prasarana ITS
9		*Firewall*	✔	Update software secara teratur
10		CCTV	✔	Terpasang di pintu masuk
				penghapusan otomatis ketika kapasitas memori penuh untuk rekaman 3 hari paling lama
				Menggunakan teknologi *motion detection*
11		*Source code*		

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
12	Perangkat lunak	*Software* berlisensi		
13		Sistem informasi	✔	Menggunakan SSO untuk sistem informasi
				Dilakukan backup database secara rutin
				Dilakukan backup aplikasi secara rutis
14	Data	Data sumber daya manusia	✔	Disimpan pada server
				Disimpan pada komputer
15		Data keuangan		
16 17		Data karyawan		
18		Data mitra		
19		Dokumentasi aset	✔	Disimpan pada server
				Disimpan pada komputer
20		Database	✔	Dilakukan backup secara rutin
				Disimpan pada server

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
21	Jaringan	*Dial-up remote access*		
22		Jaringan telepon/ Kabel jaringan	✔	Tidak ada kontrol khusus
23		*Routers*	✔	Diletakkan di ruangan khusus
				Ruangan dilengkapi dengan AC
24		*Switch* jaringan	✔	Disimpan pada rak khusus
				Disimpan pada ruangan yang memiliki AC
25		Akses *virtual private networking (VPN)*		
26		Layanan kolaborasi *(*contoh *microsoft sharepoitnt)*		
27		*Domain Name System (DNS)*		

No	Tingkat Aset	Aset	Checklist	Kontrol di perusahaan
28		*Dynamic host configuration protocol (DHCP)*		
29		*Access point*	✔	Di kerangkeng untuk *Access point* yang berada diluar DPTSI
30	Manusia	Pegawai	✔	Peraturan organisasi

No.	Ancaman	Checklist
Bencana		
1	Kebakaran	✔
2	Banjir	
3	Gempa bumi	✔
4	Badai	
5	Serangan teroris	
6	Kerusuhan	
7	Tanah longsor	
8	Salju longsor	
9	Kecelakaan industri	✔
Kesalahan Mekanik		
10	Mati listrik	✔
11	Kesalahan kontrol lingkungan	✔
12	Kecelakaan konstruksi	✔
Non-orang jahat		
13	Kurangnya informasi pegawai	
14	Kurangnya informasi pengguna	
Orang jahat		
15	*Hacker, cracker*	✔
16	*Computer criminal*	
17	Spionase industri	
18	Spionase pemerintah	
19	*Social engineering*	
20	Pegawai yang tidak puas	
21	Bekas pegawai yang tidak puas	
22	Teroris	
23	Pegawai lalai	
24	Pegawai yang tidak jujur	
25	*Code mobile* berbahaya	
Perangkat keras		
26	Kerusakan	✔
27	Pencurian	

No.	Ancaman	Checklist
28	Kesalahan konfigurasi	✔
Perangkat lunak		
29	*Bug* pada perangkat lunak	✔
30	Serangan virus	✔
31	Kesalahan konfigurasi	✔
32	Kesalahan *input* data	
33	Pembobolan sistem	✔
Jaringan		
34	Gangguan pada *router*	
35	Kerusakan kabel jaringan	✔
36	Hilang/pencurian perangkat jaringan	
37	Gangguan koneksi internet	✔

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
1	Fisik	Pintu yang tidak terkunci		
2		Fasilitas komputer yang tidak dijaga		✔
3		Sistem pemadaman api tidak memadai		
4		Desain gedung yang buruk		
5		Konstruksi gedung yang buruk		
6		Konstruksi menggunakan		

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
		material yang mudah terbakar		
7		*Finishing* menggunakan material yang mudah terbakar		
8		Jendela yang tidak terkunci		
9		Dinding yang rentan terhadap serangan fisik (rapuh)		
10		Dinding ruangan tidak tertutup rapat		
11	Alam	Fasilitas berada di tempat yang salah		
12		Fasilitas berada di zona banjir		
13		Fasilitas berada di zona longsor		
14	Perangkat keras	Terdapat *patch* yang hilang		

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
15		*Firmware* yang telah usang		✔
16		Kesalahan konfigurasi sistem		✔
17		Sistem tidak terlindungi secara fisik		✔
18		Protokol manajemen terbuka untuk umum		
19	Perangkat lunak	Antivirus yang kadaluarsa (tidak *update*)		✔
20		*Patch* yang tidak lengkap atau hilang		✔
21		Aplikasi yang ditulis dengan buruk	*Cross site scripting*	
22		Aplikasi yang ditulis dengan buruk	SQL *injection*	
23		Aplikasi yang ditulis dengan buruk	Kelemahan pada *code* seperti *buffer overflows*	

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
24		Kesengajaan membuat kelemahan	*Vendor backdoors* untuk manajemen atau *system recovery*	
25		Kesengajaan membuat kelemahan	*Spyware* seperti *keyloggers*	
26		Kesengajaan membuat kelemahan	*Trojan horses*	
27		Kesengajaan membuat kelemahan		
28		Kesalahan konfigurasi	Sistem tidak diamankan	
29		Kesalahan konfigurasi	Sistem tidak diaudit	
30		Kesalahan konfigurasi	Sistem tidak dipantau	
31	Media	Gangguan listrik		
32	Jaringan	Protokol jaringan yang tidak terenkripsi		

No	Kelas kerentanan	Kerentanan	Contoh (opsional)	Checklist
33		Koneksi terhubungan ke banyak jaringan		
34		Mengizinkan protokol yang tidak perlu		
35		Tidak ada penyaringan antara segmen jaringan		
36	Manusia	Prosedur didefinisikan dengan buruk	Respon yang tidak memadai	
37		Prosedur didefinisikan dengan buruk	Penyediaan secara manual	
38		Prosedur didefinisikan dengan buruk	*Disaster recovery plans* yang tidak memadai	
39		Prosedur didefinisikan dengan buruk	Melakukan *testing* pada sistem produksi	
40		Prosedur didefinisikan dengan buruk	Kontrol perubahan yang buruk	

Halaman ini sengaja dikosongkan

LAMPIRAN C

HASIL PENILAIAN RISIKO

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
Perangkat Keras	Server	Kesalahan konfigurasi	Kurangnya pengawasan ketika *maintenance*	HR-01	Kerusakan Perangkat Keras	Proses bisnis terganggu terkait dengan penggunaan server	5	2	Sedang
		AC diruangan server mati	Monitoring AC yang kurang baik	HR-02			5	1	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Memory server penuh	Monitoring kapasitas memory tidak dilakukan dengan baik	HR-03			3	2	Sedang
		Overload Akses	Kapasitas memory tidak sanggup melayani akses yang banyak sekaligus	HR-04	Sistem informasi/server tidak bisa diakses		3	1	Rendah
		Server terserang virus/malware	Tidak dilakukan update	HR-05	Kerusakan Perangkat Keras		2	1	Rendah

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
			antivirus secara berkala	HR-06	Sistem informasi/server tidak bisa diakses		2	1	Rendah
		Pasokan listrik terputus	Tidak ada backup daya/genset tidak berfungsi	HR-07	Kerusakan Perangkat Keras		5	2	Sedang
				HR-08	Sistem informasi/server tidak bisa diakses		5	2	Sedang
		Debu/korosi	Maintenance hardware yang tidak teratur	HR-09	Kerusakan Perangkat Keras		2	1	Rendah

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Serangan *cybercrime*	Terdapat celah keamanan yang luput dari pengawasan	HR-10	Sistem informasi/server tidak bisa diakses		4	1	Sedang
				HR-11	Kerusakan Perangkat Keras		4	1	Sedang
		Bencana (Gempa bumi, kebakaran)	DRP belum disiapkan dengan baik	HR-12	Kerusakan Perangkat Keras		5	1	Sedang
	Komputer Desktop/Laptop	Terkena virus/malware	Update antivirus yang tidak berkala	HR-13	Kerusakan Perangkat Keras	Proses bisnis yang bergantung pada penggunaan Komputer *desktop*/laptop terganggu	1	2	Rendah
		Pencurian/hilang	Ruangan yang tidak terkuci	HR-14			1	1	Rendah

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Perawatan yang kurang baik	Tidak dilakukan maintenance dengan baik terhadap perangkat	HR-15			1	2	Rendah
	AC Presisi	Hilangnya pasokan listrik	Tidak ada backup daya/genset tidak berfungsi	HR-16	Server overheat	Sistem informasi tidak berjalan dengan baik/ tidak bisa diakses	5	1	Sedang
		Debu dan kotoran	Tidak dilakukan maintenance dengan baik	HR-17	Kerusakan Perangkat Keras	Sistem informasi tidak berjalan dengan baik/ tidak bisa diakses	5	1	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
			terhadap perangkat						
	AC Konvensional	Hilangnya pasokan listrik	Tidak ada backup daya/genset tidak berfungsi	HR-18	Server overheat	Server *overheat*	2	2	Rendah
		Debu dan kotoran	Tidak dilakukan maintenance dengan baik terhadap perangkat	HR-19	Kerusakan Perangkat Keras	Kerusakan pada perangkat	2	2	Rendah

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
	Genset	Genset tidak mampu bekerja dengan baik	Perawatan yang tidak dilakukan dengan benar	HR-20	Kerusakan Perangkat Keras	Proses bisnis tidak dapat berjalan ketika terjadi pemadaman PLN	5	1	Sedang
	Firewall	Kesalahan konfigurasi	Maintenance perangkat yang kurang baik	HR-21	Pembobolan sistem oleh pihak yang tidak bertanggung jawab	Proses bisnis tidak dapat berjalan dengan baik	3	1	Rendah

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
			Tidak dilakukan update firewall secara berkala	HR-22	Server terserang virus/malware	pencurian/pengubahan informasi yang ada pada server	3	1	Rendah
	CCTV	CCTV Mati	Maintenance perangkat yang kurang baik	HR-23	Aktivitias tidak dapat terpantau	Terjadi pembobolan	2	1	Rendah
		Kualitas gambar yang kurang baik		HR-24	aktivitias tidak dapat terpantau dengan baik		2	1	Rendah
		Perawatan yang tidak dilakukan dengan benar		HR-25	Kerusakan Perangkat Keras		2	1	Rendah
Perangkat Lunak	Sistem Informasi	Database error	Kesalahan konfigurasi/input pada database	SR-01	Sistem informasi tidak bisa diakses/tidak	Terganggunya proses bisnis unit	5	1	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Server mati	Tidak ada backup daya/genset tidak berfungsi dengan baik	SR-02	berjalan dengan baik		5	2	Sedang
		storage/memory penuh (belum fleksibel/cloud)	Kurangnya monitoring terhadap space memory yang tersedia	SR-03			4	1	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Cyber crime	Terdapat celah keamanan yang luput dari pengawasan	SR-04	Pembobolan sistem oleh pihak yang tidak bertanggung jawab	Pencurian/pengubahan informasi yang ada pada sistem informasi	5	1	Sedang
		Hak akses pegawai yang mutasi/pensiun belum diganti/dihapus	Kurangnya pengawasan terhadap hak akses yang ada pada sistem	SR-05	Orang dapat mengakses data/informasi yang bukan haknya/ Penyalahgun	Data/informasi pada sistem menjadi tidak benar/invalid	2	3	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
					aan wewenang				
Data	Database	Data *corruption*	Tidak dilakukan backup	DR-01	Data penting rusak/tidak dapat diakses	Proses bisnis menjadi terganggu	4	2	Sedang
		Kesalahan konfigurasi		DR-02			4	3	Sedang
		Data *loss*		DR-03			5	2	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Cyber crime		DR-04	Data penting diubah/dicuri	Data penting organisasi disalahgunakan	5	3	Tinggi
Jaringan	Kabel *fiber optic* / UTP	Putus/rusak	Tidak ada maintenance secara berakala	NR-01	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Proses bisnis terganggu	3	1	Rendah
	Router	Hilangnya pasokan listrik	Kurangnya pengawasan terhadap perangkat	NR-02	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Jaringan down	5	1	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Kesalahan konfigurasi		NR-03			5	1	Sedang
	Access Point	Hilangnya pasokan listrik	Kurangnya pengawasan terhadap perangkat	NR-04	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Jaringan down	1	3	Rendah
		Kesalahan konfigurasi		NR-05			1	1	Rendah
		Debu dan kotoran		NR-06	Kerusakan Perangkat Keras		1	2	Rendah
	Switch	Hilangnya pasokan listrik	Kurangnya pengawasan terhadap perangkat	NR-07	Sistem informasi tidak bisa diakses/tidak berjalan dengan baik	Jaringan down	3	1	Rendah
		Kesalahan konfigurasi		NR-08			3	1	Rendah

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
		Debu dan kotoran		NR-09	Kerusakan Perangkat Keras		3	3	Sedang
Manusia	Pegawai	Penyalahgunaan wewenang	Kurangnya monitoring terhadap aktivitas pegawai	PR-01	Pembobolan sistem oleh pihak yang tidak	Informasi organisasi diakses oleh pihak yang tidak	5	1	Sedang

Kategori Aset	Aset	Ancaman	Kerentanan	Risk ID	Risiko	Dampak	Nilai Dampak	Nilai Probabilitas	Level
					bertanggung jawab	bertanggung jawab			
		Pegawai yang lalai		PR-02	Kecelakaan kerja	SDM berkurang	1	2	Rendah
				PR-03	*Social engineering*	Informasi organisasi diakses oleh pihak yang tidak bertanggung jawab	1	1	Rendah
				PR-04	Pencurian data		1	1	Rendah

Halaman ini sengaja dikosongkan

LAMPIRAN D

PEMETAN HASIL REKOMENDASI PENGENDALIAN RISIKO PADA KASUBDIT PENGEMBANGAN SISTEM INFORMASI DPTSI ITS

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
Server	11.1.4 *Protecting against external and environment threat*	Kontrol yang memastikan perlindungan fisik seperti bencana alam, serangan jahat, atau kecelakaan	Mencari saran spesialis mengenai bagaimana cara untuk menghindari kerusakan yang diakibatkan oleh kebakaran, banjir, gempa bumi, ledakan, dan bentuk lain dari bencana alam atau yang diakibatkan oleh manusia.
	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan	Aset pendukung (listik, telekomunikasi, pasokan air, gas, ventilasi, dan pendingin udara) harus : • Sesuai dengan spesifikasi pabrikan peralatan, dan persyaratan hukum lokal

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		kegagalan dalam aset pendukung	• Dinilai secara berkala untuk memenuhi pertumbuhan kapasitas kebutuhan bisnis dan interaksi dengan aset pendukung lainnya • Diperiksa dan diuji secara teratur • Jika perlu, siaga terhadap malfungsi • Jika perlu, memeiliki beberapa umpan balik dengan berbagai rute fisikal • Pencahayaan dan komunikasi darurat harus disediakan. Saklar darurat dan katup untuk menutup aliran listrik, gas, air, atau aset lain harus ditempatkan didekat pintu keluar darurat atau ruang peralatan.
	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau	• Peralatan/aset harus dipelihara sesuai dengan interval dan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	spesifikasi layanan yang direkomendasikan oleh pemasok • Hanya personil personil perawatan yang memiliki wewenang untuk melakukan perbaikan • Catatan harus dijaga dari segala bentuk kesalahan dan dari segala bentuk pemeliharaan preventif dan korektif • Kontrol yang sesuai harus dilaksanakan ketika peralatan sedang dilakukan pemeliharaan • Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi • Pemeriksaan harus dilakukan untuk memastikan tidak terjadi

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			kerusakan atau malfungsi setelah perawatan dilakukan
	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	Dokumentasi prosedur harus disiapkan untuk aktivitas operasional yang berhubungan dengan pemrosesan informasi dan komunikasi fasilitas, seperti prosedur pembukaan dan penutupan komputer, backup, pemeliharaan, penanganan media termsuk didalamnya prosedur operasional : • Instalasi dan konfigurasi sistem • Pengolahan dan penanganan informasi baik secara otomatis ataupun manual • *Backup* • Kebutuhan penjadwalan • Instruksi penanganan masalah atau kondisi lainnya.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Kontak dukungan termasuk kontak dukungan eksternal jika terjadi kesulitan operasional atau kesalahan teknis. • Keluaran khusus dan instruksi penanganan media • Sistem *restart* dan prosedur pemulihan untuk penggunaan jika terjadi kegagalan sistem • Pengolahan jejak audit dan informasi log sistem • Presedur pemantauan
	12.1.3 *Capacity management*	Kontrol yang memastikan penggunaan dari sumber daya haruslah dipantau, disesuaikan, dan proyeksi untuk kebutuhan kapasitas di masa yang akan datang untuk	Kebutuhan kapasitas harus diidentifikasi, dengan pertimbangan kekritisan bisnis dari sistem yang bersangkutan. Proyeksi kebutuhan kapasitas di masa yang akan datang harus mempertimbangkan kebutuhan bisnis. Menyediakan kapasitas yang

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		memastikan kinerja sistem sesuai dengan kebutuhan	memadai dapat dicapai dengan meningkatkan kapasitas atau dengan mengurangi permintaan. Beberapa contoh pengelolaan permintaan : • Menghapus data yang sudah usang • Menonaktifkan aplikasi, sistem, *database*, atau lingkungan. • Mengoptimalkan pemrosesan dan penjadwalan *batch*. • Mengoptimalkan logika aplikasi atau *query database*. • Menolak atau membatasi *bandwidth* untuk layanan yang boros.
	12.3.1 *Information backup*	Kontrol yang memastikan salinan dari cadangan informasi, perangkat lunak, dan gambar sistem	• Dokumentasi catatan yang akurat dan lengkap dari salinan cadangan dan prosedur pemulihan.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		harus dilakukan dan diuji secara berkala sesuai dengan kebijakan yang berlaku	• Tingatan dan frekuensi *backup* harus mencerminkan persyaratan bisnis organisasi, kebutuhan keamanan informasi, dan kekritisan informasi dari keberlanjutan operasional organisasi. • *Backup* harus disimpan di lokasi yang terpencil, berjarak cukup jauh untuk menghindari kerusakan dari bencana pada situs utama. • Informasi *backup* harus diberikan tingkat perlindungan sama dengan standar yang ditetapkan pada situs utama. • Media *backup* harus diuji secara berkala untuk memastikan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			keandalan jika diperlukan pada kondisi darurat • *Backup* harus dilindungi dengan menggunakan enkripsi.
AC Presisi	11.2.1 *Equipment siting and protection*	Kontrol yang memastikan peralatan atau aset diletakkan dan dilindungi untuk mengurangi risiko dan ancaman dari lingkungan dan kemungkinan akses dari pihak yang tidak sah	• Peralatan/aset harus ditempatkan pada tempat dengan minimal akses yang tidak perlu pada area kerja • Fasilitas pemrosesan yang menangani data yang sensitif harus ditempatkan dengan hati-hati untuk mengurangi risiko informasi dapat dilihat oleh orang yang tidak berwenang • Fasilitas penyimpanan harus diamankan untuk menghindari akses yang tidak sah • Barang/aset yang membutuhkan perlindungan khusus harus dijaga

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			dengan perlindungan yang umum untuk meminimalkan potensi risiko • Kontrol yang diadopsi harus meminimalkan potensi ancaman fisik dan lingkungan seperti pencurian, kebakaran, bahan peledak, asap, air, debu, getaran, bahan kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik, dan vandalisme. • Pedoman untuk makan, minum, dan merokok disekitar fasilitas pengolahan informasi harus ditetapkan. • Kondisi lingkungan, seperti suhu dan kelembaban serta yang

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			mempengaruhi kondisi kinerja fasilitas harus dipantau. • Perlindungan petir harus diterapkan pada semua bangunan dan filter pelindung petir harus diapasang pada semua jalur daya dan komunikasi. • Penggunaan metode perlindungan khusus harus dipertimbangkan pada peralatan dalam lingkungan industri. • Informasi rahasia terkait alat pemrosesan harus dilindungi untuk meminimalkan risiko kebocoran informasi.
	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan	Aset pendukung (listik, telekomunikasi, pasokan air, gas, ventilasi, dan pendingin udara) harus :

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		lainnya yang mengakibatkan kegagalan dalam aset pendukung	• Sesuai dengan spesifikasi pabrikan peralatan, dan persyaratan hukum lokal • Dinilai secara berkala untuk memenuhi pertumbuhan kapasitas kebutuhan bisnis dan interaksi dengan aset pendukung lainnya • Diperiksa dan diuji secara teratur • Jika perlu, siaga terhadap malfungsi • Jika perlu, memeiliki beberapa umpan balik dengan berbagai rute fisikal Pencahayaan dan komunikasi darurat harus disediakan. Saklar darurat dan katup untuk menutup aliran listrik, gas, air, atau aset lain harus ditempatkan didekat pintu keluar darurat atau ruang peralatan.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	• Peralatan/aset harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok • Hanya personil personil perawatan yang memiliki wewenang untuk melakukan perbaikan • Catatan harus dijaga dari segala bentuk kesalahan dan dari segala bentuk pemeliharaan preventif dan korektif • Kontrol yang sesuai harus dilaksanakan ketika peralatan sedang dilakukan pemeliharaan • Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Pemeriksaan harus dilakukan untuk memastikan tidak terjadi kerusakan atau malfungsi setelah perawatan dilakukan
	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	Dokumentasi prosedur harus disiapkan untuk aktivitas operasional yang berhubungan dengan pemrosesan informasi dan komunikasi fasilitas, seperti prosedur pembukaan dan penutupan komputer, backup, pemeliharaan, penanganan media termsuk didalamnya prosedur operasional : • Instalasi dan konfigurasi sistem • Pengolahan dan penanganan informasi baik secara otomatis ataupun manual • *Backup* • Kebutuhan penjadwalan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Instruksi penanganan masalah atau kondisi lainnya. • Kontak dukungan termasuk kontak dukungan eksternal jika terjadi kesulitan operasional atau kesalahan teknis. • Keluaran khusus dan instruksi penanganan media • Sistem *restart* dan prosedur pemulihan untuk penggunaan jika terjadi kegagalan sistem • Pengolahan jejak audit dan informasi log sistem • Presedur pemantauan
Genset	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang	Aset pendukung (listik, telekomunikasi, pasokan air, gas, ventilasi, dan pendingin udara) harus :

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		mengakibatkan kegagalan dalam aset pendukung	• Sesuai dengan spesifikasi pabrikan peralatan, dan persyaratan hukum lokal • Dinilai secara berkala untuk memenuhi pertumbuhan kapasitas kebutuhan bisnis dan interaksi dengan aset pendukung lainnya • Diperiksa dan diuji secara teratur • Jika perlu, siaga terhadap malfungsi • Jika perlu, memeiliki beberapa umpan balik dengan berbagai rute fisikal Pencahayaan dan komunikasi darurat harus disediakan. Saklar darurat dan katup untuk menutup aliran listrik, gas, air, atau aset lain harus ditempatkan didekat pintu keluar darurat atau ruang peralatan.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	• Peralatan/aset harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok • Hanya personil personil perawatan yang memiliki wewenang untuk melakukan perbaikan • Catatan harus dijaga dari segala bentuk kesalahan dan dari segala bentuk pemeliharaan preventif dan korektif • Kontrol yang sesuai harus dilaksanakan ketika peralatan sedang dilakukan pemeliharaan • Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			Pemeriksaan harus dilakukan untuk memastikan tidak terjadi kerusakan atau malfungsi setelah perawatan dilakukan
Sistem Informasi	9.2.3 *Management of previlaged access rights*	Kontrol yang memastikan alokasi dan penggunaan hak akses harus dibatasi dan dikontrol/ dikendalikan	• Hak akses terkait dengan setiap sistem atau proses seperti sistem operasi, sistem manajemen basis data, setiap aplikasi dan pengguna harus dialokasikan harus diidentifikasi • Hak akses harus dialokasikan ke pengguna berdasarkan kebutuhan penggunaan dan atas dasar kebijakan kontrol sesuai dengan peran dan fungsional mereka. • Proses otorisasi dan catatan semua hak akses yang dialokasikan harus disimpan.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Kebutuhan jangka waktu hak akses harus didefinisikan. • Hak akses harus dibedakan dengan penggunaan proses bisnis. • Kompetensi pengguna harus ditinjau secara berkala untuk memverifikasi kesesuaian dengan hak akses. • Prosedur harus ditetapkan dan disimpan untuk menghindari penggunaan yang tidak sah dari pengguna ID Admin Untuk hak akses admin kerahasiaan informasi otentifikasi harus dipertahankan ketika dibagikan menjadi beberapa user.
	9.2.6 *Removal or adjusment of access rights*	Kontrol yang memastikan hak akses untuk semua karyawan dan pengguna	Setelah penghentian, hak akses individu terhadap informasi dan aset yang terkait dengan fasilitas dan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan kerja, kontrak, atau perjanjian atau disesuaikan dengan perubahan	layanan pemrosesan informasi harus dihapus atau ditangguhkan. Ini akan menentukan apakah perlu untuk menghapus hak akses. Perubahan pekerjaan harus tercermin dalam penghapusan semua hak akses yang tidak dibolehkan untuk pekerjaan yang baru. Hak akses yang harus dihapus atau disesuaikan termasuk akses fisik dan logis. Penghapusan atau penyesuaian dapat dilakukan dengan penghapusan, pencabutan atau penggantian kunci, kartu identifikasi, fasilitas pemrosesan informasi atau langganan
	9.4.1 *Information access restriction*	Kontrol yang memastikan akses terhadap informasi dan fungsi sistem aplikasi harus dibatasi	Pembatasan akses harus didasarkan pada persyaratan aplikasi bisnis individual dan sesuai dengan kebijakan kontrol akses yang

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		berdasarkan kebijakan kontrol akses	ditetapkan. Hal-hal berikut harus dipertimbangkan untuk mendukung persyaratan pembatasan akses: • Menyediakan menu untuk mengontrol akses ke fungsi sistem aplikasi; • Mengontrol data mana yang dapat diakses oleh pengguna tertentu; • Mengontrol hak akses pengguna, misalnya membaca, menulis, menghapus, dan mengeksekusi; • Mengontrol hak akses dari aplikasi lain; • Membatasi informasi yang terdapat dalam output; • Menyediakan kontrol akses fisik atau logis untuk isolasi aplikasi sensitif, data aplikasi, atau sistem

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
	10.1.1 *Policy on the use of cryptographic controls*	Kontrol yang memastikan penggunaan kriptografi secara tepat dan efektif untuk melindungi data atau informasi yang pada organisasi	• Pendekatan manajemen terhadap penggunaan kontrol kriptografi pada seluruh organisasi, termasuk prinsip-prinsip umum di mana informasi bisnis harus dilindungi. • Berdasarkan penilaian risiko, tingkat perlindungan yang diperlukan harus diidentifikasi dengan pertimbangkan jenis, kekuatan, dan kualitas dari algoritma enkripsi yang diperlukan. • Penggunaan enkripsi untuk perlindungan informasi yang dipindahkan melalui *mobile* atau *removable media* atau melalui jaringan komunikasi. Pendekatan manajemen

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
	11.1.4 *Protecting against external and environment threat*	Kontrol yang memastikan perlindungan fisik seperti bencana alam, serangan jahat, atau kecelakaan	Mencari saran spesialis mengenai bagaimana cara untuk menghindari kerusakan yang diakibatkan oleh kebakaran, banjir, gempa bumi, ledakan, dan bentuk lain dari bencana alam atau yang diakibatkan oleh manusia.
	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung	Aset pendukung (listik, telekomunikasi, pasokan air, gas, ventilasi, dan pendingin udara) harus : • Sesuai dengan spesifikasi pabrikan peralatan, dan persyaratan hukum lokal • Dinilai secara berkala untuk memenuhi pertumbuhan kapasitas kebutuhan bisnis dan interaksi dengan aset pendukung lainnya • Diperiksa dan diuji secara teratur

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Jika perlu, siaga terhadap malfungsi • Jika perlu, memeiliki beberapa umpan balik dengan berbagai rute fisikal Pencahayaan dan komunikasi darurat harus disediakan. Saklar darurat dan katup untuk menutup aliran listrik, gas, air, atau aset lain harus ditempatkan didekat pintu keluar darurat atau ruang peralatan.
	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	• Peralatan/aset harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok • Hanya personil personil perawatan yang memiliki wewenang untuk melakukan perbaikan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Catatan harus dijaga dari segala bentuk kesalahan dan dari segala bentuk pemeliharaan preventif dan korektif • Kontrol yang sesuai harus dilaksanakan ketika peralatan sedang dilakukan pemeliharaan • Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi Pemeriksaan harus dilakukan untuk memastikan tidak terjadi kerusakan atau malfungsi setelah perawatan dilakukan
	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	Dokumentasi prosedur harus disiapkan untuk aktivitas operasional yang berhubungan dengan pemrosesan informasi dan komunikasi fasilitas, seperti prosedur

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			pembukaan dan penutupan komputer, backup, pemeliharaan, penanganan media termsuk didalamnya prosedur operasional : • Instalasi dan konfigurasi sistem • Pengolahan dan penanganan informasi baik secara otomatis ataupun manual • *Backup* • Kebutuhan penjadwalan • Instruksi penanganan masalah atau kondisi lainnya. • Kontak dukungan termasuk kontak dukungan eksternal jika terjadi kesulitan operasional atau kesalahan teknis. • Keluaran khusus dan instruksi penanganan media

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Sistem *restart* dan prosedur pemulihan untuk penggunaan jika terjadi kegagalan sistem • Pengolahan jejak audit dan informasi log sistem • Presedur pemantauan
	12.1.3 *Capacity management*	Kontrol yang memastikan penggunaan dari sumber daya haruslah dipantau, disesuaikan, dan proyeksi untuk kebutuhan kapasitas di masa yang akan datang untuk memastikan kinerja sistem sesuai dengan kebutuhan	Kebutuhan kapasitas harus diidentifikasi, dengan pertimbangan kekritisan bisnis dari sistem yang bersangkutan. Proyeksi kebutuhan kapasitas di masa yang akan datang harus mempertimbangkan kebutuhan bisnis. Menyediakan kapasitas yang memadai dapat dicapai dengan meningkatkan kapasitas atau dengan mengurangi permintaan. Beberapa contoh pengelolaan permintaan : • Menghapus data yang sudah usang

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Menonaktifkan aplikasi, sistem, *database*, atau lingkungan. • Mengoptimalkan pemrosesan dan penjadwalan *batch*. • Mengoptimalkan logika aplikasi atau *query database*. • Menolak atau membatasi *bandwidth* untuk layanan yang boros.
	12.4.1 *Event logging*	Kontrol yang mengatur mengenai log kejadian yang merekam aktivitas pengguna, kesalahan, dan kejadian terkain keamanan informasi yang harus dibuat dan ditinjau secara berkala	Dalam *event* harus berisi, jika relevan: • ID pengguna • Aktivitas sistem • Tanggal, waktu, dan detail acara penting, misalnya *log-on* dan *log-off* • Identitas perangkat atau lokasi jika memungkinkan dan pengenal sistem

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Catatan dari upaya akses sistem yang berhasil dan ditolak • Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya • Perubahan konfigurasi sistem • Penggunaan hak akses istimewa • Penggunaan utilitas sistem dan aplikasi • *File* yang diakses dan jenis akses • Alamat dan protokol jaringan • Alarm yang dibangkitkan oleh sistem kontrol akses • Aktivasi dan de-aktivasi sistem perlindungan, seperti sistem anti-virus dan sistem deteksi intrusi
Database	8.2.1 *Clasification of information*	Informasi harus diklasifikasikan dalam	Pemilik aset bertanggung jawab atas klasifikasi aset.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		kebutuhan kebijakan/ hukum, nilai, kekritisan, dan kepekaan terhadap pengungkapan atau modifikasi yang tidak sah	Skema klasifikasi harus mencakup ketentuan dan kriteria untuk dilakukan peninjauan klasifikasi dari waktu ke waktu. Tingkat perlindungan dalam skema harus dinilai dengan analisis kerahasisan, integritas, dan ketersedian, serta persyaratan lainnya yang dianggap perlu dalam pertimbangan.
	10.1.1 *Policy on the use of cryptographic controls*	Kontrol yang memastikan penggunaan kriptografi secara tepat dan efektif untuk melindungi data atau informasi yang pada organisasi	• Pendekatan manajemen terhadap penggunaan kontrol kriptografi pada seluruh organisasi, termasuk prinsip-prinsip umum di mana informasi bisnis harus dilindungi. • Berdasarkan penilaian risiko, tingkat perlindungan yang diperlukan harus diidentifikasi dengan pertimbangkan jenis,

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			kekuatan, dan kualitas dari algoritma enkripsi yang diperlukan. • Penggunaan enkripsi untuk perlindungan informasi yang dipindahkan melalui *mobile* atau *removable media* atau melalui jaringan komunikasi. • Pendekatan manajemen
	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	• Peralatan/aset harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok • Hanya personil personil perawatan yang memiliki wewenang untuk melakukan perbaikan • Catatan harus dijaga dari segala bentuk kesalahan dan dari segala

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			bentuk pemeliharaan preventif dan korektif • Kontrol yang sesuai harus dilaksanakan ketika peralatan sedang dilakukan pemeliharaan • Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi Pemeriksaan harus dilakukan untuk memastikan tidak terjadi kerusakan atau malfungsi setelah perawatan dilakukan
	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	Dokumentasi prosedur harus disiapkan untuk aktivitas operasional yang berhubungan dengan pemrosesan informasi dan komunikasi fasilitas, seperti prosedur pembukaan dan penutupan komputer, backup, pemeliharaan, penanganan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			media termsuk didalamnya prosedur operasional : • Instalasi dan konfigurasi sistem • Pengolahan dan penanganan informasi baik secara otomatis ataupun manual • *Backup* • Kebutuhan penjadwalan • Instruksi penanganan masalah atau kondisi lainnya. • Kontak dukungan termasuk kontak dukungan eksternal jika terjadi kesulitan operasional atau kesalahan teknis. • Keluaran khusus dan instruksi penanganan media

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Sistem *restart* dan prosedur pemulihan untuk penggunaan jika terjadi kegagalan sistem • Pengolahan jejak audit dan informasi log sistem • Presedur pemantauan
	12.3.1 *Information backup*	Kontrol yang memastikan salinan dari cadangan informasi, perangkat lunak, dan gambar sistem harus dilakukan dan diuji secara berkala sesuai dengan kebijakan yang berlaku	• Dokumentasi catatan yang akurat dan lengkap dari salinan cadangan dan prosedur pemulihan. • Tingatan dan frekuensi *backup* harus mencerminkan persyaratan bisnis organisasi, kebutuhan keamanan informasi, dan kekritisan informasi dari keberlanjutan operasional organisasi. • *Backup* harus disimpan di lokasi yang terpencil, berjarak cukup jauh untuk menghindari

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			kerusakan dari bencana pada situs utama. • Informasi *backup* harus diberikan tingkat perlindungan sama dengan standar yang ditetapkan pada situs utama. • Media *backup* harus diuji secara berkala untuk memastikan keandalan jika diperlukan pada kondisi darurat • *Backup* harus dilindungi dengan menggunakan enkripsi.
	12.4.1 *Event logging*	Kontrol yang mengatur mengenai log kejadian yang merekam aktivitas pengguna, kesalahan, dan kejadian terkain keamanan informasi yang	Dalam *event* harus berisi, jika relevan: • ID pengguna • Aktivitas sistem • Tanggal, waktu, dan detail acara penting, misalnya *log-on* dan *log-off*

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		harus dibuat dan ditinjau secara berkala	• Identitas perangkat atau lokasi jika memungkinkan dan pengenal sistem • Catatan dari upaya akses sistem yang berhasil dan ditolak • Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya • Perubahan konfigurasi sistem • Penggunaan hak akses istimewa • Penggunaan utilitas sistem dan aplikasi • *File* yang diakses dan jenis akses • Alamat dan protokol jaringan • Alarm yang dibangkitkan oleh sistem kontrol akses • Aktivasi dan de-aktivasi sistem perlindungan, seperti sistem anti-virus dan sistem deteksi intrusi

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
Router	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	Dokumentasi prosedur harus disiapkan untuk aktivitas operasional yang berhubungan dengan pemrosesan informasi dan komunikasi fasilitas, seperti prosedur pembukaan dan penutupan komputer, backup, pemeliharaan, penanganan media termsuk didalamnya prosedur operasional : • Instalasi dan konfigurasi sistem • Pengolahan dan penanganan informasi baik secara otomatis ataupun manual • *Backup* • Kebutuhan penjadwalan • Instruksi penanganan masalah atau kondisi lainnya. • Kontak dukungan termasuk kontak dukungan eksternal jika

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			terjadi kesulitan operasional atau kesalahan teknis. • Keluaran khusus dan instruksi penanganan media • Sistem *restart* dan prosedur pemulihan untuk penggunaan jika terjadi kegagalan sistem • Pengolahan jejak audit dan informasi log sistem Presedur pemantauan
	11.2.2 *Supporting Utilities*	Kontrol yang memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung	Aset pendukung (listik, telekomunikasi, pasokan air, gas, ventilasi, dan pendingin udara) harus : • Sesuai dengan spesifikasi pabrikan peralatan, dan persyaratan hukum lokal • Dinilai secara berkala untuk memenuhi pertumbuhan kapasitas

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			kebutuhan bisnis dan interaksi dengan aset pendukung lainnya • Diperiksa dan diuji secara teratur • Jika perlu, siaga terhadap malfungsi • Jika perlu, memeiliki beberapa umpan balik dengan berbagai rute fisikal Pencahayaan dan komunikasi darurat harus disediakan. Saklar darurat dan katup untuk menutup aliran listrik, gas, air, atau aset lain harus ditempatkan didekat pintu keluar darurat atau ruang peralatan.
	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset	• Peralatan/aset harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		dapat digunakan dalam proses bisnis	• Hanya personil personil perawatan yang memiliki wewenang untuk melakukan perbaikan • Catatan harus dijaga dari segala bentuk kesalahan dan dari segala bentuk pemeliharaan preventif dan korektif • Kontrol yang sesuai harus dilaksanakan ketika peralatan sedang dilakukan pemeliharaan • Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi Pemeriksaan harus dilakukan untuk memastikan tidak terjadi kerusakan atau malfungsi setelah perawatan dilakukan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
Switch	11.2.1 *Equipment siting and protection*	Kontrol yang memastikan peralatan atau aset diletakkan dan dilindungi untuk mengurangi risiko dan ancaman dari lingkungan dan kemungkinan akses dari pihak yang tidak sah	• Peralatan/aset harus ditempatkan pada tempat dengan minimal akses yang tidak perlu pada area kerja • Fasilitas pemrosesan yang menangani data yang sensitif harus ditempatkan dengan hati-hati untuk mengurangi risiko informasi dapat dilihat oleh orang yang tidak berwenang • Fasilitas penyimpanan harus diamankan untuk menghindari akses yang tidak sah • Barang/aset yang membutuhkan perlindungan khusus harus dijaga dengan perlindungan yang umum untuk meminimalkan potensi risiko

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Kontrol yang diadopsi harus meminimalkan potensi ancaman fisik dan lingkungan seperti pencurian, kebakaran, bahan peledak, asap, air, debu, getaran, bahan kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik, dan vandalisme. • Pedoman untuk makan, minum, dan merokok disekitar fasilitas pengolahan informasi harus ditetapkan. • Kondisi lingkungan, seperti suhu dan kelembaban serta yang mempengaruhi kondisi kinerja fasilitas harus dipantau. • Perlindungan petir harus diterapkan pada semua bangunan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			dan filter pelindung petir harus diapasang pada semua jalur daya dan komunikasi. • Penggunaan metode perlindungan khusus harus dipertimbangkan pada peralatan dalam lingkungan industri. Informasi rahasia terkait alat pemrosesan harus dilindungi untuk meminimalkan risiko kebocoran informasi.
	11.2.4 *Equipment Maintenance*	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna memastikan aset dapat digunakan dalam proses bisnis	• Peralatan/aset harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok • Hanya personil personil perawatan yang memiliki wewenang untuk melakukan perbaikan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Catatan harus dijaga dari segala bentuk kesalahan dan dari segala bentuk pemeliharaan preventif dan korektif • Kontrol yang sesuai harus dilaksanakan ketika peralatan sedang dilakukan pemeliharaan • Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi • Pemeriksaan harus dilakukan untuk memastikan tidak terjadi kerusakan atau malfungsi setelah perawatan dilakukan
	12.1.1 *Documented operations procedures*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	Dokumentasi prosedur harus disiapkan untuk aktivitas operasional yang berhubungan dengan pemrosesan informasi dan komunikasi fasilitas, seperti prosedur

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			pembukaan dan penutupan komputer, backup, pemeliharaan, penanganan media termsuk didalamnya prosedur operasional : • Instalasi dan konfigurasi sistem • Pengolahan dan penanganan informasi baik secara otomatis ataupun manual • *Backup* • Kebutuhan penjadwalan • Instruksi penanganan masalah atau kondisi lainnya. • Kontak dukungan termasuk kontak dukungan eksternal jika terjadi kesulitan operasional atau kesalahan teknis. • Keluaran khusus dan instruksi penanganan media

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Sistem *restart* dan prosedur pemulihan untuk penggunaan jika terjadi kegagalan sistem • Pengolahan jejak audit dan informasi log sistem • Presedur pemantauan
Pegawai	6.1.1 *Information security roles and responsibilities*	Kontrol yang memastikan semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan	Alokasi tanggung jawab keamanan informasi harus dilakukan sesuai dengan kebijakan keamanan informasi. Tanggung jawab untuk melindungi aset dan melaksanakan proses keamanan informasi yang spesifik harus diidentifikasi. Tanggung jawab manajemen risiko keamanan informasi, bila perlu dilengkapi dengan panduan yang lebih rinci untuk situs tertentu dan fasilitas pemrosesan informasi.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			Area tanggung jawab individu yang harus ditentukan, khususnya pada hal beriku : • Aset dan prses keamanan informasi harus diidentifikasi dan didefinisikan • Entitas yang bertanggung jawab untuk setiap aset atau proses keamanan informasi harus ditugaskan dan rincian tanggung jawab harus didokumentasikan. • Tingkat otoritas harus ditentukan dan didokumentasikan • Untuk memenuhi tanggung jawab bidang keamanan informasi, individu yang ditunjuk harus kompeten pada bidang tersebut. • Koordinasi dan pengawasan aspek keamanan informasi dengan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			pemasok harus diidentifikasi dan didokumentasikan.
	7.1.2 *Term and conditions of employment*	Kontrol yang menngatur mengenai perjanjian mengenai tanggung jawab pegawai, kontraktor, dan organisasi terhadap keamanan informasi	Kewajiban kontrak untuk karyawan atau kontraktor harus mencerminkan kebijakan keamanan informasi : • Semua karyawan dan kontraktor yang diberi akses ke informasi rahasisa harus menandatangi perjanjian kerahasian sebelum diberikan akses ke fasilitas pemrosesan informasi • Tanggung jawab dan hak hukum karyawan atau kontraktor, misalnya mengenai undang-undang hak cipta • Tanggung jawab untuk klasifikasi informasi dan manajemen aset organisasi terkait dengan informasi, fasilitas pemrosesan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			informasi dan layanan informasi yang ditangani oleh karyawan atau kontraktor • Tanggung jawab karyawan atau kontraktor untuk penanganan informasi yang diterima perusahaan lain atau pihak eksternal • Tindakan yang harus diambil jika karyawan atau kontraktor mengabaikan persyaratan keamanan organisasi
	7.2.2 *Information security awareness, education, and training*	Kontrol yang mengatur mengenai pendidikan dan pelatihan terhadap karyawan dan kontraktor mengenai keamanan informasi secara rutin	Program kesadaran keamanan informasi harus bertujuan untuk membuat karyawan dan atau kontraktor menyadari tanggung jawab mereka untuk keamanan informasi Program kesadaran keamanan informasi harus ditetapkan sesuai

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		sesuai dengan fungsi masing-masing	dengan kebijakan keamanan informasi organisasi dengan mempertimbangkan informasi yang akan dilindungi dan kontrol yang diterapkan untuk melindungi informasi. Program penyadaran harus mencakup sejumlah kegiatan peningkatan kesadaran seperti kampanye Program direncanakan dengan pertimbangan peran karyawan dalam organisasi dan dijadwalkan dari waktu ke waktu. Pendidikan dan pelatihan keamanan informasi juga harus mencakup aspek-aspek umum seperti: • Komitmen manajemen terhadap keamanan informasi di seluruh organisasi

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Kebutuhan peraturan dan kewajiban keamanan informasi yang berlaku, sebagaimana didefinisikan dalam kebijakan, standar, hukum, peraturan, kontrak, dan perjanjian. • Pertanggungjawaban pribadi atas tindakan dan tidak adanya tindakan, dan tanggung jawab umum untuk mengamankan atau melindungi informasi milik organisasi dan pihak eksternal • Dasar prosedur keamanan informasi (seperti pelaporan insiden keamanan informasi) dan kontrol dasar (seperti keamanan kata sandi, kontrol malware) • Titik kontak dan sumber daya untuk tambahan informasi dan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			saran tentang masalah keamanan informasi, termasuk materi pendidikan dan pelatihan keamanan informasi lebih lanjut.
	9.2.3 *Management of previlaged access rights*	Kontrol yang memastikan alokasi dan penggunaan hak akses harus dibatasi dan dikontrol/ dikendalikan	• Hak akses terkait dengan setiap sistem atau proses seperti sistem operasi, sistem manajemen basis data, setiap aplikasi dan pengguna harus dialokasikan harus diidentifikasi • Hak akses harus dialokasikan ke pengguna berdasarkan kebutuhan penggunaan dan atas dasar kebijakan kontrol sesuai dengan peran dan fungsional mereka. • Proses otorisasi dan catatan semua hak akses yang dialokasikan harus disimpan.

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
			• Kebutuhan jangka waktu hak akses harus didefinisikan. • Hak akses harus dibedakan dengan penggunaan proses bisnis. • Kompetensi pengguna harus ditinjau secara berkala untuk memverifikasi kesesuaian dengan hak akses. • Prosedur harus ditetapkan dan disimpan untuk menghindari penggunaan yang tidak sah dari pengguna ID Admin • Untuk hak akses admin kerahasiaan informasi otentifikasi harus dipertahankan ketika dibagikan menjadi beberapa user.
	9.2.6 *Removal or adjusment of access rights*	Kontrol yang memastikan hak akses untuk semua karyawan dan pengguna	• Setelah penghentian, hak akses individu terhadap informasi dan aset yang terkait dengan fasilitas

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
		eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan kerja, kontrak, atau perjanjian atau disesuaikan dengan perubahan	dan layanan pemrosesan informasi harus dihapus atau ditangguhkan. Ini akan menentukan apakah perlu untuk menghapus hak akses. Perubahan pekerjaan harus tercermin dalam penghapusan semua hak akses yang tidak dibolehkan untuk pekerjaan yang baru. Hak akses yang harus dihapus atau disesuaikan termasuk akses fisik dan logis. Penghapusan atau penyesuaian dapat dilakukan dengan penghapusan, pencabutan atau penggantian kunci, kartu identifikasi, fasilitas pemrosesan informasi atau langganan

Aset	Kontrol ISO/IEC 27002:2013	*Control Objective*	Petunjuk Pelaksanaan ISO/IEC 27002:2013
	12.4.3 *Administrator and operator logs*	Kontrol yang memastikan aktivitas admin dan operator sistem harus dicatat dan dilindungi dan dilakukan peninjauan secara berkala	Log akses admin harus dilindungi dan ditinjau secara berkala untuk mempertahankan akuntabilitas admin.

LAMPIRAN E

PERATURAN REKTOR NOMOR 10 TAHUN 2016

Bagian Ketiga
Direktorat Pengembangan Teknologi dan Sistem Informasi

Pasal 62

(1) Direktorat Pengembangan Teknologi dan Sistem Informasi mempunyai tugas melaksanakan penyiapan perumusan kebijakan pengembangan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan di bidang teknologi dan sistem informasi.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Direktorat Pengembangan Teknologi dan Sistem Informasi menyelenggarakan fungsi:
    a. pengelolaan dan pengembangan infrastruktur dan keamanan informasi;
    b. pengelolaan dan pengembangan sistem informasi; dan
    c. pengelolaan dan pengembangan layanan sistem dan teknologi informasi.
(3) Direktorat Pengembangan Teknologi dan Sistem Informasi dipimpin oleh seorang Direktur, yang dalam menjalankan tugasnya bertanggung jawab kepada Wakil Rektor III.

Pasal 63

(1) Direktorat Pengembangan Teknologi dan Sistem Informasi terdiri atas:
    a. Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi;
    b. Subdirektorat Pengembangan Sistem Informasi; dan
    c. Subdirektorat Layanan Teknologi dan Sistem Informasi.

(2) Subdirektorat Pengembangan Sistem Informasi, sebagaimana dimaksud pada ayat (1) huruf b, dibantu oleh Seksi Pengembangan Aplikasi pada Perangkat Bergerak.
(3) Subdirektorat Layanan Teknologi dan Sistem Informasi sebagaimana dimaksud pada ayat (1) huruf c, dibantu oleh Seksi Layanan Data dan Informasi.

Pasal 64

(1) Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan untuk pengembangan dan pengkajian infrastruktur dan keamanan teknologi informasi.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi menyelenggarakan fungsi:
    a. penyiapan bahan perumusan kebijakan dan standar mutu pengembangan infrastruktur dan keamanan teknologi informasi;
    b. pelaksanaan pengembangan infrastruktur dan keamanan teknologi informasi;
    c. pelaksanaan pengawasan dan pemantauan pengembangan infrastruktur dan keamanan teknologi informasi;
    d. pelaksanaan pemeliharaan infrastruktur dan keamanan teknologi informasi; dan
    e. pelaksanaan evaluasi dan pelaporan infrastruktur dan keamanan teknologi informasi.
(3) Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi dipimpin oleh seorang Kepala Subdirektorat, yang dalam melaksanakan tugasnya bertanggung jawab kepada Direktur Pengembangan Teknologi dan Sistem Informasi.

Pasal 65

(1) Subdirektorat Pengembangan Sistem Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan pengembangan sistem informasi.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdirektorat Pengembangan Sistem Informasi menyelenggarakan fungsi:
    a. penyiapan bahan perumusan kebijakan dan standar mutu pengembangan sistem informasi;
    b. pelaksanaan pengembangan sistem informasi;
    c. pelaksanaan pengawasan dan pemantauan pengembangan sistem informasi;
    d. pelaksanaan pemeliharaan data dan sistem informasi; dan
    e. pelaksanaan evaluasi dan pelaporan pengembangan sistem informasi.
(3) Subdirektorat Pengembangan Sistem Informasi dipimpin oleh seorang Kepala Subdirektorat, yang dalam melaksanakan tugasnya bertanggung jawab kepada Direktur Pengembangan Teknologi dan Sistem Informasi.

Pasal 66

(1) Seksi Pengembangan Aplikasi pada Perangkat Bergerak mempunyai tugas melakukan penyusunan bahan perumusan kebijakan, pelaksanaan pengembangan, pengawasan dan pengendalian, pemeliharaan, serta pemantauan, evaluasi, dan pelaporan untuk pengembangan aplikasi pada perangkat bergerak.
(2) Seksi Pengembangan Aplikasi pada Perangkat Bergerak dipimpin oleh seorang Kepala Seksi yang dalam melaksanakan tugasnya bertanggung jawab kepada Kepala Subdirektorat Pengembangan Sistem Informasi.

Pasal 67

(1) Subdirektorat Layanan Teknologi dan Sistem Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, operasional layanan, pengawasan dan pemantauan, evaluasi, dan pelaporan untuk layanan teknologi dan sistem informasi.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdirektorat Layanan Teknologi dan Sistem Informasi menyelenggarakan fungsi:
    a. penyiapan bahan perumusan kebijakan dan standar mutu layanan teknologi dan sistem informasi;
    b. pelaksanaan operasional layanan teknologi dan sistem informasi;
    c. pelaksanaan pengawasan dan pemantauan layanan teknologi dan sistem informasi; dan
    d. pelaksanaan evaluasi dan pelaporan layanan teknologi dan sistem informasi.
(3) Subdirektorat Layanan Teknologi dan Sistem Informasi dipimpin oleh seorang Kepala Subdirektorat, yang dalam melaksanakan tugasnya bertanggung jawab kepada Direktur Pengembangan Teknologi dan Sistem Informasi.

Pasal 68

(1) Seksi Layanan Data dan Informasi mempunyai tugas melakukan penyusunan bahan perumusan kebijakan, penyiapan dan pengorganisasian data, pengawasan dan pengendalian, serta pemantauan, evaluasi, dan pelaporan untuk layanan data dan informasi.
(2) Seksi Layanan Data dan Informasi dipimpin oleh seorang Kepala Seksi yang dalam melaksanakan tugasnya bertanggung jawab kepada Kepala Subdirektorat Layanan Teknologi dan Sistem Informasi.

LAMPIRAN F
DOKUMENTASI VALIDASI WAWANCARA

FORM VALIDASI WAWANCARA

Berikan checklist (√) pada kolom di bawah ini:

Komponen validasi	Sesuai fakta di lapangan	
	Ya	Tidak
Daftar Aset	√	
Daftar Kontrol	√	
Daftar Ancaman	√	
Daftar Kerentanan	√	
Daftar Risiko	√	
Penilaian Risiko	√	

Telah dilakukan penggalian data melalui wawancara langsung terhadap informan penelitian sebagai berikut:

Nama Informan : Cahya Purnama Dani, A.Md.
Jabatan : Staff Pemeliharaan Jaringan dan Perangkat Keras
Tanggal Wawancara : 23 Mei 2018
Lokasi Wawancara : DPTSI ITS
Hasil Penelitian :**TERLAMPIR SESUAI LAPORAN PENELITIAN**

Pernyataan:
Bersama dengan ini, saya menyetujui bahwa komponen validasi sesuai dengan fakta di lapangan.

Cahya Purnama Dani, A.Md.

F-2

FORM VALIDASI WAWANCARA

Berikan checklist (√) pada kolom di bawah ini:

Komponen validasi	Sesuai fakta di lapangan	
	Ya	Tidak
Daftar Aset	✓	
Daftar Kontrol	✓	
Daftar Ancaman	✓	
Daftar Kerentanan	✓	
Daftar Risiko	✓	
Penilaian Risiko	✓	

Telah dilakukan penggalian data melalui wawancara langsung terhadap informan penelitian sebagai berikut:

Nama Informan : Anny Yuniarti, S.Kom., M.Comp.Sc.
Jabatan : KaSubDit Pengembangan Sistem Informasi
Tanggal Wawancara : 23 Mei 2018
Lokasi Wawancara : Gedung Departemen Informatika ITS Lt. 2
Hasil Penelitian :**TERLAMPIR SESUAI LAPORAN PENELITIAN**

Pernyataan:
Bersama dengan ini, saya menyetujui bahwa komponen validasi sesuai dengan fakta di lapangan.

Anny Yuniarti, S.Kom., M.Comp.Sc

FORM VALIDASI WAWANCARA

Berikan checklist (√) pada kolom di bawah ini:

Komponen validasi	Sesuai fakta di lapangan	
	Ya	Tidak
Daftar Aset	✓	
Daftar Kontrol	✓	
Daftar Ancaman	✓	
Daftar Kerentanan	✓	
Daftar Risiko	✓	
Penilaian Risiko	✓	

Telah dilakukan penggalian data melalui wawancara langsung terhadap informan penelitian sebagai berikut:

Nama Informan : Radityo Prasetianto Wibowo, S.Kom., M.Kom.
Jabatan : Kasi Layanan Data dan Informasi
Tanggal Wawancara : 6 Juli 2018
Lokasi Wawancara : DPTSI ITS
Hasil Penelitian :**TERLAMPIR SESUAI LAPORAN PENELITIAN**

Pernyataan:
Bersama dengan ini, saya menyetujui bahwa komponen validasi sesuai dengan fakta di lapangan.

Radityo Prasetianto Wibowo, S.Kom., M.Kom.